OPEN OPTIONS®
ACCESS TECHNOLOGY

Access Control System Hardening Guide

The DNA Fusion™ Access Control Software and SSP™ Security System Processor use equipment that generates, uses, and radiates radio frequency energy. If not installed and deployed in accordance with the guidelines of this installation manual, they may cause harmful interference to radio communications. Operation of this equipment in a residential area may cause harmful interference, in which case the user will be required to correct the interference at their own expense.

The DNA Fusion™ Access Control Software and SSP™ Security System Processor shall be installed in accordance with this installation manual and in accordance with the National Electric Code (N.E.C), ANSI and NFPA 70 Regulations and recommendations.

Publish Date: June 16, 2020
Manual Number: HG-2.0

Warranty

All Open Options products are warranted against defect in materials and workmanship for one year from the date of shipment. Open Options will repair or replace products that prove defective and are returned to Open Options within the warranty period with shipping prepaid. The warranty of Open Options products shall not apply to defects resulting from misuse, accident, alteration, neglect, improper installation, unauthorized repair, or acts of God. Open Options shall have the right of final determination as to the existence and cause of the defect. No other warranty, written or oral is expressed or implied.

16650 Westgrove Dr | Suite 150
Addison, TX 75001
Phone: (972) 818-7001
Fax (972) 818-7003
www.ooaccess.com

Open Options Software License Agreement

THE ENCLOSED SOFTWARE PACKAGE IS LICENSED BY OPEN OPTIONS, LLC. TO CUSTOMERS FOR THEIR NON-EXCLUSIVE USE ON A COMPUTER SYSTEM PER THE TERMS SET FORTH BELOW.

DEFINITIONS: Open Options shall mean Open Options, LLC, which has the legal right to license the computer application known as DNA Fusion herein known as the Software. Documentation shall mean all printed material included with the Software. Licensee shall mean the end user of this Open Options Software. This Software Package consists of copyrighted computer software and copyrighted user reference manual(s).

LICENSE: Open Options, LLC, grants the licensee a limited, non-exclusive license (i) to load a copy of the Software into the memory of a single (one) computer as necessary to use the Program, and (ii) to make one (1) backup or archival copy of the Software for use with the same computer. The archival copy and original copy of the Software are subject to the restrictions in this Agreement and both must be destroyed or returned to Open Options if your continued possession or use of the original copy ceases or this Agreement is terminated.

RESTRICTIONS: Licensee may not sub license, rent, lease, sell, pledge or otherwise transfer or distribute the original copy or archival copy of the Software or the Documentation. Licensee agrees not to translate, modify, disassemble, decompile, reverse engineer, or create derivative works based on the Software or any portion thereof. Licensee also may not copy the Documentation. The license automatically terminates without notice if Licensee breaches any provision of this Agreement.

TRANSFER RIGHTS: Reseller agrees to provide this license and warranty agreement to the end user customer. By installation of the software, the end user customer and reseller agree to be bound by the license agreement and warranty.

LIMITED WARRANTY: Open Options warrants that it has the sole right to license the Software to Licensee. Upon registration by the Licensee, Open Options further warrants that the media on which the Software is furnished will be free from defects in materials and workmanship under normal use for a period of twelve (12) months following the delivery of the Software to the Licensee. Open Options' entire liability and your exclusive remedy shall be the replacement of the Software if the media on which the Software is furnished proves to be defective. EXCEPT AS PROVIDED IN THIS SECTION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE EXPRESSLY DISCLAIMED. IN PARTICULAR, EXCEPT AS PROVIDED IN THIS SECTION, WITH RESPECT TO ANY PARTICULAR APPLICATION, USE OR PURPOSE, LICENSOR DOES NOT WARRANT THAT THE PRODUCTS WILL MEET THE LICENSEE'S REQUIREMENTS, THAT THE PRODUCTS WILL OPERATE IN THE COMBINATIONS OF 3RD PARTY SOFTWARE WHICH THE LICENSEE MAY SELECT TO USE, OR THAT THE OPERATION OF THE PRODUCTS WILL BE UNITERRUPTED OR ERROR FREE. NEITHER OPEN OPTIONS, NOR ITS VENDORS SHALL BE LIABLE FOR ANY LOSS OF PROFITS, LOSS OF USE, INTERRUPTION OF BUSINESS, NOR FOR INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES OF ANY KIND WHETHER UNDER THIS AGREEMENT OR OTHERWISE. IN NO CASE SHALL OPEN OPTIONS' LIABILITY EXCEED THE PURCHASE PRICE OF THE SOFTWARE.
The disclaimers and limitations set forth above will apply regardless of whether you accept the Software.

TERMINATION: Open Options may terminate this license at any time if licensee is in breach of any of its terms or conditions. Upon termination, licensee will immediately destroy the Software or return all copies of the Software to Open Options, along with any copies licensee has made.

APPLICABLE LAWS: This Agreement is governed by the laws of the State of Texas, including patent and copyright laws. This Agreement will govern any upgrades, if any, to the program that the licensee receives and contains the entire understanding between the parties and supersedes any proposal or prior agreement regarding the subject matter hereof.

Table of Contents

Hardening Guide

In This Guide

The Hardening Guide explains how to maximize security when installing and configuring SSP controllers and downstream SIO devices as well as the Open Options DNA Fusion access control system. This guide will identify critical security features, recommend procedures based on system protection requirements, and define best practices for securing the hardware and software.

What is "Hardening?"

