

AJAR Technology



Ajar Cloud XProtect CVMS

London, Greater Manchester, The Hague Security Delta Campus,

About Ajar Technology.....	3
Introduction to Cloud XProtect.....	4
Open platform	6
XProtect Extensions	6
Web Client.....	7
Operating The Web Client	8
Cloud System Server Architecture.....	9
Interconnect Centralisation	11
GDPR.....	12
FIPS 140-2 Compliance	12
Support	13
Contract Terms	13
Warranty.....	14
Terms and conditions.....	15

About Ajar Technology

Ajar Technology is an independent Audio Visual and Electronic Security Systems Integrator. We offer the end-to-end solution designed for each client using tried and tested technologies from our valued technology partners.

We have vast in-house subject matter expertise, and we continually review our solution offerings and adapt to market conditions to offer products and services that are relevant and valued by our clients.

Our vision

To be the preferred trusted partner to help our clients overcome barriers and complex challenges using technology.

Our Value Proposition:

- We are an independent specialist end-to-end single-source partner
- We propose technical solutions after thorough analysis and consideration of the client's requirement
- We have in-house skilled, experienced personnel
- Direct vendor relations to access leading-edge technologies
- Consistent point of contact within our project and commercial teams

Our company values.

- **Collaboration** – Open mind.
- **Teamwork** – Work towards the same objective
- **Professional** – Act with professionalism throughout
- **Trusted partner** – Provide constructive feedback and deliver
- **Community** – Support our work community and local communities.

We offer end-to-end project and managed service.

- Solution design and agnostic advisory service
- Survey and pre-sales
- Vendor management and procurement
- Project management
- Offsite test, build, configuration
- Systems Programming
- Onsite installations and commissioning
- End-user training
- Account management
- Ongoing support and maintenance (customisable support from 24/7 x 365 to business as usual, onsite and remote)



Website & LinkedIn

<https://ajartechnology.com/>

<https://www.linkedin.com/company/ajartec-limited>

Introduction to Cloud XProtect

XProtect is a global market leader in Cloud Video Management Software (CVMS) that connects the puzzle pieces of a video surveillance installation in a solution that keeps people, premises, and property safe today and tomorrow.

Built on an open platform architecture, you can customise your surveillance system and integrate other business applications into it for increased usability and performance. With over 25 years in the market, XProtect has proven to be the right answer for more than 500,000 installations worldwide.

Cloud Surveillance and Video management offer low capital costs and pay-as-you-go pricing with no up-front expenses or long-term commitments. We can build and manage a global infrastructure at scale and pass the cost-saving benefits onto you in the form of lower prices.

Agility and Instant Elasticity provide a massive global cloud infrastructure that allows you to innovate, experiment, and iterate quickly. Instead of waiting weeks or months for hardware, you can instantly deploy new applications, instantly scale up as your workload grows, and instantly scale down based on demand.

Whether you need one virtual server or thousands, whether you need them for a few hours or 24/7, you still only pay for what you use.

Open and Flexible. XProtect is an agnostic open platform. You choose the development platform or programming model that makes the most sense for your business. You can choose which services you use, one or several, and choose how you use them. This flexibility allows you to focus on innovation, not infrastructure.

Cyber Secure. Our hosted cloud offering is a durable technology platform with industry-recognized certifications and audits: ISO 27001, FISMA Moderate, FedRAMP, HIPAA, SOC 1 (formerly referred to as SAS 70 and/or SSAE 16) and SOC 2 audit reports. Our data centres have multiple layers of operational and physical security to ensure the integrity and safety of your data.

