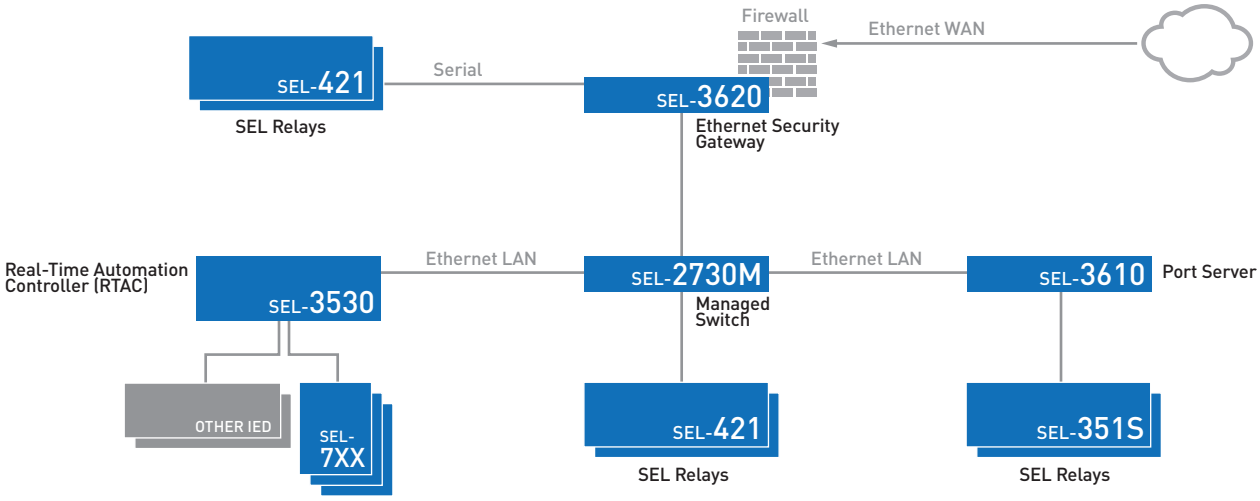
SEL-3620

ETHERNET SECURITY GATEWAY

STRONG ACCESS CONTROL FOR YOUR ELECTRONIC SECURITY PERIMETER



KEY FEATURES

Centralized Access to Relays and Intelligent Electronic Devices (IEDs)

Use the SEL-3620 Ethernet Security Gateway to provide a central point of entry to critical cyber assets with user-based access controls and detailed activity logs. Log onto the SEL-3620, not individual IEDs. Manage user accounts and group memberships centrally using Lightweight Directory Access Protocol (LDAP)-accessible systems, such as Microsoft® Active Directory®. Additional Remote Authentication Dial-In User Service (RADIUS) functionality enables the use of multifactor authentication technology, such as RSA tokens.

Embedded Whitelist Antimalware

Resist known and unknown malware attacks against SEL Security Gateways with exe-GUARD™ embedded antivirus. Powerful rootkit resistance technology, embedded Linux® mandatory access controls, and process whitelisting help mitigate attacks against the gateway itself and eliminate costly patch management and antivirus signature updates.

Substation Firewall and IPsec VPN Endpoint

Secure your substation network from malicious traffic with a powerful deny-by-default firewall. Manage status and configuration with an intuitive, menu-driven interface. Securely connect critical networks to the control center using Internet Protocol Security (IPsec) virtual private networks (VPNs). Use X.509 certificates with Online Certificate Status Protocol (OCSP) to centrally manage trust. The SEL-3620 is interoperable with Lemnos®-compliant devices.

Strong Auditability and User Activity Reports

Log and time-stamp user access and every command entered on critical IEDs. Integrate event records into existing log management systems using Syslog. Protect IEDs with strong passwords, and block shared or default accounts. Granular access controls limit users' access to their assigned roles on individual IEDs.

IED Password Management

Enforce strong passwords on IEDs, and have them automatically changed on a configurable schedule. Satisfy regulatory password requirements, and ensure that no weak or default passwords are in use. Manage passwords on IEDs that use command-line interfaces and on devices that use Modbus® protocol, such as GE UR series relays.

