

# Dantel Network Security Vulnerability Primer

WebMon Edge ES, Matrix ES and PointMaster Eagle ES



2991 N ARGYLE AVE  
FRESNO, CA 93727, USA  
[WWW.DANTEL.COM](http://WWW.DANTEL.COM)

<b>Table of Contents</b>	<b>Page Number</b>
Introduction and overview.....	3
Cyber Vulnerability Monitoring, Detection, Mitigation and Validation.....	4
Multilevel User Access .....	5
Secure Browser Access.....	6
Authentication.....	6
Secure Command Line Interface.....	7
RADIUS and RADIUS over TLS.....	7
SNMP and SNMP over TLS Event Notification and Configuration.....	8
IPv4 and IPv6 Support.....	9
System Audit Log (Syslog) and TELNET.....	9
Conclusion.....	11

## Introduction

For the past three years, Dantel has directed much of its development resource to creating robust and secure remote monitoring solutions in accordance with rapidly emerging Information and Communication Technology (ICT) standards. Dantel has incorporated an Enhanced Security (ES) portfolio in all of its fourth generation remote monitoring products. WebMon ES and PointMaster Eagle ES now include a new security centric architecture based on an advanced multi-core CPU with a hardware encryption engine and firmware secured by a tightly integrated Network Security Suite.

## Overview

According to the US Department of Homeland Security, industrial networks, including networks in telecommunications, power generation, transmission and distribution, continue to be threatened by cyberattacks with ever increased frequency. Network operators worldwide are painfully aware of the fact that most network connected devices are facing this growing threat. These Internet of Things (IoT) devices reside ubiquitously in the cars we drive, communication networks we use and even in our home appliances. Without the adoption of vigilant safeguards, our economy and public safety may ultimately be at risk. The following table illustrates the growing and ever present threat of cyberattacks on various IoT devices:

Target	Threat Level	Reported by
Federal agencies, critical infrastructure, and the Department's industry partners	68 % Increase in cyberattacks (2011 to 2012)	2012 US Department of Homeland Security
IoT and Industrial IoT	70% of IoT devices are vulnerable to attack	2015 HP Labs Research Study
Embedded Devices	540,000 vulnerable embedded devices scanned in 140 countries	Quantitative Analysis of the Insecurity of Embedded Devices  Columbia University Research Study

**Table 1.** Threat of increasing cyberattacks

As demonstrated in table 1, cyber security breaches are on the rise due to the proliferation of IP network connected devices across all industries and criminal hacking activity sponsored by unsavory individuals and unfriendly nation-states. These hostile entities are busy trying to gain access to various networks via unprotected and susceptible network devices outside traditional firewalls, or by using various bots and techniques to "sniff" weaker or outdated security implementations in order to disrupt or damage network based services.

## **Dantel Cyber Vulnerability Monitoring, Detection, Mitigation and Validation**

At Dantel, sound cyber security implementation begins early, at the product requirements phase. During development, this transcends into an architectural foundation before application layer security measures such as encryption, authentication and authorization features are implemented. .

Our main goal is to prevent unauthorized access of information by an internal or external entity and minimize any attempt to place malicious malware in the application layer or rootkit deep in the imbedded software. In order to implement such safeguards, the Dantel product architecture group relied on the guidelines of the National Institute of Standards' Cyber Security Framework, ISO 27001 and OWASP (Open Web Application Security Project) to ensure the code, data at rest and the OS, is "sanitized" against unauthorized code access to minimize risk.

Cyber risk mitigation efforts have resulted in a state-of-the-art security vulnerability mitigation core which consists of:

### **1). Risk Aware Architecture**

The risk mitigation is designed in the product architecture from the start rather than an afterthought.

### **2). Layered Security Suite**

The security layers such as SSL, TLS 1.2, SSH. AES encryption are added to enhance product security and minimize cyber vulnerability.

