Delta Electronics, Inc

Security Handbook

Network Card

Model: InsightPower IPv6 Card, AIO Card, SNMP G3 Mini Card, EMS2000
Doc. Version: v01

Contents

1. Introduction

This guide describes the security features applicable to Delta Network Management Cards and devices with embedded components of Delta Network Management Cards. These functions enable devices to operate remotely over the network.

1.1 Purpose of this Guide

This document describes the following protocols and functions, choose the protocols and functions suitable for your network environment, and the way to set up and use them within a security system:

- Telnet and SSH
- FTP and SFTP
- HTTP and HTTPS
- SNMPv1, v2c and v3
- Modbus TCP

Furthermore, the guide documents how to harden Delta network management cards, enhancing the security of your facilities.

2. Checklist of Security Enhancement

2.1 Keep your firmware up-to-date

Delta Software Center website provides the latest firmware for your device network cards. Please regularly check on the website and update your network management cards with the latest firmware. This will help you ensure the security holes and features are up-to-date.

2.2 Disable HTTP and enable HTTPS

For a more reliable and encrypted channel of communication, please disable HTTP (if it was enabled) and enable HTTPS.

2.3 Upload a custom HTTPS certificate

The network management card enabled device adopts a default HTTPS certificate. It is recommended that you use OpenSSL utility to create custom certificates to enhance authenticity.

2.4 Disable Telnet and enable SSH

For a more reliable and encrypted channel of communication, please disable Telnet (if it was enabled) and enable SSH.

2.5 Disable FTP and enable SFTP

For a more reliable and encrypted channel of communication, please disable FTP if (it was enabled) and enable SFTP.

2.6 Disable SNMPv1 and enable SNMPv3

If the device needs to communicate through SNMP. It is recommended to use SNMPv3 as it is more secure than SNMPv1.

If SNMPv1 is necessary, it is recommended to specify the management host IP address, enable read-only permission and assign a strong enough community string.

2.7 Disable Modbus TCP

Disable Modbus TCP if it was enabled. Alternatively, specify the management host IP address and enable read-only permission.

2.8 Use custom network ports where applicable

To prevent from being confused by scans looking only at standard ports, please use custom network ports instead. These apply to protocols such as HTTPS, SSH, SFTP, SMTP, etc.

2.9 Change default account and password

Please change the default account and password of administrator, device and user after installation and configuration. Make sure the password is strong enough.

2.10 Enable SNTP

Enable SNTP function to synchronize the network time which enables the network management cards to record event in the log file to track issues.

2.11 Disable NBNS Service

NBNS service response allows your devices to respond host name. It is recommended that you disable this feature to enhance your device security.

3. Authentication by Certificates and Host Keys

Authentication verifies the identity of users or network devices. Passwords are often used for identifying users. However, for communication between Network Management Cards and devices, a stricter security authentication method is required.

- **Secure Sockets Layer / Transport Layer Security (SSL/TLS)**

  SSL/TLS is the technology uses digital certificates for authentication to keep Web access secure and protect sensitive data sent between two systems. A digital CA root certificate is issued by a Certificate Authority (CA) as part of a public key infrastructure, and its digital signature must match the digital signature on a server certificate on the Management Card or device.

- **Secure SHell (SSH)**

  SSH is used for remote terminal access to the command line interface of the network card or device, uses a public host key for authentication.

3.1 Generate a private SSL certificate file (in PEM format) for HTTPS

To ensure connection security between network enabled devices and your workstation, you can create a private SSL certificate file. Please download and install OpenSSL Toolkit from http://www.openssl.org. Launch Shell or DOS prompt mode, and refer to the following command to create your own certificate file:

openssl req –x509 –nodes –days 3650 –newkey rsa:1024 –keyout cert.pem –out cert.pem

Then, proceed with the given directions. When it is completed, a file named **cert.pem** will be created in the current working directory.

Upload **cert.pem** to the network enabled device through web interface (Login with Administrator privilege).

3.2 Create a SSH Host Key

1) Please download and install **PuTTY** from http://www.putty.org.
2) Run **puttygen.exe** from the installed directory.

3) Select SSH-2 RSA from the Parameters area and click Key → Generate key pair to generate a RSA key.

4) Click Conversions → Export OpenSSH Key and assign a filename to the RSA key. Please ignore it when prompted to provide key passphrase.

5) Select SSH-2 DSA from the Parameters, click Key → Generate key pair to generate a DSA key.

6) Click Conversions → Export OpenSSH Key and assign a filename to the DSA key. Please ignore it when prompted to provide key passphrase.

7) Copy the generated key from the text box, paste in a text editor and save as a text file.

8) Upload the DSA/ RSA/ Public keys files to the network enabled device through web interface.

4. Security Depolyment Guide

This document provides general security guidance to help you decide on an appropriate secure deployment based on your specific security requirements.

To maintain security throughout the deployment lifecycle, the following considerations are required to be reviewed:

- **Security of Physical Environment**
- **Security of Devices**
- **Security of Network**

4.1 Security of Physical Environment

The device owner should protect the network enabled device from unauthorized physical access.

- Access should be restricted to those who require access to maintain the equipment.
- Restricted areas should be clearly marked for authorized personnel only.
- Restricted areas should be secured by locked doors.
- A physical or electronic audit trail should be conducted when entering the restricted zone.

4.2 Security of Devices

The device security includes the following items:

- Firmware updates

  Customers ensure their devices have been updated with the latest firmware versions prior to deployment. For information on new and updated firmware, please visit the Delta web page.
- Certificates

  The default certificates are not intended for use in production deployments and should be replaced. Delta recommends that customers configure the device to use certificates either from a reputable Certificate Authority (CA) or appropriate certificates from your enterprise CA.
- No Unnecessary Services

  If a network service is not necessary for the intended purpose or operation of the device, ensure that service is not running or accessable.

- Logging

  Please enable SNTP and ensure that the system time of the network-enabled device is correctly synchronized with the current network time. The event log records the historical events of devices and network cards, and can be used to track login/logout events of devices, network cards and accounts.

4.3 Security of Network

When deploying a Network Card to a production environment, Delta strongly recommends that the below key configuration changes are made.

- Firewall

  Delta strongly recommends that the device not be exposed on the public Internet and be deployed behind an appropriate stateful packet inspection (SPI) firewall.

- Network Segmentation

  Delta strongly recommends that the network traffic on the device management interface be physically or logically separated from normal network traffic. The flat network architecture makes it easier for malicious actors to move around the network. With network segmentation, organizations can enhance network security by controlling access to sensitive data by enabling or denying network access. A strong security policy requires that the network be divided into multiple areas based on different security requirements, and strictly enforce the policy on allowing movement between areas.

- Other Security Detection and Monitoring Tools

  Delta recommends protecting and monitoring the environment through appropriate physical, technical, and management tools for network intrusion and monitoring.