Open Options
P.O. Box 703822
Dallas, TX 75370

O: 972.818.7001
F: 972.818.7003

www.ooaccess.com

March 26th, 2021

Newport Mesa Unified School District

Attn: Mr. Jonathan Geiszler

2985 Bear St., Bldg. A
Costa Mesa, CA 92626

Open Options Response to the Request for Information #104-21

Install and Implementation of Districtwide Integrated Security System.

Open Options is a manufacturer of access control software solutions and our product is installed and serviced by local authorized resellers who are trained and certified on our products. We are confident that our products and support, both through the Open Options Team and that of our resellers. Open Options also allows our end users to get trained and certified on our products as we know it's critical to large customers to have expertise on solutions in house. Open Options will consider a customized approach for Newport Mesa's needs, as a substitute to our standard business practices.

We hereto commit to the information detailed in this response being true and correct.

Respectfully,

Scot Sturges | Director of Business Development, US

Open Options | ssturges@ooaccess.com | Office: 972-818-7001 | Cell: 214-564-6396

16650 Westgrove, Suite 150

Addison, TX

75001

972.818.7001

Open Options
P.O. Box 703822
Dallas, TX 75370

O: 972.818.7001
F: 972.818.7003

www.ooaccess.com

Cover Letter

01- Tab 1 Executive Summary
02- Tab 2 Solution Narrative
03- Tab 3 Copy of RFI
04- Tab 4 RFI Responses
    a. K-12 References and Open Options Local Integrators
    b. Budgetary Costs Based on Exhibit A
05- Supplemental Data
    a. DNA Fusion Datasheet
    b. DNA Client-Web-Thick-Mobile Comparison
    c. Education infographic
    d. FlexAPI
    e. Fusion ID
    f. Fusion Mobile
    g. Fusion Web
    h. Intrusion Detection/Alarm Panels
    i. Lockdown Procedures in DNA Fusion
    j. OO+ Zenitel Infographic
    k. OpenDX
    l. System-Hardening- Guide

Open Options
P.O. Box 703822
Dallas, TX 75370

O: 972.818.7001
F: 972.818.7003

www.ooaccess.com

March 26th, 2021

Newport Mesa Unified School District

Attn: Mr. Jonathan Geiszler

2985 Bear St., Bldg. A
Costa Mesa, CA 92626

Request for Information #104-21

Install and Implementation of Districtwide Integrated Security System.

Dear Mr. Geiszler,

Open Options is pleased to participate in the Request for Information #104-21 process.

Open Options, headquartered in Addison, Texas is a pioneer in the access control open-platform community. We are focused on helping improve security by building trust and providing the most connected experience for our customers. Our company is a leading provider of innovative access control solutions with the most experienced, highly qualified service and support teams in the industry. Open Options' flagship access control platform, DNA Fusion, seamlessly connects with leading security technologies — including video, biometrics, wireless locks, and more — to provide customers with a best-in-class security solution. Our customer-first, open business culture and dedication to customer care is how we stand apart from others in our space.

Open Options was founded in 1997 and operated as a privately held, independent entity until November of 2018, at which time the company was acquired by ACRE (Access Control Related Enterprises). ACRE is a private equity backed global leader in the delivery of integrated, intelligent technologies and services. Founded in 2012, ACRE has played an instrumental role in development and implementation of security technology initiatives on a global scale.

Open Options products are available through our network of Authorized Dealers who sell, install, support, and maintain our solutions. Open Options has resources to supplement our resellers that include: Professional Engineering Services, Custom Solutions, Remote Managed Services, End-User Training and certification, and Technical Support Services. As a company based locally in Addison, Texas, all of our development and support resources are local to DFW Airport. With our factory resources based locally, we will provide a dedicated team from Open Options as part of our proposal that will help ensure a seamless physical access control upgrade for DFW Airport.

For over 20 years, Open Options has built an access control platform that connects information and technology to deliver a fully scalable solution based on each customer's unique requirements. Open Options is known for:

- Rapid development of solutions
- Customer-driven feature enhancements
- Adapting to customers' existing & evolving technology environment
- World class tech support and customer support

Open Options is committed to providing our customers new and innovative solutions. For instance, our recent developments in mobile credentialing and next generation thin client application drives operational efficiencies for our customers. Our customer focus is exemplified by our backwards compatibility with hardware and software which allows our customers to retain their investments for decades to come.

We work closely with our customers who operate in highly regulated environments and who have varied requirements across their facilities both in the US and abroad. We currently are the system of choice by many government and critical infrastructure companies. Our solutions support our customer's goals of having a corporate badge across all facilities, a common (single) database for all access control locations, a flexible API that provides a powerful data interface, and a robust reporting and alarm management engine built for high volume and maximum efficiency.

The DNA Fusion platform is engineered for scalability and can support an unlimited number of cardholders, card readers, and client workstations on a single server. Deployments can be supported in virtual environments, clustering configurations, and much more.

Open Options has built its brand on developing the most feature rich access control platform in the market. Our company name speaks volumes to our focus. We provide open technology solutions that allow customers to connect to other technologies unique to their environment.

Our open business culture and dedication to service and support are what set us apart; when you do business with Open Options, you're doing business with people who genuinely care about your experience. We are confident that Open Options is the right choice for Newport Mesa's access control needs. We trust our response to this inquiry is acceptable, and accurately conveys the value our solutions offer our clients. We welcome the opportunity to meet with the Newport Mesa's team and your supporting staff, to share more information about our company, our unique value-proposition, and our approach to ensure this replacement and upgrade is a success.

Sincerely,

Scot Sturges | Director of Business Development, US | Open Options | ssturges@ooaccess.com

Office: 972-818-7001 | Cell: 214-564-6396

Open Options
P.O. Box 703822
Dallas, TX 75370

O: 972.818.7001
F: 972.818.7003

www.ooaccess.com

Open Options delivers our software, services or hardware through authorized dealers in each market, so our approach would involve Newport Mesa, the Open Options support team and the selected Open Options dealer. When Newport Mesa implements a migration to Open Options', DNA fusion software is fairly straight forward.
Below we have outlined the steps that typically transpire to ensure a successful implementation:

1. Traditional RFP with Site Survey for the dealers to assess the existing infrastructure
2. Award to Open Options dealer. The awarded dealer would meet with Newport Mesa to create a project schedule to transition existing systems and hardware over to the new DNA Fusion system. The project schedule should address:
    a. Timelines, planning, integration requirements, desired operational functionality.
    b. Proposed phases and major milestones.
    c. Completion of project within Newport Mesa's desired timeframes (full implementation by "xx" days from Effective Date of Contract.
    d. Details regarding number of resources for each major activity
    e. Details regarding knowledge transfer to specified end user's employees and/or designated representatives.
    f. Data transition.
    g. Plan for assessment of current database, new database, and corresponding level of effort for migration.
    h. Planned approach for consulting/working with vendor of the current systems
    i. Identification of risks to successful project completion; and proposed mitigation strategies
3. Once a plan is in place the dealer would setup the new DNA Fusion Server
4. Program the required readers, time zones and access levels into the DNA Fusion system
5. The dealer would leverage the project schedule to transition existing controllers over to the new Mercury panels
6. Test and do final programming of the Mercury controllers
7. Depending on the quality of Newport Mesa's current access control database, the district can decide if they want to leverage the existing cardholder database and have Open Options' Professional Services Team perform a database conversion of the cardholder records of the existing systems.
    a. Import the converted cardholder data into the new DNA Fusion system
    b. If the customer didn't want to leverage their existing database, Open Options could assist with an Active Directory integration to populate cardholders into DNA Fusion system with access rights based on their job description.

8. The dealer would start to decommission existing door hardware and replace with new Mercury controllers
9. Test each card reader door on that new controller to make sure it is functioning properly
10. Continue this process based on the project schedule until all existing controllers are decommissioned.

Solution Architecture.

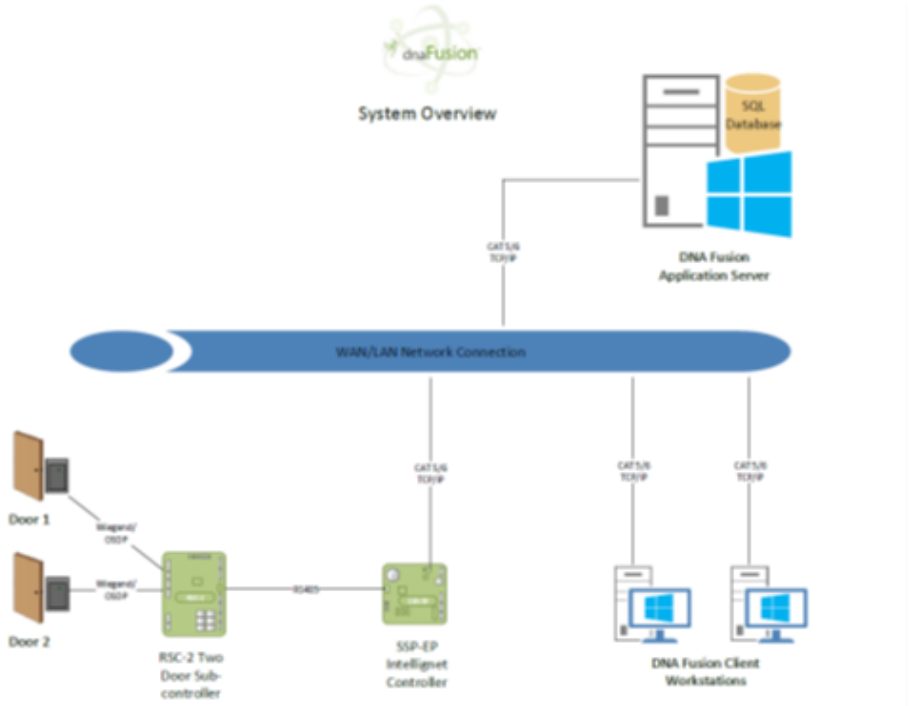
The image below, *Image 1: DNA Fusion Network Architecture*, depicts the proposed network architecture to implement DNA Fusion. The proposed architecture is one option based on the information provided in the RFI documents, but could change during deployment.

The details of Image 1 show only the relevant components for DNA Fusion and do not list any network infrastructure components. It is assumed that the current network infrastructure will remain in place and that DNA Fusion and other components will reside on the same.

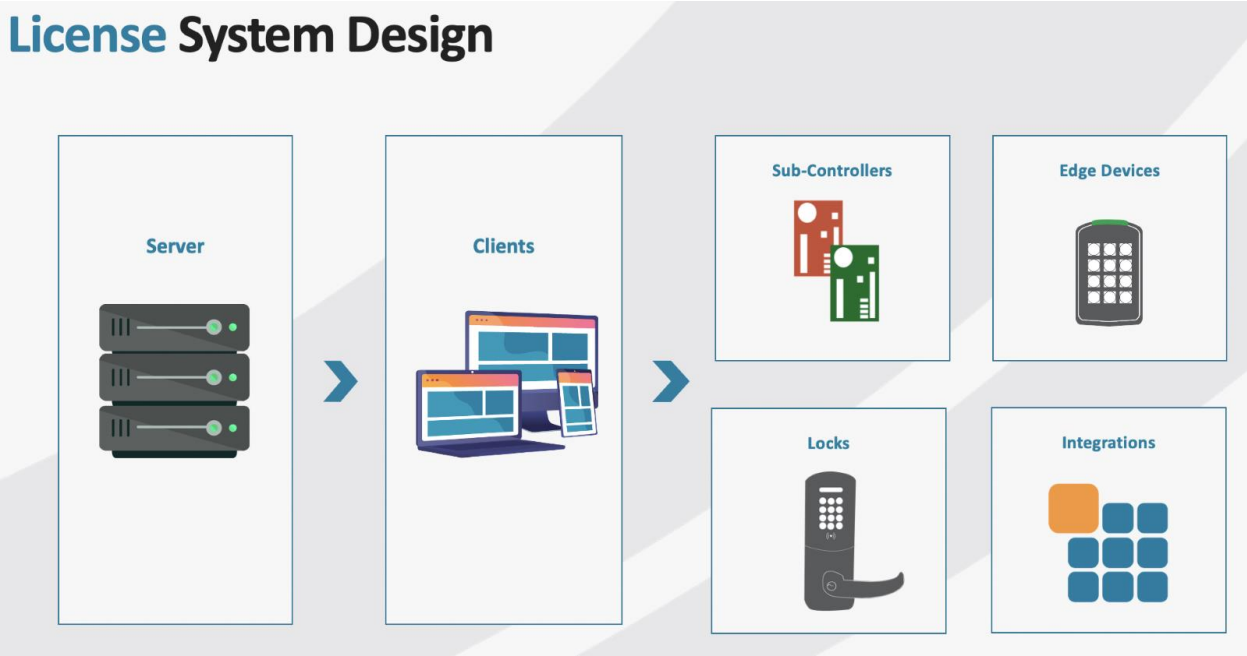
It is assumed that the respective Production and potential Training/Testing servers all will be virtualized and run on Newport Mesa's current VMWare solution.

The server must run Microsoft Windows Server 2016/2019 Standard edition as well as Microsoft SQL Server 2017/2019.

Image 1: DNA Fusion Network Architecture



DNA Fusion Licensing



At Open Options we take a simplified approach to software licensing that enables our customers to have the best experience with our products without the costly headaches of complex software licensing. The simplified model consists of the server, clients, sub-controller (readers), edge devices, wireless locks, and integrations. Below are the key value points that allow our customers the freedom to choose their software options that best fit their needs and budget:

Single Software platform with a consistent pricing model. We do not penalize a customer through higher license fees for having a larger size system. Our licensing options and price are consistent regardless of system size.
(No Small, Medium or Large sizes)
Software that is a full featured scalable solution. Regardless of system size our software comes fully featured.
License per device or integration as needed – if the customer needs to add just one reader, they can buy a single reader license with the hardware.
There is no force bulk purchasing
Unlimited Video Management Integrations. Open Options does not charge video channel license fees. There is a one-time connector charge to turn the VMS integration on, and from that point forward, the video integration has unlimited camera channels.
no per channel licensing fees
Lower integration costs (Active Directory, API Utilization, Custom Functions, etc.) We are often told by our customers that we have the best value when it comes to integration and customization.
Independent service and license for each integration, this is important when that particular service can be upgraded without upgrading the entire application.

DNA Fusion API



As it relates to Open Options API and connecting information with DNA Fusion, we have a couple options. The first option is our OpenDX software which provides an easy-to-use interface for configuring the data you want to transfer into the DNA Fusion. This is a powerful tool that removes the time-consuming task of manually entering data across all of your various business systems; saving customers time and valuable resources. OpenDX performs automated data transfers from any valid data source.

