DYMEC

American Industrial

DYMEC Application Notes

Cyber-Security using Service Control & IEEE802.1X



NSA Endpoint

IEE802.1X



Cyber Security Best Practices





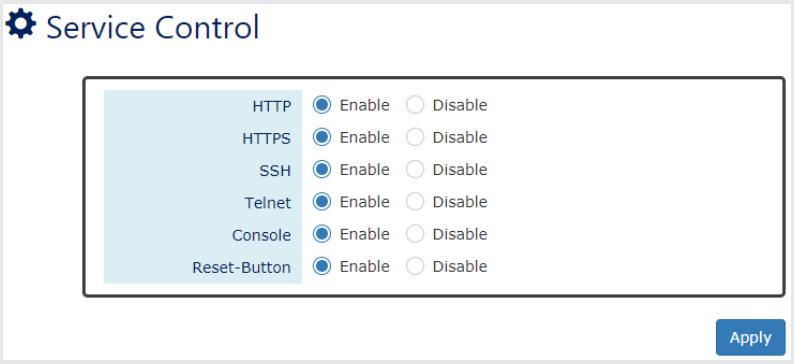
DYMEC
Kansas City, Missouri, USA
Web: DYMEC.com
Email: Sales@DYMEC.com

» DYMEC's Service Control Solution

DYMEC offers a comprehensive solution for secure networking for Smart Cities, Connected Industry, Smart Transportation, Smart Energy (generation, transmission and distribution - allowing fast, secure and economical deployment of thousands of new remote IIoT sites with always-on reliability and mission-critical protection.

» Key Benefits

» Easy Configuration
» Control over All Services
» Secure Console Port
» Secure Reset
» Secure Chassis



HTTP

Enable or Disable to access the management interface by **HTTP** - which is the foundation for data communications for the **World Wide Web (WWW)**

HTTPS

Enable or Disable to access the the management interface by **HTTPS**, which is an adaptation of HTTP for security. The communication will be **Encrypted in HTTPS**

SSH

Enable or Disable to access the management interface by **SSH**: a **cryptographic network** protocol. SSH provides a **secure channel** over an unsecured network in the client-server architecture. The switch plays the role of SSH server and hosts plays the role of SSH client.

TELNET

Enable or Disable to access the management interface by **TELNET**: which is a text oriented, virtual terminal connection. Less secure than SSH: it does not encrypt data or passwords.

RESET BUTTON

Enable or Disable to react when users press the **Reset Button.** The Reset Button provides different functions, including **REBOOT** and RESET FACTORY Default. Disabling the Reset Button - provides protection from **System Reboot** or **Restoring the system to a Default State**

NSA Secure Endpoint Console Port & Chassis

NSA Network Endpoint Guideline Certified for Console Port Shutdown & Chassis Full Security (Patent Pending) - Used for High Network Security / IIOT Deployments. This is a Security Feature for Turning OFF or Disabling the Console Port of the Device.

* Fully Secures the Console Port of Remote, Unsecured or Un-Attended Device.
* Prevents Un-Authorized Configuration or Device Penetration via the Console Port
* Secures the Device Chassis and Renders it Secure from Tampering or Virus Placement

NSA Secure Endpoint Console Port & Chassis



Ruggedized ITS & SCADA-Gateway Managed Switches & Routers



Security Switch & Router

Layer3 , Router and Firewall



PoE, Layer 3 Routers & Switches

High Security IIOT Networking

» For more information visit: DYMEC.com

DYMEC and 3170 are registered trademarks of K-USA. ©2019 DYMEC. All rights reserved.

Cyber-Security for ITS Cabinets

Cyber-Security for ITS networks is a complicated and never ending task. The network professional must embrace the task of security as a continual procss instead of one and done. Excellence in the field of cyber-security is a daily review and analysis of security features and habits. From the traffic cabinet to the Traffic Management Center (TMC) - all touch-points represent unique hazards to the IT Security Professional. **DYMEC Industrial Ethernet Switches** contain innovative and modern security features not found in other manufacturers products.

- **DYMEC Security Feature - Secure Console**, only DYMEC switches&routers have the ability to turn off the console port preventing unauthorized entry or tampering with the device.
- **DYMEC Security Feature - Secure Reset Button**, only DYMEC switches & routers have the ability to turn off the reset button preventing unauthorized entry or resetting of the device.
- **DYMEC Security Feature - Secure Chassis**, only DYMEC switches & routers have the ability to turn off the console port, reset button, and Management Services preventing unauthorized use or tampering of the entire Industrial Ethernet chassis. This network practice is recommended by the **NSA** as a standard security procedure for non-secure or isolated network elements.

