VALIANT COMMUNICATIONS

VCL-UNMS

Unified Network Management System

VCL-UNMS (Unified Network Management System):

The VCL-UNMS (Unified Network Management System) is a certificate based "Secured MQTT" protocol that is designed for Utilities and SCADA networks to access and retrieve industrial data securely and instantly from remote locations to be monitored from a central administrative and control centre.

VCL-UNMS offers several benefits including a very high level of security, scalability, and an efficient information distribution of data with a dramatically reduced network bandwidth consumption. The VCL-UNMS enables data to be validated and retrieved securely from several remote locations and updated simultaneously, within seconds, by using a permission-based security protocol.

The VCL-UNMS is a comprehensive "Network Management Software" that can used by network administrators to securely communicate in real-time with the various VCL "Beyond the Firewall" network security elements to enhance and fortify the organizations "distributed infrastructure" through improved surveillance and real-time management and control.

VCL-UNMS Key Features:

- LDAP/Active Directory user authentication
- MAC based device validation
- Simple and fast device on-boarding
- Device connectivity analytics
- Real-time alerts and notifications
- Network administrator defined role-based access control
- Secure sign-on with password strength Monitoring
- Rich, visual appearance with high-definition graphics
- Graphs and charts for network overview and easy problem identification
- On-premise installation for secure deployment.
- Does not require any proprietary hardware. May be installed in any "Server Grade" computer.

VCL-UNMS Highlights include:

- Secure (supports TLS/SSL for encrypting connections between devices)
- Permission-based security
- Uses Software Defined Perimeter (SDP), the username/ password login are replaced with Single-Packet Authorization (SPA) and the receiving device cannot be seen by hackers. This introduces an additional layer of security and is beneficial with or without SSL/TLS.G
- Guaranteed message delivery (no data loss or duplication of data)
- Scalable (from few devices to thousands of connected devices)
- High-throughput and low-latency, low bandwidth usage for transmission
- Server/client 1+1 redundant architecture availability
- Supports architecture to make it possible to use in a 1-to-1; 1-to-Many; Many-to-1; or Many-to-Many Communication / messaging network architecture.
- Ideal for monitoring IT Infrastructure, Sub- Stations, SCADA networks, Oil and Gas pipelines and Distributed Assets installed in remote locations through low-bandwidth radio/satellite links.
- Supports TCP/IP networks.

VCL-2143: Network-Mouse-Trαp™ (Network Decoy Server)

- This device can be programmed by the user to emulate (i.e. to appear to an attacker) as a Server, Router, Switch, SCADA Server, Relay, IEC-61850 Protection Relay, IEC 60870-5-104 Remote Terminal Unit (RTU), MODBUS RTU, Data Storage Device, ATMs and other devices used by financial organizations etc.
- Multiple Network-Mouse-Trαps™ may be installed by the network administrator at various vantage points in their network to attract the "hostile" elements / network infiltrators.
- Assists in identifying and isolating the source of problem / points of customer network vulnerability by providing intrusion or attack trace route and forensic analysis in real-time.
- Compatible with VCL-UNMS (Unified Network Management System). The Network-Mouse-Trαp™ alert the network administrator of a network intrusion / cyber-attack in real-time. Alerts of a network intrusion or cyber-attack in real-time with an audio and visual alarm.

VCL-5001: Network Traffic Sniffer:

- This device detects network intrusions that could lead to Data Theft, Ransomware Attack, Denial of Service (DoS) or a Cyber-Attack aimed to bring-down the target network.
- Flags unusual traffic flows for both inbound and out bound traffic by providing an advance warning mechanism of the data traffic anomalies.
- The VCL-5001: Network Traffic Sniffer alerts the network administrator of a network intrusion / cyber-attack in real-time.
- Compatible with VCL-UNMS (Unified Network Management System) for remote monitoring over a secured network link.
- Alerts of a network intrusion or cyber-attack in real-time with an audio and visual alarm.