Additionally, you can connect information through our FLEX API. FlexAPI is a clean and easy-to-use application programming interface for developing third-party integrations into DNA Fusion. Our FLEX-API provides robust function options and data exchanges. Flex-API is full featured on the information side to add / remove access levels, change personnel records, receive acknowledge events / alarms, status of hardware, etc.

We have a robust library of samples that help implementation such as:

- Access levels
- Personnel tree
- Events (Polling/Get method)
- Subscription based events.
    - The Flex API will send events and alarms directly to you.
    - Also demonstrates alarm handling
- Hardware tree with status (this duplicates the hardware tree as seen in DNA Fusion)
    - This also demonstrates how to control hardware, for example, change the door modes or momentarily unlock a door.

- Personnel, how to search, add, modified delete as well as assign credentials and access levels to them.
- Sending Events to DNA
- Viewing cameras

Open Options offers assistance with our API through our tech support and development team. We firmly believe in assisting our customers in getting the most out of their investment by leveraging the data and interoperability between their existing technology environment.

DNA Fusion Training

Open Options offers extensive education tools for new and continuing students. Training by Open Options is a highly respected program with state-of-the-art training methodologies available online and on site. Our training services are designed to enable the student to competently manage, program, configure and operate the product that will meet or exceed their expectations. Most courses are a combination of lecture/lab instruction with emphasis on hands-on lab activities. Operational up-to-date system software & hardware simulates actual customer environment wherever practical.

The Open Options training and certification program consists of three levels: DNA Fusion Essentials, DNA Fusion Intermediate, and DNA Fusion Advanced.

Certifications are personal and valid for 3 years. As long as the Open Options dealer/end user maintains at least one certified person on staff then the company will remain certified.

To maintain your Open Options Certified status, you will be required to complete one of the following recertification options every three years:

Attend one Open Options training every three years. (on-line recertification would be available).
Re-take and pass all exams for each certification level attained (on-line).

We offer the following courses to end users and dealers at Open Options Corporate office in Addison, TX:

Essentials Training: 3-day class
Door Essentials: 1-day class
Intermediate Training: 3-day class
Advanced Training: 3-day class
Badging Training: 1-day class
Graphic Map: 1-day class

NEWPORT MESA UNIFIED SCHOOL DISTRICT

Newport-Mesa
Unified School District

REQUEST FOR INFORMATION
#104-21

INSTALL AND IMPLEMENTATION OF
A DISTRICTWIDE INTEGRATED SECURITY SYSTEM

INFORMATION DUE DATE
Monday, April 5, 2021, at 4:00 p.m.

SUBMIT RESPONSES TO:

Jonathan Geiszler

Director of Purchasing & Warehouse
NEWPORT MESA UNIFIED SCHOOL DISTRICT
2985 Bear St., Bldg. A
Costa Mesa, California 92626

Copyright © 2021 by NMUSD. All Rights Reserved.

Executive Summary

Newport Mesa Unified School District (NMUSD) (District) is seeking a new security system to consolidate and integrate access control, alarm monitoring, and security video surveillance systems for the District. The District has identified and documented the requirements for this new system. The primary goal for this Request for Information (RFI) is to identify system manufacturers that meet the District's requirements and can be successfully deployed and maintained by the District's maintenance staff. This RFI does not include evaluations of integrators but will evaluate how manufacturers provide support to customers such as the District that maintain their own systems and the level of support provided directly by the manufacturer versus through their integrators. Integrators and the total costs associated with purchasing and maintaining systems will be evaluated after completion of the RFI submission evaluation.

This Request for Information (RFI) has been developed to solicit a range of data relative to various aspects to be considered. This RFI is aimed at helping NMUSD understand the range of vendors involved in this space.

Organization Background

Unified in 1966, The Newport-Mesa Unified School District covers 58.83 square miles in Orange County California, employs approximately 3200 staff and educators, educates approximately 22,000 students and is composed of thirty-two (32) schools: twenty-two (22) elementary schools, two (2) intermediate schools, two (2) 7-12 Middle/High Schools, two (2) 9-12 high schools, four (4) alternative education programs.

Intent of this RFI

Through the release of this RFI the District seeks to gain more information on how the following items can work as a unified system to create a comprehensive Districtwide security platform. These items are a summary of potential requirements and specifications but may be modified as information is received to help create a solution that best fits the District's needs. The District does not intend to award any contracts based on the receipt of this RFI, RFI data will be used to build comprehensive Bid and RFP packages for the ultimate purchase and installation of the Districts final security system platform.

I. General Requirements

A. Deploy systems and integration with the best value to the District

B. Implement proven and reliable technology

C. High to medium-high system maturity level

D. Scalable

E. Flexible – communication/technology issues at individual schools. Some have better connections than others.

Copyright © 2021 by NMUSD. All Rights Reserved.

F. Serviceable by NMUSD staff

G. Simple and efficient integration

H. Support for wireless solutions

I. Compatible with District's HP servers

J. Deployable in a virtual server environment

K. Active Directory integration

L. Multiple local integrators (single regional integrator is not acceptable)

M. Direct manufacturer support

N. No sole source equipment

O. Strong cyber-security support – Manufacturer responses must discuss cyber-security plan in response and also explain how firmware updates are performed.

P. No biometrics

Q. Audio capability

1. Voice communication capability desired but voice recording will be disabled per District policy

`

II. Access Control

A. Access control technology not susceptible to cloning

B. Proximity technology access cards (contactless smartcards)

C. Support for wireless solutions

D. Lockdown controls

E. Integration with Intrusion Detection Systems

F. <u>Consideration for future Cloud deployment</u>

G. Mercury Security or similar intelligent panels available to multiple manufacturers (panels supported by only one system software manufacturer are not acceptable)

III. Video Surveillance

A. Consider integration with Police Department

Copyright © 2021 by NMUSD. All Rights Reserved.

B. Local video recording server at each site

C. Redundancy/backup

D. Public monitor in admin waiting area

E. Support for video analytics

IV. Video Recording

A. Standard video compression (H.264/H.265)

B. 45 days recorded video

C. Motion sense recording

D. 5-10 frames per second recording rate

V. Video Cameras

A. Vandal resistant camera housings that conceal direction of view

B. Minimum 3 Megapixel resolution

C. Onboard storage

VI. Intrusion Detection

A. Support existing Ademco/Honeywell systems

B. Integration with the Access Control System to provide for disarming the Intrusion Detection by presenting access credentials to record an audit trail.

Response Format & Submission Instructions

Three (3) copies of RFI Responses shall be submitted in 8.5"x11" format and with tabs separating each section and (1) one digital PDF file, folders and subfolders instead of sections and tabs; file names beginning with two-digit numbers and document descriptions to sort information within folders and simplify searches through the documents; an index sheet with hyperlinks to specific documents.

Complete and well-organized information is crucial. All information shall be arranged in the following order:

a. A Title page that indicates:
   - The name, address and telephone number of the Vendor

Copyright © 2021 by NMUSD. All Rights Reserved.

- The date of the submission
- A statement that the information is in response to this RFI
- The name, title, telephone number and e-mail address of the contact person responsible for the Vendor's response.

b. Each Response must include a certification from an individual authorized to represent the Vendor:
   - That the statements made in the Vendor's Information are true and correct

c. Executive Summary not exceeding three pages, including overviews of:
   - The Respondent's perspective of what major solution attributes differentiate their offering from that of competing solutions.
   - The Respondent's ability to support initial deployment as well as ongoing management and/or maintenance of the solution on a global basis, including whether such abilities would be provided directly and/or via authorized partners.
   - The Respondent's perspective relative to its business prospects as they pertain to long-term viability and industry rank. Such discussion shall include business direction, research & development, financial health, industry rank, and other aspects as appropriate.

d. A Solution Narrative consisting of diagrams illustrating the basic functionality of the proposed security system:

   - Each component included within the diagrams shall be defined via a glossary.
   - As appropriate, diagrams illustrating optional functionality must also be submitted; such alternatives shall be accompanied by a brief discussion of the pros and cons associated with each option, contrasted with the pros and cons of the submitted primary design.
   - It is requested that this section be limited to no more than 15 pages.
   - Industry specialties not addressed in this RFI
   - Unique industry strategies not addressed in this RFI
   - Training and support for District staff to install, troubleshoot and maintain the system.

e. A complete and detailed copy of the RFI, including all information, questionnaire and binding signatures as indicated:
   - To the extent clarifications to this RFI are issued by NMUSD (typically via email), printed copies of each and every such clarification shall also be included within this section.

f. Additional RFI Response Requirements as described below:
   - A summary of similar and completed solution deployments in K-12 schools with a

Copyright © 2021 by NMUSD. All Rights Reserved.

20,000 ADA or higher. Each preferably having similar functional requirements as well as being deployed and managed/maintained on a regional basis.

- This information shall also include contact names, telephone numbers and email addresses for each discussed customer.
- Please provide budgetary costs for purchasing the proposed security solution for NMUSD. Such costs should be at list price including all options described. Estimates should be based on complete integration at all facilities Districtwide. Please describe your pricing model and pricing options including implementation costs and ongoing support (based on the Summary Budgetary Cost Response Tables herein below). Examples of actual projects are provided in Exhibit A.
- Any other documentation as required by the RFI document.

g. Supplemental Data as desired by Respondent:
   - Descriptive Marketing Documents and other material as available describing the proposed components.

Evaluation Criteria

The purpose of the RFI process is to select manufacturers that best suit NMUSD's security system goals to implement an integrated security system. Although price will be a large factor in the District's decision, a price comparison will be more effective in the next selection phase that includes integrators and total cost of ownership through a competitive pricing exercise. The evaluation of the RFI responses will focus on technical capabilities of the proposed systems and the ability of the manufacturers to support the District directly. The following are evaluation criteria and points awarded for each.

Criteria	**Points**
1. General Requirements	
a. Serviceable by NMUSD staff	20
b. High to medium-high maturity level	10
c. Scalability	10
d. Strong cyber-security support	10
e. Other general requirements	5
2. Access Control	20
3. Video Surveillance, Recording, and Cameras	

Copyright © 2021 by NMUSD. All Rights Reserved.

a. Local video recording server at each site	10
b. Support for video analytics	5
c. Other video surveillance requirements	5
4. Intrusion Detection	5

Additionally, not all requirements are mandatory. Solutions should meet the requirements provided, however, interested vendors are encouraged to provide responses.

a. To be considered by the NMUSD, each response must include a response to each section of the RFI intent section of this document.

- Any information believed to be relevant may be submitted by each Vendor as an appendix to the information, but should not be included in the answers unless responsive to the specific question.
- References to supplemental materials should be included in a response.
- All information necessary to respond to the question should be included in the response.

b. Vendors that have questions regarding this RFI should submit them in writing to Jonathan Geiszler, Director, Purchasing & Warehouse at jgeiszler@nmusd.us

- No questions will be answered after Friday March 26, 2021.
- Requests for information will be accepted no later than Monday March, 22 2021
- Questions will be answered prior to Friday March 26, 2021
- No telephone calls will be accepted relative to this RFI
- Do not contact school board members, or other district employees, administrators or representatives of the district about this solicitation.

c. Vendors should send three (3) paper copies and one (1) digital copy of their completed information to:

Jonathan Geiszler
Director, Purchasing & Warehouse
Newport Mesa Unified School District
2985 Bear St., Bldg. A
Costa Mesa, CA 92626

Copyright © 2021 by NMUSD. All Rights Reserved.

d. Vendor should follow the document instructions:
   - All documents must be delivered to the above address no later than 4:00 P.M. on Monday, March 1, 2021.
   - All RFI's shall be sealed, the envelope marked as to the RFI name and number, and delivered to the Purchasing Department, 2985 Bear St., Bldg. A Costa Mesa CA 92626, on or before the date stated herein.
   - Receipt in the District Education Center Office before this hour must be actual. Postmarking prior to this hour will not suffice.
   - All RFI's received after the established time and date for receipt will be returned to the sender unopened.
   - Responders who mail their RFI should allow sufficient time for the internal distribution of mail within the district.
   - Materials sent via facsimile or e-mail will not be considered

`

Copyright © 2021 by NMUSD. All Rights Reserved.

Exhibit A

TYPICAL EXTERIOR GATES

1. A pair of conduit pathways is provided to all exterior gates from the nearest available IDF. See attached drawings for examples.

2. A card reader will be required for entrance and exit at each pedestrian gate. Gates have a Locinox Mammoth or similar closer and Securitron GL1 electrified latch (alternates must be identified if Proposer's equipment is not compatible with existing hardware). Exterior gates include the following entries:

   - Elementary:
     - Primary entrance – Two swing gates
     - Primary entrance – Two rolling gates
     - Secondary entrance – Single swing gate
   - Intermediate:
     - Primary entrance – Two pairs of swinging gates
     - Secondary entrance – Two pairs of swinging gates
   - High School:
     - Primary entrance – Two pairs of swinging gates
     - Secondary entrance – Two pairs of swinging gates
     - Athletic use entrance – Two pairs of swinging gates
     - Stadium
     - Pool

3. Vehicle/fire lane gates are motorized and will require proximity card or other verifiable electronic access and unhindered access for first responders in the case of an emergency.