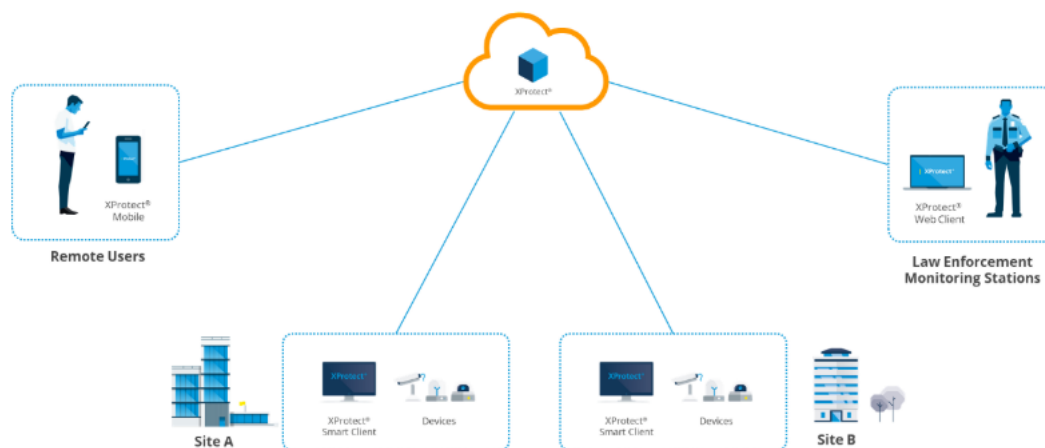


Diagram 1. High-level Cloud XProtect Solution

Speed of Deployment

Video surveillance systems are complex IT systems that are compute and storage intensive. Commissioning such a system requires careful solution design, selection of server and storage hardware, and all the logistics associated with ordering, shipping, unpacking, and installing the hardware.

With a cloud deployment of XProtect, many of these activities can be vastly simplified if not eliminated. Overall, it allows organisations to deploy XProtect CVMS faster and cheaper. Without much of the friction known from on-premises deployments, XProtect CVMS can far more easily support organisations that operate with seasonal or temporary deployments.

The actual deployment of the XProtect BYOL product into a specific customer's cloud account is orchestrated by a CloudFormation template. The CloudFormation template deploys the Windows operating system and the XProtect BYOL included in the AMI on the Elastic Compute Cloud (EC2) instance selected for the deployment. This gives an instant and predictable deployment where the CloudFormation template also defines a new dedicated VPC with subnets, Security Groups and Elastic Block Store (EBS) for CVMS configuration data and short-term storage of video data.

Elastic Scalability

Needs and operational circumstances change. AWS cloud infrastructure allows customers to grow their XProtect deployment seamlessly to meet their needs. An XProtect CVMS deployment can seamlessly scale up to hundreds and thousands of cameras on a single EC2 instance. Leveraging the ability to shift the EC2 compute platform makes the scaling instant while maintaining an attractive balance between performance and cost. In surveillance installations with higher needs, the deployment can be scaled out on additional EC2 instances to support thousands of cameras and IoT devices.

Ideal for geographically dispersed operations

Implementing geographically distributed video surveillance solutions often implies a mix of VPN networks and distributed hardware that need to be kept operational and secure at all times. In these situations, cloud deployment is a perfect alternative, where the different sites and premises are rolled into the customer's virtual cloud environment, in which XProtect is staged. Here, tangible savings can be made both in the deployment phase and even more so in the operations phase, where costly on-premises service and support visits can be reduced to a minimum.

Open platform

In a close-ended security system, each component is powerful but it's isolated from other systems. In an open platform, integrations bridge your system to connect to other security tools, creating a unified network of intelligence. That's the power of XProtect's open platform. This video technology takes you beyond security cameras to other security devices, like access control systems, intrusion detection, IoT sensors, fire alarms, and even optional AI-powered analytics. XProtect integrates seamlessly with a vast ecosystem of over 14,000 devices. Information flows freely, creating a holistic view of your security landscape.

Here's how it works: XProtect uses open APIs, like a universal language, to "talk" to these different systems. Access control systems can send entry logs to XProtect, triggering instant video verification. Additionally, video analytics can flag suspicious activity in XProtect. Highly secure sites can automatically lock down specific doors or prevent movement when necessary. It's a powerful collaboration orchestrated by the open platform.

