



LenelS2 Response for
Newport-Mesa Unified School District

REQUEST FOR PROPOSALS
FOR
INTEGRATED SECURITY SYSTEMS
STANDARDS

Submitted By: Carrier Fire & Security Americas
Corporation, LenelS2 Division, 1212 Pittsford-
Victor Road, Pittsford, New York 14534

LenelS2 Contact: Jarrod Brunsmann
Director of Business Development
Phone: +1 661.857.4160 (cell)
Email: Jarrod.Brunsmann@carrier.com
LenelS2.com

November 17, 2022





Response Certification

November 16, 2022

Re: Newport-Mesa Unified School District RFP November 2022

Dear Sir or Madame:

I represent that the statements made in the attached Request for Proposal (RFP) response prepared by LenelS2 are true and correct to the best of my knowledge.

DocuSigned by:

B12D88E335B4471...

Ryan Kaltenbaugh

Sr. Vice President, North Americas Sales
Carrier Fire & Security Americas Corporation, LenelS2 Division



Executive Summary

Carrier Fire & Security Americas Corporation, LenelS2 Division (“LenelS2”) is a global leader in advanced physical security solutions, including access control, video surveillance and mobile credentialing. Our technology includes web-based and mobile applications enhanced by cloud-based services.

Incorporating open architecture, LenelS2 provides scalable, unified security management solutions to customers ranging from global enterprises to small- and mid-size businesses. With industry-leading education, technical support, professional services, and custom solutions, LenelS2 remains committed to creating a superior experience for every customer, every time.

Easy to install and use, LenelS2 products are supported by an experienced, responsive team dedicated to providing exceptional service. LenelS2 serves many segments worldwide including corporate, education, healthcare, and government. LenelS2 has developed the NetBox unified access control and video ecosystem. NetBox is designed to be a browser based application that does not require specified computer hardware to use. A key aspect with the browser based nature of the application is that NetBox does not charge a per seat licensing fee, which you would find with traditional Windows client / server based solutions. This provides significant savings to the end user and creates a truly platform independent system. With the embedded Linux appliance as the system head end, there is no traditional maintenance and overhead of a Windows server, while offering a true plug and play security management system. The embedded appliance features Ubuntu Linux (v18.04 LTS), PostgreSQL, Apache™ web server in addition to the NetBox application. All NetBox access control appliances utilize solid state hard drives for optimum performance and are fully scalable in supporting more than 7,000 readers.

LenelS2 was established in 1991, then named Lenel, as an IP based access control and identity management software company headquartered in Rochester, New York. The initial vision was to provide superior, cutting edge software solutions to the security marketplace while continuing to evolve a seamlessly integrated suite of product offerings. Today, LenelS2 is a part of Carrier Global Corporation (NYSE: CARR), a leading global provider of healthy, safe, and sustainable building and cold chain solutions.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



End User Training and Technical Support

LenelS2 provides online training classes to system users such as Newport-Mesa Unified Schools (NMUSD). These self-paced classes will equip the NMUSD team with knowledge on how to install, configure, and support the NetBox and VRx products.

LenelS2 offers an optional program, called LenelS2 Black Support, for system users who are looking for direct technical support from the manufacturer. This would allow NMUSD to receive the same level of technical support as a Value-Added Reseller (VAR). LenelS2 NetBox standard support is available from 9:00 AM and 7:00 PM Eastern time. LenelS2 emergency support is available 24 x 7. Completion of the NetBox online training courses is a pre-requisite to be able to call LenelS2 technical support.

LenelS2 Upgrade and Support Plan

The NetBox Software Upgrade and Support Plan (SUSP) helps to maximize value of the District's LenelS2 system. All new LenelS2 NetBox systems include one year of SUSP coverage, and subsequent years may be purchased going forward. All VRx systems include three years of SUSP coverage.

A current SUSP provides the following benefits:

- Bi-annual major software updates and bi-annual minor software updates provided by LenelS2 to enhance your system and assure its robust operation.
- Telephone support from LenelS2's Framingham MA-based support team between the hours of 9AM and 7PM Eastern time.
- Live, on-line assistance from an LenelS2 support technician using LenelS2's collaborative maintenance features.
- Access to LenelS2 Support Central on-line library of documentation, software, and support tools.

LenelS2 provides the NetBox products to end users through a network of approved Value-Added Resellers (VARs). VARs procure, install, configure, provide training, and maintain the NetBox systems for the end users such as Newport-Mesa Unified School District (NMUSD). LenelS2 provides direct end user

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



training and certification as well as support programs. End users such as NMUSD are able to utilize internal personnel to maintain the NetBox system.

LenelS2 appreciates the opportunity to provide this information to Newport-Mesa Unified School District and believes that this solution will meet and exceed the requirements for the district. Scalability, low maintenance and ease of use are key elements that LenelS2 delivers with these products to meet the needs of Newport-Mesa Unified School District. The NetBox solution has been deployed to tens of thousands of customers, and over a thousand schools, since 2004 and is a market leader in security management system space.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



Solution Narrative

Overview

LenelS2 has reviewed the requirements for the Newport Mesa Unified School District (NMUSD) and has developed a solution to meet not only the district's current needs but support future needs and growth. To support organic growth within the school district, LenelS2's NetBox ecosystem provides a state-of-the-art system leveraging IT technology to ensure that the system can evolve and scale.

LenelS2 offers a comprehensive security management solution with the NetBox ecosystem of products. The NetBox ecosystem provides access control, digital video, and integration with a variety of third-party hardware and applications, in a fully scalable platform. The NetBox ecosystem is made up of software applications and hardware components, including the browser based NetBox administration application, the installed Magic Monitor unified client, multiple mobile applications as well as the NetBox access control server appliance, and the VRx video recorder appliance. The NetBox ecosystem can operate in both a Windows or a Mac environment, and the mobile apps are available in both iOS and Android support.

The core NetBox application is browser based and provides an intuitive user interface that makes for simple installation, operation, and expandability. All navigation is done through an easy to manage menu, with fully graphical configuration pages allowing a quick adoption of the solution by NMUSD. The NetBox provides for real time alarm management and monitoring, interactive floor plans, and comprehensive reporting. It allows for simple management of a card holder's life cycle in the system, including activation, badge creation, and access level assignment, as well as integration with trusted data sources, such as Active Directory. Another key aspect with the browser-based nature of the application is that the LenelS2 NetBox does not charge a per seat licensing fee like traditional Windows client / server based solutions. This leads to not only to upfront savings, but additional savings as the system grows and expands. The NetBox's browser-based nature makes it truly platform independent allowing it to run on desktops, laptops, tablets, and other devices that are able to utilize a web browser. With the embedded Linux appliance as the system head end there is no traditional maintenance and overhead of a Windows server, while offering a true plug and play security management system. The

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



embedded appliance features Ubuntu Linux (v18.04 LTS), PostgreSQL, Apache™ web server in addition to the NetBox application. All NetBox access control appliances utilize solid state hard drives for optimum performance and are fully scalable in supporting more than 7,000 readers.

LenelS2's VRx is a unique video management solution that follows the same Linux based appliance design concept as the NetBox products. The VRx integrates seamlessly with the NetBox access control product providing a unified access control and video user experience that is available via the three NetBox ecosystem applications; the NetBox browser-based client, the Magic monitor installed client, and the Mobile Security Professional mobile app. The depth of integration between the NetBox ecosystem and VRx solution is unparalleled in the security industry. The digital video is tagged with access control meta-data allowing for an efficient means of video retrieval across all three NetBox ecosystem applications. The tagged event includes the identity of the individual using their credential in a video clip and the location where the event is taking place.

