ICSA

INTEGRATED COMMAND SERVER APPLIANCE

Enterprise On-Premises Platform for Command Operations

Integrated compute, secure connectivity, operational applications, communication services and managed data infrastructure in a single appliance.



PRODUCT DATASHEET

On-Premises Deployment

Integrated Application Platform

Secure Private Infrastructure

ICSA integrates command operations, secure communications, media management and protected data services in a unified on-premises appliance.

Integrated Command Server Appliance

ICSA

ICSA is an integrated on-premises appliance designed for patrol-camera operations, incident command, secure communications, device management and operational data. It combines enterprise server hardware and pre-integrated application capabilities into a deployable system that organizations can operate inside their own data center.

PRODUCT PROFILE

1 primary 2U appliance
1 identical 2U standby
1 installed drive set
28 integrated capabilities
Maximum 5 operational areas
24 user entitlements

KEY FEATURES

- Integrated incident command and common operating picture
- Secure private connectivity for headquarters and remote sites
- Browser-based conferencing, live video and media gateways
- Mobile device management and remote technical support
- Unified application and data platform
- Central monitoring, logging, backup and recovery

Integrated platform for command operations

The appliance provides a unified operating platform for command applications and supporting capabilities. Administrators manage application availability, software maintenance and recovery through centralized appliance controls. Each ICSA appliance operates as a bounded five-area command unit. Expansion beyond five operational areas requires an additional ICSA appliance.

Designed for on-premises operation

ICSA keeps application data, video routing, device policies and operational records within infrastructure selected by the organization. Administrators can connect the appliance to existing identity services, CCTV networks, field devices and remote sites while maintaining defined access boundaries and audit records.

Operational services in one appliance

The platform consolidates command applications, secure networking, conferencing, streaming, mobile device control, remote support, data services, monitoring, logs and scheduled backup. This reduces the number of separately managed systems and provides a unified administration experience.

Deployment, management and support

ICSA is delivered as a repeatable appliance profile. Administrators deploy the system with defined network, storage and security parameters, then manage application health from a central administration interface. Controlled software releases provide a consistent update and recovery path across installations.

Service lifecycle management

The appliance provides centralized health and availability status for its integrated capabilities. Administrators can review system utilization, application availability, operational logs and backup status before applying maintenance. Configuration and operational data are protected by the appliance storage and recovery functions.

Security and access control

HTTPS protects browser access. Role-based permissions limit administrative and operational functions. Two-factor authentication can protect interactive accounts. Private overlay networking connects approved nodes and remote locations without exposing internal services directly to the public network.

Backup and hardware recovery

Scheduled jobs protect configuration, relational data and selected application content through an independently provisioned backup repository. Backup encryption, recovery-point retention and restoration checks support data recovery. An identical diskless 2U standby provides a manual hardware recovery path through controlled transfer of the complete labeled drive set.

KEY BENEFITS

- Single appliance delivery model
- Reduced infrastructure complexity
- Repeatable installation and update process
- Central health and log visibility
- Controlled application maintenance
- Private data and media handling
- Defined backup and recovery workflow
- Fixed five-area operating boundary
- Additional-area expansion through independent appliance nodes

Functional architecture

COMMAND OPERATIONS

Incident registration and classification
Priority and status workflow
Personnel, unit and vehicle assignment
Operational dashboard and activity timeline
Map layers, live position and tracking history

SECURE ACCESS & TENANCY

User and role management
Two-factor authentication
Tenant and organization isolation
Cross-tenant visibility rules
Session control and audit history

COMMUNICATION & MEDIA

Patrol-camera live video and recording
Browser video conference and operational voice
Drone feeds and CCTV integration
Media gateway and protocol conversion
TURN and STUN relay services

FIELD DEVICE SERVICES

Mobile device enrollment
Policy and application deployment
Device inventory and compliance status
Remote desktop, terminal and file transfer
Approved node and remote site connectivity

DATA SERVICES

Relational database
Cache and message services
Object and media storage
Persistent configuration volumes
Backup repository and retention policy

PLATFORM OPERATIONS

Central application management
System health and availability monitoring
Central logs and operational alerts
Scheduled backup and recovery validation
REST API, webhooks and JSON event exchange

DEPLOYMENT MODEL On-premises bounded five-area appliance / Additional areas require an independent appliance node