### **3) Vulnerability Assessment**

The soundness of product's core is validated by passing test vectors and penetration testing by internal and external independent parties based on the following OWASP criteria:

- Injection
- Broken Authentication and Session Management
- Cross-Site Scripting (XSS)
- Insecure Direct Object References
- Security Misconfiguration
- Sensitive Data Exposure
- Missing Function Level Access Control
- Cross-Site Request Forgery (CSRF)
- Using Components with Known Vulnerabilities
- Un-validated Redirects and Forwards

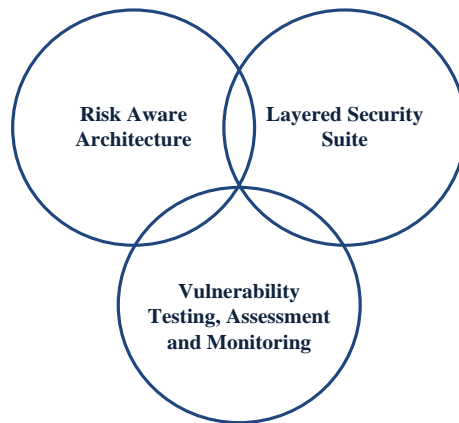


Figure 1. Security Vulnerability Mitigation Core

## Cyber Vulnerability Monitoring

Cyber vulnerabilities are continuously assessed and reported by the National Cyber Awareness System of the United States Computer Emergency Readiness Team (US-CERT), U.S Department of Homeland Security. Any such information affecting Dantel product security is evaluated by Dantel Engineering for a resolution on an urgent basis. The following are a depiction of some of the cyber security features embedded in Dantel's ES (Enhanced Security) product lines.

## Multilevel User Management and Access

The multi-tiered user access provides single factor authentication as a first line of defense against unauthorized access by providing access to users based on a need to know basis and credentials as defined by their particular organization. The tiered user level segregates users based on their role in an organization and provides varying degrees of access privilege such as Normal User with only read privilege, Super User with read and some write privileges and finally Admin rights with all privileges.

The screenshot shows the 'WebMon' user management interface. At the top is a navigation bar with 'Status', 'Device', 'System', 'Network', 'Users', and 'Logout'. Below this is the 'User Management' section with a sub-header 'Add User'. The form contains five fields: 'Account Name\*', 'Username\*', 'Password\*', 'Confirm Password\*', and 'Privilege\*'. The 'Privilege\*' field is a dropdown menu with three options: 'Normal User', 'Super User', and 'Admin'. The 'Normal User' option is currently selected and highlighted.

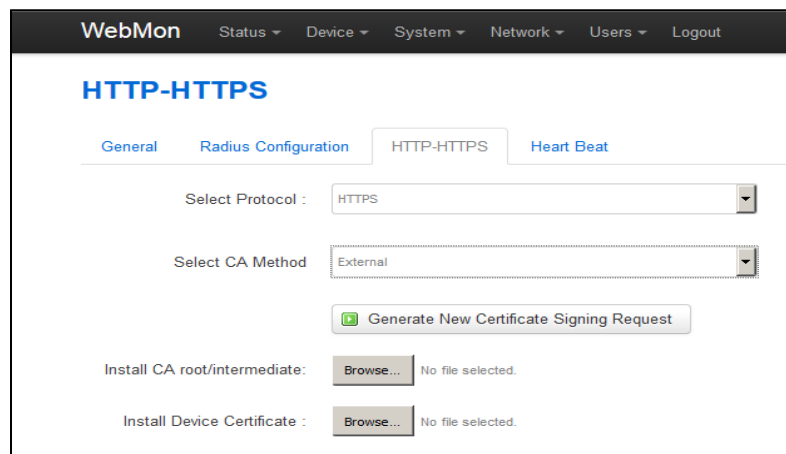
Figure 2. User management screen for creating new users and associated rights



## Secure Browser Access

Selecting the Hypertext Transfer Protocol (HTTP), where data is vulnerable to interception and attack, is no longer the only option. In the current environment of heightened cyber security risk, Dantel now offers added security that provides transmission of sensitive data through an encrypted connection. The basis of such encrypted connections are Secure Socket Link (SSL) certificates. The SSL certificates are type X.509 certificates and utilize public-key (PKI) infrastructure to authenticate the end user and the server. The HTTP data is sent over an SSL link making it a secure HTTP or (HTTPS) link.

