



AVADA CONNECT LIMITED

SERVICE DEFINITION

1. Service Summary

Avada Connect is a secure, scalable Video Management System (VMS) and Information Management System (IMS) designed for organisations that require reliable, high-performance video surveillance and incident management. The service enables customers to record, view, analyse, and manage video from a wide range of IP cameras and IoT devices, supporting deployments from small single-site installations to large multi-site estates with thousands of cameras.

The platform provides a unified environment for live monitoring, forensic search, incident handling, and system administration, with strong cybersecurity controls and flexible deployment options. Avada Connect is suitable for public sector organisations seeking a modern, resilient, and future-proof surveillance solution that supports operational efficiency, evidence integrity, and multi-site visibility.

2. Why Avada

Avada Connect is a modern, scalable Video Management System (VMS) and Information Management System (IMS) designed to record, view, analyse, and manage video footage across a wide range of security, surveillance, and IoT environments. Built for simplicity, speed, and high integration capability, it provides organisations with a centralised platform to operate from both small and extremely large CCTV deployments, ranging from a handful of cameras to tens of thousands.

At its core, Avada Connect supports multi vendor integration, automatically discovering and connecting with 99% of IP camera manufacturers—over 750+ supported devices—including PTZ cameras, fisheye devices, encoders, and legacy analogue systems. This makes it highly adaptable to diverse security infrastructures without requiring hardware replacement. Further integrations include Alarms systems, Access Control systems, AI and analytics, IOT systems, I/O devices, Networking and numerous market vertical integrations.

The platform provides real time and recorded video viewing, enhanced by features such as fisheye dewarping, advanced PTZ controls, and bi directional audio. Its high speed search engine allows users to scan through a year's footage in seconds using advanced filters such as object type, colour, vehicle details, clothing, gender, or motion based events—greatly accelerating investigative workflows.

Avada Connect includes powerful security and reliability features, such as AES-256 end to end encryption, custom encryption keys, and two factor authentication (2FA). Organisations can choose from flexible storage integrations, supporting on premises hardware (NVR/DVR, NAS, SAN, iSCSI) or Avada's own Cloud Hot Storage and Evidence sharing options, enabling hybrid or cloud native retention strategies with resilient failover options.

The system is designed to be lightweight, easy to install, and accessible from any device, including desktop, web, and mobile. Through the Avada Connect mobile apps (iOS/Android), users can securely monitor live feeds, review recordings, receive push notifications, and remotely control cameras with low latency streaming.

Enterprise systems can benefit from our user focused information management features such as Incident and Video Management, alarm aggregation and escalation work streams, while our automated reporting engine allows critical data to be received by stakeholders in and out of the control room.

Large installations benefit from features such as enhanced camera grouping, selective backups, recording failover, timeline thumbnails, and remote secure access to integrated devices via an inbuilt proxy. These capabilities streamline system management and ensure continuity even during hardware failures.

With over 20 years of industry experience, thousands of clients, and continuous development focused on security and integration, Avada Connect delivers a dependable, customisable, and future proof platform for organisations seeking a unified approach to video surveillance management.

3. Service Scope

This service covers the provision, deployment, configuration, and ongoing support of the Avada Connect VMS/IMS platform. The scope includes the core software, optional cloud based connectivity features, mobile applications, and integration with supported third party devices and analytics systems.

3.1 Included Services:

- System installation and configuration
- Device discovery and onboarding
- User and role configuration
- Access to desktop, mobile, and browser clients
- Optional cloud connectivity and identity services
- Ongoing updates, patches, and security enhancements
- Second and third line support via the Avada UK Helpdesk

3.2 Excluded Services:

- Customer owned network infrastructure
- Unsupported or end of life operating systems
- Third party hardware or software not compliant with standard protocols
- Custom development outside the standard product roadmap

4. Technical Overview

4.1 System Overview

- Client-Server Architecture, utilising hive redundancy and on premise Server and Client deployments and Cloud and mobile client command options.
- Desktop, mobile and web clients providing live, playback, search and system admin functionality.
- Scaling between 1-10,000+ cameras at ease.
- Supporting 1000s of different device types for integration through Avada Connect.
- High speed analytic search engine which can analyse years of recording in seconds. With object-based filtering such as vehicle colour, gender, object type etc.
- Local and Cloud based video storage.
- Hive based recording failover.
- Enterprise class security including AES-256 and 2FA.