The DYMEC ITS Cabinet Solutions



In addition to a full range of Industrial Ethernet Din-Rail and 19" Cabinet Switches. DYMEC offers the 3170 line of ITS Input File Switches.

1. **KY-3170EM4** - 10 Port, Managed, Layer 2, Gigabit Industrial Ethernet Switch (Temperature Hardened, ERPsv2 Redundant Fiber Rings, NSA Certified Endpoint)
2. **KY-3170EM4 - P** -10 Port, Managed, Layer 2, PoE++ (IEEE802.3bt), Gigabit Industrial Ethernet Switch (Temperature Hardened, ERPsv2 Redundant Fiber Rings, NSA Certified Endpoint)
3. **KY-3170XM** - 10 Port, Managed, Layer 2, Ten Gigabit Industrial Ethernet Switch (Temperature Hardened, ERPsv2 Redundant Fiber Rings, NSA Certified Endpoint)
4. **KY-3170XR**- 10 Port, Managed, Layer 3, Ten Gigabit, Industrial Ethernet Router & Switch (Temperature Hardened, ERPsv2 Redundant Fiber Rings, NSA Certified Endpoint) with IPv4 / IPv6, RIP, OSFP, and GRE (Generic Routing Encapsulation)
   ****Easy Installation, Saves space, Fiber & Copper Port Diagnostics****

DYMEC IEEE 802.1x Network Access Industrial Ethernet Solution & Enhancement

802.1X is an IEEE standard defined Port-based Network Access Control. It provides a more secured authentication mechanism for the devices, which would like to connect to a LAN or a WAN. The Port-based Network Access Control protocol is a convenient method for the users because the authentication is per-port and once the port passes the authentication, it is not required to authenticate again when changing to another device, i.e., without security. Therefore, MAC-based access control is provided. It is a more secure, but less convenient method for authentication. Only the device with the MAC Address that has passed the authentication can be added to the networks. These two methods are optional on each port and the users can select one of them on different ports.

DYMEC IEEE802.1x Authentication Standard ENHANCEMENT: In the Transportation Industry, network infrastructure (ITS Equipment) is often located in publicly-accessible and unmonitored areas such as on the side of a road or adjacent to the sidewalk. A person with the right equipment (Think Traffic Cabinet #2 Key - you can purchase on the net - Used everywhere from Maine to California) might be able to open the traffic enclosure and attempt to connect through the local switch if they knew where to look. The IEEE802.1x MAC Authentication is an important security feature to enable for that reason, as it can help prevent unauthorized connections through local switch ports. However, 802.1x sometimes loses association with learned MAC addresses after power cycles or link disconnects. For this reason, it's extremely valuable to have the ability to statically assign MAC address to switch ports that remain associated with that port after connections are broken. Since equipment at these locations often sits untouched for sometimes years at a time, the need for re-learning or re-authenticating isn't really applicable, and it's important to keep someone from being able to connect by power cycling the switch or breaking existing connections.
DYMEC SOLUTION: The DYMEC Switch & Router software now has the ability to disable port MAC learning and utilize an entered static MAC address only. **Industrially safe and Cyber-Secure.**

What this is in DYMEC Security Terms: Most vendors software IEEE802.1X Secure Network Access configurations can by by-passed using a simple trick..... **RESET the Device**. DYMEC has modified its software into a fixed static configuration for permanent deployment and operation. We protect Secure Network Access Control (NAC) in 2 ways

1. Static configuration and Protection of IEEE802.1X. A reset device keeps its IEEE802.1 X configuration.
2. Through our "SERVICE CONTROL" mechanism we completely disable the RESET button.





The Age of Digital Transformation

The industrial internet of things (IIoT) is set to enable digital transformation across all industrial and critical infrastructure sectors. By 2020, IIoT is expected to be a $225 billion market, encompassing millions of highly distributed intelligent devices:

Question - Will your IIOT devices and their network be secure?

Power Utilities

- Smart Grid
- Re-closers
- Load breakers
- RTUs/SCADA
- Secondary substations
- Meters concentrators

Gas Utilities

- Flow meters
- Volume/pressure/level sensors

Water Utilities

- Flow control
- Quality
- Leakage detection
- Pump/valve control
- Meters

Transportation

- Traffic control
- Info boards
- Kiosks

Connected Industry

("Smart Factory/Industrie 4.0/Society 4.0")

- Production floor monitoring
- Remote PLC control
- Automated quality control

Smart Cities

- Smart parking
- Traffic monitoring & control
- Bike sharing
- Smart lighting
- Public safety
- Payment kiosks (PoS)

This signifies a revolution in the industrial world, which is now shifting its focus to increased efficiency and lower costs using smart edge devices and Big Data analytics.