   - One vehicle entrance per school

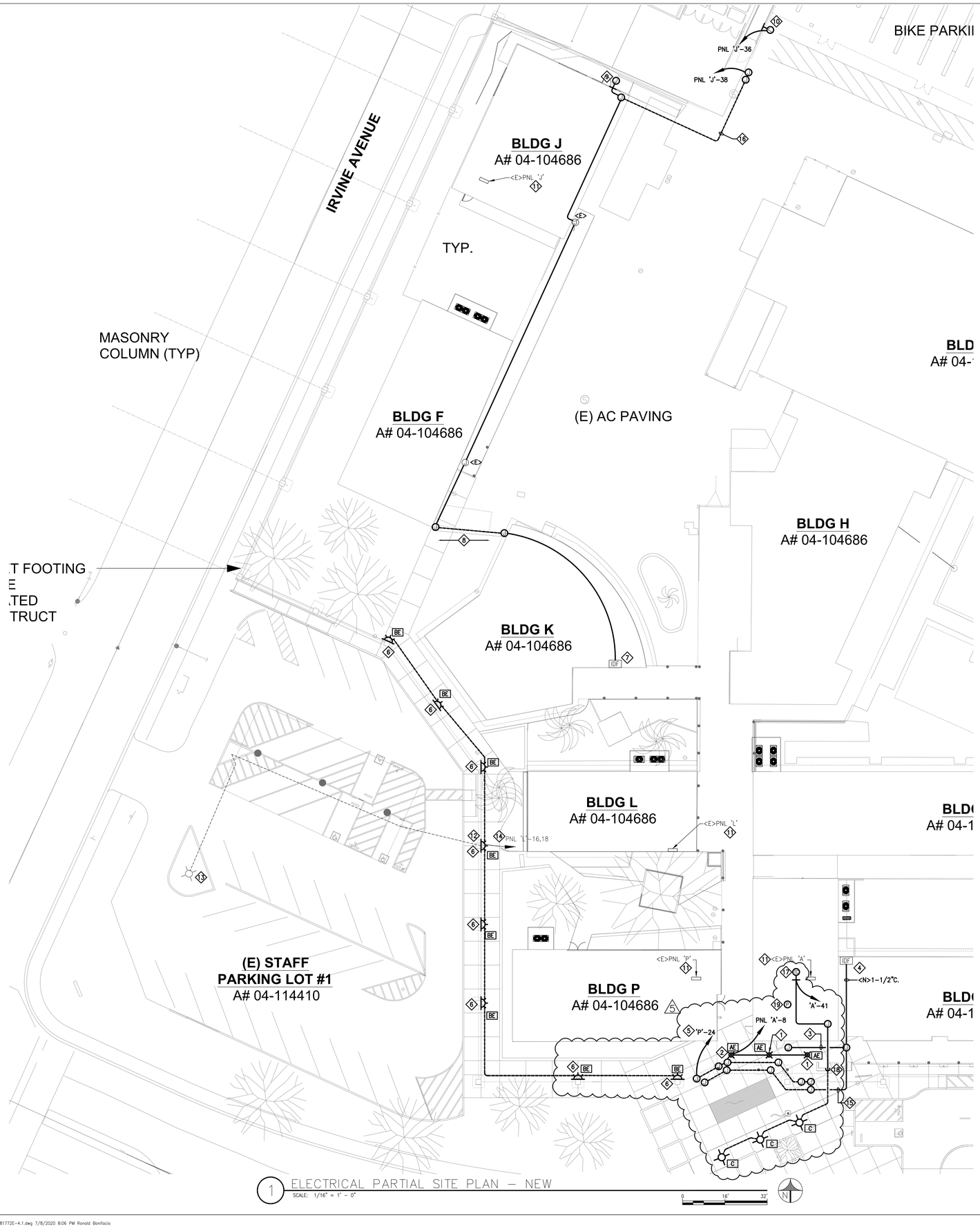
TYPICAL DOOR CONTROLS

1. High security doors and entrances to the following areas must have proximity card readers. Typical installations include hollow metal, solid wood or store front doors.

   Multiple devices may be required to provide the appropriate level of security. In lieu of using a proximity card reader, Proposer may identify entrances that could be secured by other means without hindering safe egress. For instance, if there are multiple doors leading into the gymnasium, only one door would be provided with a proximity card reader to control access while the rest of the doors could be opened from the inside and placed in passage by "dogging down" the panic bar.

There is no existing pathway or conduit provided for doors:

- Elementary School:
    - Exterior Doors:
        - Main Office
        - Kitchen
        - Technology Lab
    - Interior Doors:
        - File room in the office
- Intermediate School:
    - Exterior Doors:
        - Main Office
        - Kitchen
        - Technology Lab
        - Gymnasium
    - Interior Doors:
        - File room in the office
- High School:
    - Exterior Doors:
        - Main Office
        - Kitchen
        - Technology Labs (3 at each high school)
        - Gymnasium (2 gyms at each high school)
        - Theater
        - ASB Room
        - Stadium Control Booth
    - Interior Doors:
        - ASB Room
        - Theater Control Room
        - Black Box Control Room
        - Theater Equipment/Utility Room
        - Athletic Equipment Storage
        - Records/Archive Room (3 at each high school)
        - Kitchen Office
        - Campus Safety Office



1 ELECTRICAL PARTIAL SITE PLAN – NEW
SCALE: 1/16" = 1' – 0"

GENERAL SHEET NOTES

A. INSTALL A PULL BOX FOR EVERY 270 DEGREES OF CONDUIT BENDS AND WHERE THE PULLING TENSION ACHIEVED WOULD EXCEED THE MAXIMUM ALLOWABLE FOR THE CABLE TO BE INSTALLED.

B. CONTRACTOR SHALL FIELD VERIFY ALL EXISTING AFFECTED UNDERGROUND CONDUITS AND JUNCTION BOXES.

C. COORDINATE WITH ARCHITECT AND STRUCTURAL ENGINEER FOR MOUNTING LOCATION OF WEATHERPROOF GFCI RECEPTACLES.

D. CONTRACTOR SHALL COORDINATE WITH THE DISTRICT FOR TEMPORARY POWER REQUIREMENT.

E. CONTRACTOR SHALL SCAN CONCRETE PRIOR TO CUTTING TO PREVENT CUTTING REBAR.

F. ALL INDOOR CONDUITS SHALL BE CONCEALED IN WALL/TILES/CEILING.

REFERENCE SHEET NOTES

1. FURNISH AND INSTALL SURFACE-MOUNTED LIGHTING FIXTURE UNDER CANOPY. INTERCEPT AND EXTEND POWER CONNECTION.
2. CONTRACTOR SHALL RUN 2#12,1#12GND. POWER CONNECTION ABOVE CANOPY AND THRU CANOPY TO SURFACE-MOUNTED LIGHTING FIXTURE.
3. CONTRACTOR SHALL FURNISH AND INSTALL 3/4"C WITH CAT-6E CABLE FROM SECURITY CAMERA TO IDF IN BUILDING 'A'. CONTRACTOR SHALL FIELD VERIFY EXACT ROUTING. VERIFY WITH ARCHITECT FOR LOCATION OF CAMERA. CONDUIT SHALL BE CONCEALED IN WALL/TILES/CEILING.
4. CONTRACTOR SHALL COORDINATE WITH NMUSD IT DEPARTMENT FOR TERMINATION POINT FOR IDF IN BUILDING 'A'.
5. PROVIDE DEDICATED 120V CIRCUIT FOR ACCESS CONTROL PROXIMITY READERS AT GATES AND GATE POWER SUPPLIES FROM PANEL 'P'.
6. CONTRACTOR SHALL FURNISH AND INSTALL COLUMN-MOUNTED LED WALL PACK. CONTRACTOR SHALL COORDINATE WITH ARCHITECT FOR EXACT MOUNTING HEIGHT, AND SHALL COORDINATE WITH STRUCTURAL FOR CONDUIT INSTALLATION DIRECTION.
7. CONTRACTOR SHALL COORDINATE WITH NMUSD IT DEPARTMENT FOR TERMINATION POINT FOR IDF IN BUILDING 'K'.
8. RELOCATE (2) EXISTING 4" CONDUITS TO UNDERGROUND. CONTRACTOR SHALL RUN LOW VOLTAGE WIRING IF EXISTING CABLES DO NOT HAVE ENOUGH LENGTH. FOLLOW TRENCH DETAIL FOR CONDUITS DEPTH AND SEPARATION. FIELD VERIFY FOR ALL TERMINATION OF LOW VOLTAGE WIRING.
9. CONTRACTOR SHALL FURNISH AND INSTALL CAT-6E CABLE FROM SECURITY CAMERA TO IDF IN BUILDING 'K' VIA EXISTING TELECOM CONDUIT. CONTRACTOR SHALL COORDINATE WITH ARCHITECT TO VERIFY EXACT ROUTING AND LOCATION OF CAMERA.
10. CONTRACTOR SHALL RELOCATE EXISTING IRRIGATION CONTROLLER TO TRASH ENCLOSURE. REROUTE 120V CIRCUIT WITH 3/4"C. – 2#12 + 1#12 GND. FROM PANEL 'J' AT BUILDING 'J'. COORDINATE WITH NMUSD FOR EXACT LOCATION.
11. SEE PANEL SCHEDULE FOR CIRCUIT BREAKERS REQUIREMENT.
12. INTERCEPT AND EXTEND <E>POWER CONNECTION TO NEW AND EXISTING LIGHT FIXTURES.
13. <E>LIGHT POLE TO REMAIN. PROTECT IN PLACE.
14. REUSE <E>LIGHTING CIRCUIT FOR COLUMN LIGHTS AND <E>LIGHT POLE. FIELD VERIFY FOR EXACT LOCATION. RUN NEW WIRING AS REQUIRED.
15. CONTRACTOR SHALL FURNISH AND INSTALL 1"C. WITH (4) CAT-6 CABLES FROM GATES TO IDF IN BUILDING 'A'. CONTRACTOR SHALL FIELD VERIFY EXACT ROUTING. CONDUIT SHALL BE CONCEALED UNDERGROUND.
16. CONTRACTOR SHALL FURNISH AND INSTALL CAT-6 CABLE FROM GATE TO IDF IN BUILDING 'K' VIA EXISTING TELECOM CONDUIT. INTERCEPT AND EXTEND EXISTING LOW VOLTAGE CONDUIT TO NEW GATE. CONTRACTOR SHALL COORDINATE WITH ARCHITECT FOR EXACT ROUTING.
17. CONTRACTOR SHALL FURNISH AND INSTALL ASTRONOMICAL TIME CLOCK (INTERMATIC #ET90215CE 2 CIRCUITS) FOR BOLLARD LIGHTS WITH 3/4"C. IN EXISTING LIGHTING CONTROL BOX. FIELD-VERIFY FOR EXACT LOCATION.
18. CONTRACTOR SHALL FURNISH AND INSTALL PHOTOCELL ON ROOF. INTERTIE AND CONNECT WITH ASTRONOMIC TIME CLOCK FOR BOLLARD LIGHTS. VERIFY WITH DISTRICT FOR EXACT REQUIREMENT.
19. CONTRACTOR SHALL TRANSITION CONDUIT TO UNDERGROUND DOWN BRICK WALL. SAW CUT HARDSCAPE AND PATCH TO MATCH EXISTING. COORDINATE WITH ARCHITECT FOR EXACT CONDUIT ROUTING. REFER TO DETAIL 1/E5.1 FOR TRENCHING DETAIL.

Agency Approval:

APPROVED
DIV. OF THE STATE ARCHITECT
APP. 04-118248 INC:
REVIEWED FOR
SS ☑ FLS ☑ ACS ☑
DATE: 07/21/2020

studio+
20520 SW Acacia, Suite 100, Newport Beach, California 92660 | P: 949.315.1993

SALASO'BRIEN
|expect a difference|
305 South 11th Street
San Jose, California 95112-2218
408.282.1500 | 408.297.2995 (f)
salasobrien.com
Bozeman | Los Angeles | Monterey
Oakland | Orange County | Sacramento
San Diego | San Luis Obispo | Seattle

Architect/Engineer

REGISTERED PROFESSIONAL ENGINEER
MATTHEW K.T. CHUN
No. E18090
ELECTRICAL
STATE OF CALIFORNIA

LICENSED ARCHITECT
JASON A. DONATE
No. C-32176
REN. 07-31-21
STATE OF CALIFORNIA

Project Title:

ENSIGN INTERMEDIATE SCHOOL
SITE CONTROLLED ACCESS UPGRADES

2000 CLIFF DR
NEWPORT BEACH, CA 92663

Revisions:

	12/11/2019	ADDENDUM 1
	03/27/2020	CCD 1
	05/18/2020	CCD 2
	06/03/2020	CCD 3
4	07/08/2020	CCD 4

Project #: **CA18023 (SOBE #181772)** Drawn: **RB**
Date: **02/19/2019** Checked: **AC**

Sheet Title:

ELECTRICAL
PARTIAL SITE PLAN - NEW

E-4.1

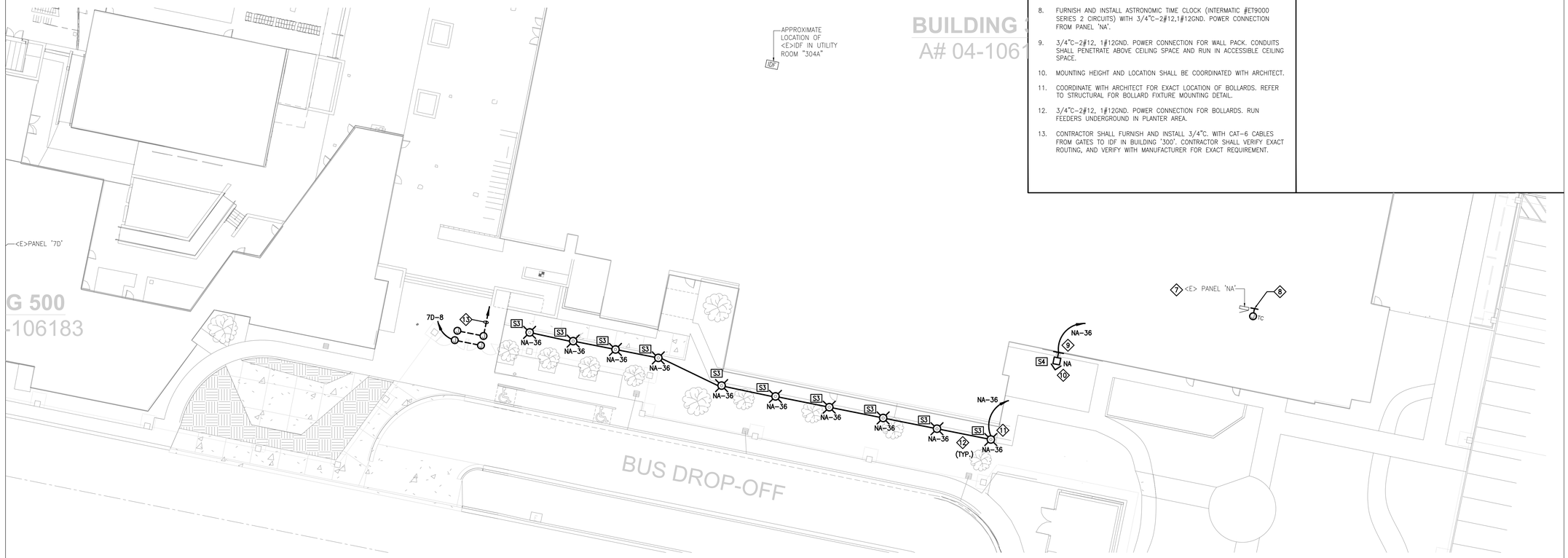
REFERENCE SHEET NOTES

1. EXISTING LIGHTING CIRCUITS HOMERUN. CONTRACTOR SHALL FIELD VERIFY FOR EXACT LOCATION.
2. EXISTING LIGHT POLE TO REMAIN.
3. FURNISH AND INSTALL 3/4"C-3#10,1#10GND. FOR RELOCATED POLE LIGHT.
4. RELOCATE EXISTING LIGHT POLE TO NEW LOCATION. VERIFY WITH ARCHITECT FOR EXACT LOCATION. REFER TO STRUCTURAL FOR CONCRETE BASE MOUNTING DETAIL.
5. RECONNECT EXISTING LIGHT POLE WITH NEW 3/4"C-3#10,1#10GND. POWER CONNECTION.
6. CONTRACTOR SHALL FURNISH AND INSTALL 3/4"C. WITH CAT-6 CABLES FROM GATES TO IDF IN BUILDING '400'. CONTRACTOR SHALL VERIFY EXACT ROUTING, AND VERIFY WITH MANUFACTURER FOR EXACT REQUIREMENT.
7. USE <E>SPARE CIRCUIT BREAKER FOR SITE LIGHTING.
8. FURNISH AND INSTALL ASTRONOMIC TIME CLOCK (INTERMATIC #ET9000 SERIES 2 CIRCUITS) WITH 3/4"C-2#12,1#12GND. POWER CONNECTION FROM PANEL 'NA'.
9. 3/4"C-2#12, 1#12GND. POWER CONNECTION FOR WALL PACK. CONDUITS SHALL PENETRATE ABOVE CEILING SPACE AND RUN IN ACCESSIBLE CEILING SPACE.
10. MOUNTING HEIGHT AND LOCATION SHALL BE COORDINATED WITH ARCHITECT.
11. COORDINATE WITH ARCHITECT FOR EXACT LOCATION OF BOLLARDS. REFER TO STRUCTURAL FOR BOLLARD FIXTURE MOUNTING DETAIL.
12. 3/4"C-2#12, 1#12GND. POWER CONNECTION FOR BOLLARDS. RUN FEEDERS UNDERGROUND IN PLANTER AREA.
13. CONTRACTOR SHALL FURNISH AND INSTALL 3/4"C. WITH CAT-6 CABLES FROM GATES TO IDF IN BUILDING '300'. CONTRACTOR SHALL VERIFY EXACT ROUTING, AND VERIFY WITH MANUFACTURER FOR EXACT REQUIREMENT.