4.2 System Detail

Avada Connect is a On-Premises solution with optional components for SaaS, IaaS and cloud distribution of data. Solving the core problem of data ownership with still needing data and operational availability for surveillance. Covering solutions from small alarm and retroactive CCTV driven environments to large multi-site pro-active surveillance operations within public space, government site and asset protection, industrial and corporate covers and multi-site estates.

4.3 Multi-Cloud Support

Avada Connect cloud and distribution features are provided and managed by Avada are not installable by 3rd parties across their own cloud platforms. Deleting devices, systems and users from Avada Connect cloud features permanently deletes them from the cloud.

4.4 Public Sector Connectivity.

Avada Connect requires no access to PSN, HSCN, JANET, PNN, SWAN or any other public sector network to function either in stand-alone or cloud connective options and has no dependencies upon them.

5. Service Features

5.1 Core technical capabilities include:

1. Distributed Server-Hive Architecture: allowing multiple servers to automatically synchronise configuration and share load, enabling scalability from small installs to thousands of cameras. Any server can act as a backup for another, supporting built in redundancy.
2. Multi-Platform Client: Desktop, Mobile, Browser, and Cloud—allowing operational access from virtually any device or operating system
3. High Performance Media Server: Avada platform is engineered for efficient device discovery, stream handling, and storage management. It integrates with over 790 manufacturers and is optimized for high throughput, low latency video processing.
4. Mass Device Integration: auto discovers and integrates with 99% of IP cameras and 790+ IoT device manufacturers, supporting ONVIF, RTSP/HTTP/UDP streams, I/O devices, encoders, and NVRs.
5. Highly Optimised performance: Can decode up to 64 high resolution streams per monitor.
6. Event Driven automation: Advanced Rules engine for event automation and metadata creation and ingestion that can classify and sort objects for fast data recall.

Integrations are too numerous to list but please contact Avada for more information about any specific challenge.

5.2 Security Features include:

1. User rights and roles access control (RBAC): Allowing fully customisable roles and fine-grained function permissions such as PTZ, export, video wall access etc.
2. Account Security: Strength and NIST list enforcement, secure multi-level salted and hashed storage, optional service reset linked to users email and brute force protections.
3. 2FA: Fully supporting 2FA options with optional cloud connectivity.
4. Secure communications: TLS, HTTPS, TLS/SSL enforced by default support for custom SSL certificates.
5. Data Integrity: Built in integrity checks to detect modified or tampered video and built in watermarking for chain of custody.

5.3 Reporting Features include:

1. Full Audit Trail
2. Video Search and Forensic Tools
3. Reporting for chain of evidence and operational state.

5.4 Administration Features include:

1. User and System Management
2. System Setup and Security Configuration.
3. Scalable Hive Architecture
4. LDAP integration
5. Cloud Administration is linked to cloud.

6. Service Benefits

6.1 Improved Operation Efficiency:

Avada Connect dramatically reduces the time required to respond to events, manage devices, and search video archives.

- Smart search and analytics allow operators to find critical events in seconds instead of hours.
- Automatic camera discovery and rapid setup reduce onboarding time for new sites.

Outcome: Faster investigations, quicker resolutions, and lower operational labour costs.

6.2 Enhanced Security Posture & Risk Reduction

Avada Connect includes strong cybersecurity protections, reducing the risk of breaches or unauthorized access.

- Advanced user rights, audit trails, TLS/SSL communications, encrypted video, and password hardening improve system safety.

Outcome: Reduced compliance risk, better evidence integrity, and fewer vulnerabilities in critical surveillance infrastructure.

6.3 Scalable growth with no Architecture re-design

Avada server hive architecture means organisations can scale from a few cameras to thousands without redesigning their system.

- Instant integration of new servers enables seamless expansion.
- Support infinite multi site scalability.

Outcome: Future proof infrastructure that grows with the business, without expensive rip and replace projects.

6.4 Centralised Multi-Site Visibility & Control

Avada Connect enables centralised oversight for distributed organisations.

- Allowing unified camera views of all systems, simplified user management, and remote system access anywhere.

Outcome: Better multi-site situational awareness, reduced travel time for IT/security teams, and unified policy governance.

6.5 Higher Decision Quality Through Integrated Analytics & Data

Avada Connect integrates deeply with third party analytics, access control, POS and other business systems. AI analytics (object detection, LPR, behaviour analysis) provide actionable insights rather than just video.