NERC CIP Requirement Support

Implement strong user-based access control to the electronic security perimeter (ESP) while protecting IEDs with strong passwords and blocking shared or default accounts. Granular access control limits a user's access to assigned roles on individual IEDs. Log all user activity, and quickly alert system operators via remote Syslog destinations.

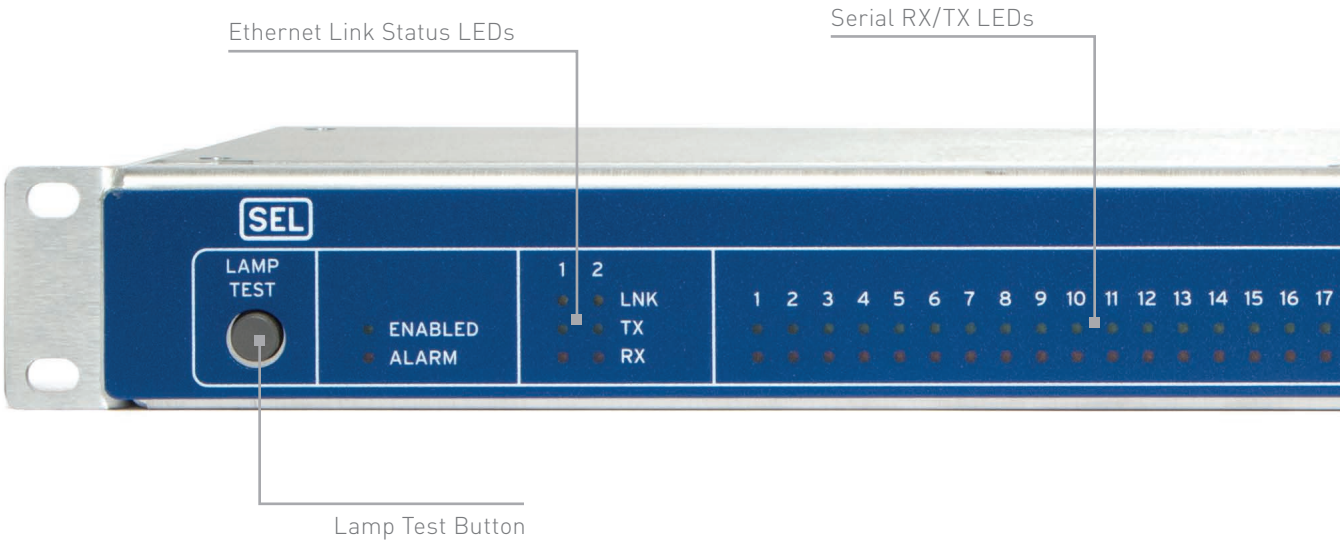
