GE

Energy Connections

Lentronics Cyber Secured Service Unit

Improved Cyber Security for Lentronics SONET/SDH Multiplexers

GE's Lentronics™ Cyber Secured Service Unit (CSSU) protects Lentronics Multiplexers against cyber threats, specifically those that target the reliability of the Bulk Electric System (BES). The CSSU is an essential security appliance that takes the place of a legacy Service or IP Service Unit, to better protect against malicious and unintentional network changes. It utilizes defense-in-depth strategies, allowing utilities to meet demanding security standards such as NERC® CIP.

Acting as a secure gateway between Lentronics Multiplexers and the Lentronics VistaNET NMS software, CSSUs employ strong AES 256 bit encryption, SSL/TLS and X.509 digital certificates to ensure privacy and authenticity of users attempting to access the network. Controlling access to all management ports is critically important to protect BES cyber systems that rely on Lentronics critical communication solutions. Each CSSU enforces a single security policy that is distributed across the entire network domain, ensuring accuracy and real-time operation of actions (i.e. user revocation). The CSSU also maintains accountability by securely logging events.

Key Benefits

- Single hardware platform supporting two operating modes
  - Legacy mode: Interoperable with existing Service Unit
  - Secure mode: Network-wide AAA supported for improved access control and confidentiality
- Eliminates 2kHz tie cables between rings
- Extends network domains beyond 100 nodes
- Supports Dual-Homed NMS paths
- Drop-in replacement without SONET/SDH payload traffic disruptions

Security Features

- Secures access-control with policy replication and distribution between all networked CSSUs to ensure implementation of a single, consistent security policy
- Prevents unauthorized user actions with hardware-based authorization
- Supports RADIUS for centralized authentication as well as local authentication when the central service is unavailable or if RADIUS is not implemented
- Provides event logging and secure event storage
- Provides confidentiality for NMS traffic with strong AES encryption
- Achieved Wurldtech Achilles Level I Certification, indicating that the CSSU meets industry security standards
- 2-factor Authentication capable (future firmware upgrade)

imagination at work

Security

- Supports OpenSSL
- Supports Transport Layer Security (TLS)
- Strong AES 256 encryption
- X.509 Digital Certificates
- Digitally signed communications to EMS clients (Lentronics VistaNET)
- Digitally signed firmware to authenticate trusted source operating code

Access Control

- Integrates with central authentication server (RADIUS) for centralized user administration
- Supports dual RADIUS servers and gateways
- Authenticates users locally if RADIUS is absent
- Integrated Access Control List (ACL) for local authentication and authorization
- Distributes ACL between sites over SONET/SDH overhead
- Enforces user authentication
- Optional unit password to control craft console port access

Connectivity

- Encrypted front and rear Ethernet ports
- Supports concurrent network management sessions
- Secured console port
- Inter-Ring Tie port to bridge NMS domains

Utility Hardened

- Meets IEEE® 1613 and IEC® 61850-3 environmental specifications
- Reliable operation in extreme temperature from -4°F to +140°F (-20°C to +60°C)
- Meets Earthquake risk Zone 4 shock and vibration specification

Securing the Critical Energy Infrastructure

Central to protecting the Bulk Electric System (BES), a secure and dependable communications solution is required to be Cyber Secure. In many parts of the world, regulatory requirements govern the classification of cyber assets and systems, and define procedures to safe-guard against attacks on critical infrastructure within electrical transmission and distribution networks, oil and gas pipelines and transportation corridors.

Lentronics SONET/SDH Multiplexers are traditionally employed within such harsh industrial environments to monitor, protect and facilitate control of critical assets. Their contribution within the BES and through association with BES cyber systems of medium impact, securing Lentronics Multiplexers is becoming increasingly important.

Protecting the underlying communications infrastructure from malicious security threats and unintentional configuration errors is imperative. Securing Lentronics Multiplexers to the latest security standards is now possible through a new security appliance, the Cyber Secured Service Unit (CSSU).

