ultraSync

UltraSync Whitepaper

September 2025

Mitch Parker

ARITECH

Executive Summary

UltraSync by Aritech is a secure cloud-based communications platform that enables remote monitoring, management, and integration of Aritech security, access control and CCTV systems.

This whitepaper outlines the architecture, security mechanisms and data flows of UltraSync, providing IT and security teams with the assurance required for deployment in all environments.

1. Introduction

UltraSync provides a secure channel between field devices (Tecom, Reliance, Axon, TruVision) and cloud-based services. It enables event reporting, configuration, and remote control while ensuring data confidentiality, integrity, and availability.

2. System Architecture

- **Field Devices:** Tecom Discovery, Tecom ChallengerPlus, Reliance XR series, Axon and TruVision UltraSync Recorder range.
- **Communication Path:** Encrypted IP tunnel over the public internet.
- **UltraSync Cloud:** Resilient infrastructure hosted in geographically redundant data centers. Australia primary, United States secondary.
- **Management Interfaces:** Mobile applications, integrator software, and web portal.

3. Data Flow

- Devices initiate outbound encrypted connections to UltraSync servers.
- Events and commands traverse the secure tunnel.
- UltraSync routes traffic to authorised applications (monitoring stations, apps, APIs).
- Acknowledgements and responses are returned securely to the device.

4. Security Architecture

- **Encryption:**
    - **Device:** communications use a custom protocol with AES-256 encryption and HMAC-SHA256 authentication.
    - **Web access and mobile app:** communication use TLS1.2 with AES-256 encryption minimum.
- **Authentication:** Mutual authentication between devices and the UltraSync platform.
- **UltraSync Web Portal security**
    - **Authentication:** MFA for portal operator accounts ensures any held data is secure
    - **Segregation:** A portal operator is only able to view devices to which they are assigned.
    - **Hierarchy:** Portal operators are assigned permissions based on their required actions
    - **Operator events:** All operator events are captured and can be reviewed on demand using the portal. For company administrator events, a request must be submitted to Aritech.
- **Session Management:** Unique session keys are generated per connection.
- **Firewall Traversal:** Outbound-only communication minimises attack surface.
- **Integrity:** Message signing prevents tampering and replay attacks.
- **Redundancy:** Load-balanced servers with failover capability ensure continuity.
- **Device security:** In addition to above, any connection from mobile, software or web applications to a device is secured using the following:
    - **SID:** A unique 12-digit identification number assigned to all UltraSync compatible devices.
    - **Passcode:** An 8-digit, user defined, numerical passcode that must match between device and application before session will be established.
    - **User credentials:** To access any device, an authorised username and password/pin code is required. This access is governed by the respective device's programming and must be created, and match exactly the application before a session will be established.

5. Compliance & Standards

UltraSync is designed to align with key industry standards and frameworks, including:

- **Cybersecurity:** Triple-Shield CNPP NFA2P; penetration-tested (not available for viewing for security reasons)
- **Service Platform:** EN 50136 – Compliant alarm transmission provider (Europe)
- **Data Privacy and Governance:** GDPR compliance (Europe), NIS2, IEC 62443, NIST SP 800-53

6. Deployment Considerations

- **Network Requirements:**
  - Intrusion panels and alarm communicators: outbound TCP on port 443 or 10443 (configurable) only.
  - Video recorders: outbound UDP on port 1194 (cloud connection) and outbound HTTPS (TCP port 443) for firmware upgrades.
  - It is required to “whitelist” the URL relevant to the device, as UltraSync employs load balancers that often will change the IP address the device is communicating to when interacting with UltraSync services. See Table 1 at the end of this document.
  - No inbound firewall rules required.
- **Monitoring:** Logging and audit trails available from web portal.
- **Scalability:** Supports small business to enterprise deployments.
- **Resilience:** Automatic retry and reconnection mechanisms.

7. Risk Management

- **Threat Mitigation:**
  - End-to-end encryption ensures confidentiality.
  - Authentication prevents impersonation.
  - Cloud redundancy mitigates single point of failure.
- **Customer Responsibility:**
  - Secure configuration of panels and user accounts.
    - Account per user, no common logins
    - Enable MFA
    - Non-standard passwords used for device connections
    - Regular updates and password management
  - Compliance with corporate cybersecurity policy.

8. Data Storage

- **Personal information:** is only stored for UltraSync operators (a person who has cloud portal access) and is limited to basic information (name and email address).
- **Device information:** device or “site” information is held only so the operator can identify the correct device for desired interactions. Only a “name” is required information.
- **Device data:** UltraSync only stores the event transmissions from the device as requested by the panel programming for the purpose of transmission to a central station, push notification provider or for interrogation by an UltraSync operator. Transmission logs are stored for 30 days; Device event history is stored for 90 days.
- **Video:** No video is stored by UltraSync. All clips or other video media are stored on the device and are accessed at the time of request by web or mobile applications.

9. Conclusion

UltraSync provides a secure, reliable, and standards-aligned platform for modern security and access control communications. With encrypted cloud-based architecture, redundancy, and compliance with industry standards, UltraSync is suitable for enterprise environments requiring high levels of assurance in alarm and access control communications.

Table 1: Device URLs

Device	URL/s Primary	URL/s Secondary
Tecom (Discovery, ChallengerPlus)	z65.ultraconnect.com	z65.zerowire.com
Axon	ax1.ultraconnect.com	ax1.zerowire.com
Reliance XR series	zw1.ultraconnect.com	zw1.zerowire.com
TruVision UltraSync Recorders	tvr-registration.ultraconnect.com tvpn-pra.ultraconnect.com	tvr-registration.zerowire.com tvpn-prb.ultraconnect.com