Serial-to-Ethernet Transceiver

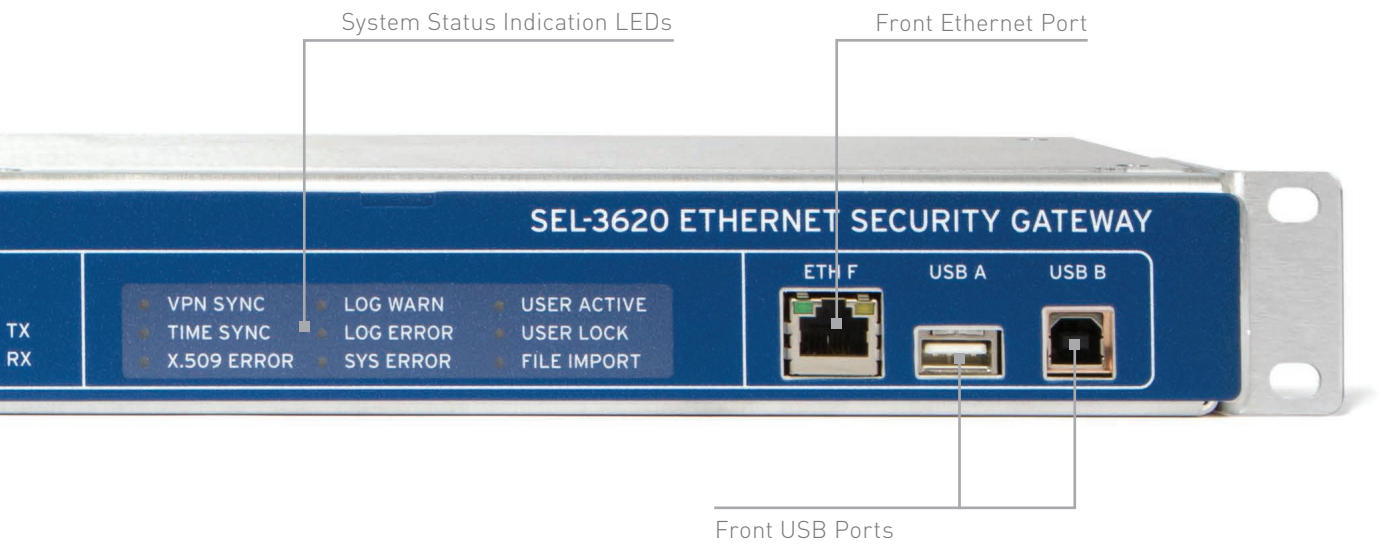
Expand your protocol compatibility by converting serial DNP3 and Modbus to Ethernet DNP3 Transmission Control Protocol (TCP) and Modbus TCP on the fly. Establish an Ethernet connection using Secure Shell (SSH), Telnet, or raw TCP encapsulation to create a persistent tunnel between a logical Ethernet port and a physical serial port.