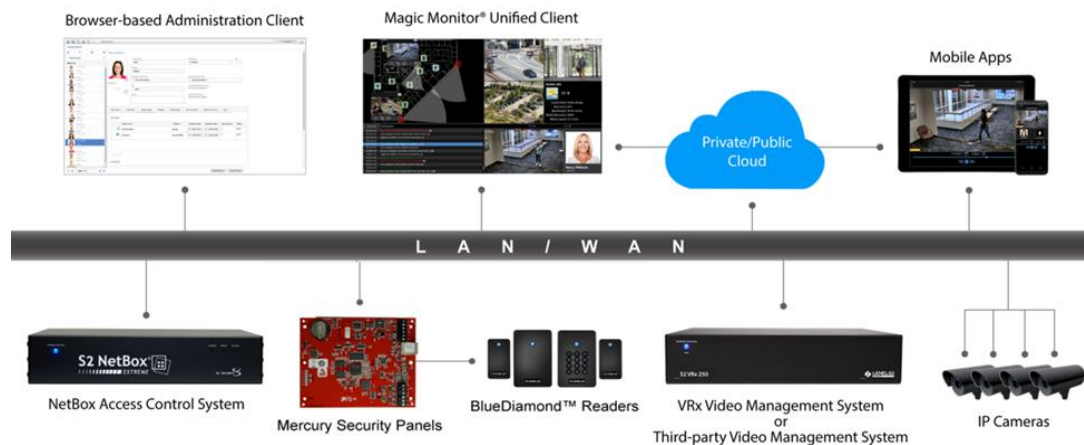
The LenelS2 Magic Monitor software provides a unified client application incorporating access control, digital video, identity management and third party information, such as floorplans, news feeds, traffic feeds and weather feeds. Magic Monitor software can be used on a client workstation or as part of key component Security Operation Center. Magic Monitor software supports event driven displays, meaning if a door alarms occurs it will display a specified layout that incorporates multiple cameras, floor plans, text instruction, and a multitude of other data. Magic Monitor software allows for full user layout customization, which can include up to 400 simultaneous camera streams.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



NetBox Ecosystem Architecture



NetBox Access Control Overview

The NetBox Enterprise system is a powerful, web-based access control and event monitoring system designed for deployments with demanding security requirements. Optional high availability offers automatic system failover between a redundant pair of servers. In addition, optional system partitioning allows the entire database to be separated into multiple smaller systems for entities such as field offices or smaller sites.

The NMUSD system would include a single NetBox Enterprise server, either a physical server or a server deployed in VMware, at the district's main datacenter or server and multiple Mercury Security access control panels at each school or other district building in the IT or IDF closets. The Mercury data gathering panels communicate to the NetBox server over the NMUSD LAN/WAN allowing for all the panels to be centrally managed from a single user interface. The Mercury panels deployed at each school will incorporate a variety of panels including reader boards, input boards, and output boards all communicating back to the NetBox system through the intelligent system controller. These Mercury panels then communicate to the security devices deployed at each door, including the card reader, door contact, request to exit and locking mechanism, as well as other security devices including motion detectors, glass break sensors and sounders. An Enterprise Class LenelS2 NetBox server can support up to 7,168 readers throughout the NMUSD infrastructure.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



Key NetBox Features and Capabilities

The browser based NetBox software also includes the LenelS2 Threat Level Manager which provides the ability to instantaneously lockdown a facility. Threat Level Manager is located on the LenelS2 monitoring desktop as well as being available through the LenelS2 Mobile Security User (MSU) app. The dynamic threat level manager icon provides quick and easy identification of the current threat level to all users and is visible in the upper right corner of all screens. The Threat Level Manager also supports user-definable graphics and naming conventions allowing it to be customized to the user's needs. The NetBox allows for up to eight distinct threat levels, and each school can be in a different threat level depending on the severity of the situation at the school. Threat levels can be configured to provide full system lockdown, limiting which cardholders can utilize their cards, and triggers sounds and strobes to notify personnel the school is in lockdown.

The NetBox ecosystem incorporates a variety of preconfigured reports covering configuration, history, and people. History reports include the general event history, which incorporates both access control events and associated video. The NetBox ecosystem incorporates full audit trail capabilities that keep track of system changes by operator. The NetBox also allows for a user to customize reports, and schedule them to be emailed to desired users weekly or monthly.

The NetBox solution is able to trigger alarm events based on hardware malfunctions as well as storage thresholds. Examples of monitored hardware malfunctions include if a panel loses communication with the server, has a power failure, or if there is tampering with the panel enclosure. The NetBox ecosystem also monitors camera communication and can trigger an event if the camera loses communication with the VRx. Additionally, through use of OSDP, the NetBox will provide an alarm event if the reader is tampered with or loses communication to the panel. Finally, the NetBox also allows for monitoring of storage on the NetBox server, by setting a threshold for warning and critical, typically at 75% and 90% respectively. All of these alarm events would be displayed on the NetBox monitoring desktop screen and are fully customizable with detailed instructions for the operator, as well as being able to play audio files, and send an email or text message. LenelS2 also offers a cloud health monitoring service called Cumulus that can notify system administrators if the NetBox server itself goes offline, as well as providing a variety of other monitoring options for Magic Monitor clients, cameras, and video recorders.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



The LenelS2 NetBox ecosystems support integration of identity with active directory or LDAP for both access control and video servers, thus allowing a user of the NetBox ecosystem to use their same username and password they use for other systems. The password management would then follow all the rules of active directory when it comes to password strength, password change policies, and additional Active Directory measures.

NetBox Enterprise Key Features:

- Portals: Supports up to 7,168 doors or other access points.
- Event and Alarm Monitoring: Includes comprehensive event logging, notification, and escalation.
- Threat Level Management: Provides configurable system status and response actions such as system lock downs.
- Person Record Management: Maintains detailed, credential-driven user records and access history.
- Reporting: Offers pre-defined and custom reports
- Web Interface: Delivers browser-based, unified system management and administration.
- Solid-State Design: Extends product lifecycle, lowering total cost of ownership.
- Video Integration: Works with LenelS2 VRx series video management systems and other third party video systems.
- API Support: Integrates with third party products such as human resource databases via an open source API.
- Automated System Management: Automatically discovers LenelS2 Nodes and handles system backups.
- Mobile App: Allows for mobile security management using LenelS2 Mobile Security Officer.
- System Partitioning Option: Allows the entire database to be separated into multiple smaller systems.
- High Availability Option: Offers automatic system failover between a redundant pair of servers.

Specifications – LenelS2 NetBox Enterprise

- Cardholders – 150,000
- Access Levels - Unlimited

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



- Unique User Roles - 16
- Simultaneous Users - 35
- Time Specifications - 512
- Portal Capacity – 7,168
- Maximum Inputs / Outputs - 2,000 / 2,000
- Online Transactions - Up to 160 million records

Client Requirements

- Operating System - Any; for badging use Windows 7 or later.
- Browser - Chrome, Internet Explorer, Firefox, and Safari
- Processor - Intel Core i3 or higher
- Memory (RAM) - 8GB
- Hard Drive - 100GB minimum

Appliance

- Storage Capacity - 128GB
- Processor - Intel Pentium
- Memory (RAM) - 4GB total
- Operating System - Ubuntu Linux
- Ethernet Ports - 1
- MTBF – 172,199
- Chassis - Rack Mount: 1.67in x 17.25in x 21.8in
- Weight - 18 lbs. (4.54 kg)
- Operating Temperature - 50° – 95°F (10° – 35°C)
- Storage Temperature – (-)4° – 158°F (-20° – 70°C)
- Operating Environment - Humidity 85%, non-condensing 35°C
- AC Input - 86 – 264 VAC, 47/440 Hz, 1.5A
- BTU Maximum - 256 per hour
- Regulatory Approvals - UL, CE, FCC, RoHS
- Warranty - 2 years, hardware; 1 year, software

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



Mercury Hardware

LenelS2 NetBox utilizes authentic Mercury access control hardware for system deployments. LenelS2 NetBox communicates directly from the NetBox server to the Mercury access control hardware without the use of third party or propriety hardware or gateways. LenelS2 has partnered with Mercury for over 20 years, is a Mercury Platinum Premier partner, and is Mercury's largest global partner. LenelS2 prides itself on not only having one of the longest standing partnerships in the industry with Mercury, but also one of the most in-depth utilization of the Mercury panel's capabilities.

