

CYBERSECURITY



ZIV focuses on **cybersecurity** throughout the **entire life** cycle of its products from design, implementation, testing and manufacturing through to deployment, operation, maintenance and disposal





For all Procedures & Products





Key Features

Role Based Access Control (RBAC)

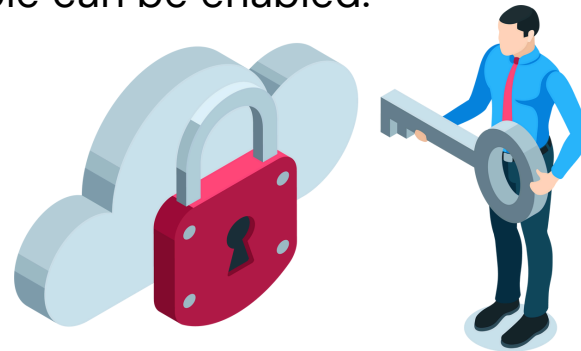
Up to **20 roles** can be configured in the devices, each containing one or more permissions (**up to 8**) to comply with least privilege and segregation of duty policies.



Local and Centralised User Authentication

Users can be authenticated against LDAP or RADIUS centralised repositories, or against local user databases in the device, where up to **20 local users** can be defined applying strong password policies.

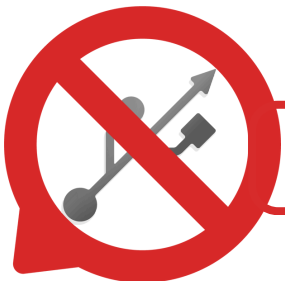
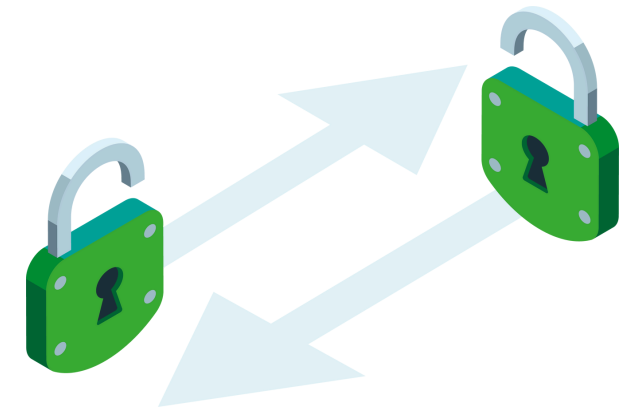
Return to local authentication when centralised repositories are not available can be enabled.



Secure Communications

Secure versions of the protocols are available in the devices (SSH, SFTP, HTTPS, PROCOM over TLSv1.2, LDAPS / StartTLS).

Mutual authentication is available in TLS communications.



Physical Ports and Services can be configured, so that unused ports and services can be disabled.

Credential Management (PKI)

Each device has a unique X.509 identity, signed by ZIV's Certificate Authority. Trusted Certificate Authorities can be configured (CAs). Revocation (based on CRL and/or OCSP) and expiration of remote certificates are checked during TLS communications and firmware upgrade processes.



Firmware Security

The firmware of the devices is digitally encrypted and signed by ZIV based on X.509 certificates using CMS/PKCS#7 DER format, so that only authorised and valid firmware can be uploaded to the devices.