Developing and implementing security measures and best practices is known as "hardening." Hardening is a continuous process of identifying and understanding security risks and taking appropriate steps to negate them. The process is dynamic because threats, and the systems they target, are continuously evolving.

This guide focuses on the IT settings and techniques used, as well as physical security, which is also a vital part of hardening. For example, use physical barriers to protect servers and client computers, and make sure that components like camera enclosures, lock, tamper alarms, and access controls are secure.

The following are the actionable steps for hardening a DNA Fusion system deployment:

1. Understand the component to protect.
2. Harden the access control system components:
   - ☐ Harden the servers (physical and virtual), and client computers and devices.
   - ☐ Harden the network.
   - ☐ Harden the access control hardware.
3. Document and maintain security settings on each system.
4. Train, and invest in people and skills, including supply chain.

Some of the recommendations in this guide require you to perform the following actions:

- Disable one or more ports.
- Stop, disable, or remove services.
- Remove one or more features of the operating system.
- Uninstall software.
- Lock down shares.
- Disable access to Null sessions or anonymous connections.
- Ensure antivirus, malware, and firewall solutions are installed and enabled.
- Enforce strong passwords and least privilege policies.
- Ensure sufficient logging is enabled.
- Utilization of effective Microsoft Active Directory design and management.
- Enable encryption for data "at rest" and "in transit."

The recommendations in this guide were developed using recognized standards, third-party recommendations, and hardening best practices. Before proceeding, recognition of the following points are important:

- Understand what you have and the associated risks.
- Hardening standards are not "one-size-fits-all" and must consider the lines of business, governance requirements, and the criticality of the assets and information.
- There may be third-party integrations to DNA Fusion that are negatively impacted by hardening practices.

The Open Options hardware portfolio contains various generations of intelligent controllers and interface modules whose security parameters and hardening instructions evolve over time. This hardening guide will cover the following SSP controllers and SIO devices:

SSP Series Controllers	SSP-EP, SSP-D2, SSP-LX, DController
Series 3 SIO Modules	RSC-1, RSC-2, ISC-16, OSC-16, NSC-200
Series 2 SIO Modules	RSC-1, RSC-2, ISC-16, OSC-16, NSC-100
M5 Bridge Controllers	M5-IC
Honeywell Controllers	PW6K1IC, PRO32IC

The M5 Bridge and Honeywell controllers follow the same hardening procedures as the SSP Series in this guide. The Series 3 (LP) boards are distinguished by the red coloring of the board.

The guide is organized into nine (9) sections:

- Section 1, "DNA Fusion Hardening Configuration," defines steps required for hardening the DNA Fusion software.
- Section 2, "Protection Levels," recommends security settings based on the system's size and needs.
- Section 3, "Installation," defines best practices when installing the hardware devices.
- Section 4, "Internal Webpage," describes the security features available in the Configuration Manager.
- Section 5, "User Accounts," explains how to modify user account information to reduce risk.
- Section 6, "Information Services," instructs the user how to disable discovery services.
- Section 7, "Encryption and Authentication," includes AES/TLS encryption settings and recommended peer certificate values for two-way authentication.
- Section 8, "Port-Based Network Access Control," details 802.1x authentication for the SSP-LX and SSP (LP) controllers.
- Section 9, "Equipment Replacement," explains how to perform a bulk erase to sanitize controllers and the NSC-200 as well as how to clear the EEPROM from downstream SIO modules.
- Section 10, "Network Ports," describes which network ports are utilized by the controllers, NSC-100, and NSC-200

DNA Fusion Hardening Configuration

1

Hardening your DNA Fusion components is more than a single step in securing the environment. The following steps should be part of a comprehensive "defense-in-depth" security plan:

- **Plan** the installation and deployment of the operating system and other components for the server.
- **Install**, **configure**, and **secure** the underlying operating system.
- **Install**, **configure**, and **secure** the server software.
- **Ensure** that all servers are installed in a physically secured environment.
- Use strong passwords
  - Enable NT Authentication in DNA Fusion to streamline passwords.
- Follow "least privilege" privilege assignments and segmentation of duties for operating system accounts and DNA Fusion accounts.
- **Ensure** all critical servers/services are part of your business continuity and disaster recovery plan.
- **Employ** appropriate network protection mechanisms (e.g., firewall, packet filtering router, and proxy).
  - Choosing the mechanisms for particular situation depends on several factors, including the location of the server's clients (e.g., Internet, internal, and remote access), the location of the server on the network, the types of services offered by the server, and the types of threats against the server.
- **Employ** secure administration and maintenance processes, ensuring application of patches and upgrades are up to date for both software and firmware, monitor of logs, backups of data and operating system, and periodic security testing.
- **Maintain** proper alert, records, and logs.
  - This information can be used to alert of a potential attack, as legal and forensic evidence, as part of the recovery plan, for continuous improvement.
- **Implement** ongoing security training practices.

NOTES:

Protection Levels 2

The following table outlines three (3) protection levels—Basic, Intermediate, and Enterprise—based on a system's size and security requirements. Each level adopts the previous level's recommended procedures.