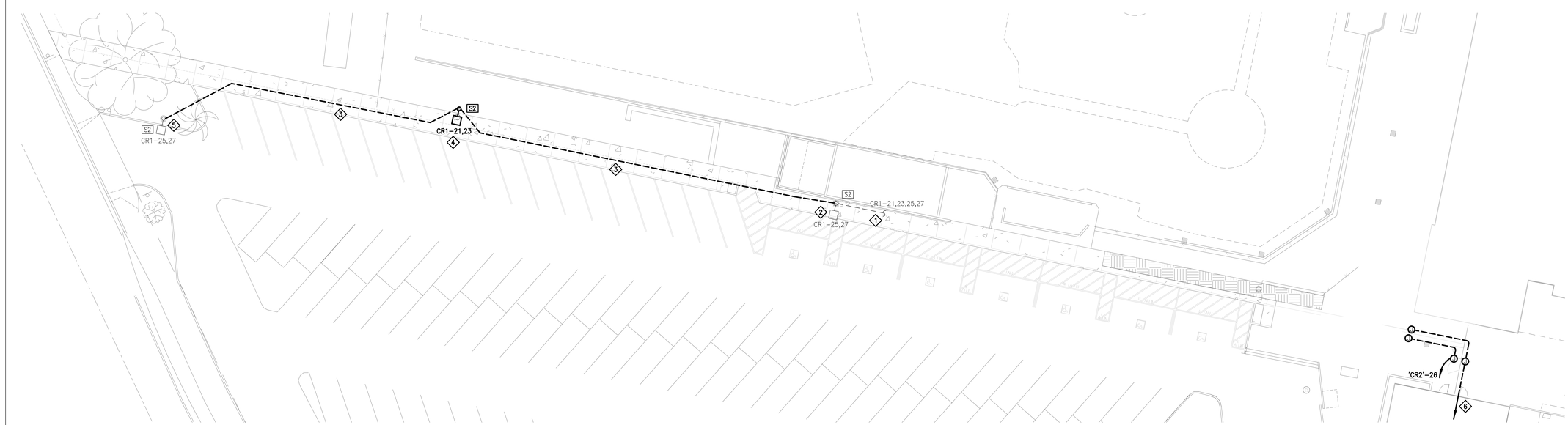
GENERAL SHEET NOTES

A. CONTRACTOR IS RESPONSIBLE TO FIELD VERIFY ALL EXISTING LIGHT FIXTURES LOCATION, UNDERGROUND CONDUITS ROUTING, PULLBOX/JUNCTION BOX/MAN HOLE LOCATION.

B. COORDINATE WITH NMUSD FOR ANY POWER SHUTDOWN OR LIGHTING SYSTEM INTERRUPTION. PROVIDE TEMP POWER, LIGHTING, FIRE WATCH AS REQUIRED BY NMUSD TO MAINTAIN SCHOOL ACTIVITY.



2 SITE PLAN - NEW
SCALE: 1/16" = 1' - 0"
0 16' 32'
N



1 SITE PLAN - NEW
SCALE: 1/16" = 1' - 0"
0 16' 32'
N

Agency Approval:

IDENTIFICATION STAMP
DIV. OF THE STATE ARCHITECT
APP. 04-118247 INC:
REVIEWED FOR
SS ☑ FLS ☑ ACS ☑
DATE: 08.06.19

studio+
20520 SW Acacia, Suite 100, Newport Beach, California 92660 | P: 949.315.1993

SALAS O'BRIEN
expect a difference
305 South 11th Street
San Jose, California 95112-2218
408.282.1500 | 408.297.2995 (f)
salasobrien.com
Bozeman | Los Angeles | Monterey
Oakland | Orange County | Sacramento
San Diego | San Luis Obispo | Seattle

Architect/Engineer

LICENSED ARCHITECT JASON A. BOMAR NO. C32176 REN. 07-31-21 STATE OF CALIFORNIA

REGISTERED PROFESSIONAL ENGINEER GIT KIT CHAN No. E18090 ELECTRICAL STATE OF CALIFORNIA

Project Title:

CORONA DEL MAR HIGH SCHOOL
SITE CONTROLLED ACCESS UPGRADES

2101 EASTBLUFF DR
NEWPORT BEACH, CA 92660

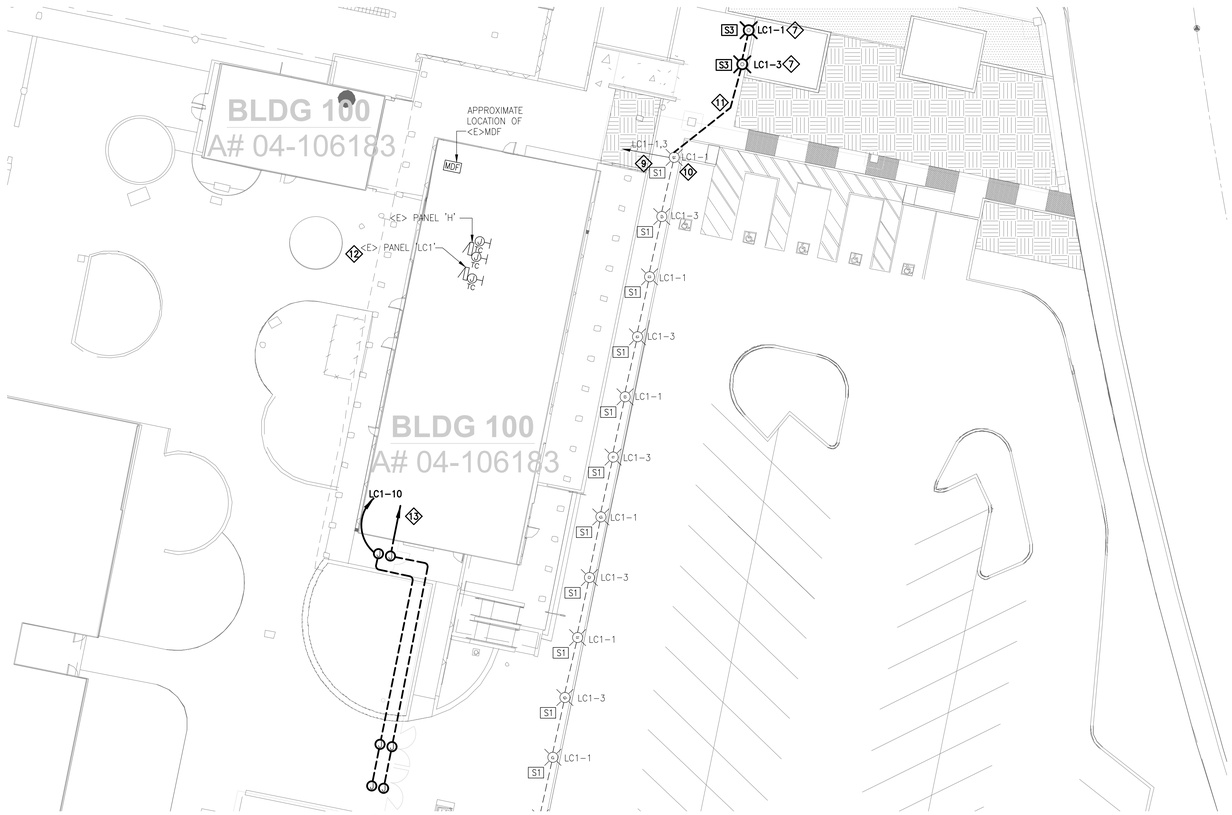
Revisions:

Project #: **CA18022 (SOBE #181773)** Drawn: **TP**
Date: **07/16/2019** Checked: **AC**

Sheet Title:

ELECTRICAL
ENLARGED SITE PLAN - NEW

E-4.2



2 SITE PLAN - NEW

SCALE: 1/16" = 1' - 0"

1 SITE PLAN - NEW

SCALE: 1/16" = 1' - 0"

GENERAL SHEET NOTES

A. CONTRACTOR IS RESPONSIBLE TO FIELD VERIFY ALL EXISTING LIGHT FIXTURES LOCATION, UNDERGROUND CONDUITS ROUTING, PULLBOX/JUNCTION BOX/MAN HOLE LOCATION.

B. COORDINATE WITH NMUSD FOR ANY POWER SHUTDOWN OR LIGHTING SYSTEM INTERRUPTION. PROVIDE TEMP POWER, LIGHTING, FIRE WATCH AS REQUIRED BY NMUSD TO MAINTAIN SCHOOL ACTIVITY.

REFERENCE SHEET NOTES

1. INTERCEPT AND EXTEND <E>LIGHTING CIRCUIT TO RELOCATED <E>LIGHT POLE. FIELD VERIFY FOR EXACT LOCATION OF UNDERGROUND FEEDER. PROVIDE NEW WIRING (#10), CONDUIT AND JUNCTION BOX AS REQUIRED.
2. NEW LOCATION OF <E>LIGHT POLE. COORDINATE WITH ARCHITECT FOR EXACT LOCATION. REFER TO STRUCTURAL FOR CONCRETE BASE MOUNTING DETAIL.
3. INTERCEPT AND EXTEND <E>FEEDER TO UNDER PARKING LOT ASPHALT TO AVOID NEW TREES PLANTING. COORDINATE WITH ARCHITECT FOR EXACT LOCATION. PROVIDE NEW WIRING (#10), CONDUITS AND JUNCTION BOX AS REQUIRED.
4. <E>LIGHT POLE TO REMAIN. PROTECT IN PLACE. TERMINATE NEW LIGHTING CONNECTION AS REQUIRED.
5. INTERCEPT AND EXTEND <E>FEEDER TO RELOCATED <E>LIGHT POLE. PROVIDE NEW WIRING (#10), CONDUIT AND JUNCTION BOX AS REQUIRED.
6. EXTEND <E>LIGHTING CIRCUIT WITH 3/4"C-2#12,1#12GND. TO BOLLARDS WITH SAME CONTROL WIRING. COORDINATE WITH ARCHITECT FOR UNDERGROUND CONDUITS ROUTING.
7. COORDINATE WITH ARCHITECT FOR EXACT LOCATION OF BOLLARDS. REFER TO STRUCTURAL FOR BOLLARD FIXTURE MOUNTING DETAIL.
8. CONTRACTOR SHALL FURNISH AND INSTALL 3/4"C. WITH CAT-6 CABLES FROM GATES TO MDF IN BUILDING '200'. CONTRACTOR SHALL VERIFY EXACT ROUTING, AND VERIFY WITH MANUFACTURER FOR EXACT REQUIREMENT.
9. INTERCEPT AND EXTEND <E>LIGHTING CIRCUITS TO BOLLARDS. CONTRACTOR SHALL FIELD VERIFY FOR EXACT UNDERGROUND LOCATION.
10. <E>BOLLARDS (TYPICAL) TO REMAIN. PROTECT IN PLACE. EXTEND LIGHTING CIRCUIT TO NEW BOLLARDS.
11. FURNISH AND INSTALL 3/4"C-3#12, 1#12GND. UNDERGROUND FEEDER TO BOLLARDS. COORDINATE WITH ARCHITECT FOR UNDERGROUND CONDUITS ROUTING.
12. <E>ELECTRICAL PANEL WITH TIME CLOCK FOR EXISTING LIGHTING CIRCUIT. REUSE <E>LIGHTING CIRCUITS AND CONTROL FOR NEW LIGHT FIXTURES.
13. CONTRACTOR SHALL FURNISH AND INSTALL 3/4"C. WITH CAT-6 CABLES FROM GATES TO MDF IN BUILDING '100'. CONTRACTOR SHALL VERIFY EXACT ROUTING, AND VERIFY WITH MANUFACTURER FOR EXACT REQUIREMENT.