EEC Technology Co., Ltd. | info@eec-techno.com

Integrated product capabilities

Command operations and situational management

CAPABILITY	DEPLOYMENT	PRODUCT FUNCTION
Core Application	**1 System**	Common operating picture with activity timeline, map layers, live position, tracking history, cross-area visibility, service health and audit history.
Incident Intake	**5 Operational Areas**	Caller and location capture, classification, priority, validation, queue handling, dispatcher handoff, shared coordination and acceptance status.
Dispatcher	**5 Operational Areas**	Personnel availability, duplicate-assignment prevention, instructions, media exchange, acknowledgement and mission-completion tracking.
Mission Planning	**5 Operational Areas**	Mission objectives, tasks, schedules, routes, resource plans, checklists and controlled operational plan updates.
Emergency Alert System	**5 Operational Areas**	Targeted operational alerts with severity, affected area, audience, acknowledgement state, escalation and alert history.
Operational Area Management	**5 Operational Areas**	Management of operational zones, jurisdictions, sites, boundaries, map areas and responsibility assignments.
Dashboard	**5 Operational Areas**	Operational dashboards for incident status, resources, device availability, service health, trends and management indicators.

Operational rights are limited to five areas and 24 user entitlements within the assigned appliance.

Integrated product capabilities

Video, consultation and operational communication

CAPABILITY	DEPLOYMENT	PRODUCT FUNCTION
Patrol Camera	**5 Operational Areas**	Map-based live access, multi-area viewing, adjustable video grids, personnel and incident association, and time-range video export.
CCTV Display	**5 Operational Areas**	Authorized live display and recorded playback through connected camera, VMS or NVR infrastructure, including multi-channel views.
Video Recording	**5 Operational Areas**	Continuous or event-based recording, retention control, indexed playback, incident association, export and access history.
Live Media Streaming	**1 System**	Live media gateway for patrol camera, CCTV and drone feeds, including stream routing and protocol conversion.
Video Conferencing	**1 System**	Browser-based audio and video conferencing without client installation, with chat, screen sharing, meeting control, recording and no meeting-duration limit.
Virtual Consulting	**5 Operational Areas**	Browser-based WebRTC consultation for at least three participants, with shared operational context and patrol-camera participation.
Voice Communication	**5 Operational Areas**	Two-way voice by individual, full group or selected subgroup, including authorized central microphone control.

Integrated product capabilities

Connectivity, devices, assets and access control

CAPABILITY	DEPLOYMENT	PRODUCT FUNCTION
Private Network	**1 System**	Encrypted overlay network with node enrollment, device revocation, communication rules, route control and approved remote-site connectivity.
Mobile Device Management	**1 System**	QR enrollment, group policy, APK deployment, kiosk mode, device status, compliance and policy-controlled location tracking.
Remote Device Management	**1 System**	Authorized remote desktop, terminal, file transfer and maintenance access with device, access and administrative action history.
Tools and Equipment Management	**5 Operational Areas**	Inventory, assignment, availability, custody, condition, maintenance status and operational equipment history.
Units	**5 Operational Areas**	Organizational unit structure, operational hierarchy and relationships among units, personnel, vehicles and assigned resources.
Web Gateway and TLS	**1 System**	Reverse proxy and secure application gateway for HTTPS termination, certificate handling, routing and controlled external access.
User Access Rights	**24 User Entitlements**	Role, tenant, unit and area scope with auditability. Twenty-four entitlements are associated with the assigned five-area appliance identity.

Access to devices, assets, services and operational data is governed by role, organization, tenant and configured security policy.

Integrated product capabilities

Data and platform services

CAPABILITY	DEPLOYMENT	PRODUCT FUNCTION
Relational Database	1 System	Persistent relational data service for application records, transactions, configuration data and structured operational information.
Cache and Session Store	1 System	In-memory cache and session store for application sessions, temporary state, frequently accessed data and service coordination.
Object Storage	1 System	S3-compatible object storage for images, documents, recordings and exports, with bucket administration, access control and encrypted transfer.
TURN and STUN Relay	1 System	Authenticated media traversal and relay with TLS, restricted relay ports and controls against unauthorized use.
Metrics Collection	1 System	Collection and retention of system and application metrics for health status, resource utilization and operational alerts.
Centralized Logging	1 System	Central collection, search and retention of application, infrastructure, security and administrative logs.
Backup and Recovery	1 System	Scheduled encrypted backup to independent storage, multiple recovery points, job verification and controlled restoration. Hardware recovery uses an identical diskless 2U standby.