LenelS2 NetBox has standardized on the Series 3 Mercury panels, and utilizes the full suite of Mercury panels, including:

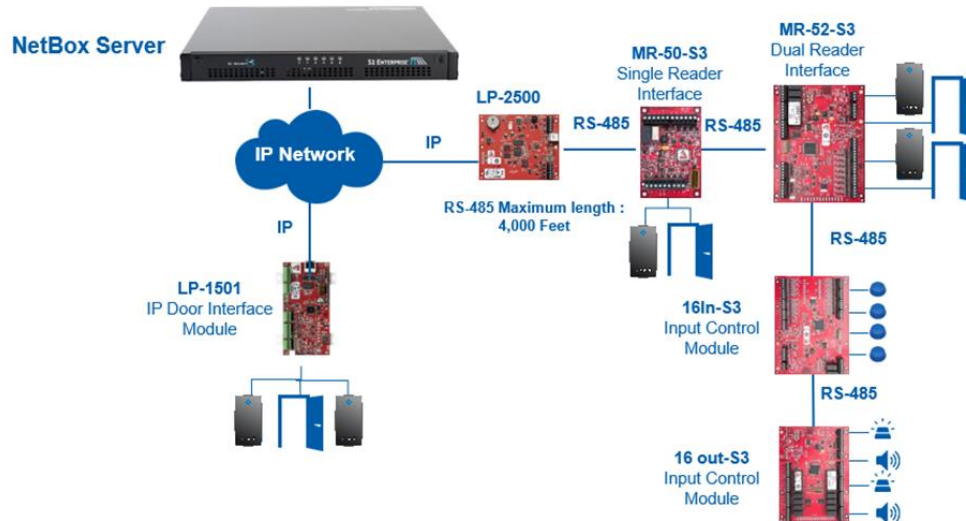
- LP-4502 - Advanced Dual Reader Controller with downstream support for up to 32 additional panels
- LP-2500 - Intelligent System Controller with downstream support for up to 64 additional panels
- LP-1502 - Intelligent Dual Reader Controller with downstream support for up to 32 additional panels.
- LP-1501 - Intelligent Single Reader Controller with downstream support for up to 8 additional panels
- MR-16IN-S3 – 16 Input Module
- MR-16OUT-S3 – 16 Output Module
- MR-50-S3 – Single Reader Interface Module
- MR-52-S3 – Dual Reader Interface Module
- MUX-8 – Star Multiplexer

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



NetBox Access Control Architecture with Mercury Panels



LenelS2 BlueDiamond

LenelS2 has developed the BlueDiamond family of products that incorporates both readers and credentials. The BlueDiamond reader is a full Multi-Technology reader that can read 13.56 MHz smart card credentials including DESFire, Mifare, and iClass, 125 KHz proximity credentials and mobile credentials. BlueDiamond readers would be a great transition reader to support the existing credentials and allow for support of multiple future credential technologies.

BlueDiamond products provide flexibility in reader communication by offering support for secure channel OSDP, as well as traditional Wiegand communication. The support of OSDP secure channels allows the BlueDiamond reader to be a part of the LenelS2 OnGuard end to end encrypted solution. Utilization of BlueDiamond readers will allow future migration to the BlueDiamond Bluetooth based Mobile Credentials, if ever desired. The BlueDiamond Mobile Credential can be automatically provisioned from the LenelS2 NetBox system quickly and effortlessly. BlueDiamond readers are available in multiple form factors, including single gang, single gang with keypad, and mullion mount, allowing for a form factor that best fits NMUSD needs.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



LenelS2 BlueDiamond Readers



Intrusion

The NetBox solution provides complete alarm monitoring management capability. NetBox include live monitoring of all system alarms, providing the ability to configure individual alarm priorities and coloring, trigger audible alerts when an alarm occurs, as well as sending email and text alerts when alarms occurs. NetBox includes full alarm filtering allowing an operator to only focused on desired alarms based on type or priority. NetBox also includes a formalized alarm escalation workflow whereby if an alarm is not responded to within a user defined amount of it will automatically escalate to another NetBox operator. NetBox alarms can be fully integrate with video, allowing for live video to be displayed within the NetBox browser based client application when an alarm occurs, as well as tagging each event with the associated recorded video accessible through a video icon to the right of the event.

Integration with Alarm Panels

NetBox offers the monitoring of all doors as either a system input or it could be part of a portal that will annunciate a forced or a held door condition. NetBox also offers a keypad command feature that will allow you to arm/disarm any input. NetBox also has a network integration with DMP and Bosch Intrusion Panels. In addition, we can get integrate with hardwire relays to other intrusion panels for arm and disarming the system.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



LenelS2 VRx Video Management System

Based on the number of schools and the variable number of cameras LenelS2 recommends the VRx video management system. VRx is a next-generation video management platform available as either a physical Network Video Recorders (NVR) or as a software only solution that can run on user provider Video Recorder class servers that support Ubuntu Linux. The VRx is a key component to a unified access control and video surveillance experience when used in conjunction with the NetBox ecosystem access control system and Magic Monitor unified client.

Real-time video monitoring and recorded video playback of VRx stored video is accessible through the LenelS2 NetBox browser-based interface, Magic Monitor client or Mobile Security Professional mobile app. By clicking on an icon in the activity log, users can instantly play back recorded video associated with an event and save it to the case library. Additional features include onscreen PTZ controls and integration of live video views into floor plan graphics. VRx seamlessly fits into the NetBox ecosystem, allowing the entire solution to easily scale with organizational growth. The Linux-based VRx appliance is plug-and-play and operates similarly to other NetBox ecosystem products, making it easy to set up, configure and maintain.

VRx Key Features:

Video Management

- Cameras: Various models support 16, 32, 64 or 128 IP cameras
- High Quality Video: Supports H.264 and H.265
- Crowdsourced Video: Manages video submitted from the organizational community, making it available for playback during forensic investigation.
- Real-Time Surveillance: Allows for live video tours and on-screen PTZ controls using Magic Monitor.
- Forensic Search: Locates recorded video of interest with a single click and saves it.
- Storage: Various models support 4TB, 48TB, 144TB or 288TB of internal JBOD video storage
- Storage Management: Provides a simple user interface to add or replace media drives in the field.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



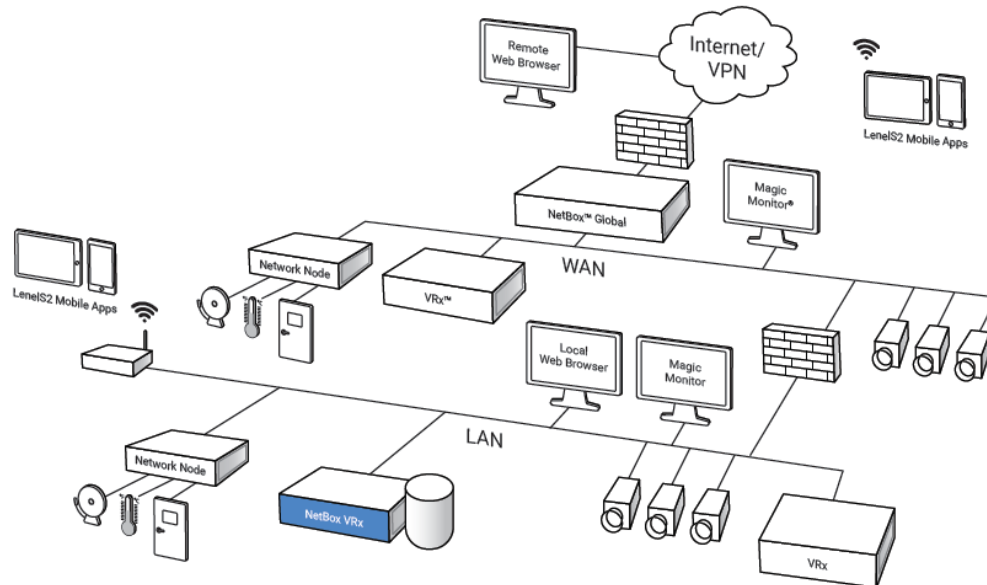
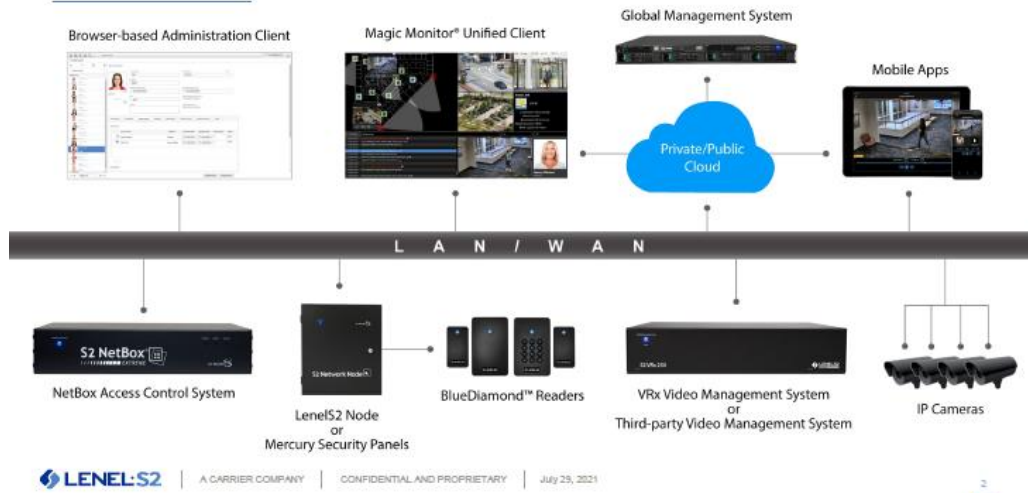
- Access Control Integration: Integrates with NetBox access control systems for unified system management and administration.
- Customizable Monitoring Displays: Provides customization of real-time monitoring displays, with single or multi-camera views.
- Mobile App: Allows for mobile security management using the Mobile Security Professional app.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534

System Diagram

NetBox Ecosystem Network Diagram





System Requirements

System requirements for off-the-shelf computer equipment utilized by the system.