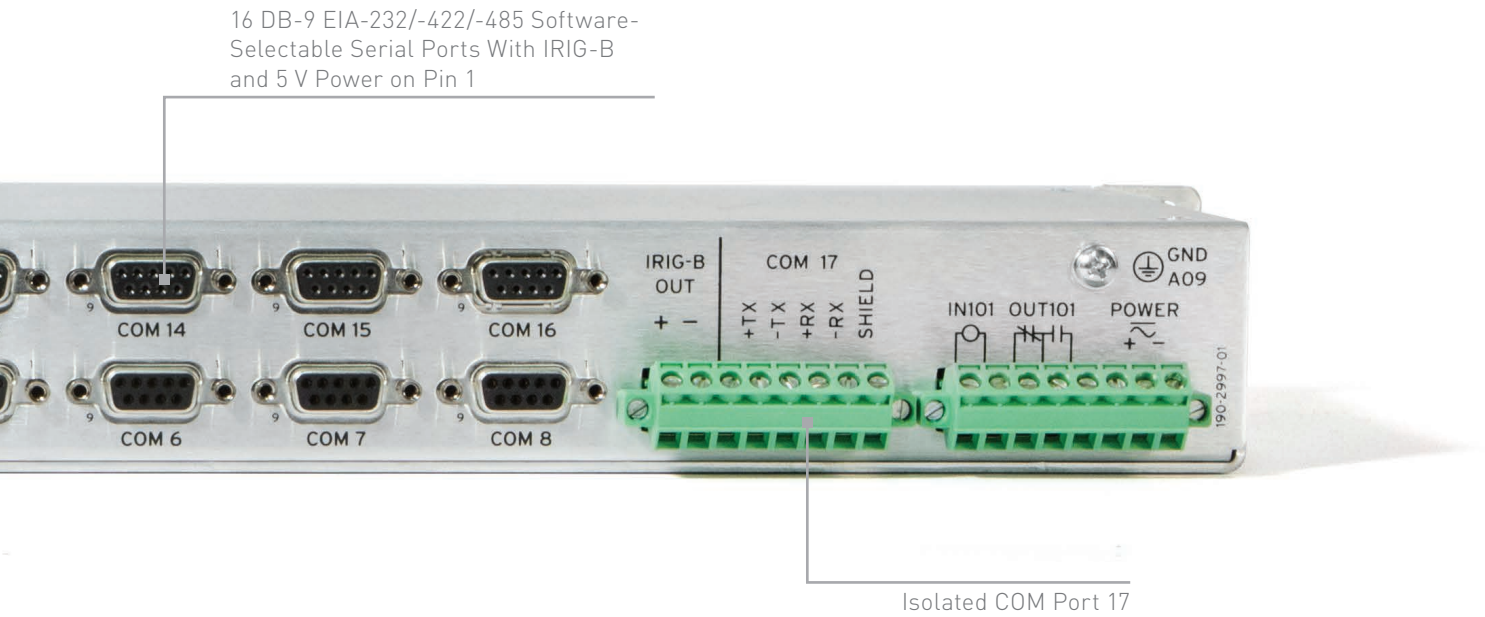
Virtual Software Client Support

Transform unsecure serial or legacy Ethernet communications on Windows® computers to cryptographically secure channels by using SEL-5827 Virtual Connect Client or SEL-5828 Virtual Port Service Software. These applications are provided free by SEL to make remote SEL-3620 ports available for existing software and terminal applications on your PC, including those using Modbus TCP/RTU. Data are secured using SSH with SEL-3620 port groups, master ports, and serial ports.

PRODUCT OVERVIEW




System Status Indication LEDs
Front Ethernet Port
SEL-3620 ETHERNET SECURITY GATEWAY
TX
RX
VPN SYNC
TIME SYNC
X.509 ERROR
LOG WARN
LOG ERROR
SYS ERROR
USER ACTIVE
USER LOCK
FILE IMPORT
ETH F
USB A
USB B
Front USB Ports

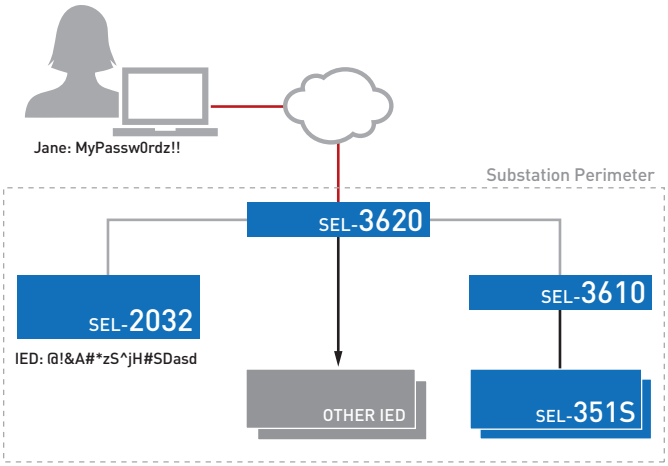

16 DB-9 EIA-232/-422/-485 Software-Selectable Serial Ports With IRIG-B and 5 V Power on Pin 1
COM 14
COM 15
COM 16
COM 6
COM 7
COM 8
IRIG-B OUT
+ –
COM 17
+TX
–TX
+RX
–RX
SHIELD
GND A09
IN101
OUT101
POWER
+ –
Isolated COM Port 17