Outcome: Better decision making, reduced fraud, enhanced situational understanding, and improved cross department collaboration.

6.6 Increased System Uptime & Resilience

- Automatic failover and distributed redundancy ensure uninterrupted recording during server failure.

Outcome: Continuous evidence capture with no downtime, ensuring compliance for critical infrastructure.

6.7 Lower Total Cost of Ownership (TCO)

Avada Connect requires no proprietary hardware and is extremely resource efficient.

- Runs on non-specialised COTS hardware
- Efficient code enables high performance with minimal CPU/GPU load.

Outcome: Reduced hardware expenses, extended lifecycle of existing servers, and lower maintenance costs.

6.8 Faster Incident Response & Real Time Awareness

With event driven rules and live alerts:

- The system can auto trigger alarms, PTZ actions, notifications, or recording enhancements.

Outcome: Faster threat detection, better real time situational response, and enhanced safety outcomes.

7. Cloud Deployment Model

7.1 AWS Regions

Avada Connect uses public containers hosted on Amazon Web Services (AWS) if cloud functionality is enabled. This proxy and connectivity option allows relay and mediator services, secure connectivity without port forwarding, health monitoring and event notifications outside of the on-premises deployment.

By default, cloud connectivity does not store any video or use any 3rd party cloud providers for services and uses Major AWS regions including eu-west-2 (London), eu-north-1 (Sweden), eu-west-1 (Ireland) and eu-central-1 (Germany).

7.2 Cloud Tenancy

Avada Connect tenancy works as each site is its unique own tenant that is on premise. The optional cloud layer allows a multi-tenancy identify layer to allow system linking with granular permissions. Optional cloud video storage options are unique tenancy and can be configured for per site or per multi-site as required.

7.3 Cloud Security & Limitations

Avada Connect provides strong segregation and security by isolating each system as its own self contained environment while enforcing strict role based access so users only see the cameras, layouts, and features assigned to them. It protects system access with secure passwords, two factor authentication, and LDAP/Active Directory integration while encrypting all communications with TLS/SSL and allowing optional encryption of video streams to prevent interception. To maintain data integrity, Avada connect includes archive tamper detection and digital watermarking on exported footage, and all user actions are logged in an audit trail for accountability. Cloud services are limited to identity and connectivity—not video storage—ensuring each organisation's data remains fully segregated and locally controlled.

Avada Connect supports various options for migration and portability on premise, but the cloud option is not portable to other providers.

8. Service Constraints & Customer Responsibilities

8.1 Constraints

There are performance constraints on the on-premises hardware where the number of cameras recorded and shown are related to the hardware specifications, please Contact Avada for details. For the cloud the constraints consist of:

1. Internet connection Quality: uptime, bandwidth, latency and packet loss are key criteria if the cloud options are enabled.
2. Local Security: Local servers and NVRS must be kept in an appropriate environment to maintain security.
3. Off Site backups: Must be kept as per project requirements.
4. Firewall restrictions: AWS URLs and Ports must be enabled.
5. Video Transcode: High CPU and GPU impact.

Maintenance of on-premise systems is done at agreed points with the site and will never occur unplanned. Cloud features are given notice before action.

Support limitations include any unsupported or End-of-life operating systems. No support for 3rd party systems outside of official capacity such as a camera that doesn't follow standard RTSP standards, Firewall rules that don't allow AWS access, version mismatch of backups, modifying of Avada Connect files or database and no video issues caused by 3rd party cameras.

8.2 Customer Responsibilities

Customers are responsible for ensuring that their network, servers, and storage infrastructure meet the minimum system requirements. This includes providing adequate bandwidth, maintaining firewall rules that allow AWS connectivity (if cloud features are enabled), and ensuring physical security of on premise hardware.

Customers must manage user accounts, maintain compliance with local data protection laws, and ensure that any third party devices connected to the system follow standard protocols such as ONVIF or RTSP.

8.3 System Requirements

Hardware as per price list, cloud options require:

- Modern, standards compliant browser with HTML5
- A stable internet connection scaled as per site requirements if cloud options are enabled.
- Remote connections enabled for site support.
- Mobile client compatible with iOS and Android.

9. Service Levels (SLAs)

Avada Connect provides the following standard service levels:

9.1 Service Availability

- Core on premise system availability is determined by customer infrastructure.
- Optional cloud connectivity services are available 99.9% of the time, excluding planned maintenance.