Agency Approval:

IDENTIFICATION STAMP
DIV. OF THE STATE ARCHITECT
APP. 04-118247 INC:
REVIEWED FOR
SS ☑ FLS ☑ ACS ☑
DATE: 08.06.19

studio+
20520 SW Acacia, Suite 100, Newport Beach, California 92660 | P: 949.315.1993

SALASO'BRIEN
expect a difference
305 South 11th Street
San Jose, California 95112-2218
408.282.1500 | 408.297.2995 (f)
salasobrien.com
Bozeman | Los Angeles | Monterey
Oakland | Orange County | Sacramento
San Diego | San Luis Obispo | Seattle

Architect/Engineer

LICENSED ARCHITECT JASON A. DOMINGUEZ NO. C-32176 REN. 07-31-21 STATE OF CALIFORNIA

REGISTERED PROFESSIONAL ENGINEER CITY "KIT" GRAY No. E19090 ELECTRICAL STATE OF CALIFORNIA

Project Title:

CORONA DEL MAR HIGH SCHOOL
SITE CONTROLLED ACCESS UPGRADES

2101 EASTBLUFF DR
NEWPORT BEACH, CA 92660

Revisions:

Project #: **CA18022 (SOBE #181773)** Drawn: **TP**
Date: **07/16/2019** Checked: **AC**

Sheet Title:

ELECTRICAL
ENLARGED SITE PLAN - NEW

E-4.1

K:\drawings\NMUSD\181773 Corona Del Mar H.S. Site Lighting\181773E-4.1.dwg 8/5/2019 11:21 AM Mario Gobea

Budgetary Costs

All Hardware and software licenses required to implement DNA Fusion based on counts shown in Exhibit A:

Enterprise Server Recommended Minimum Hardware Requirements:
Processor: Intel Core i5 2.8 GHz + (or equivalent, multi-core)
System memory: 8 GB
Disk space: 500 GB
Display: Support for 1024x768 or higher/512 MB VRAM
NIC: 10/100 Ethernet
OS: Windows 2012 R2 Server/Windows Server 2016, Windows 2019 Server
Database: Supported Microsoft SQL 2012 through 2016
Notes:
• DNA Fusion is not supported on home, education, or mobile versions of Windows OS or Windows 10 S.
• RAID hardware configuration and backup medium recommended for Enterprise servers.

Client/PC Workstation Recommended Minimum Hardware Requirements:
Processor: Intel Core i3 2.4 GHz + (or equivalent)
System memory: 4 GB
Disk space: 250 GB
Display: Support for 1024x768 or higher/512 MB VRAM
NIC: 10/100 Ethernet
OS: Windows 10 (32 and 64 bit support)
Note: DNA Fusion is not supported on home, education, or mobile versions of Windows OS or Windows 10 S.

Production Environment Current Counts:
Elementary School:
- -5 Gates (entry & exit readers)
- -3 Exterior Doors
- -1 Interior Door
- -1 Vehicle Entrance

Intermediate:
- -4 Gates (entry & exit readers)
- -4 Exterior Doors
- -1 Interior Door
- -1 Vehicle Entrance

High School:
- -8 Gates (entry and exit readers)
- -8 Exterior Doors
- -10 Interior Doors
- -1 Vehicle Entrance

Production Environment Licensing/Mercury Hardware required for DNA Fusion (based on counts detailed in Exhibit A)

Primary Server Licensing:

DNA-New (1) - Initial DNA Fusion Server license and licensing for 10 Sub-Controllers
-MSRP: $500.00

DNA-New-CWS (1) – Client Workstation for DNA Fusion
-MSRP: $500.00

OpenDX (1) - Database exchange utility (Active Directory Integration).
-MSRP: $10490.00

OO-VMS (1) – Integration to video management solution.
-MSRP: $7350

TR-E-V (1)- Essentials 3 day virtual training
-MSRP: $2400

Total: $21,240

Elementary School Licensing/Hardware*:

DController (6) - IP-Based Intelligent single door controller
- MSRP: $1768

E2-SSP-D2-RSC2 (1) - Enclosure with Power Supply and Power Distribution Board, SSP-D2 and RSC-2
- MSRP: $4092

E3-1RSC2 (1) - Enclosure and 1 RSC-2
- MSRP: $1522

DNA-SC1 (9) - 1 Sub-Controller License
- MSRP: $104

Subtotal per school: **$17,158**
Total for all (22) elementary schools: **$377,476**

***Assumes all electrified hardware is operating off of 12v power. If 24v is required we would require a power supply with 24v output and appropriate gauge wire.*

Intermediate School Licensing/Hardware*:

DController (5)- IP-Based Intelligent single door controller
- MSRP: $1768
E2-SSP-D2-RSC2 (1)- Enclosure with Power Supply and Power Distribution Board, SSP-D2 and RSC-2
- MSRP: $4092
E3-1RSC2 (1)- Enclosure and 1 RSC-2
- MSRP: $1522
DNA-SC-1 (8)- 1 Sub-Controller License
- MSRP: $104

Subtotal per school: **$15,286**
Total for all (2) intermediate schools: **$30,572**

***Assumes all electrified hardware is operating off of 12v power. If 24v is required we would require a power supply with 24v output and appropriate gauge wire.*

Intermediate/ High School Licensing/Hardware*:

DController (14)- IP-Based Intelligent single door controller
- MSRP: $1768
E2-SSP-D2-RSC2 (1)- Enclosure with Power Supply and Power Distribution Board, SSP-D2 and RSC-2
- MSRP: $4092
E3-2RSC2 (5)- Enclosure and 2 RSC-2
- MSRP: $2440
DNA-SC-1 (8)- 1 Sub-Controller License
- MSRP: $104
DNA-SC-10 (2)- 10 Sub-Controller License
- MSRP: $1042

Subtotal per school: **$43,960**
Total for all (2) intermediate/ high schools: **$87,920**

***Assumes all electrified hardware is operating off of 12v power. If 24v is required we would require a power supply with 24v output and appropriate gauge wire.*

High School Licensing/Hardware*:

DController (9)- IP-Based Intelligent single door controller
- MSRP: $1768
E2-SSP-D2-RSC2 (1)- Enclosure with Power Supply and Power Distribution Board, SSP-D2 and RSC-2
- MSRP: $4092
E3-2RSC2 (4)- Enclosure and 2 RSC-2
- MSRP: $2440
E3-1RSC2(1)- Enclosure and 1 RSC-2
- MSRP: $1522
DNA-SC-10 (2)- 10 Sub-Controller License
- MSRP: $1042

Subtotal per school: **$33,370**
Total for all (2) high schools: **$66,740**

***Assumes all electrified hardware is operating off of 12v power. If 24v is required we would require a power supply with 24v output and appropriate gauge wire.*

Alternative Schools Licensing/Hardware*:

DController (9)- IP-Based Intelligent single door controller
- MSRP: $1768
E2-SSP-D2-RSC2 (1)- Enclosure with Power Supply and Power Distribution Board, SSP-D2 and RSC-2
- MSRP: $4092
E3-2RSC2 (4)- Enclosure and 2 RSC-2
- MSRP: $2440
E3-1RSC2(1)- Enclosure and 1 RSC-2
- MSRP: $1522
DNA-SC-10 (2)- 10 Sub-Controller License
- MSRP: $1042

Subtotal per school: **$33,370**
Total for all (4) alternative schools: **$133,480**

***Assumes all electrified hardware is operating off of 12v power. If 24v is required we would require a power supply with 24v output and appropriate gauge wire.*

OPEN OPTIONS REFERENCE LIST

K-12

Imperial USD
Mike Dibley
760-355-3233
Mdibley@imperialusd.org

Central USD
Cesar Castro
760-879-1497
Ccastro@cuhsd.net

El Centre Elementary USD
Antonio Romayor
760-790-9050
Aromayor@ecesd.org

PaloVerde USD
Tim Slagan
760-899-3835
Tslagan@pvusd.us

Dallas ISD
Melissa Manning
MJUAREZ@dallasisd.org
972-749-2481

Northside ISD
Allan Dufault
allan.dufault@nisd.net
210-397-7722

Leander ISD
James Hindman
James.Hindman@leanderisd.org
512-570-0136

Dripping Springs ISD
Bonnie Drane

Bonne.Drane@dsisdtx.us
512-858-3045

Hutto ISD
Chris Contreras
Christopher.contreras@huttoisd.net
512-759-4700 ext. 6108

Lake Travis ISD
Ryan Petru
petrur@ltisdschools.org
512-533-6565

San Maros CISD
Greg Hubenak
Greg.hubenak@smcisd.net
512-393-6909

La Porte ISD
Eddie Hill
HillE@lpisd.org
281-684-3324

Alvin ISD
Jeff Wilson
jwilson@alvinisd.net
281.245.2914

Bridge City ISD
Natasha Ray
natash.ray@bridgecityisd.net
409-554-2123

Nederland ISD
Adam Busby
abusby@nederlandisd.org
409-726-2243

Waco ISD
Andrea Lively
Andrea.lively@wacoisd.org
254-755-9501

Boerne ISD
Hector Hernadez
Hector.hernandez@boerneisd.net
830-357-2161

Corpus Christi ISD
Darrell Dubuque
Darrell.Dubuque@CCISD.US
361-533-5106

Judson ISD
Mustafa Hussein
mhussein@judsonisd.org
210-722-2703

Castleberry ISD
Lenny Lasher
lasherl@castleberryisd.net
817-909-0095

Everman ISD
Glenn Brown
gbrown@eisd.org
817-615-3604

Lumberton ISD
Daniel Cazares
dcazares@lumberton.k12.tx.us
409-658-2560

Alief ISD
Dan Turner
dan.turner@aliefisd.net
281-498-3542

Dayton ISD
Nathan Davis
Nathan.davis@daytonisd.net
936-258-2667

Trinity ISD
Barry Coleman
bcoleman@trinityisd.net
936-594-3569

Annuciation Orthodox School
Bryant Richardson
brichardson@aoshouston.org
713-470-5640

Open Options - Advantage Dealer Programs

At Open Options we strive to forge strong partnerships with our dealer network and create a fair incentive program that rewards such partnerships. The Advantage and Advantage Platinum programs are designed to distinguish and reward our partners who have consistently demonstrated loyalty and growth with Open Options.

Program benefits begin immediately once all requirements are met. The dealer company is eligible to receive these benefits throughout the remainder of the year as well as the entire next calendar year.

Program membership will be determined by Open Options based on the following performance measures:

Advantage Requirements • $250,000 or more in annual sales • Open Options Software Maintenance on at least 50% of accounts • At least 4 new DNA Fusion site installments per year • Display Open Options logo with link on company website **Advantage Benefit** • 5% discount on products*	**Advantage Platinum Requirements** • $500,000 or more in annual sales • Open Options Software Maintenance on at least 50% of accounts • At least 5 new DNA Fusion site installments per year • Display Open Options logo with link on company website • 1 advanced trained technician **Advantage Platinum Benefit** • 7.5% discount on products*

Open Options, LLC Dealer List

AMERICAN SECURITY GROUP

	Chase Keene American Security Group 760-212-9772 Ckeene@amergroup.com

CONTI

	Craig Garner Conti Corporation 702-544-8162 cgarner@conticorporation.com

RD SYSTEMS, INC.

	Patrick Bailey RD Systems, Inc. 949-936-0100 patrickb@rd-systems.com

Listed below is a list of current integrations with third party solutions for DNA Fusion and Flex API:

Video Management Systems
HanWha
Milestone Systems
ExacqVision
3XLogix
ACTI
Avigilon
Bosch VMS
Dedicated Micros
General Solutions
HikVision
Instek
March
ONSSI Ocularis
Panasonic
Pelco
Salient
Verint
Video Insight

Intrusion Detection Systems
DMP
Bosch

Elevator Integrations
thyssen krupp
Kone
Schindler
Otis
Mitsubishi

Audio
Zenitel

Asset Tracking
Traka

Visitor Management Systems
Stopware
Splan
EasyLobby

Mustering/Event Management
Telaeris

FIPS 201-2
HID pivClass

Biometric Systems
Suprema Bioconnect
IDEMIA
Schlage Handkey
PoPID
Invixium
eyeLock

Third Party Access Control Hardware
Isonas
Intelligent Locks
Allegion
ASSA Abloy

Card Printers
Fargo
Magicard

High Availability/Failover
NEC ExpressCluster
Neverfail

External Data Sources
Active Directory
Oracle
Microsoft SQL Server
Secure LDAP

License Plate Recognition
Inex Tech

DNA Fusion & Alarm Interfaces

OPEN OPTIONS
ACCESS TECHNOLOGY

BOSCH
Invented for life

Overview

DNA Fusion™ interfaces with DMP and Bosch alarm panels allowing customers to interact with both access control and intrusion detection from a single, common user interface. Users can display alarm zones from supported alarm panels and arm/disarm points and zones directly from within DNA Fusion.

Features

- DNA Fusion™ can monitor single points to multiple zones received from Bosch or DMP alarm panels
- Receive alarm panel events in DNA Fusion
- Arm/Disarm zones via DNA Fusion host-based macros or direct control
- Monitor access control and intrusion detection from single user interface
- Bosch and DMP panels act as dialer
- Auto discover alarm points

Intrusion Detection

Supported DMP Panel: XR550DN

The XR550DN Command Processor Panel has 574 zones, 96 doors of access, 506 Form C relays, 32 areas, and 10,000 users. It communicates via the digital dialer.

Supported Bosch Panel: Mode 2

Available with DNA Fusion version 7, the Bosch Mode 2 integration features a cleaner user interface and easier configuration as well as a broader range of support. Operators can continue to receive alarm panel events and arm/disarm zones in DNA Fusion, but can also take advantage of extended capabilities such as programming users within the panel, controlling points from the graphics maps, and much more.

Supported Panels

DMP:

- DMP XR550DN

BOSCH:

Model	Areas Supported	Points (Zones) Supported
B6512	6	96
B5512	4	48
B4512	2	28
B9512G	32	599
B8512G	8	99

© 2019 Open Options, DNA Fusion and SSP are trademarks of Open Options, All other trademarks are the property of their respective owners. Information within this document is subject to change without notice. (0619)

Access Control Software

OPEN OPTIONS®
ACCESS TECHNOLOGY



Overview

DNA Fusion delivers a complete and scalable access control solution for any organization ranging from the multi-campus enterprise to a single lobby entrance. DNA Fusion takes full advantage of the distributed network architecture model and open platform control panels allowing organizations to monitor and manage several integrated systems through a single common interface.

Software Architecture

DNA Fusion is developed using the latest Windows technology and utilizes a combination of both native and managed technologies to maximize speed as well as productivity. DNA Fusion takes full advantage of Visual Studio's C++ and .NET tools and leverages Microsoft's remoting technologies to communicate securely across the network. Microsoft SQL Server is employed for the DNA Fusion database to permit easy connectivity, management, and synchronization across other business systems.

DNA Fusion™

Features

- Intuitive graphical interface
- InfoReady reporting system
- Advanced graphic maps
- Elevator Control up to 128 floors
- Personnel & credential management
- Photo verification on events
- Segmented database (tenants)
- Easy drag and drop throughout
- Powerful video integrations
- Anti-passback
- Photo ID production
- Triggers and Macros
- Alarm management
- Auto e-mail alarms and events
- Fully customizable interface
- Built-in web browser
- Database import/export/sync
- Open platform database
- Authentic Mercury hardware
- Wireless lock integration
- Biometric interfaces
- FIPS 201 Compliance
- Web and Mobile solutions available

DNA Fusion

PC Specifications for DNA Fusion

NOTE: The following minimum specifications are meant to serve as a baseline to configuring the DNA Fusion system and do not take into account all the variables of your system. These recommendations are based on the current release version of DNA Fusion and are subject to change without notice.