APPLICATIONS

SENSIBLE, MANAGEABLE, SCALEABLE CYBERSECURITY SOLUTIONS

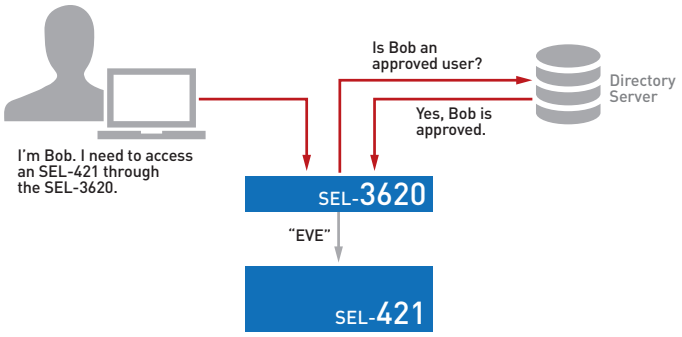
Protected Device Password Management

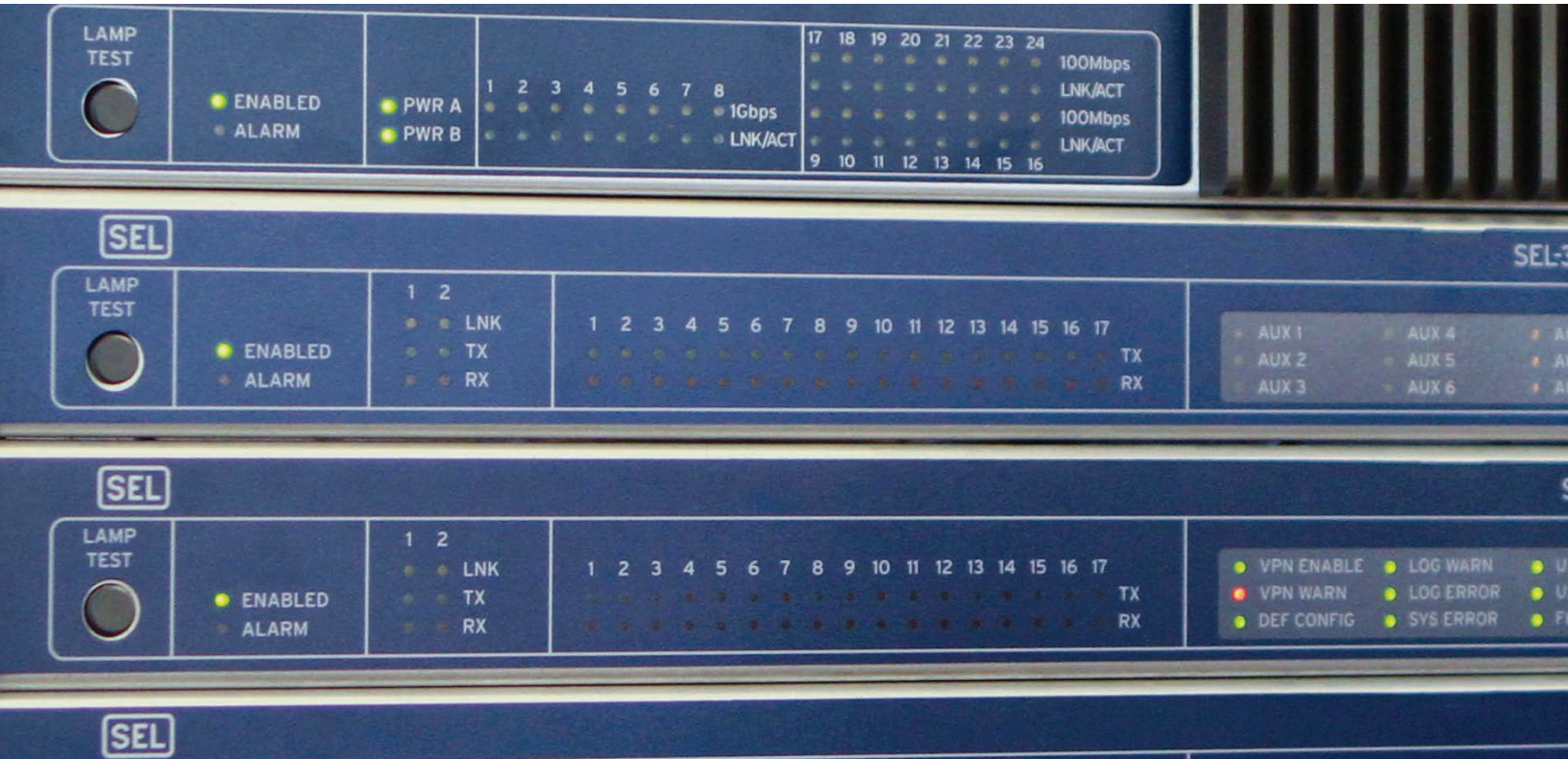
Manage IED passwords quickly and efficiently with the SEL-3620. Enforce strong passwords on IEDs that automatically change on a configurable schedule, and ensure that no default or weak passwords are in use on critical networks. Users only need to know their own password, not the IED's.