INTEGRATED SERVICE MANAGEMENT

Integrated services are centrally managed through the appliance administration layer with controlled networking, persistent data protection, health monitoring, operational logs and recovery procedures.

The standard product profile supports five operational areas and 24 user entitlements.

ICSA appliance specifications

STANDARD FIXED HARDWARE CONFIGURATION	
Processor	1 × Intel Xeon 6730P processor, 32 physical cores / 64 threads, 2.5 GHz base frequency and up to 3.8 GHz turbo frequency.
Main Memory	64 GB DDR5 ECC RDIMM across an eight-channel memory architecture with eight DIMM slots.
System Storage	2 × 1.92 TB enterprise SSD in the rear 2.5-inch hot-swap bays, configured as RAID 1 for system software, applications and operational data.

VIDEO AND APPLICATION STORAGE	
Drive Bays	12 × front 3.5/2.5-inch and 2 × rear 2.5-inch hot-swap NVMe/SAS/SATA bays. Two internal M.2 PCIe 5.0 x2 NVMe slots are also provided.
Installed Video Storage	8 × 20 TB enterprise-class SATA HDD, Seagate Exos X20 or equivalent, 7,200 RPM and hot-swap capable; four front bays remain available for service expansion or hot spare.
Raw Capacity	160 TB installed raw HDD capacity in the standard product configuration.
Data Protection	Broadcom SAS3916 hardware RAID controller supporting RAID 0, 1, 5, 6, 10, 50 and 60. RAID 6 provides approximately 120 TB nominal usable capacity before file-system and application overhead.

EXTERNAL INTERFACES	
Data Network	2 × 10GbE RJ45 ports using the onboard Intel X550 controller for media ingest, application access, viewing, playback and storage traffic.
Out-of-Band Management	1 × dedicated 1GbE RJ45 BMC/IPMI management port using the ASPEED AST2600 management controller.
Local Service I/O	2 × rear USB 3.2 Gen 1 Type-A ports and 1 × rear VGA port. Internal headers provide 2 additional USB 3.2 Gen 1 ports and 1 COM interface.
Expansion	3 × PCIe 5.0 x16 and 3 × PCIe 5.0 x8 low-profile slots; one slot is occupied by the factory storage controller.

POWER AND SERVICEABILITY	
Power Supplies	2 × 1,200 W redundant (1+1), 96 percent Titanium-level hot-plug power-supply modules.
Cooling	3 × heavy-duty, speed-controlled 80 × 80 × 38 mm PWM fans with one internal air shroud.
Physical	2U rack-mount enclosure, approximately 437 mm wide × 89 mm high × 650 mm deep.
Service Access	Twelve front and two rear hot-swap drive bays, hot-plug power supplies, remote BMC/IPMI administration and compatible sliding rails support routine maintenance.

ICSA software features

MANAGEABILITY	
Appliance Administration	Web-based administration for application health, system status and configuration.
Application Management	Controlled application operation, maintenance and health validation.
Deployment Profiles	Repeatable appliance settings for network, security, storage and site deployment.
Software Updates	Controlled software release, rollout and rollback procedures.
Monitoring	System metrics, application availability, resource utilization and operational alerts.
Central Logging	Aggregated operational logs with filtering and retention controls.

DATA PROTECTION	
Scheduled Backup	Policy-based encrypted backup to independently provisioned storage for configuration, databases, files and operational records.
Recovery Points	Retention settings preserve multiple recovery points according to operational policy.
Hardware Standby	One identical diskless 2U appliance is maintained for manual hardware recovery.
Drive-Set Recovery	The complete labeled system SSD and data HDD set is transferred to matching bays; bay order is preserved.
Restore Verification	Backup jobs and controlled restoration procedures support periodic recovery validation.
Database Protection	Scheduled relational-database backup with encrypted retention, job verification and documented restoration procedure.

INTEGRATION	
Federation Interface	RESTful API, webhook and JSON event-stream interfaces for approved system integrations.
Federated Data	Incident summaries, event coordinates, resource status and authorized live-media links.
Video Interface	Media gateway supports configured streaming protocols and source normalization.
Network Integration	HTTPS reverse proxy, private overlay networking and segmented service networks.