Recommended Minimum Server Specifications

Enterprise Server / SQL Server* (> 20 doors / > 5 clients)

Processor:	Intel Core i5 2.8 GHz + (or equivalent, multi-core)
System memory:	8 GB
Disk space:	500 GB
Display:	Support for 1024x768 or higher/512 MB VRAM
NIC:	10/100 Ethernet
OS:	Windows 2012 R2 Server, Windows Server 2016, Windows Server 2019

*SQL Server provided by customer
(Supported versions 2012 through 2019)

NOTE: RAID hardware configuration and backup medium recommended for Enterprise servers.

Corporate Server / SQL Express* (< 20 doors / < 5 clients)

Processor:	Intel Core i5 2.8 GHz + (or equivalent)
System memory:	4 GB
Disk space:	250 GB
Display:	Support for 1024x768 or higher/256 MB VRAM
NIC:	10/100 Ethernet
OS:	Windows 2012 R2 Server, Windows Server 2016, Windows 10 (32 and 64 bit support), Windows Server 2019

*SQL Server Express 2012 included / 10 GB database limit

IMPORTANT! DNA Fusion is NOT supported on home or mobile versions of Windows OS.

Recommended Client Specification

Client / Photo ID Client*

Processor:	Intel Core i3 2.4 GHz + (or equivalent)
System memory:	4 GB
Disk space:	250 GB
Display:	Support for 1024x768 or higher/512 MB VRAM
NIC:	10/100 Ethernet
OS:	Windows 10 (32 and 64 bit support)

*Photo ID Clients should have required ports (USB, serial, etc.) for any external capture or printing devices.

Network Requirements

- Open Options strongly recommends that all computers running DNA Fusion are connected on a Windows domain.
- DNA Fusion may be ran across different domains provided a bi-direction trust is in place between domains.
- If configuring in a Windows workgroup, all computers running DNA Fusion must be members of single dedicated workgroup. This configuration is less secure than a domain.

© 2021 Open Options, DNA Fusion and SSP are trademarks of Open Options. All other trademarks are the property of their respective owners. Information within this document is subject to change without notice. (0221)

OPEN OPTIONS
ACCESS TECHNOLOGY

www.ooaccess.com
Main: 877.818.7001
Support: 855.818.7001

DNA Fusion™ PC | Web | Mobile

OPEN OPTIONS®
ACCESS TECHNOLOGY



PC Client

Within the traditional DNA Fusion client, customers can easily access all their system data with InfoReady design, assign global access levels, drag and drop data, create custom direct commands, and much more. DNA Fusion also takes full advantage of the Authentic Mercury open hardware platform and connects with numerous industry-leading security technologies, including video management systems, intercom, wireless locks, and more for a comprehensive solution.

Web & Mobile Clients

DNA Fusion's Fusion Web and Fusion Mobile applications provide customers a secure way to manage their facility's security remotely or on-the-go. Through these applications, customers can access the critical features of their DNA Fusion system – such as video management systems, alarms, personnel, and hardware – from their mobile device or supported web browser.

Feature Comparison	PC Client	Web Client	Mobile Client
Mercury Hardware	●	●	●
Assa Abloy Wi-Fi Locks	●	●	
Assa Abloy PoE Locks	●	●	
Isonas Panel	●		
Milestone VMS	●	●	●
Exacq Vision VMS	●	●	●
Graphic Maps	●		
Add/Remove/Edit Hardware	●		
Add/Remove/Edit Access Levels	●		
Add/Remove/Edit Time Schedules	●		
Filter Hardware in Events Grid	●	●	
Filter Hardware through Hardware Filters	●		
Tenants Available	●	●	
Add/Remove/Edit Cards	●	●	
Add/Remove/Edit Personnel	●	●	●
Take Photos	●	●	●
Photo Badging	●	●	
Control Door Modes (Mercury hardware only)	●	●	●
View Events	●	●	
View Alarms	●	●	●
InfoReady Reports available	●	●	
Direct Commands	●	●	●

© 2019 Open Options. DNA Fusion and SSP are trademarks of Open Options. All other trademarks are the property of their respective owners. Information within this document is subject to change without notice. (1019)

an ACRE brand


REMOTE LOCKDOWN
Lockdown settings can be initiated by the click of a button and accessed remotely through our Fusion Web & Mobile applications.
INTEGRATIONS
Integrations with VMS, intrusion detection, visitor management, and more offer an extra layer of security.
TRANSFER FILES
OpenDX database exchange software allows operators to easily transfer data into DNA Fusion.
DATABASE
Option for database partitioning leads to increased manageability of cardholders.
GRAPHIC MAPS
Graphic maps allow operators to visualize and manage doors, alarms and more from an interactive interface.
Benefits of DNA Fusion in Education

DNA Fusion

The access control platform that connects education.

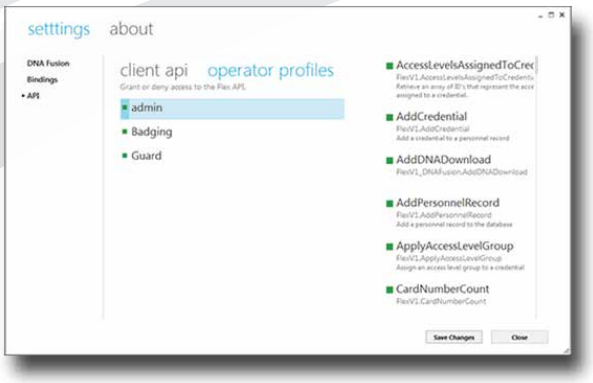


www.ooaccess.com

OPEN OPTIONS®
ACCESS TECHNOLOGY

877.818.7001

FlexAPI™ Application Programming Interface



Features

- Add, delete, modify Personnel records and the Credentials assigned to them.
- Assign, remove, modify Access Levels Groups, Access Levels and Precision Access Levels to Credentials.
- Control hardware devices and receive their state and status.
- Receive Events and Alarms with Alarm Management (Acknowledge, Clear, Dismiss and Dispatch Text).
- Auditing of any actions taken through the API Key.

Requirements

- Windows 10 or later
- DNA Fusion version 6 or higher
- Administrator Privileges
- .NET 4.0
- XML-RPC

FlexAPI™

Open. Powerful. Easy-to-use.

Overview

FlexAPI is a clean and easy-to-use application programming interface for developing third-party integrations into Open Options' powerful access control software.

The Fusion Flex API provides a robust mechanism for external parties to develop an interface into DNA Fusion to accomplish a myriad of tasks or receive information from the application or database.

Flex API is used by a host of Open Options partners to tightly integrate systems such as video recording, visitor management, and biometrics.

Flex API is also the backbone of DNA Fusion Web and Mobile applications allowing integration into a wide variety of operating systems and development platforms.

Integrations

- Visitor management
- Intelligent locks
- High availability
- Elevator control
- Critical communications
- Bridge technology
- Biometrics
- Video
- Cards & Readers
- Alarm Panel Interface
- Government solutions

Main: 877.818.7001
Support: 855.818.7001

an ACRE brand

Integrated Credential Management

OPEN OPTIONS®
ACCESS TECHNOLOGY



Fusion ID™

ID Badging

Overview

Create, manage, and print all of your ID cards and access credentials from one central location with Fusion ID. Designed to work exclusively with the DNA Fusion security management system, Fusion ID is scalable from entry-level to enterprise applications. Fusion ID works with the Valcam 9000 professional series camera as well as supported TWAIN capture devices.

The included Badge Designer software gives you the power to create great looking ID cards with support for unlimited images, shapes, text, and data. Designing badge templates is simple using the intuitive editors for text and image placement and advanced users will love the built-in scripting capability.

Fusion ID is the best integrated solution available for ID badge production and because it works with DNA Fusion, your data is shared between both systems for easy input and personnel management.

Fusion ID™

- Works with the Valcam camera or TWAIN capture devices*
- No additional capture hardware required
- User-friendly interface
- Badge Designer included

Badge Designer

- Grid line support
- Background images
- Alignment tools for placement of images and text
- Magstripe encoding and Barcode support
- Text and Image Editors
- Built in scripting functionality

* Contact Open Options for supported models and additional information.

Fusion ID™

Features

Operating Environments

Runs on Microsoft Windows (See DNA Fusion supported operating systems).
Based on Microsoft Win-32 API
Support for long file names

Printing Environments

Support for Windows compatible ID card, inkjet, and laser printers
Dual-sided printing
Industry standard and custom page sizes with landscape and portrait printing
WYSIWYG print previewing

Help and Documentation

PDF User Manual

Card Printing

Print cards individually
Batch print cards with user-defined selection
Batch print using multiple badge templates at once
Encode magnetic stripe cards at print time*
Encode smart chips at print time*
Read proximity and iClass cards at print time*
*Single mode printing only

Image Capture

Supports Valcam Digital camera
Supports TWAIN devices
(Contact Open Options for specific models and additional information)



Image Support

Supports unlimited user-definable image types
Supports most industry standard image file formats
Crop images at time of acquisition

Card Design

Dual-sided card design with different orientations
All design objects can be rotated
Snap to grid feature
Fill background w/ solid color or an image
Flip between front and back layouts
Adjust layout object to fit target printer
Sample layouts included
Draw lines and shapes
Draw static text objects (non-changing text items)
Draw dynamic text objects (database dependent items)
Add bar codes with user-definable properties and values
Add images
Make object same height and width
Align multiple objects
Flip non-text objects
Create 3D drop shadows from text fields
User-defined object attributes (line, fill, colors, etc.)
Select colors from standard or custom palettes
Print all design objects based on conditions
"Ghost" (reduce opacity) Images and Bitmap objects
Remove background pixels from Images
Enforce date format on print and preview
Printer Independent image transparency and fading
Full True Type and ATM font support
Support for standard type styles
Horizontal and Vertical justification
Scripting language available for custom adjustments

© 2019 Open Options, DNA Fusion and SSP are trademarks of Open Options, LLC. All other trademarks are the property of their respective owners. Information within this document is subject to change without notice. (0419)

OPEN OPTIONS®
ACCESS TECHNOLOGY

www.ooaccess.com
Main: 877.818.7001
Support: 855.818.7001

Mobile Access Control

OPEN OPTIONS
ACCESS TECHNOLOGY



Fusion Mobile Features

- Available for Apple and Android devices
- Secure Login with SSL Encryption
- Add, edit and assign access levels
- Snap and store personnel photos on the fly
- Favorites menu for quick access to frequent items
- View and email system reports
- Easily view associated camera feed
- Execute commands quickly in emergency situations
- Respond to alarms in seconds
- Acknowledge and clear alarms with one simple swipe
- Real time camera feeds
- Full control of PTZ cameras

Fusion Mobile

Remote management app

Overview

Fusion Mobile is a remote management app for Open Options DNA Fusion access control software. Fusion Mobile allows users to take advantage of critical features of their DNA Fusion system while on the go.

Users can easily monitor and edit personnel and control hardware directly from their mobile device. The application also has the capability to run trace history and email reports. Advanced features include real time reporting, acknowledging alarms with a simple swipe and a favorites menu for quick access to common functions. In addition mobile users can execute pre-defined direct commands in emergency situations as well as view and control real time feeds from fixed or PTZ cameras.

Fusion Mobile is available for iOS 6 and higher on the iPhone and ICS 4.0 and up for all android mobile devices or tablets. The application can be used with DNA Fusion V6 and greater.

Fusion Mobile - Remote Management Application



Secure login

SSL encryption
Follows DNA Fusion logins and security profile



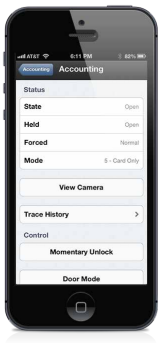
Alarms

Respond to alarms in seconds
Acknowledge and clear alarms with one simple swipe



Favorites menu

Stores doors, cameras and time schedules for quick and easy access to frequent items



Door status & control

Obtain door status and send fast commands
Easily view associated camera feed



Personnel record

Add, edit and assign access levels
Snap and store photos on the fly



Direct Commands

Execute commands quickly in emergency situations



Trace history

View and email reports on people and hardware with ease



Camera view

Portrait to landscape views with PTZ controls

© 2019 Open Options, DNA Fusion and SSP are trademarks of Open Options, LLC. All other trademarks are the property of their respective owners. Information within this document is subject to change without notice. (0419)

OPEN OPTIONS
ACCESS TECHNOLOGY

Available on the App Store

GET IT ON Google play

www.ooaccess.com
Main: 877.818.7001
Support: 855.818.7001

Fusion Web Client

OPEN OPTIONS®
ACCESS TECHNOLOGY



Fusion Web™

DNA Fusion Web Interface

Overview

Fusion Web provides a secure way to remotely manage your DNA Fusion access control system from any supported web browser. Fusion Web allows current users to search, view, and edit personnel as well as view and control system hardware right from a web browser. Alarms and Events can also be viewed, acknowledged, and cleared within Fusion Web.

Fusion Web lets you access the system remotely to manage or react to specific situations such as granting access after hours or controlling doors remotely. Fusion Web was designed for ease of use and makes it simple to accomplish a variety of common tasks in DNA Fusion without having to resort to a thick client.

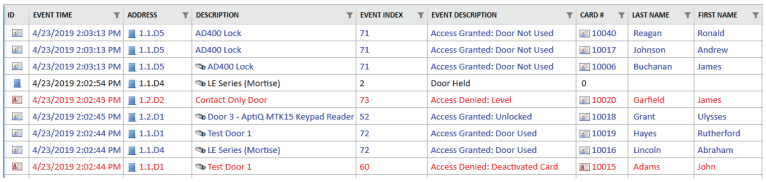
Fusion Web was developed using Microsoft Silverlight and requires the .NET framework. This powerful web application is the perfect solution for the remote management of your access control system.