The NetBox's browser based nature makes it truly platform independent, allowing it to run on desktops, laptops, tablets, and other devices that are able to utilize a web browser.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



Cybersecurity Program

Overview

When it comes to physical security, the complexity and interconnectedness of today's systems provide multiple potential entry points for would-be attackers. This is why LenelS2 incorporates information security into every phase of its products. LenelS2's comprehensive approach also empowers customers to implement cybersecurity best practices while remaining vigilant.

Design

At LenelS2, secure products are designed from the ground up. This means designing within a secure environment and reviewing all of the code to minimize potential vulnerabilities. The entire LenelS2 system architecture is protected from cloud to network to server to panels using the TLS 1.2 protocol. Inaccessible from outside its facility, the design process ensures that would-be attackers cannot gain an early advantage. LenelS2 teams operate within a series of firewalls and antivirus redundancies, and access to these systems is also highly restricted within the company.

Development and Quality Assurance

Developers follow coding best practices to ensure that no shortcuts are taken which could result in a product weakness. Both the development and quality assurance teams run a variety of scans to detect any potential vulnerabilities along the way. These scans range from static scans to dynamic scans, each of which detect different types of vulnerabilities. LenelS2 teams also run daily scans on new and existing codebases to ensure no vulnerabilities have cropped up over time.

Manufacturing

Once development and quality assurance have signed off on the product code, a golden copy – verified to be secure and virus free – is provided to manufacturing. As in the other stages of the process, manufacturing does its job almost entirely offline and always behind a series of firewalls. When manufacturing is "online," it is on a closed network. In fact, no product spends more than approximately five minutes connected to any sort of intranet. These brief periods are used for quick testing and licensing to make sure the product is working as intended.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



Installation and Deployment

The installation and deployment phase involves collaboration between LenelS2, Value Added Resellers (VAR) and end users. Systems that are installed or in use, run the risk of being compromised if appropriate measures are not taken to secure the operating environment. To mitigate this risk, LenelS2 provides cybersecurity best practices training to our Value Added Resellers and end users. Product requirements and guidelines – from forced default credential changes to networking recommendations – help secure systems in the field. When an installation is complete, the Value Added Reseller should perform a survey that reviews safe computing practices with the end user. This empowers the end user to employ best practices while monitoring for potential vulnerabilities.

Maintenance

Following deployment, Value Added Resellers receive timely updates with information and tools to keep systems secure. LenelS2 conducts daily scans for vulnerabilities and monitor for generalized cybersecurity threats. The LenelS2 Technical Support Team also immediately reports issues to end users and the Value Added Resellers.

If a vulnerability or exploit is found, LenelS2 systematically determines the best course of action whether it is an immediate patch within 24 hours, or simply a notification to raise awareness. LenelS2 receives bi-annual feedback from end users on our Cybersecurity Advisory Council to address emerging concerns.

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



Price Proposal

LenelS2 NetBox Budgetary Pricing Model

LenelS2 has a promotion in progress that is shown below:

NetBox Solution Package for K-12 Schools

K-12 schools have one of the most important jobs: to provide children with the educational foundation for future success while keeping them safe and healthy. To fulfill that expectation, schools require security technology that gives students the confidence to focus on learning. With over 2,000 unique deployments in school districts, LenelS2 provides scalable solutions for K-12 schools' most critical security challenges. Our NetBox™ solution package offers a comprehensive approach to school security. With every new NetBox Extreme or NetBox Enterprise access control system purchase, it includes discounts on hardware, training and additional software support.

The NetBox system is part of Carrier's Healthy Buildings Program, a suite of solutions and services that help support building and occupant health.

Solution Package Details*

Access Control

5 years of software support with new NetBox Extreme or NetBox Enterprise access control system (S2-SUSP)

Active Directory integration (S2-AD)

Database Partitioning (S2-DBP)

Magic Monitor® Professional unified client (S2-MM-PRO)

10% discount on Network Nodes and Mercury Security hardware

25% discount on BlueDiamond™ readers

Video Management

5 years of software support with new VRx™ video management system (S2-SUSP)

10% discount on any VRx system hardware or camera licenses

Training

2 seats of NetBox virtual training for end users

The below pricing model will include the following discounts:

- 5 years of software support with new NetBox Extreme or NetBox Enterprise access control system (S2-SUSP)
- Active Directory integration (S2-AD)
- Database Partitioning (S2-DBP)
- Magic Monitor® Professional unified client (S2-MM-PRO)
- 10% discount on Network Nodes and Mercury Security hardware
- 25% discount on BlueDiamond™ readers
- 5 years of software support with new VRx™ video management system (S2-SUSP)
- 10% discount on any VRx system hardware or camera licenses
- 2 seats of NetBox virtual training for end users

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



The pricing is based on counts ascertained from the provided NMUSD RFP. All assumptions and quantities are described within the description of each school. All pricing is based on the LenelS2 NetBox Manufacturer Suggested Retail Price (MSRP). The pricing includes the NetBox access control server and software, the VRx video recorder and software, Mercury access control panels, LifeSafety power enclosures, LenelS2 BlueDiamond readers. The pricing does not include cabling, conduit, electrical outlets, data connections, switches, cameras, door hardware, sensors, or labor.

Note: The chart depicted below states that each school has a quantity of intrusion detection panels per school. Each intrusion panel is required to be wired to an input module on the NetBox system which has 16 inputs. According to the chart, there 331 intrusion panels district wide. This will result in an equal number of input control modules.

Facility Type	Number of This Type	Card Readers		Cameras		Intrusion Panels		Equipment Locations	
		Each	Total	Each	Total	Each	Total	Each	Total
Elementary Campuses+Back Bay/Monte Vista+Early College	23	3	69	14	322	12	276	1	23
Middle School Campuses+Lincoln	3	7	21	12	36	5	15	1	3
7-12 (CdM & Costa Mesa) and 9-12 (Estancia & Newport Harbor) Campuses	4	10	40	12	48	10	40	6	24
			0		0		0		0
			0		0		0		0
			0		0		0		0
			0		0		0		0
Total Quantities	30		130		406		331		50

The typical system for a single elementary school is based on sixteen (3) BlueDiamond card readers (Part number S2-R10320-05TB), one (1) Mercury Intelligent Controller (Part number S2-LP-1502), one (1) Mercury MR52 Dual Reader Interface Modules (Part number S2-MR52-S3), one (1) LifeSafety Power Supply Enclosures (Part number LSP-8DR-E4M1), and one VRx 1000 Video Recorder (Part number S2-



VRX1000) with 12 TB of total storage, using three (3) 4 terabyte hard drives (Part number S2-NETVR-4TB-HDD) and 14 camera licenses. (Part number S2-VRX-1C).