VCL "Beyond the Firewall" *Cyber-Smart Rack* Elements include:

VCL-2754: Cyber-Smart Rack Monitoring and Control Unit:

- Monitors DC voltage (range 15V DC to 60V DC).
- Includes "6" binary inputs for monitoring up to 6 dry contact relay open loop / closed loop inputs. These inputs can be also connected to equipment alarms; rack-door open alarm; smoke-alarm, AC power failure alarm; DC power failure alarm, water-level alarm etc.
- Three zone temperature sensors. Monitors the Rack Temperature in 3 separate temperature zones in a rack and alerts network administrator the user defined temperature threshold is exceeded in any zone.
- Fan Performance Monitoring and Fan Failure Alerts. User configurable fan speed (RPM) threshold and Daily Automatic Fan Test and Priming Routine. Alerts if any of the rack fans fail; or if it is not operating at its specified RPM and requires service / replacement.
- Saves Power. Controls the operation of up to 3 rack-ventilation fans (or their multiples) by switching ON / switching OFF, based on user programmed environment parameters. Extends fan MTBF life. Extends equipment MTBF life by alerting against over-heating due to failure of ventilation fans.
- NTP/SNTP synchronization. Ensures that all alarms and events being reported / logged are accurately time-stamped.
- Real-time Alarm and Event Logging.
- 10/100BaseT Ethernet Port for Remote Monitoring.
- Compatible with VCL-UNMS (Unified Network Management System). Allows the network administrator to monitor '000s of racks securely from a central management server.
- Compact size, DIN rail mount. May be mounted on Standard DIN Rail. Does not occupy precious rack space.

VCL-2754: Cyber-Smart Rack Monitoring and Control Unit:

- LCD Display. May be installed outside on the door panel of each rack. Locally displays all parameters and alarms of each rack for viewing without opening the rack-door.

VCL-2778: SafeComm-E: 1+1 Ethernet Failover Protection / AB Fallback Switch:

- This device provides 1+1 Automatic Ethernet Failover / AB Fallback Protection between an "active" and "standby" terminal equipment; or between "main" and "standby" networks / firewalls and routers.
- Fail-Safe. The equipment never becomes a point of failure, even in a power down condition.
- Provides equipment (e.g. Server, Router, Switch) or network redundancy (i.e. Network uplink) for applications which require 99.99% up-time.
- Compatible with VCL-UNMS (Unified Network Management System) for remote monitoring over a secured network link.

VCL-2702: Network Kill Switch:

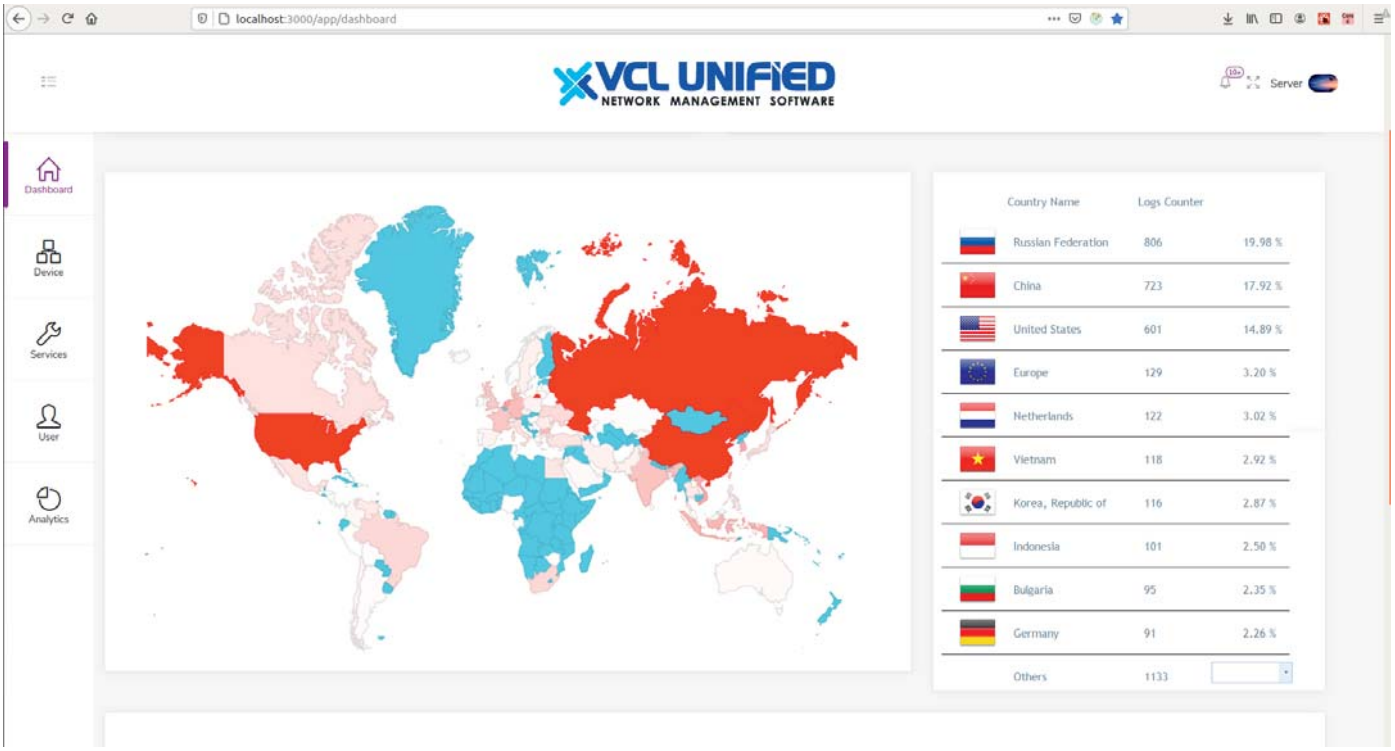
- The Network Kill Switch becomes the last line of defence after the Firewall breach, to "repel" and "block" a cyber-attack - while it is progress.
- The Network Kill Switch is designed to connect to and monitor the various "Beyond the Firewall" security elements and send "alerts" of a network intrusion or cyber-attack to the network administrator in real-time.
- It also generates audio and visual alarms to "alert" the maintenance staff for local administrative action.
- This device provides manual and automatic isolation from network, to initiate defensive counter-measures in an event of a cyber-attack.
- Can be used with VCL-5001 Network Traffic Sniffer; VCL-2143, Network-Mouse-Trap™ (Decoy Network Servers) to isolate the network in the event of the detection of a network intrusion / breach of the cyber-security perimeter / hostile intrusion in the demilitarized security zone.
- The Network Kill Switch may be connected to though a wide variety of communication interfaces that include "Secured Ethernet", RS232, RS485 and Dry Contact Relay Inputs to monitor the various "Beyond the Firewall" security elements if any "hostile intrusions" are being reported.
- Compatible with VCL-UNMS (Unified Network Management System) for remote monitoring over a secured network link.

VCL-5000: 1+1 Redundant Firewalls:

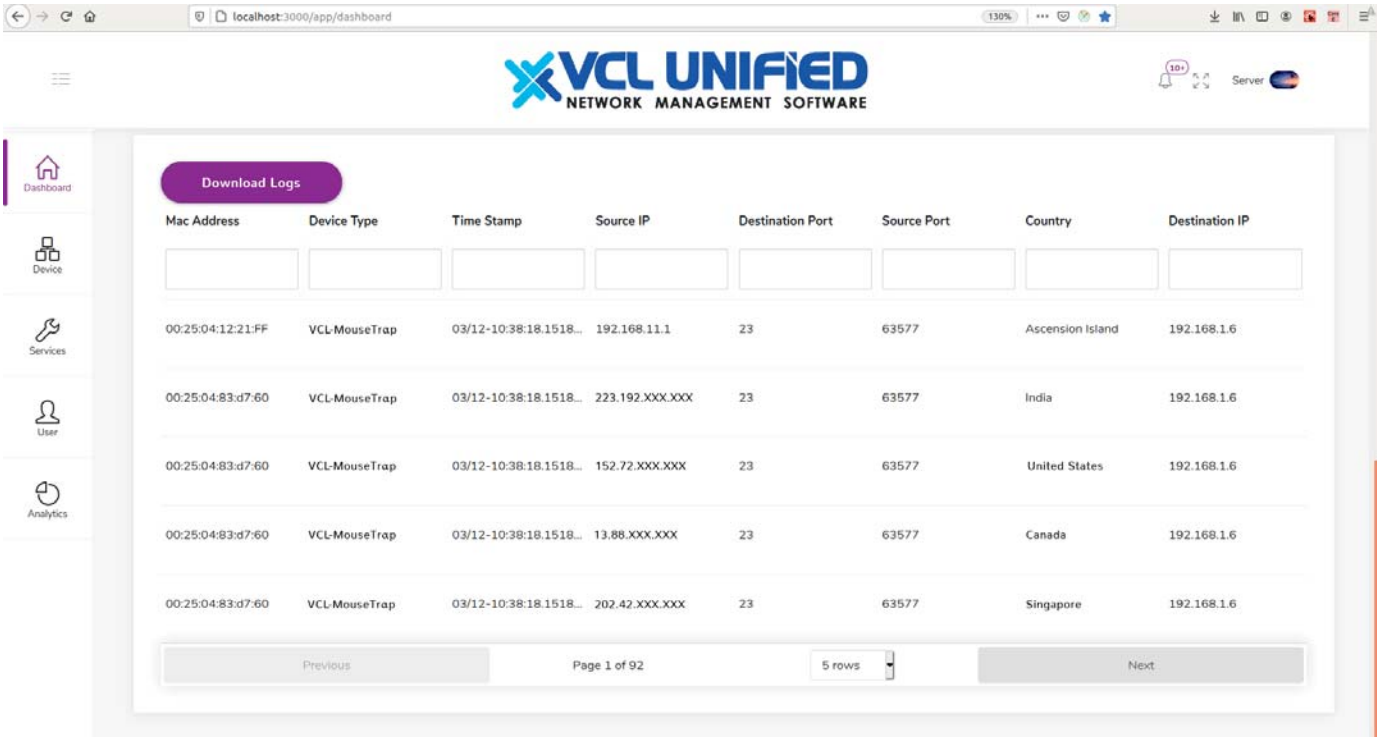
- 1+1 redundant configuration firewalls, with automatic fail-over switching. Industrial and ruggedized VCL-Firewall can be used in 1+1 redundant configuration to thwart and protect customers from cyber-attacks with a seamless option to switch to a back-up Firewall in case of breach of primary Firewall.

VCL-UNMS (Unified Network Management System)

Real-Time Global Cyber-Attack View



Real-Time Forensic Analysis and Trace Route



Technical specifications are subject to changes without notice.
All brand name and trademarks are the property of their respective owners.
Revision – 1.2, July 15, 2020

U.K.
Valiant Communications (UK) Ltd
Central House Rear Office,
124 High Street, Hampton Hill,
Middlesex TW12 1NS, United Kingdom
E-mail: gb@valiantcom.com

U.S.A.
Valcomm Technologies Inc.
4000 Ponce de Leon Blvd.,
Suite 470, Coral Gables,
FL 33146, U.S.A.
E-mail: us@valiantcom.com

INDIA
Valiant Communications Limited
71/1, Shivaji Marg,
New Delhi - 110015,
India
E-mail: mail@valiantcom.com