Level	Recommendation	Procedures
Basic	Minimum protection—Small businesses or office installations where the operator is also the administrator.	*Installation* (section 2) — Place device on a private network, in a secured enclosure, with updated firmware and normal DIP switch settings. *Internal Webpage* (section 3) — Enable HTTPS. *User Accounts* (section 4) — Remove the default user credentials, create a unique user account, and set a strong password. *Equipment Replacement* (section 8) — Bulk erase the controller and clear the EEPROM from downstream modules.
Intermediate	Medium protection—Corporations with a dedicated system administrator.	*Internal Webpage* (section 3) — Add authorized IP addresses. *Web Services* (section 3) - Disable web service. *Information Services* (section 5) — Disable discovery and SNMP services. *USB and SD Interfaces* (section 6) — Disable USB and SD interfaces. *Encryption and Authorization* (section 6) — Enable AES or TLS encryption.
Enterprise	Maximum protection—Large networks with an IT/IS department. Intended for integration into an enterprise network infrastructure.	*Information Services* (section 5) — Enable SNMPv3 (SSP-LX and SSP (LP) controllers). *Encryption and Authentication* (section 6) — Generate and load customized peer certificates to validate the host/controller. *Enable Data Encryption "At Rest"* (SSP-LX, Series 3) *Port-Based Network Access Control* (section 7) — Enable IEEE 802.1X (SSP-LX and SSP (LP) controllers).

Installation 3

Open Options recommends the following installation procedures:

- Private Network — Do NOT install any Ethernet products on the public Intranet.
- Secured Enclosure — Place the hardware in a secure enclosure to shield it from harsh environments; use a cabinet tamper to generate notifications when the enclosure is opened.
- Updated Firmware — Update the intelligent controllers and SIO modules to the latest firmware so that the hardware contains all recent changes and security improvements.
- Normal Operation — Set all DIP switches to the OFF position. This setting only applies to network controllers.

NOTES:

Internal Webpage

To reduce security risks, modify the HTTPS, Session Timer, and Authorized IP Addresses in the device's internal web interface, also known as the Configuration Manager.

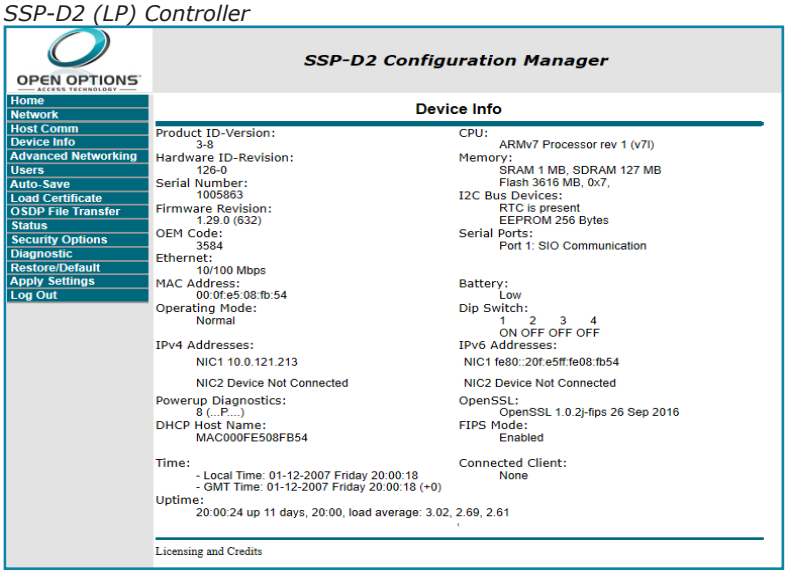
HTTPS

Hypertext Transfer Protocol Secure (HTTPS), which encapsulates the HTTP and SSL/TLS protocols, is used to secure communication over a network. It provides encrypted communication with the web server. HTTPS should be enabled as the default protocol.

Set DIP switch 3 to the OFF position to enable HTTPS. The DIP switch positions can be viewed in the Device Info screen of the Configuration Manager.

> *The SSP-LX and Series 3 controllers do not support HTTP; any HTTP request is redirected to HTTPS.*

SSP-D2 (LP) Controller

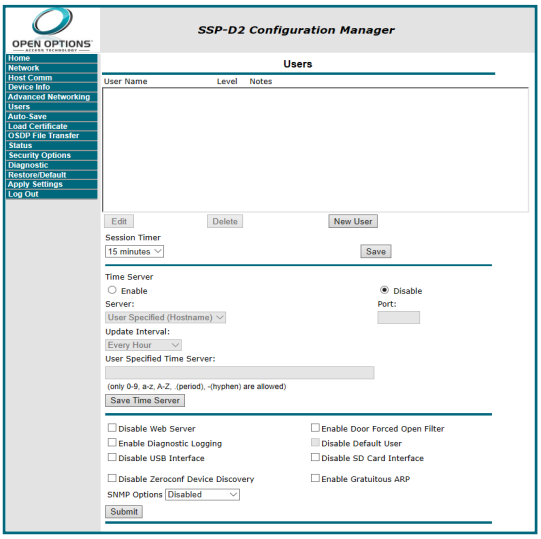


Session Timer

The session timer automatically logs out the user after a specified length of time (default = 15 minutes). Open Options recommends setting the timer to 5 minutes to minimize the risk of an attacker breaching active sessions. However, the timer accepts values ranging from 5 to 60 minutes in five-minute increments.

Access the Session Timer from the Users page of the web interface.