The benefits include streamlined operations, faster response times, and proactive security. You're not just watching; you're predicting, preventing, and reacting with laser focus. XProtect remains secure, ensuring only authorised information exchanges within its controlled environment.

XProtect Extensions

XProtect empowers your security, but what if you need even more specialised tools? Enter XProtect Extensions, an add-on that supercharges your security ecosystem with targeted functionalities.

Think of them as building blocks, each addressing specific needs:

- Remote patient monitoring in hospitals with XProtect Hospital Assist
- Streamlined incident logging and collaboration using XProtect Incident Manager
- Automatic license plate recognition with XProtect LPR
- Panoramic situational awareness across video monitor walls with XProtect Smart Wall
- Fast video review and object/person search with XProtect Rapid REVIEW
- Seamless integration of access control and intrusion systems through XProtect Access
- These XProtect Extensions adapt to your unique needs, scaling your security alongside your business. Explore the possibilities and unlock a world of enhanced security tailored to your business requirements.

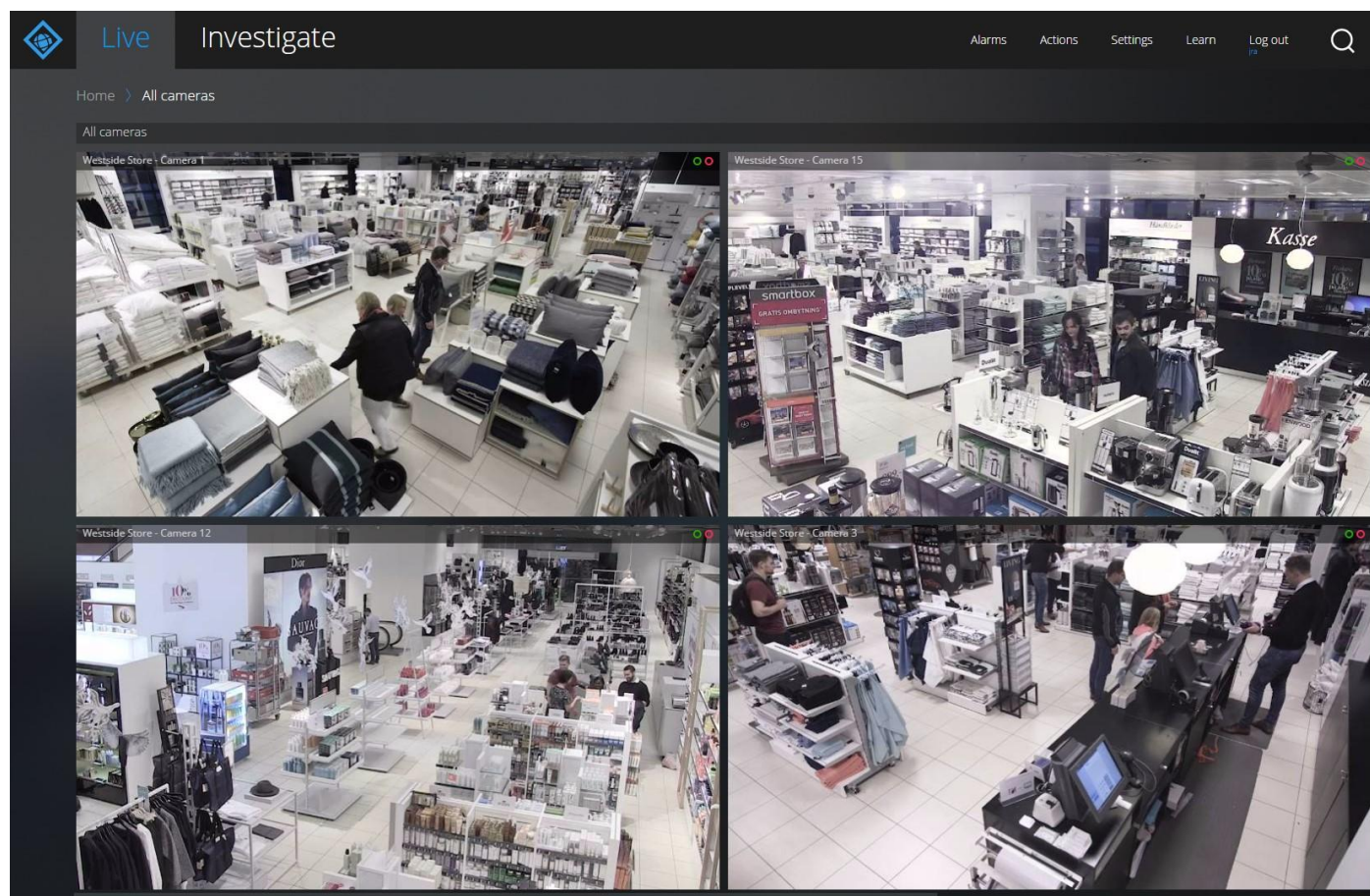


Image 1. The operator view of XProtect through the Web client

Use XProtect Web Client to:

- View live video and video recordings in your web browser.

In XProtect Web Client, the time information displayed in the app inherits the time zone set on your computer. This includes the time shown in live and playback mode, alarms, bookmarks, and so on.

- Add bookmarks to live videos and video recordings.
- Play incoming and outgoing audio in live video and video recordings.
 - Use the push-to-talk (PTT) feature while you are watching live video from one camera.
 - Broadcast audio to multiple cameras in live mode.
 - Play back incoming and outgoing audio in playback mode.
- Create investigations.
- Download video exports with or without recorded incoming and outgoing audio.
- Activate actions that trigger events in your video surveillance system.
- View videos for alarms that are triggered by various events.

Operating The Web Client

Operate the web-based surveillance app on a computer with internet access. The following features and functions are available to operators as per the rules and permissions configured in the user profile

- Logging in
- Home page overview
- Search for camera
- Navigate to camera
- Viewing live video (explained)
- Bookmarks (usage)
- Listen to incoming audio in live video
- Use push-to-talk in live video from one camera
- Broadcast audio to multiple cameras in live video
- Using the timeline in playback mode (explained)