Features

- Remotely manage your DNA Fusion access control system from any supported web browser
- Manage personnel:
    - Add/remove access
    - Set use limits
    - View photos
    - Activate/deactivate cards
    - Trace history reporting
- View and manage entire system hardware by site, controller, or door pages
- Control hardware:
    - Momentary unlock of doors
    - Change reader mode
    - View status of system hardware
    - Arm/disarm areas or points
    - Control & view status of time schedules
    - Trace history reporting
- View live events with custom sorting and grouping options
- View and manage real time alarms
- Use standard browser controls for navigation

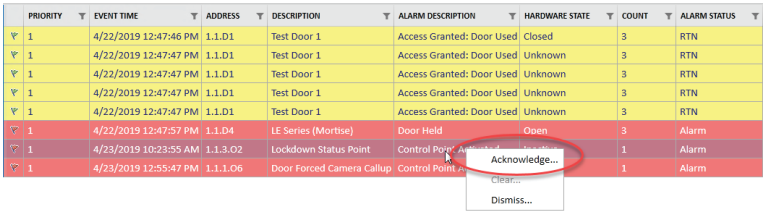
Fusion Web ™

View Real Time Events



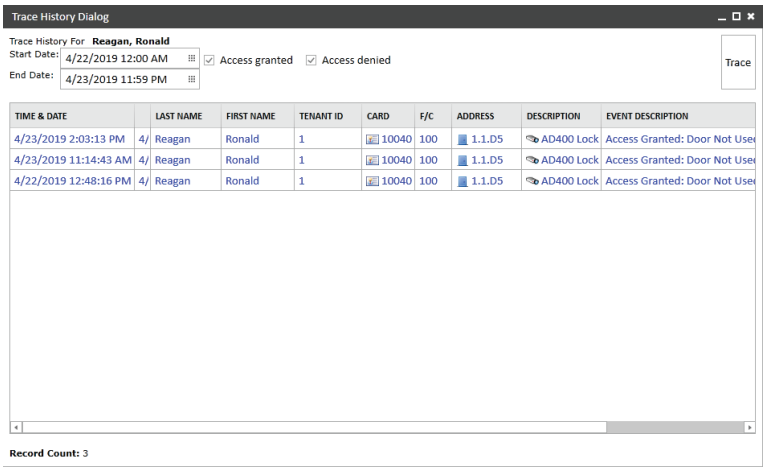
ID	EVENT TIME	ADDRESS	DESCRIPTION	EVENT INDEX	EVENT DESCRIPTION	CARD #	LAST NAME	FIRST NAME
	4/23/2019 2:03:13 PM	1.1.D5	AD400 Lock	71	Access Granted: Door Not Used	10040	Reagan	Ronald
	4/23/2019 2:03:13 PM	1.1.D5	AD400 Lock	71	Access Granted: Door Not Used	10017	Johnson	Andrew
	4/23/2019 2:03:13 PM	1.1.D5	AD400 Lock	71	Access Granted: Door Not Used	10006	Buchanan	James
	4/23/2019 2:02:54 PM	1.1.D4	LE Series (Mortise)	2	Door Held	0		
	4/23/2019 2:02:45 PM	1.2.D2	Contact Only Door	73	Access Denied: Level	10020	Garfield	James
	4/23/2019 2:02:45 PM	1.2.D1	Door 3 - AptiQ MTK15 Keypad Reader	52	Access Granted: Unlocked	10018	Grant	Ulysses
	4/23/2019 2:02:44 PM	1.1.D1	Test Door 1	72	Access Granted: Door Used	10019	Hayes	Rutherford
	4/23/2019 2:02:44 PM	1.1.D4	LE Series (Mortise)	72	Access Granted: Door Used	10016	Lincoln	Abraham
	4/23/2019 2:02:44 PM	1.1.D1	Test Door 1	60	Access Denied: Deactivated Card	10015	Adams	John

Acknowledge and Clear Alarms

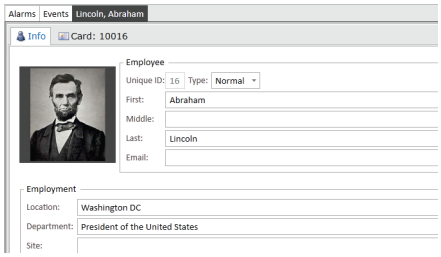


	PRIORITY	EVENT TIME	ADDRESS	DESCRIPTION	ALARM DESCRIPTION	HARDWARE STATE	COUNT	ALARM STATUS
	1	4/22/2019 12:47:46 PM	1.1.D1	Test Door 1	Access Granted: Door Used	Closed	3	RTN
	1	4/22/2019 12:47:47 PM	1.1.D1	Test Door 1	Access Granted: Door Used	Unknown	3	RTN
	1	4/22/2019 12:47:47 PM	1.1.D1	Test Door 1	Access Granted: Door Used	Unknown	3	RTN
	1	4/22/2019 12:47:47 PM	1.1.D1	Test Door 1	Access Granted: Door Used	Unknown	3	RTN
	1	4/22/2019 12:47:47 PM	1.1.D1	Test Door 1	Access Granted: Door Used	Unknown	3	RTN
	1	4/22/2019 12:47:57 PM	1.1.D4	LE Series (Mortise)	Door Held	Open	3	Alarm
	1	4/23/2019 10:23:55 AM	1.1.3.O2	Lockdown Status Point	Control Point		1	Alarm
	1	4/23/2019 12:55:47 PM	1.1.1.O6	Door Forced Camera Callup	Control Point		1	Alarm

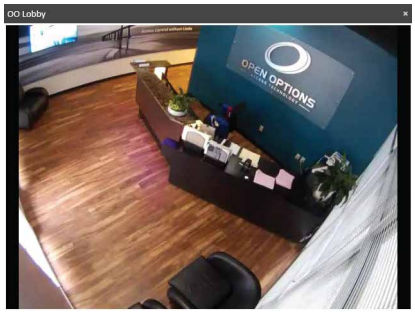
Run Trace History Reports



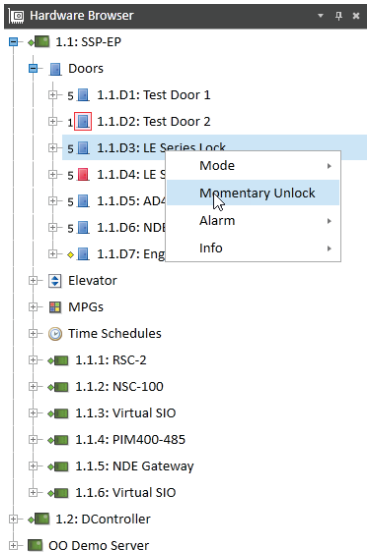
Manage Personnel



View Live Video Feeds



Control Hardware



© 2019 Open Options, DNA Fusion and SSP are trademarks of Open Options, LLC. All other trademarks are the property of their respective owners. Information within this document is subject to change without notice. (0419)

OPEN OPTIONS®
ACCESS TECHNOLOGY

www.ooaccess.com
Main: 877.818.7001
Support: 855.818.7001

Lockdown Procedures in DNA Fusion

In active shooter, shelter-in-place, lockout and lockdown situations, every second counts. Make sure your campus is equipped with the technology necessary to protect your students, faculty, staff and visitors with DNA Fusion's lockdown capabilities.

Lockdown Methodologies

There are different methodologies to create a lockdown scenario within DNA Fusion.

Deactivate all access cards except for first responders.

Disable all door schedules except for emergency response personnel schedule.

Change the mode of a door from unlocked to access card required (first responders only).

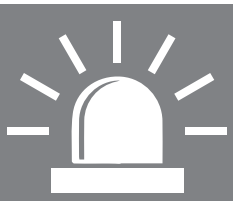
All these methodologies can be configured in any combination for different access points or doors.

Lockdown Initiation



Button/Icon with the Software

A lockdown can be initiated from the DNA Fusion software by simply clicking an icon on the toolbar in DNA Fusion. A lockdown can also be initiated in the Fusion Mobile app.



Hardwired Panic Button(s)

With a hardwired panic button, a lock down can be initiated by pressing a physical button. Once the button is pressed, a lockdown procedure will begin.



"Lockdown Card" Swipe

A lockdown procedure can be initiated by swiping a card at a specified reader or readers. This can be from one card or multiple cards.

What is happening during a lockdown?

It is easy to create and implement multiple threat levels in DNA Fusion. This can be as simple as having a change in the mode of the doors to locked or disabled, keeping everyone out. Or, the lockdown can disable building access for all except emergency personnel, allowing emergency personnel access to do their job in case of a lockdown.

OPEN OPTIONS®
ACCESS TECHNOLOGY



Connecting access control and intelligent communications for safer schools

VINGTOR STENTOFON
by ZENITEL GROUP

Enhance your campus security with an integrated access control and intelligent communications solution

Video Intercom
verify identity and access at secure entry points through dual authentication

Campus Lockdown
access control alarms can initiate communication to intelligent audio solution in event of emergency

Action on Event
trigger video action or PA broadcast based on an intercom call or lockdown in DNA Fusion



Enterprise Notification
clear communication throughout school or campus in lockdown or critical events

Managed Integration
ensures version compatibility between access control and intelligent communication

Real-Time Response
view and react to real-time events through access control, VMS and intelligent audio

Graphic Maps
plot intercom locations on map and click to answer calls or initiate announcements

800-654-3140
www.zenitel.com

877-818-7001
www.ooaccess.com

Automated Data Exchange

OPEN OPTIONS®
ACCESS TECHNOLOGY

OpendX

personnel data exchange

Overview

OpenDX delivers a seamless, automated interface from any ADO Compliant database including Microsoft's Active Directory into the DNAFusion™ access control system.

This powerful tool removes the time-consuming task of manually entering data across all your various HR and business systems ultimately saving your company money and valuable resources.

OpenDX provides an easy-to-use interface for configuring the data you want to transfer and will perform automated data transfers from any valid data source or scan a specific directory for CSV or text files generated by third party systems.

OpenDX comes standard equipped to handle most data import tasks and with built-in scripting support in two programming languages can be easily customized to tackle any challenge.

Features and Benefits

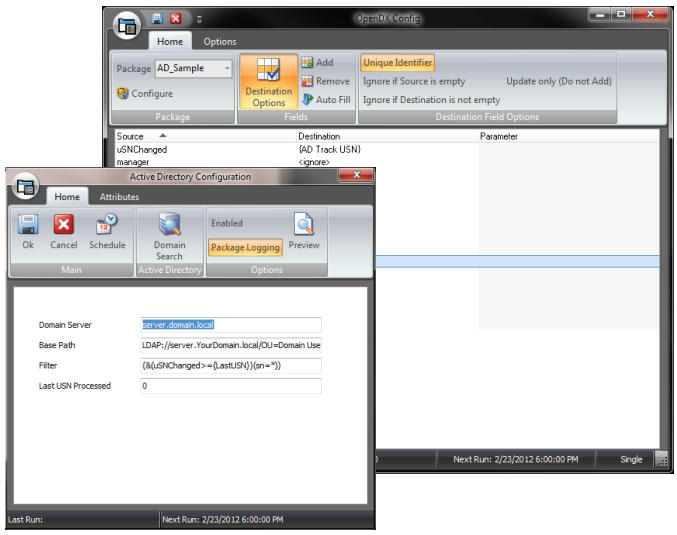
- Saves valuable time and resources by automating the data entry process of personnel/cardholder records into the DNA Fusion™ access control system
- Imports cardholder data directly and automatically into DNA Fusion™ from third-party systems such as Active Directory, HR, SAP, and legacy access systems
- No need to pre-process imported data file
- Create new cardholder records, update existing records and even delete records based on user-defined criteria
- Specifiy access privileges to be assigned at the time of the import and automatically download new cardholder information to field devices
- Built-in scripting support for both Pascal and BASIC computer languages provide the ultimate tool to tailor the product to fit any customer requirement
- Detailed logging of all import functions and changes to cardholder records showing exactly what data was modified
- Preview of data provides a simple means of verifying data integrity prior to import
- Import can be an unattended, real-time database scan based on scheduled intervals, CSV or flat file scan in a user designated directory
- Quick and simple configuration

OpendX
personnel data exchange

Additional Information

OpenDX supports the following data sources:

- All OLE DB provders
- SQL Server 2000-2017
- Microsoft Access
- Active Directory
- Oracle
- LDAP
- Text
- CSV
- XML



Simple User Interface for Configuration

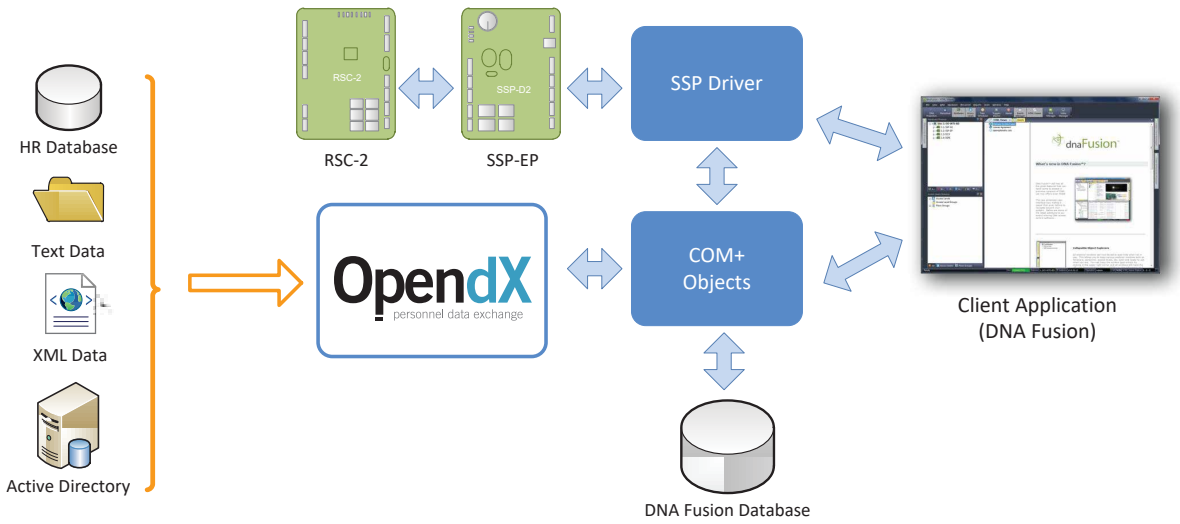
AD Operator Synch

A Powerful add-on module that allows you to easily add or remove DNA Fusion™ operators based on Microsoft AD users that are members of a selected Organizational Unit (OU) in Active Directory.

Scripting Engine

Built-in scripting engine allow for customization of data to be moved and synched between sources.

OpenDX Dataflow Diagram



© 2019 Open Options, DNA Fusion and SSP are trademarks of Open Options, LLC. All other trademarks are the property of their respective owners. Information within this document is subject to change without notice. (0419)

OPEN OPTIONS
ACCESS TECHNOLOGY

www.ooaccess.com
Main: 877.818.7001
Support: 855.818.7001



OPEN OPTIONS®
ACCESS TECHNOLOGY

Access Control System Hardening Guide



This manual is proprietary information of Open Options LLC. Unauthorized reproduction or distribution of this manual is strictly forbidden without the written consent of Open Options, LLC. The information contained in this manual is for informational purposes only and is subject to change at any time without notice. Open Options, LLC assumes no responsibility for incorrect or outdated information that may be contained in this publication.