A Cyber-Secured Appliance for Critical Communication Networks

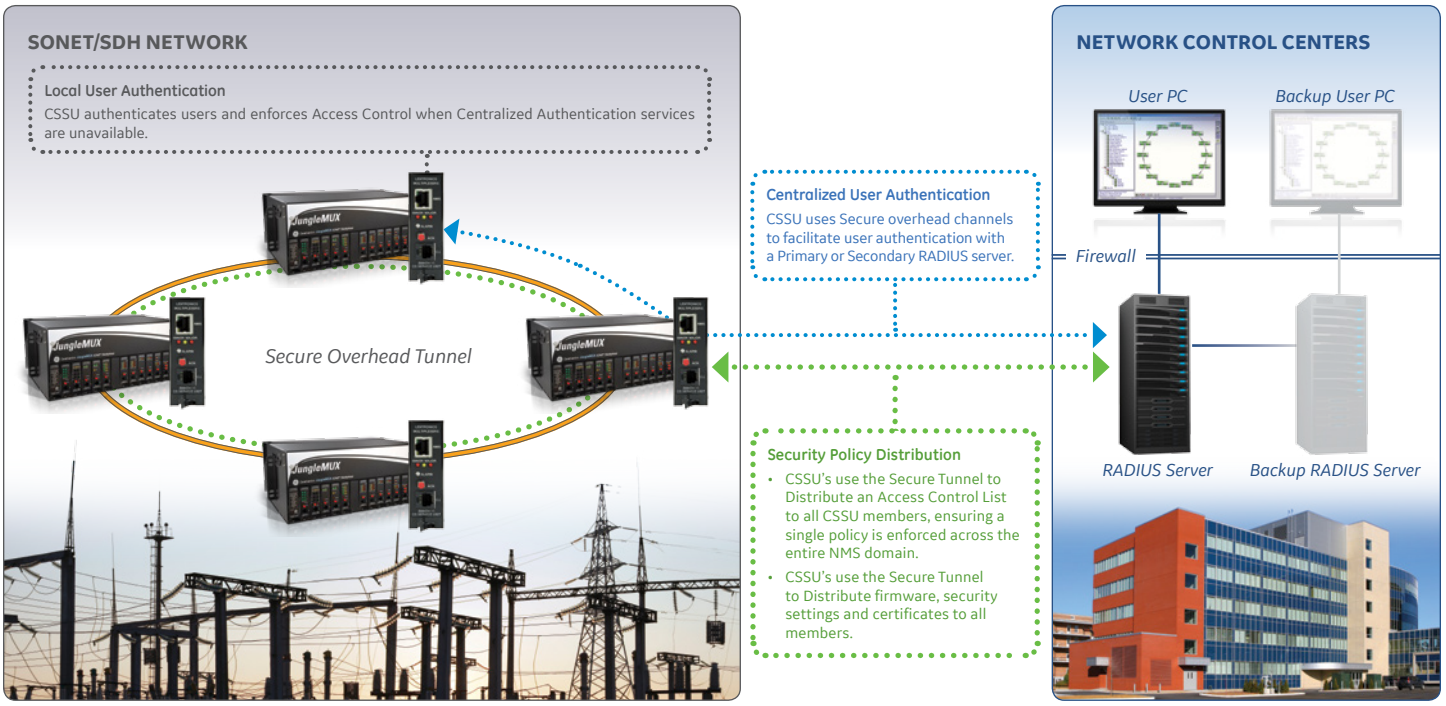
The Cyber Secured Service Unit protects Lentronics Multiplexers from unauthorized user access and remote equipment configuration. In addition, non-authenticated software clients will be actively rejected along with failed user authentication attempts. The use of strong privacy policies help prevent man-in-the-middle attacks.

Each CSSU communicates with adjacent CSSUs over the SONET/SDH overhead to facilitate:

- Centralized user authentication
- Distribution of a common, network-wide security policy
- Distribution of common security settings, including digital certificates
- Upgrade of the units operating firmware to apply any future patches
- Distribution of the current time

This extends the electronic security perimeter around each NMS access point, securing all sites, particularly remote locations containing critical assets belonging to critical BES Cyber Systems.

Cyber Secured Service Units Perform Centralized and Localized User Authentication



Isolating Management From Data Further Protects Critical Cyber Systems

GE's Lentronics Multiplexers isolate client services into unique time-divisioned 'pipes' for secure transport across the network. These 'pipes' can be thought of as lanes on a freeway, with permanent barriers in place to contain traffic. When traffic stays within its designated lane and flows at a constant rate, congestion is avoided. Consider the impact if traffic within a lane was able to influence traffic in other lanes, for instance eliminating adjacent lanes altogether and any critical emergency traffic carried within it. Lentronics Multiplexers completely decouple the management (control) from the data (traffic), ensuring malicious code potentially carried within the traffic cannot gain control over the network. The Multiplexers prevent traffic data from gaining access to network management functions, while the CSSU acts as a guardian to permit only authentic and authorized management actions.