- Play back recordings from one camera
- Playing back audio in video recordings (explained)
- Recordings from multiple cameras (explained)
- Specify time for video playback
- Remove unnecessary cameras from video playback
- Cameras in your investigation area (explained)
- Using the timeline in investigations (explained)
- Create investigations from one or more cameras
- Add a camera to an existing investigation
- Remove a camera from an existing investigation
- Update or delete your investigation
- Prepare video export and download
- Sharing the XProtect Web Client page
- View alarms
- Activate actions
- PTZ control
- Use digital zoom
- Use optical zoom (for cameras that support optical zoom)

Cloud System Server Architecture

The setup of an XProtect Cloud instance requires a set of servers configured for each end-user system specification. This allows the system to truly scale up to handle 20,000+ cameras within a single Cloud instance for a single end user. We have a live cloud environment XProtect systems operating with a small number of cameras and thousands of cameras.

Management server

The management server is the central VMS component. It stores the configuration of the surveillance system in a SQL Server database, either on SQL Server on the management server computer itself or on a separate SQL Server on the network. It also handles user authentication, user permissions, the rule system and more. The management server runs as a service and is typically installed on a dedicated server.

Failover management server

You can get failover support on the management server by installing the management server in a Microsoft Windows cluster. The cluster ensures that another server takes over the management server function in case the first server fails.

Recording server

Recording servers are computers where you have installed the Recording Server software and configured it to communicate with the management server. A surveillance system typically consists of several recording servers. The recording server is responsible for all communication, recording, and event handling related to devices such as cameras, video and audio encoders, I/O modules, and metadata sources. Examples of actions the recording server handles:

- Retrieve video, audio, metadata and I/O event streams from the devices
- Record video, audio and metadata from devices
- Provide operators with access to live and recorded video, audio and metadata
- Provide operators with access to device status
- Trigger system and video events on device failures or events
- Perform motion detection and generate smart search metadata

The recording server is also responsible for communicating with other Xprotect products when using the Interconnect technology.