SSP-D2 (LP) Controller

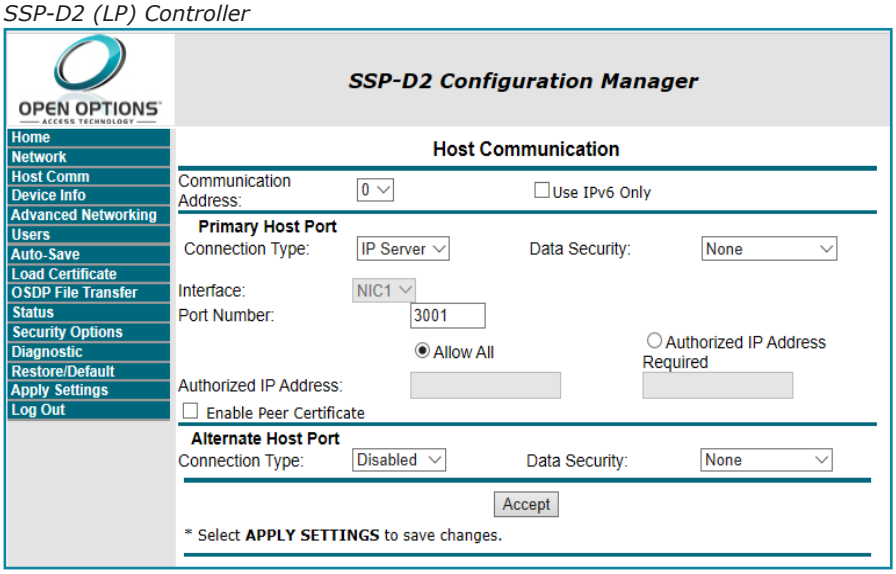


Authorized IP Addresses

When only one or two IP addresses are accessing the controller's host communication port, it is possible to restrict where the connection originates. This setting applies to the communication port established by a host application that is set to IP Server (host-initiated connection) mode. In an IP Client (controller-initiated connection) mode, the host application programs the authorized IP addresses into the controller.

1. In the Host Communication screen, **select** Authorized IP Address Required and **enter** the permitted address.
2. **Select** Apply Settings to save the changes, then **click** Accept.

SSP-D2 (LP) Controller



Disable Web Server

The web server is frequently used to perform the initial configuration of the controllers. Once the controller is configured and connected to the host, disabling web server will increase security. Web server can be disabled by clicking on the Disable Web Server check box at the bottom of the Users page. Re-enabling the server will require the operator to bulk erase the controller. See page 21 for more information on bulk erase.

User Accounts

Modifying user account information is a critical step in improving the controller's security.

Default User Login

The following default user credentials are assigned to all out-of-the-box controllers.

- Username: admin
- Password: password

Disable the default user to prevent unauthorized use:

- For firmware 1.25.6 or above, check Disable Default User on the Users page of the Configuration Manager to permanently disable the default user account.
- For firmware 1.19.4 (build 0415 or later), perform the following steps to temporarily enable the default user account (only if the default user account was not permanently disabled):
    1. **Transition** DIP switch 1 from OFF to ON to enable the default user; the user has five (5) minutes to log in to the internal webpage.
    2. **Log in** within five (5) minutes or reboot the board to disable the default user account until DIP switch 1 is transitioned again.
- For firmware below 1.19.4 (build 0415), set DIP switch 1 to OFF and **create** at least one unique user account. See Unique User Accounts below.

Unique User Accounts

Create at least one unique user after logging in to the internal webpage for the first time. The username and password for this user must be unique. Each person who accesses the Configuration Manager should possess their own unique account for auditing purposes.

Password Strength

Password strengths can be Low, Medium, or High. Maximize password security by creating a high-strength password.

> *The SSP-LX and Series 3 (LP) controllers requires a high-strength password.*

Strength Requirements

- Low Strength
    - Six-character minimum length
- Medium Strength
    - Six-character minimum length
    - Meets at least two criteria points (see below)
- High Strength
    - Eight-character minimum length
    - Must not contain the username
    - Meets at least three criteria points (see below)

Password Criteria

- Uppercase alphabet characters (A-Z)
- Lowercase alphabet characters (a-z)
- Numeral characters (0-9)
- Non-alphanumeric characters (!, $, #, or %)

NOTES:

Information Services 6

Disable discovery services by implementing the following guidelines.

Disable Discovery

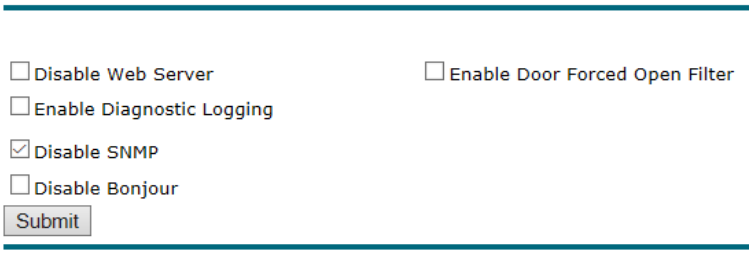
By default, the SSP controllers support device discovery using Zeroconf protocol on Windows and Linux services, such as Apple Bonjour and mDNSResponder. Once the controller is installed and configured, Open Options recommends that the discovery setting be disabled; this prevents someone with access to the same network from discovering the controllers.

Disable Zeroconf discovery through the Users screen of the internal webpage.

Disable SNMP

SNMP is disabled in the controllers by default. If SNMP is not used, leave the setting disabled.

Disable SNMP through the Users page of the internal webpage.



Disable USB and SD Interfaces

USB and SD interfaces are enabled by default. The SD Interface is used to collect the disposal of logs if the controller malfunctions. Disable these interfaces if they are not utilized. Check the boxes labelled Disable USB Interface and, or Disable SD Card Interface, located toward the bottom of the Users page.