Legacy or Secured Operational Modes

A Cyber Secured Service Unit can be deployed in one of two operational modes, Legacy or Secure.

Legacy mode (CSSU-L) offers a consistent set of features that supports interoperability with existing Service or IP Service Units.

Secure mode (CSSU-S) is a licensed component that must be applied to all CSSUs within a ring, or across the entire management domain. In this case, a network-wide security perimeter is formed to protect and control assets through Authentication, Authorization, Accountability, Privacy and Integrity.

Centralized Authentication

Within secured mode, utilities may choose to authenticate users against an enterprise-level authentication server. Typically, one or two centrally located authentication servers (supporting RADIUS) are permanently connected to primary (and secondary) CSSU-S gateways. Users attempting to configure the Lentronics Multiplexer network will be prompted by the CSSU-S for their user credentials. The request/response is then exchanged between the originating CSSU-S, the CSSU-Gateway and the RADIUS server. An operational 'accept' or 'deny' response is provided by RADIUS and enforced locally at each CSSU-S.

Digitally Signed for Trusted Authentication

Each CSSU-S utilize a crypto variable to ensure NMS communications are private and authentic. The resulting X509 digital certificates used to sign all packets are traceable to a trusted source. The CSSU is designed to interface directly with a key management solution, enabling centralized control of the certificates and in particular, alignment with a different trusted source to create a unique web-of-trust.

Access Control Lists

Each CSSU-S enforces a security policy defined within the units' Access Control List (ACL). Through a secure overhead channel, this list is replicated across a network of CSSUs. Alterations to the policy (privileges, denials, revocation) are immediately updated across the network, ensuring consistency to this policy from one site to another.

Each secured CSSU is shipped in legacy mode, preventing unauthorized setup of the unit's security policies. Activating the unit for security requires a unique activation code. A WebUI employing HTTPS ensures administrative setup is secure.

Authorization

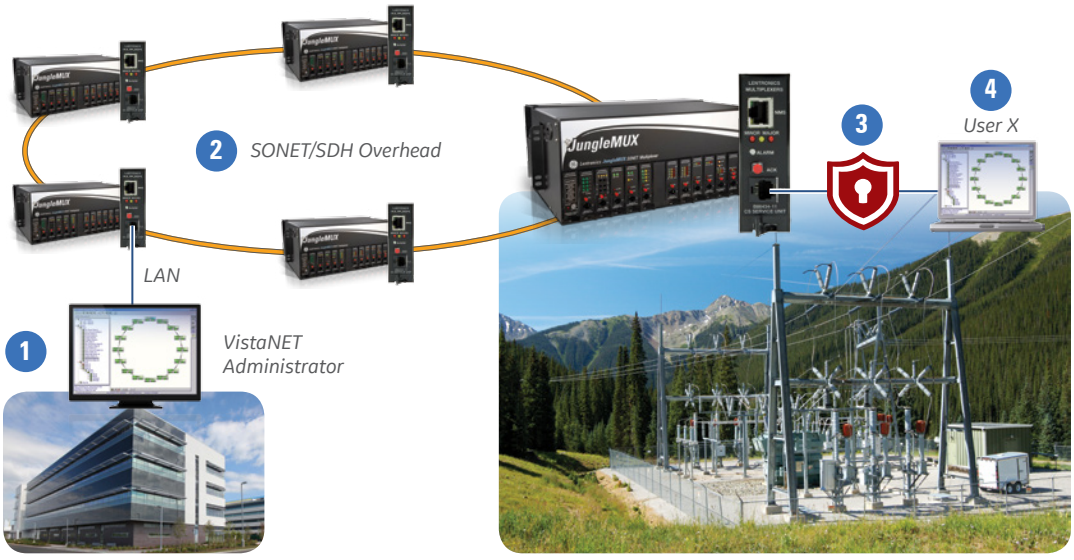
Each CSSU-S receives an Access Control List through the SONET/SDH overhead channel assigned for security maintenance functions. This list contains users, user expiry and authorization levels (groups of privileges). The local CSSU-S that received an authentication acknowledgement will then enforce user actions based on the contents of this list. Users can have read & write functions for some rings or nodes while being limited to read-only functions for the others.