The recording server supports encryption of data streams to the clients and services as well as encryption of the connection with the management server

Failover recording server

The failover recording server is responsible for taking over the recording task in case a recording server fails.

The failover recording server operates in two modes:

Cold standby for monitoring multiple recording servers

In a cold standby failover recording server setup, you group multiple failover recording servers in a failover group.

The entire failover group is dedicated to taking over from any of several preselected recording servers if one of these becomes unavailable.

You can also specify a secondary failover server group that takes over from the primary group if all the recording servers in the primary group are busy. Hot standby for monitoring a single recording server.

In a hot standby failover recording server setup, you dedicate a failover recording server to take over from one recording server only. With this approach, the failover recording server is continuously synchronised with the correct/current configuration of the recording server it is dedicated to, and it can take over much faster than a cold standby failover recording server.

Media database

The system stores the retrieved video, audio and metadata in the customised high-performance media database, which is optimised for recording and storing audio and video data.

The media database supports various unique features, including multistage archiving, video grooming, encryption and adding a digital signature to the recordings.

Event server

The event server handles the tasks related to events, alarms, and maps and also third-party integrations via The Cloud Integration Platform.

Events:

All system events are consolidated in the event server, so there is a single place and interface for partners to make integrations that use system events

The event server offers third-party access for sending events to the system via the Generic events or Analytics events interface

Alarms:

The event server hosts the alarm feature, alarm logic, alarm state, and alarm database handling.

The alarm database is stored in the same SQL Server database as the management server uses Maps:

The event server also hosts maps. You configure and use maps in the XProtect Smart Client.

Integration Platform:

You can install third-party developed plug-ins on the event server and utilise access to system events.

You can get failover support on the event server by installing the event server in a Microsoft Windows cluster.

The cluster ensures that another server takes over the event server function in case the first server fails.

Log server

The log server stores all log messages for the entire system. The log server typically uses the same SQL Server as the management server but has its own SQL Server database. The log server is also typically installed on the same cloud server as the management server. If you need to increase the performance of the management server or log server, you can install the log server on a separate cloud server and use a separate SQL Server.

The system can, through the log server, write three types of log messages:

System logs: the system administrator can choose to log errors, warnings, and information or a combination of these. The default is to log errors only

Audit logs: the system administrator can choose to log user activity in clients in addition to login and administration logs

Rule-triggered logs: the system administrator can use the rule log to create logs on specific events
SQL Server

The management server, the event server, and the log server use SQL Server databases on one or two SQL Server installations to store, for example, configuration, alarms, events and log messages.

The XProtect installer includes Microsoft SQL Server Express, which is a free edition of SQL Server.

For very large systems or systems with many transactions to and from the SQL Server databases, we recommend that you use the Microsoft® SQL Server® Standard or Microsoft® SQL Server® Enterprise edition of SQL Server on a dedicated computer on the network and on a dedicated hard disk drive that is not used for other purposes. Installing an SQL Server on its own drive improves the entire system's performance.

Mobile server

XProtect Mobile server handles logins to the system from XProtect Mobile client or XProtect Web Client.

An XProtect Mobile server distributes video streams from recording servers to the XProtect Mobile client or XProtect Web Client. This offers a secure setup where recording servers are never connected to the Internet. When a XProtect Mobile server receives video streams from recording servers; it also handles the complex conversion of codecs and formats, allowing video streaming on mobile devices.

API Gateway

The MIP VMS API provides a unified RESTful API, based on industry-standard protocols such as OpenAPI, for accessing XProtect VMS functionality, simplifying integration projects and serving as a basis for cloud-connected communication.

The XProtect VMS API Gateway supports these integration options through the Integration Platform. VMS API (MIP VMS API).

The API Gateway is installed and is intended to serve as a front-end and common entry point for RESTful API and WebSocket Messaging API services on all the current VMS server components (management server, event server, recording servers, log server, etc). An API Gateway service can be installed on the same host as the management server or separately, and more than one can be installed (each on their own host).