		ELEMENTARY SCHOOL (23)		
69	S2-R10320-05TB	BlueDiamond Mobile Ready Reader	~~\$325.00~~	~~\$22,425.00~~
69		25% Discount	\$243.75	\$16,818.75
23	S2-LP-1502	Mercury LP1502 intelligent controller	~~\$2,348.00~~	~~\$54,004.00~~
23		10% Discount	\$2,113.20	\$48,603.60
23	S2-MR-52-S3	Mercury MR52dual reader interface module	~~\$850.00~~	~~\$19,550.00~~
23		10% Discount	\$765.00	\$17,595.00
23	LSP-8DR-E4M1	LifeSafety Power Supply and Enclosure	\$1,163.00	\$26,749.00
23	S2-VRX1000	VRx 1000 Video recorder	~~\$7,997.00~~	~~\$183,931.00~~
23		10% Discount	\$7,197.30	\$165,537.90
69	S2-NETVR-4TB-HDD	4TB storage hard drive	~~\$855.00~~	~~\$58,995.00~~
69		10% Discount	\$769.00	\$53,061.00
322	S2-VRX-1C	single VRx IP camera license	~~\$206.00~~	~~\$66,332.00~~
322		10% Discount	\$185.40	\$59,698.80
276	S2-MR-16IN-S3	MERCURY MR-16IN 16 INPUT MODULE	~~\$940.00~~	~~\$259,440.00~~
276		10% Discount	\$846.00	\$233,496.00
				\$639,953.15

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



The typical system for a single intermediate school is based on seven (7) BlueDiamond card readers (Part number S2-R10320-05TB), one (1) Mercury LP1502 Intelligent Controllers (Part number S2-LP-1502), three (3) Mercury MR52 Dual Reader Interface Modules (Part number S2-MR52-S3), one (1) LifeSafety Power Supply Enclosures (Part number LSP-8DR-E4M1), and one VRx 1000 Video Recorder (Part number S2-VRX1000) with 16 TB of total storage, using two (2) 8 terabyte hard drives (Part number S2-NETVR-8TB-HDD) and 36 camera licenses. (Part number S2-VRX-1C).

		MIDDLE SCHOOL (3)		
21	S2-R10320-05TB	BlueDiamond Mobile Ready Reader	~~\$325.00~~	~~\$6,825.00~~
21		25% Discount	\$243.75	\$5,118.75
3	S2-LP-1502	Mercury LP1502 intelligent controller	~~\$2,348.00~~	~~\$7,044.00~~
3		10% Discount	\$2,113.20	\$6,339.60
9	S2-MR-52-S3	Mercury MR52dual reader interface module	~~\$850.00~~	~~\$7,650.00~~
9		10% Discount	\$765.00	\$6,885.00
3	LSP-8DR-E4M1	LifeSafety Power Supply and Enclosure	\$1,163.00	\$3,489.00
3	S2-VRX1000	VRx 1000 Video recorder	~~\$7,997.00~~	~~\$23,991.00~~
3		10% Discount	\$7,197.30	\$21,591.90
6	S2-NETVR-8TB-HDD	8TB storage hard drive	~~\$855.00~~	~~\$5,130.00~~
6		10% Discount	\$769.00	\$4,614.00
36	S2-VRX-1C	single VRx IP camera license	~~\$206.00~~	~~\$7,416.00~~
36		10% Discount	\$185.40	\$6,674.40
15	S2-MR-16IN-S3	MERCURY MR-16IN 16 INPUT MODULE	~~\$940.00~~	~~\$14,100.00~~
15		10% Discount	\$846.00	\$12,690.00
				\$69,801.75

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



The typical system for a single high school is based on ten (10) BlueDiamond card readers (Part number S2-R10320-05TB), one (1) Mercury LP1502 Intelligent Controller (Part number S2-LP-1502), four (4) Mercury MR52 Dual Reader Interface Modules (Part number S2-MR52-S3), four (4) LifeSafety Power Supply Enclosures (Part number LSP-8DR-E4M1), and one VRx 1500 Video Recorder (Part number S2-VRX1500) with 48 TB of total storage, of which 36TB are usable due to RAID-5 storage redundancy, using four (4) 12 terabyte hard drives (Part number S2-NETVR-12TB-HDD) and 48 camera licenses. (Part number S2-VRX-1C).

		HIGH SCHOOL & 9-12 (4)		
40	S2-R10320-05TB	BlueDiamond Mobile Ready Reader	~~\$325.00~~	~~\$13,000.00~~
40		25% Discount	\$243.75	\$9,750.00
4	S2-LP-1502	Mercury LP1502 intelligent controller	~~\$2,348.00~~	~~\$9,392.00~~
4		10% Discount	\$2,113.20	\$8,452.80
16	S2-MR-52-S3	Mercury MR52dual reader interface module	~~\$850.00~~	~~\$13,600.00~~
16		10% Discount	\$765.00	\$12,240.00
4	LSP-8DR-E4M1	LifeSafety Power Supply and Enclosure	\$1,163.00	\$4,652.00
4	S2-VRX1000	VRx 1000 Video recorder	~~\$7,997.00~~	~~\$31,988.00~~
4		10% Discount	\$7,197.30	\$28,789.20
16	S2-NETVR-8TB-HDD	8TB storage hard drive	~~\$855.00~~	~~\$13,680.00~~
6		10% Discount	\$769.00	\$4,614.00
48	S2-VRX-1C	single VRx IP camera license	~~\$206.00~~	~~\$9,888.00~~
48		10% Discount	\$185.40	\$8,899.20
40	S2-MR-16IN-S3	MERCURY MR-16IN 16 INPUT MODULE	~~\$940.00~~	~~\$37,600.00~~
40		10% Discount	\$846.00	\$33,840.00
				\$111,237.20

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



SUMMARY:

The pricing model total includes support for thirty (30) schools, with a total of 130 readers and 406 cameras, a single NetBox Enterprise access control server, and thirty (30) VRx video recorders, one video recorder per school.

1	S2-EX50-128	NetBox Enterprise 50 Server and Software	\$26,780.00	\$ 26,780.00
9	S2-NR64	64 portal (reader) expansion	\$4,574.00	\$ 41,166.00
	S2-SUSP24	SUPPORT EMERGENCY 24/7 SERVICES	No Charge	
	S2-MM-PRO	MAGIC MONITOR PROFESSIONAL LICENSE	No Charge	
2	TRAINING- ONLINE	Annual subscription to access NetBox online training (per person).	No Charge	
		ELEMENTARY SCHOOLS		\$ 639,953.15
		MIDDLE SCHOOLS		\$ 69,801.75
		HIGH SCHOOLS		\$ 111,237.20
		TOTAL SOLUTION COST:		\$ 888,938.10

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



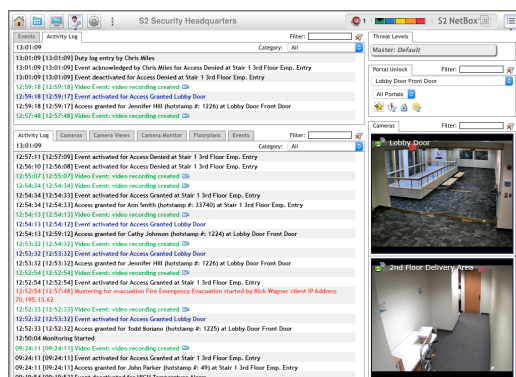
S2 NetBox® Enterprise

Overview

S2 NetBox Enterprise is a powerful, web-based access control and event monitoring system designed for deployments with demanding security requirements. The system can support over 7,000 portals and over 500 S2 Nodes. Optional high availability offers automatic system failover between a redundant pair of servers. Optional system partitioning allows the entire database to be separated into multiple smaller systems for entities such as field offices or tenants.

Features such as person record and cardholder management, event and alarm monitoring, threat level escalation and reporting are accessible from any web browser. There is no software to install. S2 NetBox Enterprise works with existing infrastructure and peripheral devices, making it easy to deploy. In addition, S2 NetBox Enterprise tightly integrates with S2 NetVR® series video management systems, providing unified system management and administration. Integration with third party video management systems is also supported.

S2 NetBox Enterprise is ideal for large, complex security deployments. For organizations that have outgrown their S2 NetBox system, the upgrade to S2 NetBox Enterprise is seamless. Distributed enterprises can manage multiple S2 NetBox Enterprise servers with S2 Global®, allowing for virtually unlimited scalability.



S2 NetBox Enterprise is web-based, with one-click access to major system functionality.