The HTTPS is selectable from a drop down menu as required by organizational security needs after a security certificate is installed to facilitate device authentication.

The image shows a screenshot of the WebMon web interface. At the top, there is a navigation bar with the 'WebMon' logo and several menu items: 'Status', 'Device', 'System', 'Network', 'Users', and 'Logout'. Below the navigation bar, the main content area is titled 'HTTP-HTTPS' in blue. There are four tabs: 'General', 'Radius Configuration', 'HTTP-HTTPS' (which is active), and 'Heart Beat'. Under the 'HTTP-HTTPS' tab, there are two dropdown menus. The first is labeled 'Select Protocol :' and has 'HTTPS' selected. The second is labeled 'Select CA Method' and has 'External' selected. Below these menus is a green button with a plus icon labeled 'Generate New Certificate Signing Request'. At the bottom, there are two file selection fields. The first is labeled 'Install CA root/intermediate:' and has a 'Browse...' button next to it, with the text 'No file selected.' to its right. The second is labeled 'Install Device Certificate :' and also has a 'Browse...' button next to it, with the text 'No file selected.' to its right.

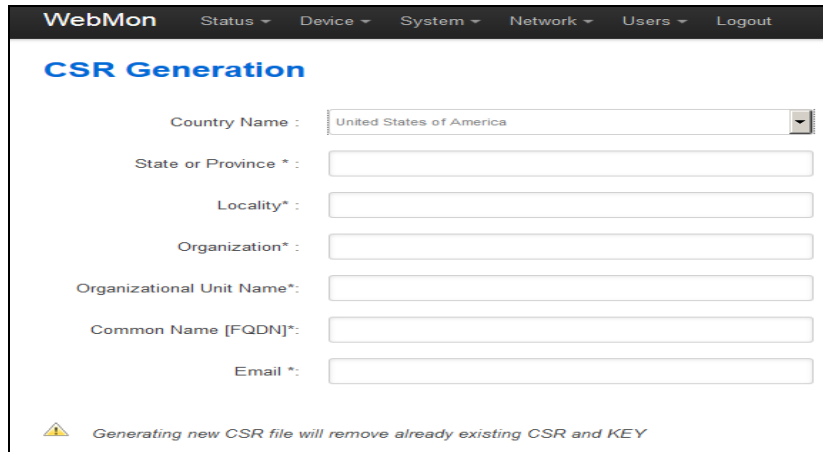
**Figure 3.** Browser access options with or without SSL

## Authentication

Dantel's network security suite supports SHA 256 authentication, which is part of the HASH-2 algorithm. SHA 256 requires a paired private /public key and an authentication certificate for providing the SSL service. SSL encrypts communication between the device and the Web browser with a session key negotiated by the SSL certificate. An SSL handshake authenticates both sides and begins a point-to-point secure session. The certificate could be optionally self-signed or externally signed by a Certification Authority (CA) such as Symantec. Self-signed certificates may result in warning messages and may be blocked.

Prior to creating a security certificate, a Certificate Signing Request (CSR) is generated. If an external SSL certificate is required, the CSR is sent to the Certification Authority for processing the SSL certificate. Upon receiving the CSR, the CA issues the certificate after validating the requesting organization (domain). At a minimum, a key size of 2048-bit (RSA) is required for SSL/TLS certificate generation.

All Dantel security enhanced (ES) products support creation of a security Certificate Signing Request.