Logging and Auditing

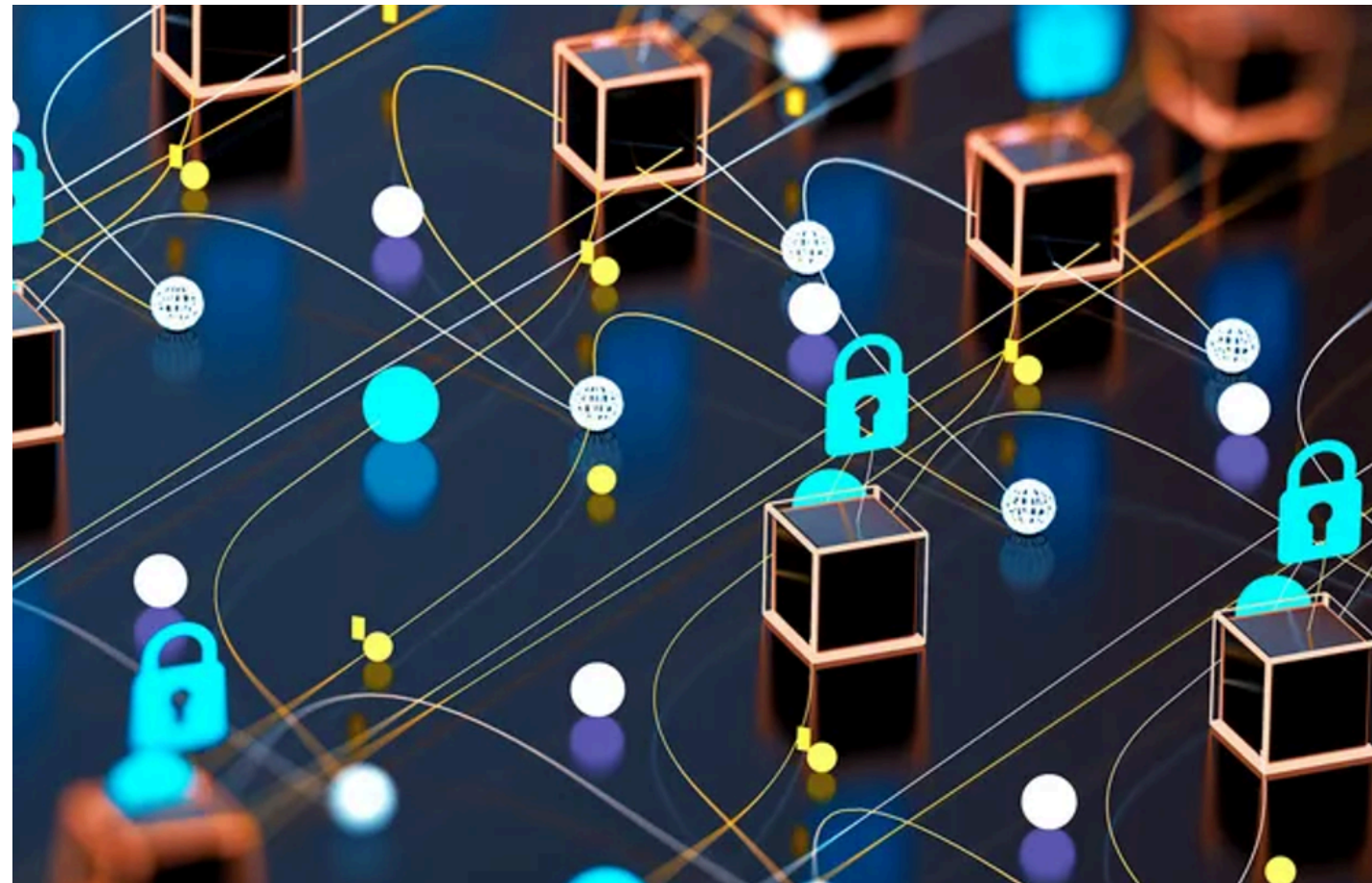
A wide range of cybersecurity events are generated, stored, and sent to centralised servers (up to 3) using Syslog, complying with RFC 5424, using a format largely based on IEC 62351-14.





Standards

ZIV cybersecurity solution has been implemented considering the **leading cybersecurity standards** and guidelines, such as IEC 62443, IEC 62351, IEEE 1686 and NERC CIP



contact us for further information at ziv@zivautomation.com



CYBERSECURITY

Applies to all of the company procedures & products



Contact us now for further information

ziv@zivautomation.com