9.2 Incident Response Times and Resolution Targets

- Priority 1 (Critical): Response within 2 hours during support hours
- Priority 2 (High): Response within 4 hours
- Priority 3 (Medium): Response within 1 business day
- Priority 4 (Low): Response within 2 business days

9.3 Planned Maintenance

- Customers are notified at least 5 working days in advance of planned maintenance affecting cloud features.
- On premise maintenance is scheduled with the customer and never performed without agreement.

9.4 Service Management

Avada provides a structured service management model aligned with ITIL principles. Incidents, service requests, and change requests are logged via the Avada Helpdesk portal or email. Each ticket is assigned a unique reference number and tracked through to resolution.

Escalation paths are in place to ensure timely handling of complex issues, with second line engineers managing operational queries and third line engineering teams addressing software level or integration issues. Customers receive updates throughout the lifecycle of each ticket, and periodic service reviews can be arranged for larger deployments.

9.5 Support Channels

Avada operates on a second and third-line basis. The first line if present will be the onsite integrator, technical specialists or IT services. The first line responder can create tickets within the Avada Connect helpdesk system or auto create a ticket from an email. The Avada UK Helpdesk will respond to the ticket or call the site to assist further until the problem has been resolved. If the problem cannot be resolved within a timely manner Avada helpdesk staff will raise it to 3rd line support so that problem can be tested and investigated locally in the Avada development office.

Avada will visit site for system updates and training through the life of the project it is not expected that site updates will be done by first line staff. Additional site time and support is detailed in the price list.

Avada UK Helpdesk standard hours are 9am – 5pm , Mon – Fri. Support costs are included with the channel licensing of the price list. Uplifted support times are available as a cost option to cater for 24/7 requirements.

Only approved parties can contact support this is specific to the site or project and consists with which members have had training and project ownership.

10. Onboarding & Offboarding Process

10.1 Onboarding

Avada Connect provides a structured onboarding process to ensure a smooth and secure deployment. Onboarding begins with a discovery and requirements phase, during which Avada works with the customer or integrator to confirm site architecture, device counts, network readiness, and security requirements.

Once prerequisites are met, Avada engineers install and configure the system, perform device discovery, and validate connectivity. Training is delivered either on site or remotely, using a “train the trainer” or full end user model depending on customer preference. Commissioning reports and documentation are provided at the end of onboarding.

Customer responsibilities include ensuring network readiness, providing access to required infrastructure, and ensuring that local IT/security teams are available during installation. Avada is responsible for configuration, validation, and ensuring the system meets agreed functional requirements.

10.2 Offboarding

Avada Connect is an on premise system, and customers retain full ownership of all data. Offboarding is therefore straightforward and does not require supplier intervention unless requested. Customers may export incident data, evidence files, and system configuration at any time using built in export tools.

Upon contract termination, Avada can provide optional support to assist with data extraction, system decommissioning, or migration to another platform. No customer data is retained by Avada, and cloud based identity or connectivity services are disabled once access is revoked. Any hardware leased from Avada is securely wiped and disposed of in accordance with ISO 14001 processes.

11. How Users Work with the Service

11.1 User Interaction

Users interact with Avada Connect primarily from the thick client application, if options are taken this can also be via a browser and/or via a mobile app. There is no portal for user access as Avada Connect is a unique instance per site / multi-site.

There is no available API for data access but Avada Connect can push information external manually or automatically.

Accessibility options include UI scaling, high visibility controls. dynamic video scaling, keyboard and mouse support so that specific accessible per user options can be used, contextual help system, multi-platform access methods and a Windows based thick client which can take advantage of the full suit of Microsoft Windows user accessibility options.

11.2 Data Importing & Exporting.

Incident and Evidence data can be exported at any time, as long with system wide configuration details. This is exported in various formats depending on source but would include .csv and .xls.

Data ownership being on premise is in the sole ownership of the site / multi-site and Avada Connect Ltd. has no ownership or unapproved access to site data.

12. Security, Governance & Staff Vetting

12.1 Asset Protection

Data is stored on premise in encrypted data stores, or with options within site encrypted site tenant. AWS data standards include but not limited to:

- ISO 27001, ISO 27017, ISO 27018
- SOC 1 / SOC 2 / SOC 3
- PCI DSS
- CSA STAR

Hardware can either be purchased or leased if leased Avada has a secure disposal process in which all data on board is wiped, permanently physically disabled and then recycled with an ISO 14001 carrier.