**Figure 4.** Security certificate signing request Web page

## Secure Command Line Interface

In a similar fashion, the Dantel Security Suite extends protection against unwarranted intrusions by deploying secure shell (SSHv2) access to the Command Line Interface (CLI). The CLI could be setup in legacy as well as secure mode and is capable of device configuration and retrieval of data such as events and environmental parameters in secure mode. The SSH session may be established either on the Ethernet or Craft/Console port via an SSH client such as Putty.

## RADIUS and RADIUS over TLS 1.2

For networks requiring access control via centralized Authentication, Authorizing and Accounting (AAA), the Dantel Network Security Suite provides Remote Authentication Dial-IN User Service (RADIUS) protocol with either PAP, CHAP, MSCHAP or EAP-MD5 authentication. In order to connect via a RADIUS server the user must be included in the Access Control List (ACL) and must know the secret key of the RADIUS server. Additionally, Transport Layer Security (TLS) may be enabled by merely selecting RADIUS over TLS on WebMon ES/PointMaster ES and the authentication RADIUS server.

The TLS certificates are similar to SSL and are known as type X.509 certificates except that TLS protocol employs a dedicated transport layer with its own cryptographic security layer for highly secure data transmission. Dantel WebMon ES and PointMaster Eagle ES products support the latest TLS 1.2 for enhanced secure communication.

WebMon Status Device System Network Users Logout

## Radius Configuration

General Radius Configuration HTTP-HTTPS Heart Beat

Enable ☐

Authentication PAP

IP Address

Port

Secret

TLS Enable ☐

**Figure 5.** RADIUS configuration page

## SNMP Event Notification and Configuration

For routine deployments SNMP v1 and v2c is available for event notification and device configuration. In order to provide secure notification and configuration of events, the Dantel security suite provides SNMP v3 with Advance Encryption Standard (AES) encryption. The AES encryption standard was established by the US National Institute of Standards and Technology (NIST) and defined in Federal Information Processing Standard FIPS PUB 197.

If higher level of privacy and security is desired, SNMP v3 over TLS 1.2 is standard on Dantel's WebMon Matrix ES and PointMaster Eagle ES products or is available as a CPU upgrade.

In summary, four options for SNMP are as follows:

- SNMP v1
- SNMP v2
- SNMP v3 (auth., priv.) (AES)
- SNMP v3 (auth., priv.) (AES) over TLS 1.2



The image shows the 'SNMP Configuration' page in the WebMon interface. At the top is a navigation bar with 'WebMon' and links for 'Status', 'Device', 'System', 'Network', 'Users', and 'Logout'. Below the navigation bar is the 'Systems' section, followed by 'SNMP Configuration'. There are two tabs: 'SNMP Profiles' (active) and 'View Profiles'. The main configuration area has two dropdown menus. The first is labeled 'SNMP Version \*' and has 'Snmpv3 - TLS' selected. The second is labeled 'Read Write \*' and has 'Snmpv3 - TLS' selected. The dropdown menu for 'Read Write \*' is open, showing options: 'Snmpv1v2', 'Snmpv3 - USM', and 'Snmpv3 - TLS'.

**Figure 6.** SNMP version selection page

## IPv4 and IPv6 Support

In order to future proof IP addressing schemes and provide larger addressing space, the WebMon ES and PointMaster ES product lines now support 32 bit IPv4 as well as 128 bit IPv6, which includes the built-in authentication header (AH) and improved quality of service as compared to IPv4 connectivity.

The image shows the 'Network Settings' page in the WebMon interface. At the top is a navigation bar with 'WebMon' and links for 'Status', 'Device', 'System', 'Network', 'Users', and 'Logout'. Below the navigation bar is the 'Network Settings' section. There are three dropdown menus. The first is labeled 'Protocol' and has 'STATIC' selected. The second is labeled 'Network Type' and has 'IPv4' selected. The third is labeled 'IP Address' and has '192.168.1.75' selected. The dropdown menu for 'Network Type' is open, showing options: 'IPv4' and 'IPv6'.