The RESTful API is implemented in part by each specific VMS server component, and the API Gateway can simply pass through these requests and responses, while for other requests, the API Gateway will convert requests and responses as appropriate.

Currently, the configuration API, hosted by the management server, is available as a RESTful API. The RESTful Events API, Websockets messaging API, and the RESTful Alarms API, hosted by the event server, are also available

Interconnect Centralisation

XProtect Interconnect allows you to integrate several XProtect installations with one XProtect Corporate central site. You can also install these sites, called remote sites, on mobile units, such as boats, buses, or trains. This means that such sites do not need to be permanently connected to a network. The central site considers the remote site as an advanced camera or multi-channel encoder with edge storage capabilities. Each remote site runs independently and can perform surveillance tasks as configured. Depending on the network connections and appropriate user permissions, Interconnect offers you direct live viewing of remote site cameras and playback of remote site recordings on the central site. It also offers you the possibility to transfer remote site recordings to the central site based on either system-defined events, rules, or schedules or by manual requests from XProtect Smart Client users. The central site can only see and access devices that the user account specified on the remote site has access to. This allows local system administrators on the remote sites to control which devices should be made available to the central site and its users.

GDPR

The European Union's (EU) General Data Protection Regulation (GDPR) puts personal data protection at centre stage with a set of laws governing personal data protection in the EU and the European Economic Area (EEA).

XProtect Corporate 2019 R2 is the first major VMS product to obtain EuroPriSe GDPR-ready certification. The certification is issued by the recognised and mi EuroPriSe – European Privacy Seal Institute, where XProtect Corporate has been checked by independent experts and approved by an impartial certification body. Building on the native XProtect cybersecurity features, the certification covers all core VMS functions in accordance with EuroPriSe's documented scope of evaluation.

The EuroPriSe GDPR-ready certification proves that XProtect Corporate fulfils EuroPriSe's certification criteria as defined in the criteria catalogue v201701*. The GDPR-ready seal and the extensive guidelines and recommendations provided by XProtect provide end users with a solid foundation for establishing a GDPR-compliant video surveillance operation while simplifying and reducing the cost of GDPR preparation.

In 2021, XProtect Corporate European Privacy Seal (EuroPriSe) introduced a new privacy seal certification that expands XProtect's GDPR compliance to cover more functions. As a strong advocate for responsible technology, we are committed to protecting people's privacy and data.

FIPS 140-2 Compliance

FIPS stands for Federal Information Processing Standards. It is a set of standards that describe encryption algorithms and other information technology processes for use within non-military federal government agencies and by government contractors and vendors who work with these agencies across the United States and Canada.

FIPS was developed by the National Institute of Standards and Technology (NIST) in the United States and the Communications Security Establishment (CSE) in Canada.

Federal Information Processing Standards 140-2 (FIPS 140-2) is an information technology security accreditation program for validating that the cryptographic modules produced by private sector companies meet well-defined security standards. FIPS 140-2 specifies what encryption modules are approved and prohibits agencies from using unapproved cryptography on sensitive data within the federal government.

This standard must be met by all software solutions deployed in US government installations and in highly regulated industries such as healthcare and finance in North America.

XProtect 2020 R3 and later versions use the latest encryption technology provided by Microsoft. This ensures that user information such as usernames, passwords, and devices is encrypted end-to-end, so you can rest assured that your personal information is always secure and projected. These developments include using only FIPS-approved cryptography modules such as Microsoft's Cryptography New Generation (CNG).

This next level of encryption also allows federal customers in the US and Canada to run XProtect in an FIPS-compliant mode. Such developments allow users to operate XProtect 2020 R3 in an FIPS 140-2 compliant mode in Windows.

Support

XProtect Care is the name of the complete service and support program for XProtect products throughout their lifetime.

Care Plus

If you have a Software Care Plus subscription, you also have access to free updates to your current XProtect VMS product and can upgrade to more advanced XProtect VMS products at an advantageous price. Care Plus also offers additional functionality:

- The Customer Dashboard service
- The Smart Connect feature
- The full Push Notification functionality

Care Premium

If you have a Care Premium subscription, you can also contact the support team directly. Please remember to include information about your Care ID when contacting support.