Administrative access is required to manage the contents of the ACL. Role-based access control is then enforced by each CSSU.

Accountability

Security event logging is performed within the CSSU, to ensure essential details associated with a user-transaction (i.e. login) is captured and safely stored. Additionally through strict user authentication, the CSSU-S ensures non-repudiation by associating actions to an individual user.

Updating the CSSUs Access Control List: Example of Revoking Users Access



1 VistaNET Administrator Creates a New Policy

- User X: Access Rights Expired
- Applies new security policy to connected CSSU

2 SONET/SDH Overhead

- CSSU synchronizes the new security policy to all connected CSSUs

3 Enforcing Security

- Each CSSU enforces the new security policy

4 Access Control Enforced

- Access is denied for User X
- Any damage caused by User X is contained to the local site where physical access was breached

Technical Specifications

PHYSICAL

Height	3.4 in. (89 mm)
Width	1.14 in. (29 mm)
Depth	8 in. (203 mm)
Weight	6 oz. (185 g)

CONNECTORS

UNIT

- RJ45, 10/100Mb/s Ethernet (NMS)
- RJ-11, 9.6kb RS232 (NMS, Console)

PADDLEBOARD

- RJ-45 for 10/100 Ethernet (NMS)
- Major & Minor Form-C Relays
- NMS-Tie (x2), Orderwire (CBUS)
- Contact In (x4)
- Power Monitor

RELIABILITY

MTBF	310,000 Hours (35 years)

ELECTRICAL

Power Consumption	3 W

MECHANICAL

Vibration	MIL-STD 810E
Bench Handling	TS 1-00446.06

SAFETY

IEC 60950-1

ENVIRONMENTAL ELECTRIC POWER

Meets IEEE 1613 and IEC 61850-3

EMI/RFI	IEEE C37.90.2 EN 61000-(6-2, 6-4) EN 55022 ETSI 300 386 V1.6.1
Isolation/SWC	IEEE C37.90.1
Temperature (Operating)	-4° to +140°F (-20° to +60°C)
Temperature (Storage)	-40° to +158°F (-40° to +70°C)
Relative Humidity	5-95% non-condensing
Earthquake	Zone 4

CPU

- 800MHz
- 256MB RAM
- 256MB FLASH

EXTERNAL MEMORY

SD Card 1 GB, 4 GB (default), 8 GB

LICENSED MODES

- Legacy-mode (CSSU-L)
- Secured-mode (CSSU-S)

ENCRYPTION

AES 256*

AUTHENTICATION

SHA-1 (OpenSSL)*

NETWORK PROTOCOLS

TCP, UDP, DHCP, NTP, HTTPS

SECURITY STANDARD

Designed for FIPS 140-2 L1
Wurldtech Achilles Level 1

** Equipped with CSSU-S code*

Order Code

Part Number	Description
B86434-11	Cyber Secured Service Unit, Legacy Mode for JungleMUX, TN1U and TN1Ue Multiplexers Ethernet 10/100BaseT via RJ-45 front connector, providing a gateway for Network Management Serial 9.6kb RS232 via RJ-11 front connector, supporting network management or local unit setup only
B86434-11/A	Activated Cyber Secured Service Unit, to operate in Secured Mode for JungleMUX, TN1U and TN1Ue Multiplexers Ethernet 10/100BaseT via RJ-45 front connector, providing a secure gateway for Network Management Serial 9.6kb RS232 via RJ-11 front connector, local unit setup
86434/A	Activation code to upgrade from CSSU-Legacy to CSSU-Secure operating mode
86434-75	TN1Ue CSSU paddleboard equipped with rear Ethernet 10/100BaseT, Major/Minor Form C relay, Power alarm input, Protected NMS Tie ports (new tie format) and Contact IN terminals
86434-81	TN1U CSSU paddleboard equipped with rear Ethernet 10/100BaseT, Major/Minor Form C relay, Power alarm input, Protected NMS Tie ports (new tie format) and Contact IN terminals
86434-92	JungleMUX CSSU paddleboard equipped with rear Ethernet 10/100BaseT, Major/Minor Form C relay, Power alarm input, Protected NMS Tie ports (new tie format) and Contact IN terminals

GE Energy Connections

Automation & Controls
2500 Austin Dr
Charlottesville, VA 22911
1-555-242-9600

GEAutomation.com

GEA-12794B(E)
English
171031

imagination at work