Encryption and Authentication 7

The following settings help improve encryption and authentication methods.

Host / Controller Encryption

The SSP controllers support Advanced Encryption Standard (AES) and Transport Layer Security (TLS) encryption for host communications. Use one of these methods to encrypt the data being transferred to and from the controller. Open Options recommends TLS over AES for data security.

AES Encryption

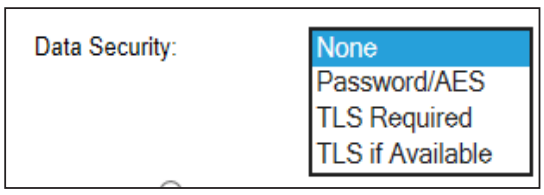
Enable AES encryption by configuring both the host and the controller. Load the encryption keys (128-bit or 256-bit) on both hardware devices prior to enabling AES. Encrytption keys can are loaded through the Load Certificate tab in the Configuration Manager.

TLS Encryption

By default, unique certificates are loaded into each controller during production. The certificates are used to encrypt communication between the host and controller. TLS encryption is enabled via the internal webpage.

The Configuration Manager contains two TLS options:

- TLS if Available – If enabled locally at the controller without host side changes, TLS encryption will be the default method.
- TLS Required – If selected, only encrypted connections will be established; requires DNA Fusion to be configured for TLS. This option is more secure.



NOTES:

Hardening TLS

Implementing TLS encryption can provide a high level of assurance that data in transit is secured from unauthorized access. While providing strong encryption, TLS is susceptible to certain methods of compromise. If an attacker can install their own private key in the trusted root store and deploy a transparent proxy, then all data, including credentials, is vulnerable to modifications or extraction.

The recommendations below are based on an application of NIST 800-52r2 and supporting best practices related to hardening TLS/SSL settings for Microsoft Windows operating systems.

Protocols

- ☐ Enable: TLS 1.2
- ☐ Disable: TLS 1.1,TLS 1.0, SSL 3.0, SSL 2.0, and PCT 1.0

Cipher Suites

The following cipher suites are listed in decreasing order of security strength.

Cipher Suites	Ciphers
TLS 1.2 AEAD SHA-2 only:	TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256
	TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256
	TLS_DHE_RSA_WITH_CHACHA20_POLY1305_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_DHE_RSA_WITH_AES_256_GCM_SHA384
	TLS_DHE_RSA_WITH_AES_128_GCM_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
TLS 1.2 SHA2 (non-AEAD):	TLS_DHE_RSA_WITH_AES_256_CBC_SHA256
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
	TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
	TLS_ECDHE_RSA_WITH_CAMELLIA_256_CBC_SHA384
	TLS_ECDHE_RSA_WITH_CAMELLIA_128_CBC_SHA256
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA256

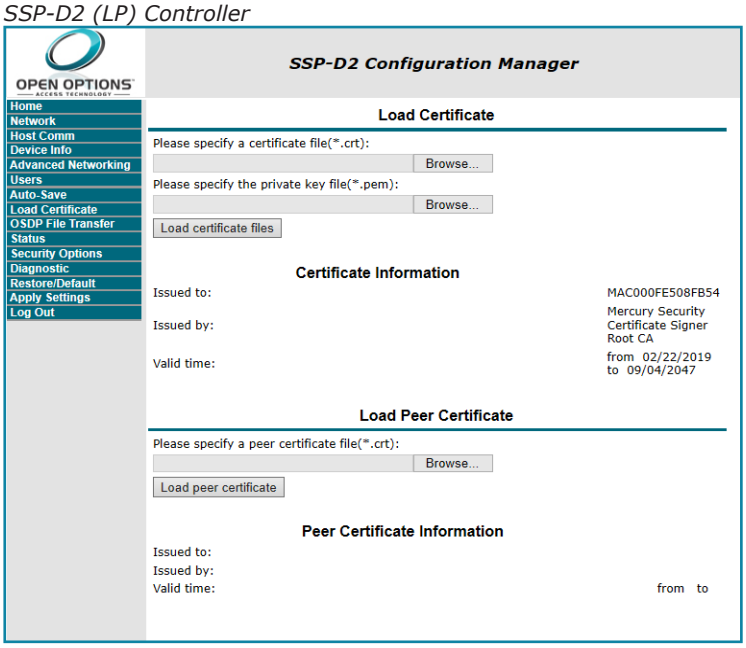
TLS 1.0 and 1.1 with modern ciphers and outdated hashes:	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
TLS 1.0 and 1.1 with older and reasonable ciphers and outdated hashes:	TLS_DHE_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_ECDHE_RSA_WITH_3DES_EDE_CBC_SHA
	TLS_ECDHE_ECDSA_WITH_3DES_EDE_CBC_SHA
Additional Ciphers:	TLS_RSA_WITH_AES_256_CBC_SHA256 (* applies to SSP-LX only)
	TLS_RSA_WITH_AES_256_CBC_SHA
	TLS_RSA_WITH_AES_128_CBC_SHA

Host / Controller Authentication

In addition to AES or TLS encryption, certificates can be used to authenticate the validity of the host and controller. Factory-loaded certificates are limited because they cannot be customized to the controller's deployment location. However, by loading customized peer certificates on the host and controller, a TLS connection proves the validity of the host and controller.

Peer certificates are loaded into the controller via the internal webpage's Load Certificate screen. The controller's peer certificate must be loaded into the host's certificate store in order to mutually authenticate the validity of the controller.