Contract Terms

The purchase order is required to secure any needed labour resources and enable procurement activity to begin.

Payment terms are 30 days from the date of invoice.

Changes to the scope of work are charged in addition to the work already quoted.

Warranty

Installation Warranty.

Ajar Technology's installation is covered by a labour warranty for 12 months from completion. The warranty covers defects due to poor workmanship affecting the product's performance or systems installed by Ajar Technology.

Ajar Technology must be notified of the defect within this warranty period, and sufficient information must be provided to evidence the cause and effect.

To notify us and request a call-out under the installation warranty, please email us at the following address and provide us with as much information as possible about the issue.

Contact Helpdesk@ajartechnology.com

Outside of installation warranty.

The installation warranty does not cover acts of nature, damage due to physical abuse or vandalism, damage caused by power surges, damage by other parties, or other causes that are not directly attributable to the quality of our installation.

The labour warranty does not include labour in general hardware failures occurring through use.

The manufacturer's warranty process will be followed in case of hardware warranty issues.

Ajar Technology recommend a service agreement including preventative maintenance and reactive response for peace of mind that there is a known incident response in the event of an issue.

Contact: Helpdesk@ajartechnology.com

Parts Warranty

The manufacturer provides a parts warranty under its terms, which are available upon request. Unless expressly stated in advance, the standard parts warranty period of 12 months offered by manufacturers begins at the point of receipt of the goods in the Ajar Technology warehouse. Some manufacturers provide a Warranty for longer than 12 months.

Warranty is provided upon return to the manufacturer's base.

The part should be returned to Ajar Technology or the manufacturer directly. The part(s) will be assessed and repaired or replaced under the warranty terms.

To notify us and request a call-out under the installation warranty, please email us at the following address and provide us with as much information as possible about the issue.

Contact: Helpdesk@ajartechnology.com

Ajar Technology recommends preventative maintenance, which is contracted with us.

Outside of warranty

Issues raised outside of warranty cover will be treated according to the terms of the maintenance contract in place. Without a maintenance contract, the quotation for the resolution will be issued and acted upon receipt of the purchase order.

The standard warranty applies to all Ajar Technology contracts and can only be superseded by an agreement signed by Ajar Technology that stipulates different terms.

Unless otherwise stated or contractually agreed, there is no obligation for resolution at our cost.

Terms and conditions

All quotations issued are subject to the company standard terms and conditions outlined in the following points.

- a) Accidental errors and omissions will be requoted with the corrections.
- b) Additions and changes to the scope of work referenced in our quotations must go through the formal change process and address commercial implications when required.
- c) Variations will only be actioned after a purchase order has been received by Ajar Technology
- d) Once any product is installed, we will record this evidence in our project management tool for quality assurance and audit purposes.
- e) The main contractor or client must sign off on installed systems on installation day.
- f) Any damage caused to the equipment by others is not Ajar Technology's liability.
- g) If remedial work is required because of damage caused by others, the project will authorise the cost.
- h) The published project plans are subject to the equipment's lead time and the stated dependencies on other parties.
- i) Unless otherwise stated, the installation works will be conducted during our normal business hours, Monday to Friday. Any work required outside the normal working hours is subject to additional charges.
- j) Anything not clearly stated in the quotation issued by Ajar Technology means that it is not included; therefore, clarification from the buyer should be sought from Ajar Technology.
- k) We expect to securely store equipment on-site with easy access. Unless otherwise agreed in writing.
- l) If the site is not ready when we arrive at the site or if the installation team is stood down with less than 24 hours notice, this time will be charged to the contracted project delivery services.
- m) Ajar Technology requires a purchase order to allocate any labour resource to a project and enable procurement activity to begin.
- n) Payment terms are 30 days from the date of invoice.
- o) Abortive fees are charged to the client at the rate for the revisit plus additional costs incurred