Key Features

Access Control

- **Portals:** Supports up to 7,168 doors or other access points
- **Event and Alarm Monitoring:** Includes comprehensive event logging, notification and escalation
- **Threat Level Management:** Provides configurable system status and response actions such as system lock downs
- **Person Record Management:** Maintains detailed, credential-driven user records and access history
- **Reporting:** Offers pre-defined and custom reports

System

- **Web Interface:** Delivers browser-based, unified system management and administration
- **Solid-State Design:** Extends product lifecycle, lowering total cost of ownership
- **Video Integration:** Works with S2 NetVR series video management systems and other third party video systems
- **API Support:** Integrates with third party products such as human resource databases via an open source API
- **Automated System Management:** Automatically discovers S2 Nodes and handles system backups
- **Mobile App:** Allows for mobile security management using S2 Mobile Security Officer®
- **System Partitioning Option:** Allows the entire database to be separated into multiple smaller systems
- **High Availability Option:** Offers automatic system failover between a redundant pair of servers

Specifications

S2 NetBox Enterprise 50

Access Control	
Cardholders	150,000
Access Levels	Unlimited
Unique User Roles	16
Simultaneous Users	25
Time Specifications	512
Portal Capacity	1,792
S2 Node Capacity ¹	128
Maximum Inputs / Outputs	2,000 / 2,000
Online Transactions	Up to 160 million records
Client Requirements	
Operating System	Any; for badging use Windows 7
Browser ²	Chrome, Internet Explorer, Firefox and Safari
Processor	Intel Core i3 or higher
Memory (RAM)	8GB minimum
Hard Drive	100GB minimum
Appliance	
Storage Capacity	128GB
Storage Configuration	N/A
Processor	Intel Pentium
Memory (RAM)	4GB
Operating System	Ubuntu Linux
Ethernet Ports	1
MTBF	172,199
Chassis	Standard 1U rack mount, rail kit included
Dimensions (H, W, D)	1.67in x 17.25in x 21.8in (4.24cm x 43.82cm x 55.37cm)
Weight	18 lbs (8.17 kg)
Operating Temperature	50° – 95°F (10° – 35°C)
Storage Temperature	-40° – 158°F (-40° – 70°C)
Operating Environment	Humidity 85%, non-condensing 35°C
AC Input	100 – 240 VAC, 50/60 Hz, 6/3A
BTU Maximum	948 per hour
Regulatory Approvals	UL, CE, FCC, RoHS
Warranty	2 years, hardware; 1 year, software
Integrations ³	
Video Management	S2 NetVR series VMS and other major VMS manufacturers
S2 NetVR Capacity	64
S2 NetVR Camera Capacity	4,096
Concurrent S2 Client Connections (S2 NetBox, S2 Magic Monitor®, S2 Mobile Security Officer)	25
Third Party VMS Camera Capacity	1,024
Access Control	Allegion, ASSA ABLOY, DMP and Mercury

S2 NetBox Enterprise 100

Access Control	
Cardholders	150,000
Access Levels	Unlimited
Unique User Roles	16
Simultaneous Users	35
Time Specifications	512
Portal Capacity	7,168
S2 Node Capacity ¹	512
Maximum Inputs / Outputs	2,000 / 2,000
Online Transactions	Up to 400 million records
Client Requirements	
Operating System	Any; for badging use Windows 7
Browser ²	Chrome, Internet Explorer, Firefox and Safari
Processor	Intel Core i3 or higher
Memory (RAM)	8GB minimum
Hard Drive	100GB minimum
Appliance	
Storage Capacity	128GB
Storage Configuration	RAID 1
Processor	Intel Xeon quad core
Memory (RAM)	8GB
Operating System	Ubuntu Linux
Ethernet Ports	1
MTBF	172,199
Chassis	Standard 1U rack mount, rail kit included
Dimensions (H, W, D)	1.67in x 17.25in x 21.8in (4.24cm x 43.82cm x 55.37cm)
Weight	18 lbs (8.17 kg)
Operating Temperature	50° – 95°F (10° – 35°C)
Storage Temperature	-40° – 158°F (-40° – 70°C)
Operating Environment	Humidity 85%, non-condensing 35° C
AC Input	100 – 240 VAC, 50/60 Hz, 6/3A
BTU Maximum	1,327 per hour
Regulatory Approvals	UL, CE, FCC, RoHS
Warranty	2 years, hardware; 1 year, software
Integrations ³	
Video Management	S2 NetVR series VMS and other major VMS manufacturers
S2 NetVR Capacity	128
S2 NetVR Camera Capacity	4,096
Concurrent S2 Client Connections (S2 NetBox, S2 Magic Monitor®, S2 Mobile Security Officer)	35
Third Party VMS Camera Capacity	1,024
Access Control	Allegion, ASSA ABLOY, DMP and Mercury

Specifications (continued)

S2 NetBox Enterprise 50

Part Numbers

S2-EX50-128

Includes 128 portal license

Portal licenses expandable in 64 portal increments to 1,792 portals.
Refer to price book for additional part numbers.

S2 NetBox Enterprise 100

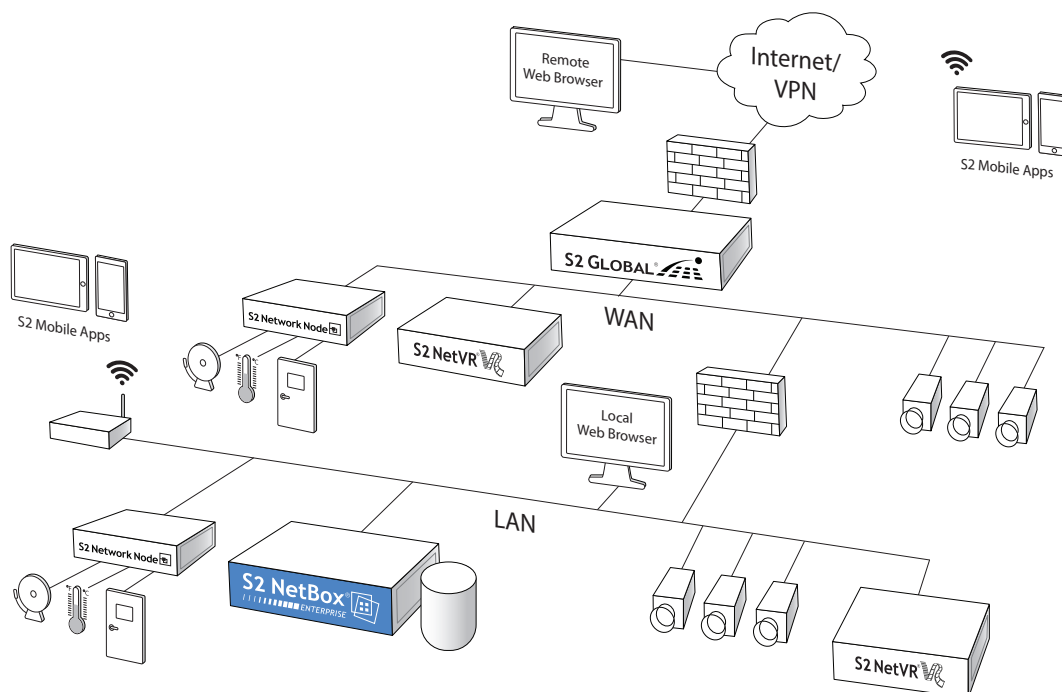
Part Numbers

S2-EX100-128

Includes 128 portal license

Portal licenses expandable in 64 portal increments to 7,168 portals.
High availability option offered. Refer to price book for additional part numbers.

Schematic Diagram - S2 Security System



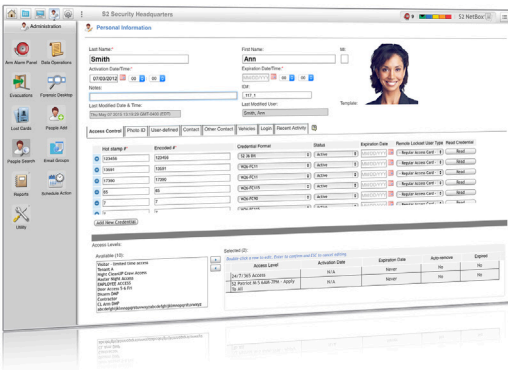
Schematic only. Not a network diagram.

¹ S2 Network Node capacity may vary depending on system design.

² Refer to the latest Release Notes for browser version compatibility.

³ For additional integration information, contact sales@s2sys.com.

For more information, please visit www.s2sys.com.