User Access Control

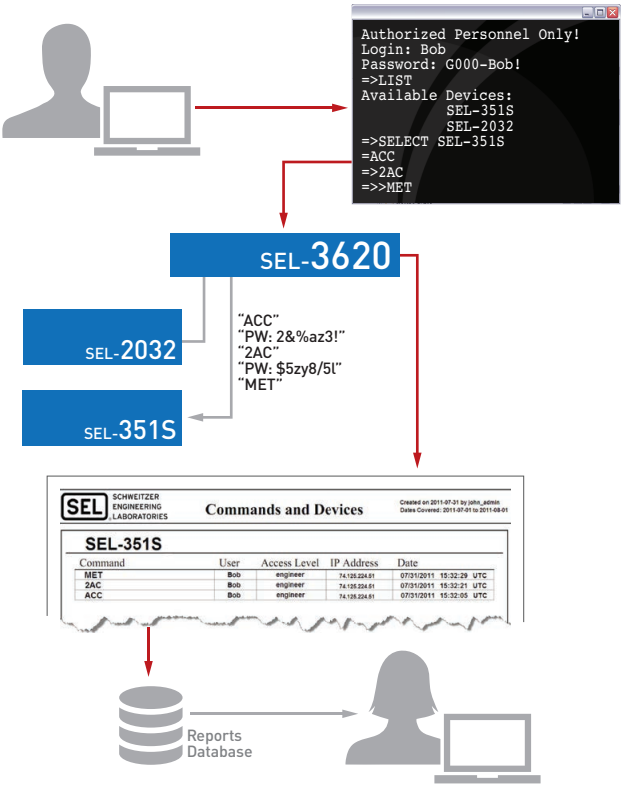
Query Microsoft Active Directory using LDAP or RADIUS. System administrators can easily add and remove user-based account access and authorized access levels to specific devices from a central location.





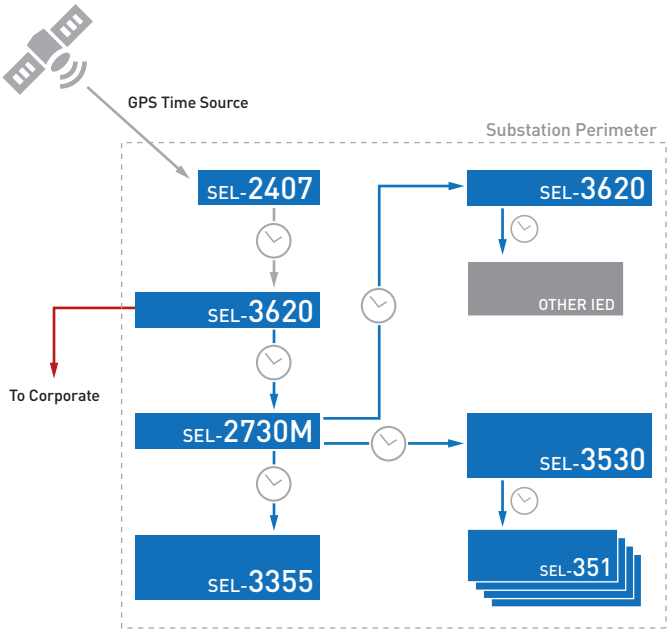
User Activity Reports

Provide granular reports that correlate unique users to individual IED commands. Thoroughly log all user activities on protected devices to know exactly who did what and when. Users with appropriate privileges can download connection reports for detailed user activity audits and to provide maximum user accountability.



Time Synchronization

Provide time synchronization to all your protected substation IEDs, data concentrators, and rugged computing devices. Distribute highly accurate time over both IRIG-B and Ethernet-based Network Time Protocol (NTP). Should a satellite time source be disrupted temporarily, the SEL-3620 will synchronize substation time using its own internal clock.



**MAKING ELECTRIC POWER SAFER,
MORE RELIABLE, AND MORE ECONOMICAL**

SCHWEITZER ENGINEERING
LABORATORIES, INC.

Tel: +1.509.332.1890
Email: info@selinc.com
Web: www.selinc.com

PF00197 · 20140115