DNA Fusion™ and SSP™ are trademarks of Open Options, LLC.

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

© Copyright 2002-2020 Open Options, LLC. All rights reserved.

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

What is "Hardening?" 1
DNA Fusion Hardening Configuration 3
Protection Levels 5
Installation 5
Internal Webpage 7
  HTTPS 7
  Session Timer 7
  Authorized IP Addresses 8
  Disable Web Server 8
User Accounts 9
  Default User Login 9
  Unique User Accounts 9
  Password Strength 9
    Strength Requirements 9
    Password Criteria 9
Information Services 11
  Disable Discovery 11
  Disable SNMP 11
  Disable USB and SD Interfaces 11
Encryption and Authentication 11
  Host / Controller Encryption 11
  AES Encryption 11
  TLS Encryption 11
    Hardening TLS 13
    Cipher Suites 13
  Host / Controller Authentication 15
  DNA Fusion Servers 16
    Network Segmentation 16
    Database Security System (Microsoft SQL Server) 16
    Password Policies 16
  Downstream Communications 16
  Reader Communications 16
  Data at Rest Encryption (SSP-LX and Series 3 (LP) Controllers) 17
  Replay Attack Protection on IP Networks 17
    Host / Controller Communications 17
    Controller / IP Based Downstream Communications 17
Port-Based Network Access Control 19
  802.1x Authentication for SSP-LX and Series 3 (LP) Controllers 19
Equipment Replacement 21
  Controllers 21
  Downstream Modules 21
    EEPROM Clearing Procedure 21

NSC-200 Board Bulk Erase 21
Network Ports 23
SSP (EP Series) Controller 23
SSP (LP Series) Controller 23
NSC-100 24
NSC-200 24

Hardening Guide

In This Guide

- √ DNA Fusion Hardening Configuration
- √ Protection Levels
- √ Installation Recommendations
- √ Internal Webpage Settings
- √ User and Password Configuration
- √ Encryption and Authentication
- √ Port-Based Network Access Control
- √ Bulk Erase Memory
- √ Network Port Settings

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.

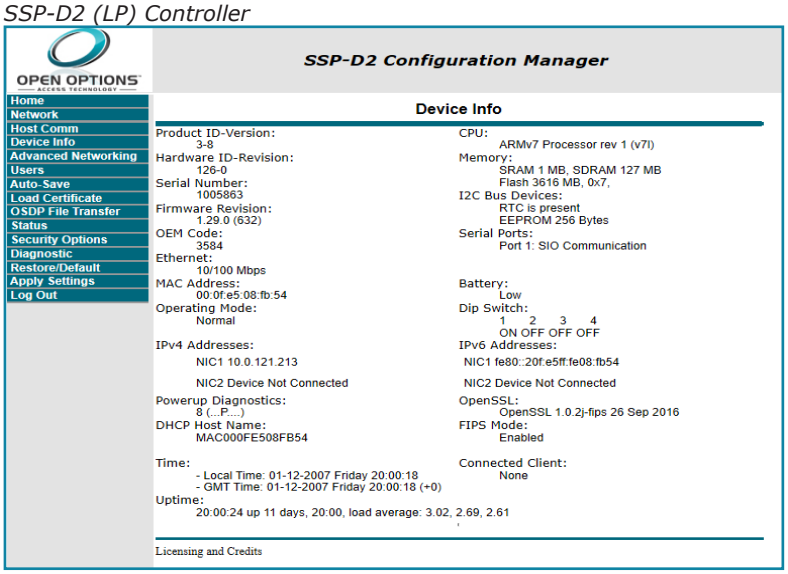
HTTPS

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

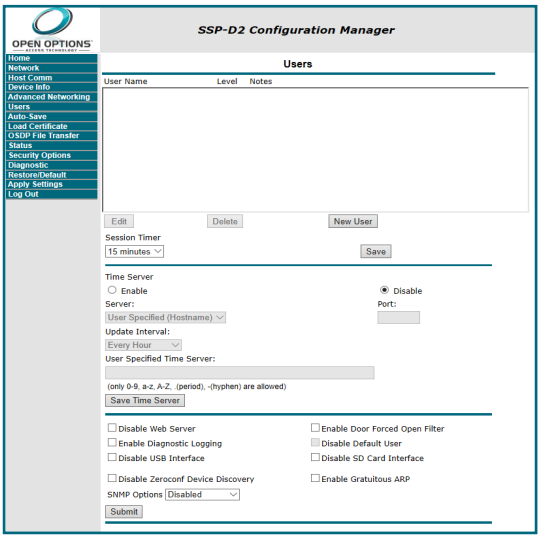


Session Timer

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

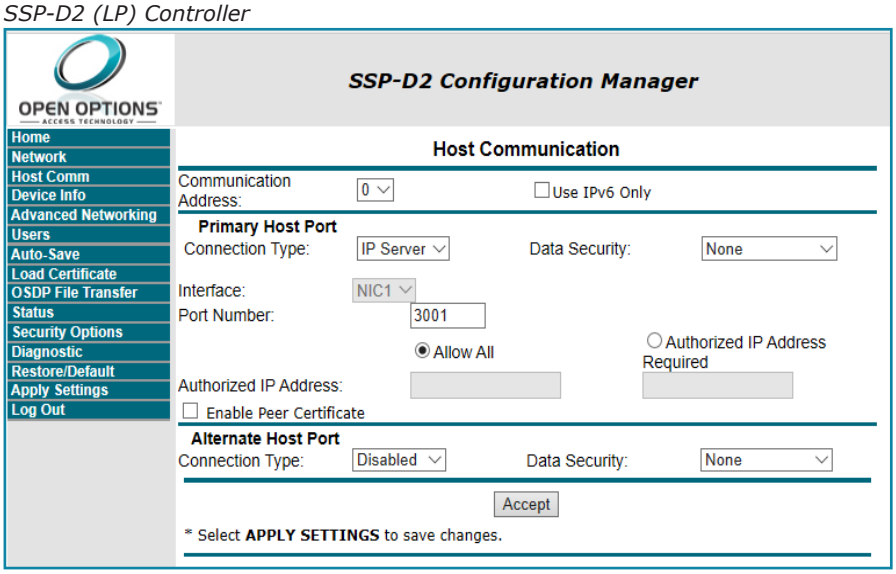


Authorized IP Addresses

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

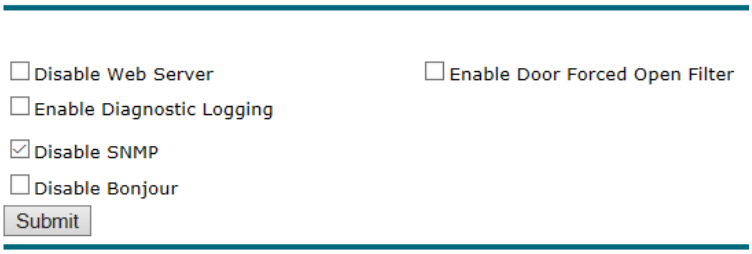
By default, the SSP controllers support device discovery using Zeroconf protocol on Windows and Linux services, such as Apple Bonjour and mDNSResponder. Once the controller is installed and configured, Open Options recommends that the discovery setting be disabled; this prevents someone with access to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

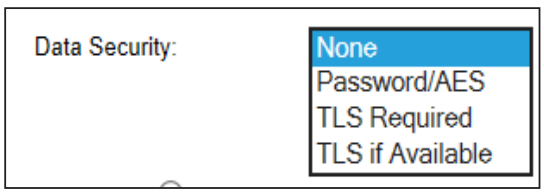
Enable AES encryption by configuring both the host and the controller. Load the encryption keys (128-bit or 256-bit) on both hardware devices prior to enabling AES. Encrytption keys can are loaded through the Load Certificate tab in the Configuration Manager.

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

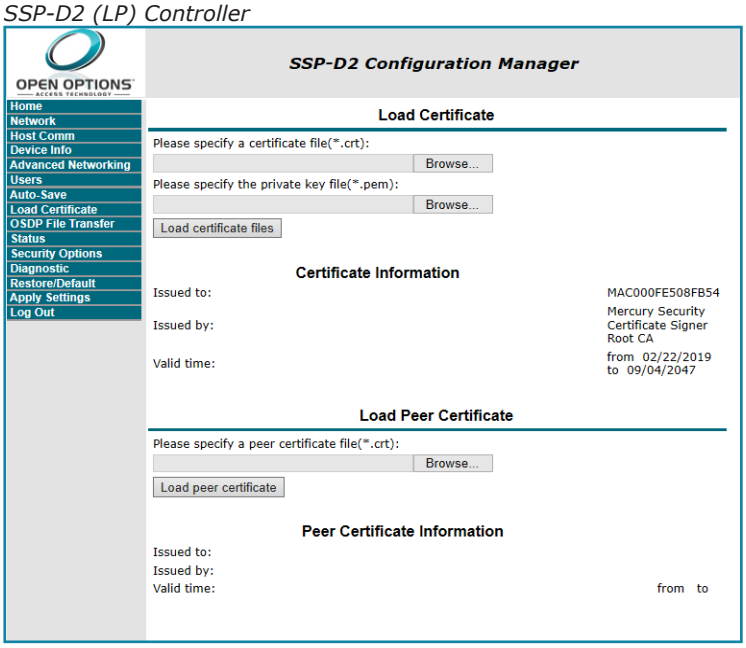
TLS 1.0 and 1.1 with modern ciphers and outdated hashes:	TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA
	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
	TLS_DHE_RSA_WITH_AES_256_CBC_SHA
	TLS_DHE_RSA_WITH_AES_128_CBC_SHA
	TLS_DHE_RSA_WITH_CAMELLIA_256_CBC_SHA
	TLS_DHE_RSA_WITH_CAMELLIA_128_CBC_SHA
	TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
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.*

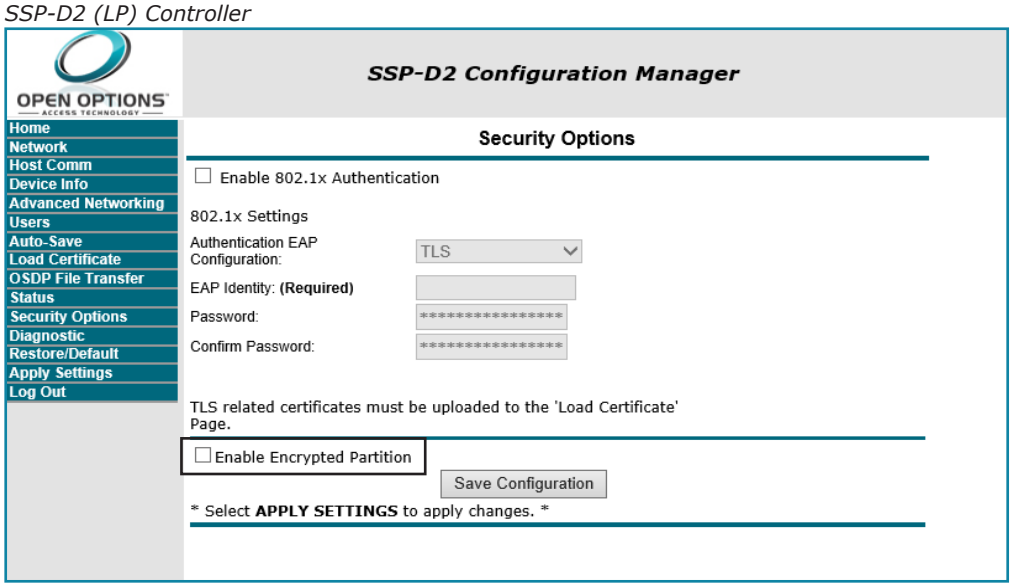
Data at Rest Encryption (SSP-LX and Series 3 (LP) Controllers)

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.

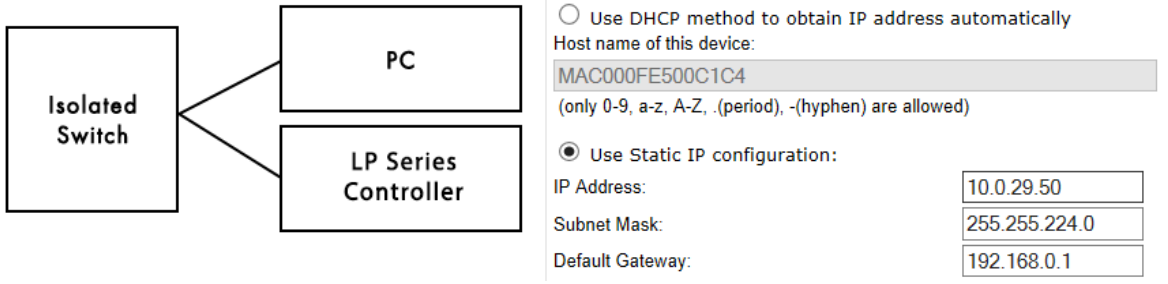
NOTES:

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.

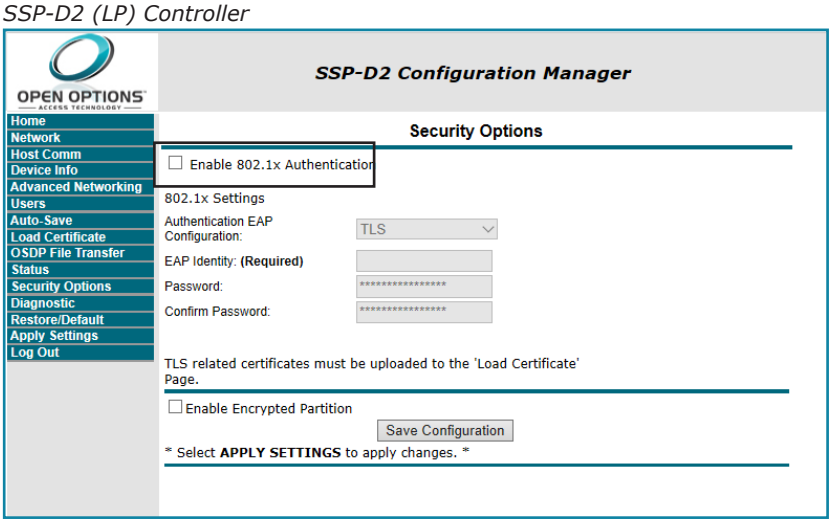


> *If TLS is used, the controller certificates must be signed by the same root certificate used by the authentication server.*

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