SSP-D2 (LP) Controller



Digital Certificates

Digital Certificates are used to strengthen TLS/SSL Security using a strong private key to help mitigate potential bad actors from impersonation attacks. This is supported by strong, valid certificates that prevent the private key to impersonate a host. Unique TLS/SSL keys should be generated for each service and stored in a secure manner, such as a Hardware Security Module (HSM). Keys should be signed by a trusted certificate authority and password protected.

Certificate Values:

- SSP (EP) Controllers: SSP-EP, SSP-D2, and DController
  - RSA Key Size: 1024-bit
  - SHA Size: sha1
  - Host, SIO Communication, and Webpage HTTPS/TLS Ciphers:

    TLS_RSA_WITH_AES_256_CBC_SHA

    TLS_RSA_WITH_AES_128_CBS_SHA
- SSP-LX, SSP (LP) Controllers
  The SSP-LX and the SSP (LP) controllers supports larger key sizes and higher SHA sizes.
  - RSA Key Size: 4096-bit maximum (factory default is 2048-bit)
  - SHA Key Size: sha384 maximum (factory default is sha256)
  - Host and SIO Communication TLS Ciphers: FIPS 140 cipher suite
  - Webpage HTTPS/TLS Ciphers:

    EECDH+AESGCM

    EDH+AESGCM

The values above represent the highest possible value before performance begins to degrade.

DNA Fusion Servers

The following recommendations are hardening steps for DNA Fusion servers and applications

Network Segmentation

- Implement network segmentation by creating a Virtual LAN (VLAN) for DNA Fusion and connected components.
- Configure DNA Fusion application server with two network interface cards (NIC).
  - One NIC on a VLAN with access control field hardware non-routable to the rest of te corporate network.
  - One NIC on A VLAN for client communication that is routable to the corporate network.

Database Security System (Microsoft SQL Server)

- Configure Transparent Data Encryption (TDE) to support encryption of data "at rest."
- Enable TSL/SSL for the SQL Server instance to support encryption of data "in transit."

Password Policies

- Change DNA Fusion default admin password.
- Configure DNA Fusion strong password policies or configure DNA Fusion to use NT Authentication.

Downstream Communications

Enable encryption between the controller and downstream devices.

Series 2 Subcontrollers (EP)	Only supports AES128 encryption; must be configured and enabled.
Series 3 Subcontrollers (LP)	Supports AES128 and AES256 encryption. For SSP-LX and SSP (LP) controllers, AES256 is enabled by default. For all other SSP controllers, AES128 is available; must be configured and enabled.
NSC-100	Only supports AES128 encryption; enabled by default.
NSC-200	Supports either AES128 encryption or TLS encryption; Enabled by default.

Reader Communications

Use OSDP secure channel (V2) for reader communications. This bi-directional protocol, which is secured using symmetric keys shared between the reader and controller. This channel provides a more secure communication method for the reader.

> ! *OSDP secure channel encryption is only available on the Series 3 subcontrollers modules; each module must have a reader that supports OSDP.*

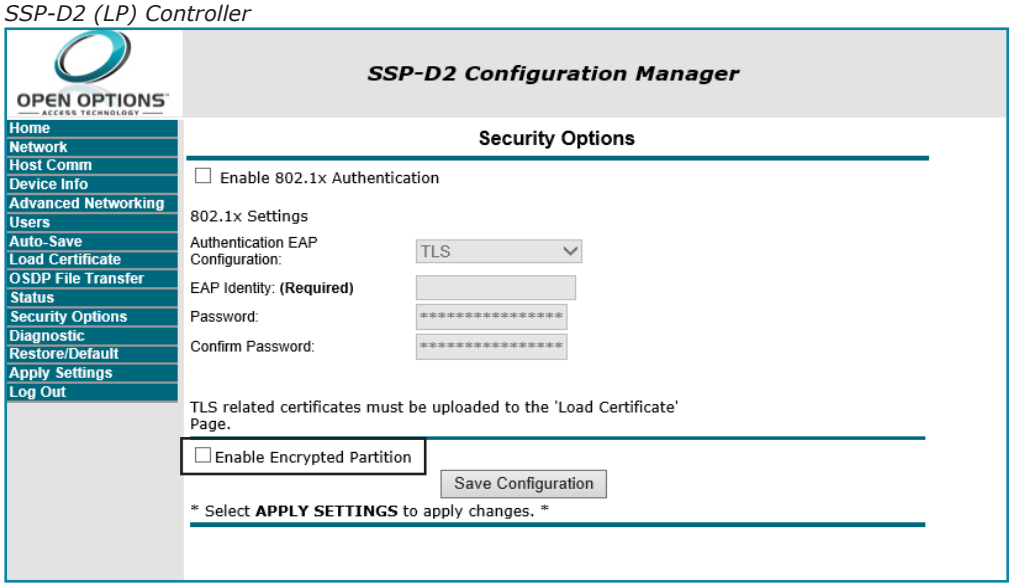
Data at Rest Encryption (SSP-LX and Series 3 (LP) Controllers)

Data at rest encryption has been implemented to satisfy end users with privacy concerns in the field. The encryption allows the configuration and data files to be stored in an encrypted container. The files will remain inaccessible if an incorrect procedure and password are used.

To enable data at rest encryption:

1. **Open** the controller's web interface (Configuration Manager).
2. **Click** on the Security Options tab.
3. **Select** the Enable Encryption Partition checkbox.
4. **Click** on the Save Configuration button.