**Figure 7.** Network options Static/DHCP, IPv4 or IPv6 selection

## System Audit Log (Syslog) and TELNET

The Dantel security suite supports Remote Logging on a remote Syslog server via optional port 514 and also offers On-device (WS Log) record of device configuration and user login record

(audit log). The logged data provides a chronological record of device and user related activity. In addition, for security reasons, TELNET connectivity is disabled by default.

The screenshot shows the 'Security Settings' page in the WebMon interface. The top navigation bar includes 'WebMon', 'Status', 'Device', 'System', 'Network', 'Users', and 'Logout'. Below the navigation bar, there are four tabs: 'General', 'Radius Configuration', 'HTTP-HTTPS', and 'Heart Beat'. The 'General' tab is selected. Under the 'SYSLOG' section, there is a table with two rows: 'Enable' with a checked checkbox, and 'IP Address' with a text input field containing '192.168.1.120'. Below this, there is a 'Port' field with a text input field containing '514'. Under the 'TELNET' section, there is a table with one row: 'Enable' with an unchecked checkbox.

SYSLOG	
Enable	<input checked="" type="checkbox"/>
IP Address	192.168.1.120
Port	514

TELNET	
Enable	<input type="checkbox"/>

**Figure 8.** Syslog server setup

The screenshot shows the 'WS Log' page in the WebMon interface. The top navigation bar includes 'WebMon', 'Status', 'Device', 'System', 'Network', 'Users', and 'Logout'. Below the navigation bar, there is a section titled 'WS Log' with a subtitle 'This list gives an overview current System Log.' Below the subtitle, there is a pagination bar with links: « Prev, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, Next ». Below the pagination bar, there is a table with the following data:

WS LOG
03-17-16 16:24:13 WebMon WSCONF: Logged in user:Dantel
03-17-16 13:36:45 WebMon WSCONF: EVT_CONF :: MOD :Discrete_8_Input_Module :: IDENTIFIER :S1_DI8_P3 :: ENABLE=Set :: POLL_FREQ=60 :: POLL_UOT asserted :: NORM_TXT=Point 3 normal :: ASSERT_LVL=Critical :: NORM_LVL=Normal :: CONTACT=1 :: REV=Set :: NOT_ON_ASSERT=Set :: NOT_NORM=Set :: DELAY_UOT=Second (CHANGED)
03-17-16 13:36:34 WebMon WSCONF: EVT_CONF :: MOD :Discrete_8_Input_Module :: IDENTIFIER :S1_DI8_P3 :: ENABLE=Set :: POLL_FREQ=60 :: POLL_UOT asserted :: NORM_TXT=Point 3 normal :: ASSERT_LVL=Critical :: NORM_LVL=Normal :: CONTACT=1 :: REV=Clear :: NOT_ON_ASSERT=Set :: NOT_NORM=Set :: DELAY_UOT=Second (CHANGED)
03-17-16 13:35:55 WebMon WSCONF: Logged in user:Dantel

**Figure 9.** On-board System Audit logging (WS Log) chart

**Figure 10.** Remote and On-board Alarm (event) History setup

## Conclusion

The explosion of network connected Internet of Things has spawned many new and innovative applications. At the same time however, this rapidly emerging technological revolution has exposed businesses in all industries to new and dangerous security vulnerabilities.

According to the US Department of Homeland Security, industrial networks, including networks in telecommunications, power generation, transmission and distribution, are adversely affected by cyberattacks and the frequency of these cyberattacks continues to increase.

In order to minimize security vulnerabilities, Dantel's security philosophy ensures that potential security vulnerabilities are accounted for from the start of product development and multiple security layers are incorporated. Finally, security penetration testing is conducted to ensure best practices are implemented and validated before Enhanced Security (ES) products leave the warehouse.

Dantel is fully committed and positioned to reinforce this structured security approach on a continuing basis as new threats and technological advances emerge.