Security and operating profile

SECURITY AND COMPLIANCE CAPABILITIES	
System Hardening	Minimal enabled services, controlled administrative access and documented configuration baseline.
Authentication	User accounts, role-based access and two-factor authentication support.
Encryption	HTTPS for browser access and encrypted private overlay networking for approved nodes.
Bounded Licensing	Five-area and 24-user entitlements are associated with the assigned appliance identity. Additional areas require another appliance.
Auditability	Administrative actions, device access and selected operational events retained for review.
Network Isolation	Separate service networks may be assigned for management, applications, CCTV, storage and external access.

OPERATIONS	
Health Monitoring	System and application status, utilization metrics and failure alerts.
Maintenance	Controlled software maintenance and configuration backup before change.
Remote Support	Authorized remote desktop, terminal, file transfer and device inventory functions.
Recovery	Documented data restoration plus manual transfer of the complete labeled drive set to an identical diskless standby appliance.
Appliance Boundary	The standard product profile supports a maximum of five operational areas. Additional areas require an independent ICSA appliance node.

ENVIRONMENTAL AND PHYSICAL	
Installation	Indoor data center or equipment room with controlled temperature, humidity and power quality.
Rack Space	2U in a standard 19-inch rack; enclosure depth is approximately 650 mm before cable allowance.
Operating Environment	10°C to 35°C and 8 to 90 percent relative humidity, non-condensing, according to the hardware platform specification.
Power Input	1,000 W output at 100–127 Vac or 1,200 W output at 200–240 Vac, 50–60 Hz.

System capacity and video retention

Standard design profile for patrol-camera ingest, recording and retention

PATROL-CAMERA CAPACITY	
Patrol Cameras	Standard profile for up to 200 registered patrol cameras and 200 concurrent live streams.
Concurrent Recording	Design profile for recording 200 patrol-camera streams concurrently at an average video bit rate of 1.5 Mbps per camera.
Aggregate Ingress	300 Mbps media payload. Network sizing allows approximately 360 Mbps after applying a 20 percent transport and operational margin.
Recording Throughput	37.5 MB/s media payload. Storage sizing allows approximately 45 MB/s sustained write throughput after applying a 20 percent margin.
Network Profile	Dual 10GbE media interfaces provide capacity for ingest, viewing, playback and operational growth.
Scale-Out	Additional media and storage nodes can expand concurrent ingest, recording throughput and retention capacity.

STORAGE, RETENTION AND CCTV INTEGRATION	
Installed Storage	8 × 20 TB enterprise HDDs, providing 160 TB raw capacity.
Recommended Protection	RAID 6 provides approximately 120 TB nominal usable capacity before file-system and application overhead.
30-Day Retention Basis	200 cameras × 1.5 Mbps requires approximately 97.2 TB for 30 days. A 15 percent storage allowance increases the estimate to approximately 112 TB.
Retention Variables	Actual duration depends on bit rate, frame rate, audio, recording schedule, event policy, RAID layout and reserved free space.
CCTV Integration	Up to 200 registered CCTV channels for authorized discovery, selection and live viewing.
CCTV Recording Model	CCTV video remains on the connected VMS or NVR. ICSA retrieves authorized live or incident-related video when required.

Hardware standby and recovery

Manual drive-set transfer to an identical diskless 2U standby appliance

PRIMARY APPLIANCE	LABELED DRIVE SET	STANDBY APPLIANCE
Identical 2U platform 2 system SSDs in RAID 1 8 data HDDs in RAID 6 Normal operational role	Transfer all SSDs and HDDs Preserve bay number and order Move only after safe power isolation Use controlled ESD handling	Identical diskless 2U platform Matching controller and interfaces Empty drive bays during standby Held ready under site procedure

CONTROLLED RECOVERY PROCEDURE	
1. Confirm failure	Record the primary failure and confirm that hardware recovery is authorized.
2. Isolate equipment	Disconnect AC power and network connections; apply safe handling and ESD controls.
3. Remove all drives	Remove both system SSDs and all data HDDs while retaining each bay label and sequence.
4. Install in standby	Insert every drive into the corresponding bay of the identical standby appliance.
5. Start and import	Connect power and network, start the standby, and confirm the expected storage configuration without initialization.
6. Validate service	Verify storage health, operating system, applications, database, media services and network access before return to operation.