SSP-D2 (LP) Controller



Replay Attack Protection on IP Networks

Host / Controller Communications

Previous sections have stated that the SSP (EP series and LP series) controller's support AES and TLS encryption for host communications. These are tools used to encrypt the data transferred to-and-from the controller. When using AES encryption (128 or 256 bit), both the host and controller are loaded with encryption keys set by the host software system. When using TLS encryption, every controller is installed with a unique certificate at the time of production and used to encrypt communication between the host and controller. Additionally, the host software system may be used to load customized peer certificate to the controller.

Encryption and network specific mutual authentication can then be realized by loading controller peer certificates on the host software system. Different controller models support different key lengths and ciphers. A session key, generated by a FIPS 140-2 (certified on SSP (LP) controllers) random number generator, is created to protect sessions of AES or TLS encryption. Additionally, only a single host connection to the controller is allowed, limiting the ability for rogue host to connect to the controller. Commands sent to the controller also utilize sequence numbers that reduce the ability to replay commands that are out of sequence.

Controller / IP Based Downstream Communications

The NSC-100 and NSC-200 IP-enabled input/output modules support AES encryption (128-bit) between the controller and downstream module by default. Additionally, the newer NSC-200 supports TLS specifically for the configuration webpages. The AES encryption on the NSC-100 and NSC-200 is synchronized using a combination of random seed and RSA1024 private/public key pairs generated every time after a reboot. A session key, generated using a FIPS 140-2 approved random number generator, is created to protect sessions of AES or TLS encryption. These security mechanisms help protect against replay command attacks.

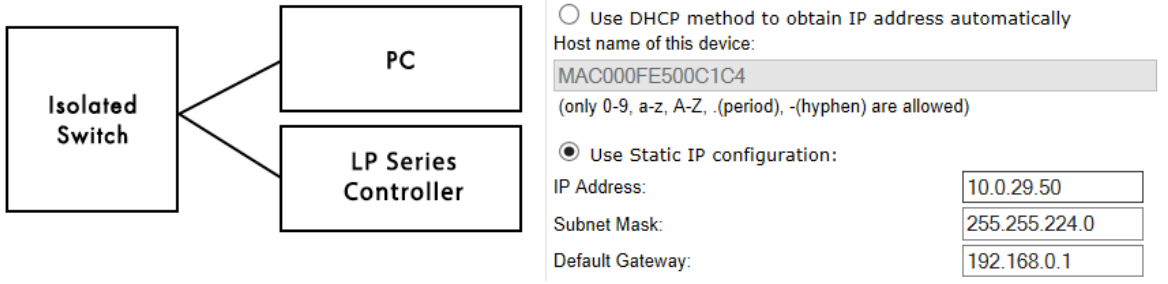
NOTES:

802.1x Authentication for SSP-LX and Series 3 (LP) Controllers

To include an additional layer of local area network (LAN) security and prevent unwanted access to a given network, add IEEE 802.1x authentication. This method is applicable to all SSP (LP) controllers as well as SSP-LX with firmware 1.24.1 and above.

In 802.1x authentication, a supplicant, or device that intends to connect to the network, must first agree on a type of Extensible Authentication Protocol (EAP) with the authentication server linked to the desired network. Afterwards, the supplicant is required to pass a series of challenges sent from the middle-man authenticator in order to establish communication with the network connected to the authentication server. EAP requirements range from simple username/password combinations to TLS certificates. By doing so, the authentication server can restrict access to any supplicant that fails to authenticate.

To activate this feature, install the controllers on an isolated network (or connect it directly to the host), configure the device with a static IP, and connect through the internal webpage.

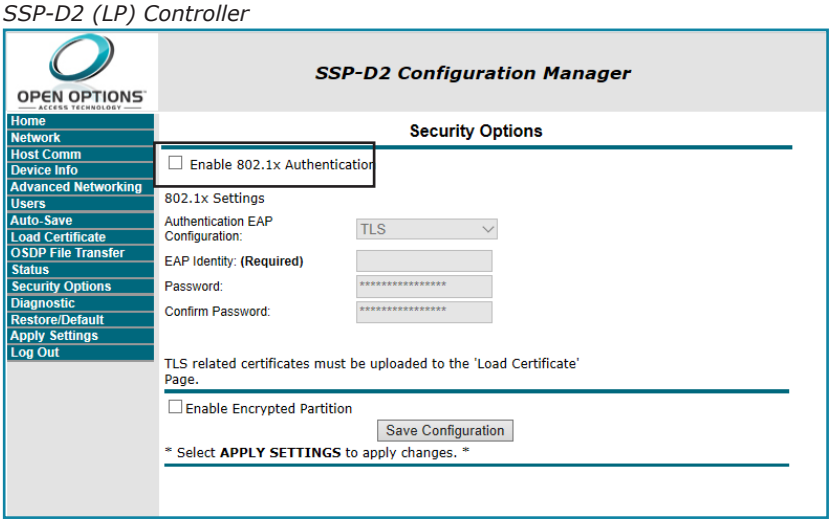


> *If TLS is used, the controller certificates must be signed by the same root certificate used by the authentication server.*

Once the controller is able to communicate using a browser, complete the following steps:

1. In the Configuration Manager webpage, **select** Security Options from the main menu.
2. **Check** Enable 802.1x Authentication.
3. **Enter** the EAP Identity and Password.
   These credentials are based on the authentication server configuration.
4. **Reboot** the controller.
5. **Connect** to the desired LAN/WLAN network.
   The controller is now authenticated using 802.1x.