12.2 Governance

Named Security lead – Sean Kettlewood Technical Director

Avada Connect Ltd. software development complies with leading security standards such as CAPPs, OSWAP, NIST and secure by design security concepts. Avada uses both a CI and CD pipeline where the automated build process is automatically integrated, tested and packaged to be deployed consistently but this is only released to the software test team where individual ratification is required, once passed this is available for engineering but is not push to customers without agreed rollout plans per site / multi-site.

For CAPPs methodologies in the event of a security flaw a cross functional task team is assembled to replicate, test and resolve in isolation to the core engineering function. Customers are made aware in line with the SVE scoring process.

Avada complies with the 14-day Cyber Essentials process for items that are classified as critical or high risk, have a SVE score of 7 or have unknown severity levels.

12.3 Staff Security

All staff members are security vetted and site engineering members include BS7858, BPSS and SC screening.

13. Data Protection, Data Location & GDPR

13.1 Data Protection & GDPR

Avada Connect operates as a data processor when cloud identity or connectivity services are used, and as a software provider when deployed fully on premise. Customers act as data controllers and retain full ownership and control of all video, metadata, and configuration data.

The service supports GDPR compliance through secure data handling, encryption, access controls, audit logging, and data export capabilities. No customer video is stored in the cloud unless optional cloud storage features are explicitly enabled. Avada provides details of sub processors (AWS) upon request and supports customers with DPIA documentation where required.

13.2 Data Location & Data Flow

All video and metadata remain on premise unless optional cloud features are enabled. When cloud connectivity is used, only identity, signalling, and health monitoring data transit through AWS regions in the UK and EU. No video is transmitted or stored in the cloud by default.

Each customer site operates as an isolated tenant, with strict separation of data and access rights. Data does not leave the UK/EU unless explicitly configured by the customer.

13.3 Backup & Disaster Recovery

Backup and disaster recovery for on premise deployments are the responsibility of the customer, as all data is stored locally. Avada Connect supports industry standard backup tools and provides export options for configuration and evidence data.

For optional cloud services, Avada maintains resilient infrastructure with multi region redundancy. Cloud service recovery time objective (RTO) is 4 hours, and recovery point objective (RPO) is 15 minutes. DR testing is performed annually.

14. Commercials & Contractual Terms

14.1 Pricing Model

Avada Connect is licensed on a per channel basis, with optional modules and cloud features available as add ons. Pricing is determined by the number of cameras, servers, and sites, as well as any required integrations or enhanced support packages.

Support is included within standard licensing, with extended hours or 24/7 coverage available as optional upgrades. Hardware can be purchased or leased, and free trials are available subject to project complexity.

14.2 Pricing and Commercial Operations

Please refer to the pricing list, Avada can confirm that free trials are available for Avada Connect software and hardware is considered per site requirement.

There is no eligibility requirement for the Avada Connect software, length of trial is relative to the complexity of the project. Hardware options would be discussed depending on requirement per site.

14.3 Termination Terms

Customers may terminate the service in accordance with the terms set out in the call off contract. Notice periods and any applicable charges depend on the commercial agreement. Upon termination, all customer data remains on premise, and Avada does not retain or access any customer information.

Optional cloud services are disabled at the end of the contract, and any leased hardware is securely wiped and returned or disposed of in line with ISO 14001 standards.

15. Compliance, Accessibility & Sustainability

15.1 Accessibility

Avada Connect is designed with accessibility in mind and supports a range of features including UI scaling, high contrast modes, keyboard navigation, and compatibility with assistive technologies available in Microsoft Windows. The service aims to meet WCAG 2.2 AA principles where applicable and provides multi platform access to support diverse user needs.

15.2 Roadmap & Versioning

Avada Connect follows a continuous development model with regular updates delivered through a controlled CI/CD pipeline. New releases undergo automated and manual testing before being made available to customers. Release notes are provided for each version, and customers are notified of upcoming changes in advance. Major updates are scheduled with customers to ensure minimal disruption.

15.3 Sustainability

Avada Connect supports sustainable operations through efficient software design that extends the lifespan of existing hardware and reduces the need for specialised equipment. Avada adheres to ISO 14001 principles for hardware recycling and disposal, and cloud services are hosted in AWS regions that operate with strong environmental and energy efficiency commitments.