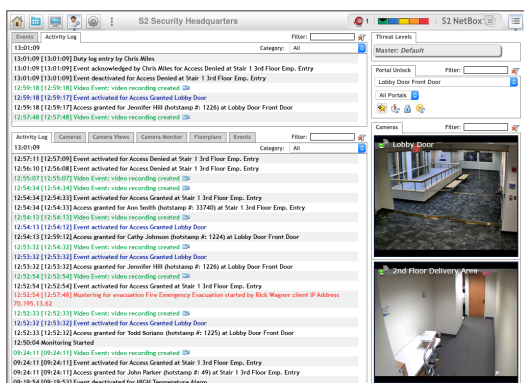
S2 NetBox® Virtual Machine

Overview

S2 NetBox Virtual Machine is a powerful, web-based access control and event monitoring system that can be installed on user-preferred hardware. The highly scalable system supports a wide range of deployments and enables users to build a system supporting over 7,000 portals and more than 500 S2 Nodes. Optional system partitioning allows the entire database to be separated into multiple smaller systems for entities such as field officers or tenants.

Features such as person record and cardholder management, event and alarm monitoring, threat level escalation and reporting are accessible from any web browser. S2 NetBox Virtual Machine works with existing infrastructure and peripheral devices, making it easy to deploy. In addition, S2 NetBox Virtual Machine tightly integrates with S2 NetVR® series video management systems, providing unified system management and administration. Integration with third-party video management systems is also supported.

S2 NetBox Virtual Machine is ideal for organizations that choose to implement an access control solution on their preferred hardware platform. Distributed enterprises can manage multiple S2 NetBox Virtual Machine servers with S2 Global®, allowing for nearly unlimited scalability.



S2 NetBox Virtual Machine is web-based, with one-click access to major system functionality.

Key Features

Access Control

- **Portals:** Supports up to 7,168 doors or other access points
- **Event and Alarm Monitoring:** Includes comprehensive event logging, notification and escalation
- **Threat Level Management:** Provides configurable system status and response actions such as system lock downs
- **Person Record Management:** Maintains detailed, credential-driven user records and access history
- **Reporting:** Offers predefined and custom reports

System

- **Custom Access Control Solution:** Operates on a user-preferred hardware platform¹
- **Web Interface:** Delivers browser-based, unified system management and administration
- **Video Integration:** Works with S2 NetVR series video management systems and other third-party video systems
- **API Support:** Integrates with third-party products such as human resource databases via an open source API
- **Automated System Management:** Automatically discovers S2 Nodes and handles system backups
- **Mobile App:** Allows for mobile security management using S2 Mobile Security Officer®
- **System Partitioning Option:** Allows the entire database to be separated into multiple smaller systems

S2 NetBox Virtual Machine - Specifications

Portal Capacity: 16 to 64

Access Control	
Cardholders	40,000
Access Levels	Unlimited
Unique User Roles	16
Simultaneous Users	10
Time Specifications	512
Portal Capacity	64
S2 Node Capacity ²	64
Maximum Inputs / Outputs	2,000 / 2,000
Online Transactions	Up to 40 million records
Client Requirements	
Operating System	Any
Browser ³	Chrome, Internet Explorer, Firefox and Safari
Processor	Intel Core i3 or higher
Memory (RAM)	8GB minimum
Hard Drive	100GB minimum
Minimum Provisioning Requirements	
Storage Capacity	128GB Pro Series SSD
Processor	Intel Xeon Quad Core
Memory (RAM)	8GB
Ethernet Ports	1
Server Host	VMWare ESXi 5.1 or later
S2 Hardware	Minimum of 1 S2 MicroNode Plus, S2 Network Node or S2 Network Node VR
Warranty	1 year, software
Integrations ⁴	
Video Management	S2 NetVR series VMS and other major VMS manufacturers
S2 NetVR Capacity	16
S2 NetVR Camera Capacity	1,024
Concurrent S2 Client Connections (S2 NetBox, S2 Magic Monitor®, S2 Mobile Security Officer)	10
Third-Party VMS Camera Capacity	256
Access Control	Allegion, ASSA ABLOY, DMP and Mercury
Part Numbers	
S2-NBVM-16	Includes 16 portal license
S2-NBVM-32	Includes 32 portal license
S2-NBVM-64	Includes 64 portal license

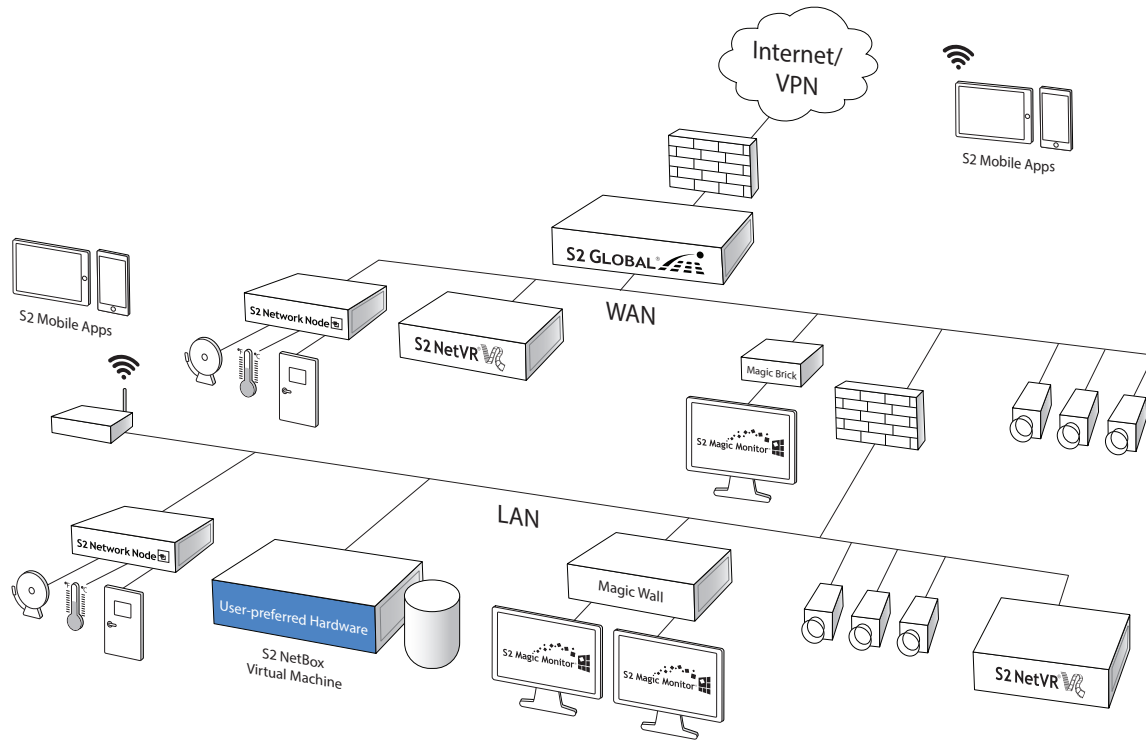
Portal licenses expandable in 64 portal increments to 7,168 portals. Refer to price book for additional part numbers.

Portal Capacity: 128 to 7,168

Access Control	
Cardholders	150,000
Access Levels	Unlimited
Unique User Roles	16
Simultaneous Users	35
Time Specifications	512
Portal Capacity	7,168
S2 Node Capacity ²	512
Maximum Inputs / Outputs	2,000 / 2,000
Online Transactions	Up to 400 million records
Client Requirements	
Operating System	Any
Browser ³	Chrome, Internet Explorer, Firefox and Safari
Processor	Intel Core i3 or higher
Memory (RAM)	8GB minimum
Hard Drive	100GB minimum
Minimum Provisioning Requirements	
Storage Capacity	128GB Pro Series SSD
Processor	Intel Xeon Quad Core
Memory (RAM)	8GB
Ethernet Ports	1
Server Host	VMWare ESXi 5.1 or later
S2 Hardware	Minimum of 1 S2 MicroNode Plus, S2 Network Node or S2 Network Node VR
Warranty	1 year, software
Integrations ⁴	
Video Management	S2 NetVR Series VMS and other major VMS manufacturers
S2 NetVR Capacity	128
S2 NetVR Camera Capacity	4,096
Concurrent S2 Client Connections (S2 NetBox, S2 Magic Monitor, S2 Mobile Security Officer)	35
Third-Party VMS Camera Capacity	1,024
Access Control	Allegion, ASSA ABLOY, DMP and Mercury
Part Numbers	
S2-NBVM-128	Includes 128 portal license

Portal licenses expandable in 64 portal increments to 7,168 portals. Refer to price book for additional part numbers.