SSP-D2 (LP) Controller



NOTES:

Controllers

Perform a bulk erase to clear the board of any programming.

1. **Disconnect** power to the board
2. **Set** DIP switches 1 & 2 to ON and 3 & 4 to OFF.
3. **Apply** power to the board.

> ! *CAUTION: Do NOT remove power during steps 4-5.*

4. **Wait** for LEDs 1 & 2 and 3 & 4 to flash alternately at a 0.5 second rate.
5. **Set** DIP switch 1 or 2 to OFF within ten (10) seconds of powering up.

> ⓘ *If neither of these switches are changed, the board reboots using the default OEM communication parameters.*

LED 2 flashes to indicate that the configuration memory is being erased. The full bulk erase takes up to 60 seconds; when complete, LEDs 1 & 4 flash for eight (8) seconds. The board reboots eight (8) seconds after LEDs 1 & 4 stop flashing (all LEDs are OFF during this time).

Downstream Modules

EEPROM Clearing Procedure

Clear the EEPROM from the downstream module(s) to erase existing program. This procedure does not work for NSC-100s.

1. **Set** all DIP switches to OFF.
2. **Cycle** power.
3. Within three (3) seconds of applying power, **set** DIP switch 8 to ON.
4. After the board's power-up sequence is finished, **set** the DIP switches to the correct state.

NSC-200 Board Bulk Erase

Perform a bulk erase to delete the information from the NSC-200.

1. **Disconnect** power to the board.
2. **Set** DIP switches 1 & 2 ON, 3 & 4 OFF.
3. **Apply** power to NSC-200.

> ! *CAUTION: Do NOT remove power during step 4.*

4. **Wait** for LEDs 1 & 2 and 3 & 4 to alternately flash at a 0.5 second rate.
5. **Set** DIP switches 1 or 2 to OFF within ten (10) seconds of powering up.

> ⓘ *If neither of these switches are changed, the board reboots using the default OEM communication parameters.*

LEDs 1 and 2 alternately flash at a 0.05 second rate while the memory is erased. Once the memory is erased, LED 1 will be on for about 3 seconds and then the NSC-200 will reboot.

NOTES:

SSP (EP Series) Controller

The table below describes the ports used by the SSP (EP) controllers. The NSC-100 and NSC-200 ports are discussed separately on page 18.

Port	Port Type	Usage	Disable
67	UDP	DHCPS	No
68	UDP	DHCPC	No
80	TCP	HTTP	Yes – Check Disable Web Server in the Users screen of the internal webpage.
161	UDP	SNMP	Yes – Check Disable SNMP in the Users screen of the internal webpage.
443	TCP	HTTPS	Yes – Check Disable Web Server in the Users screen of the internal webpage.
3001	TCP	Mercury Host Protocol (MSP2)	Yes – Set the Connection Type field in the Host Comm page to an option other than IP.
4001	TCP	PSIA	
5353	UDP	Zeroconf (Discovery)	Yes – Check Disable Bonjour in the Users screen of the internal webpage.

Configure the Mercury Host Protocol (MSP2) to use a different port; the default is 3001.

SSP (LP Series) Controller

The table below describes the ports used by the SSP (LP) controllers.

Port	Port Type	Usage	Disable
67	UDP	DHCPS	No
68	UDP	DHCPC	No
80	TCP	HTTP	Yes – Check Disable Web Server in the Users screen of the internal webpage.
161	UDP	SNMP	Yes – Check Disable SNMP in the Users screen of the internal webpage.
443	TCP	HTTPS	Yes – Check Disable Web Server in the Users screen of the internal webpage.
3001	TCP	Mercury Host Protocol (MSP2)	Yes – Set the Connection Type field in the Host Comm screen to an option other than IP.
4001	TCP	PSIA	
5353	UDP	Zeroconf (Discovery)	Yes – Check Disable Bonjour in the Users screen of the internal webpage.
47808	TCP	BACnet	Yes – BACnet is disabled by default.
47307	UDP	OTIS	Yes – Only used when the OTIS integration is enabled.
48307	UDP	OTIS	Yes – Only used when the OTIS integration is enabled.
45303	UDP	OTIS	Yes – Only used when the OTIS integration is enabled.
46303	UDP	OTIS	Yes – Only used when the OTIS integration is enabled.
46308	UDP	OTIS	Yes – Only used when the OTIS integration is enabled.
45308	UDP	OTIS	Yes – Only used when the OTIS integration is enabled.
10200	TCP	pivCLASS Embedded	Yes – Configure through the pivCLASS embedded web configuration page.

NSC-100

The table below describes the ports used by the NSC-100 subcontroller.

Port	Port Type	Usage	Disable
3001	TCP	Mecury SIO Communication Protocol (MSP1)	No

NSC-200

The table below describes the ports used by the NSC-200 subcontroller.

Port	Port Type	Usage	Disable
161	UDP	SNMP	Yes - Off by default. Configure through the web configuration page
443	TCP	HTTPS	Yes - Use Disable Web Server from the Users web configuration page.
3001	TCP	Mercury SIO Communication Protocol (MSP1)	No
5353	UDP	Zeroconfig (Discovery)	Yes - Use the Disable Bonjour option from the Users web configuration page.

This Page Intentionally Left Blank


OPEN OPTIONS®
ACCESS TECHNOLOGY