Schematic Diagram - S2 Security System



Schematic only. Not a network diagram.

¹ User-preferred hardware must meet minimum provisioning requirements.

² S2 Network Node capacity may vary depending on system design.

³ Refer to the latest Release Notes for browser version compatibility.

⁴ For additional integration information, contact sales@s2sys.com.

For more information, please visit www.s2sys.com.



S2 VRx 1000

Overview

S2 VRx 1000 video management system supports up to 32 IP cameras and up to 48TB of video storage, making the system well suited for mid-sized deployments. Real-time video monitoring and recorded video playback are accessible through the S2 VRx web interface, S2 Magic Monitor® client or S2 Mobile Security Professional® mobile app.

S2 VRx 1000 is available as a stand-alone system and also tightly integrates with S2 NetBox® access control systems. Real-time video surveillance and recorded video playback are unified with the activity log in the user interface. By clicking on an icon in the activity log, users can instantly play back recorded video associated with an event and save it to the case library. Additional features include on-screen PTZ controls and integration of live video views into floor plan graphics in S2 Magic Monitor.

S2 VRx 1000 includes the capability to manage and display crowdsourced video. Video footage submitted to the security team can be stored on the S2 VRx 1000 server and made available for forensic investigation.

Multiple S2 VRx 1000 servers can be managed with the S2 Magic Monitor client or connect to a single S2 NetBox controller, allowing the system to easily scale with organizational growth.

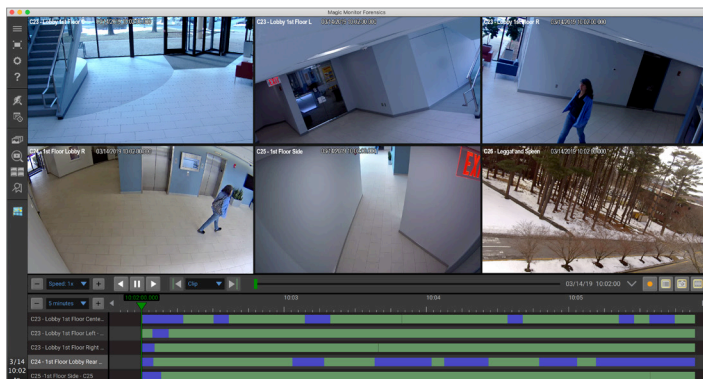
Key Features

Video Management

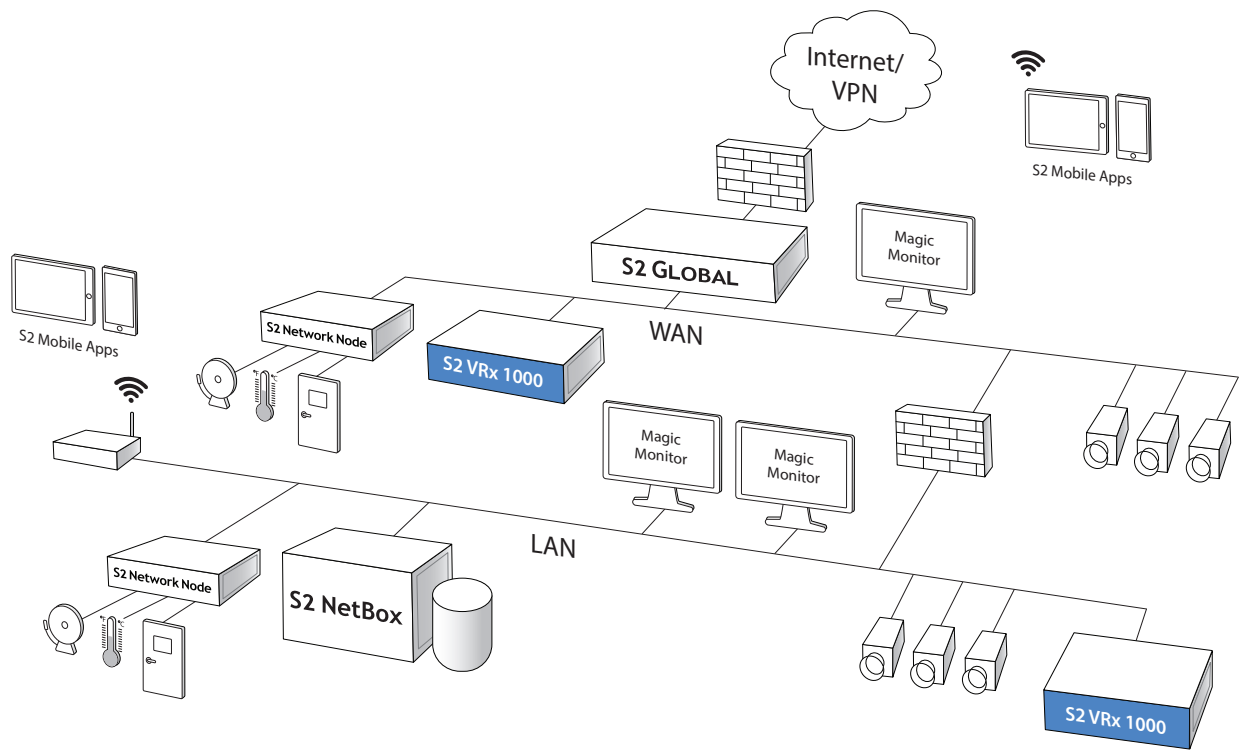
- **Cameras:** Supports up to 32 IP cameras
- **High Quality Video:** Supports 4K cameras and H.265 storage
- **Crowdsourced Video:** Manages video submitted from the organizational community, making it available for playback during forensic investigation
- **Real-Time Surveillance:** Allows for live video tours and on-screen PTZ controls using S2 Magic Monitor
- **Forensic Search:** Locates recorded video of interest with a single click and saves it to the case library
- **Storage:** Supports up to 48TB of internal JBOD video storage
- **Storage Management:** Provides a simple user interface to add or replace media drives in the field

System

- **IP Video Server:** Delivers real-time and recorded video to client
- **Access Control Integration:** Integrates with S2 access control systems for unified system management and administration
- **Customizable Monitoring Displays:** Provides customization of real-time monitoring displays, with single or multi-camera views
- **Mobile App:** Allows for mobile security management using S2 Mobile Security Professional



Easily search, review and catalog video with Magic Monitor Forensics.



Schematic only. Not a network diagram.

Specifications – S2 VRx 1000

Video Management

IP Camera Streams	Up to 32
IP Camera Resolution	IP camera dependent
IP Camera Frame Rate	IP camera dependent
Compression Type	H.264 or H.265 (camera dependent)

Appliance

Video Storage	48TB maximum capacity using 4TB, 8TB, or 12TB removable 3.5in drives
Storage Configuration	JBOD
Processor	Intel Xeon E3-1220v5
Memory (RAM)	8GB
Operating System	Ubuntu Linux
OS/Application Storage	80GB SSD minimum
Ethernet Ports	2, expandable to 4
Max Video Throughput (Aggregate Inbound)	400 Mbps
MTBF	51,700
Chassis	Standard 1U rack mount, rail kit included
Dimensions (H, W, D)	1.75in x 19.0in x 21.8in (44.45mm x 482.60mm x 553.72mm)

Appliance (continued)

Weight	23 lbs (10.4 kg) maximum
Operating Temperature	50° – 95°F (10° – 35°C)
Storage Temperature	-40° – 158°F (-40° – 70°C)
Operating Environment	Humidity 85%, non-condensing 35°C
AC Input	100 – 240 VAC, 50/60 Hz, 6A/3A
BTU Maximum	1,075 per hour
Regulatory Approvals	UL, CE, FCC, RoHS
Warranty	3 years, hardware; 3 years, software

Client Requirements

Operating System	Windows 10 (64 bit), macOS High Sierra and later
Processor	Intel Core i3 or higher
Memory (RAM)	8GB minimum
Hard Drive	100GB minimum

Part Numbers

S2-VRX1000	IP camera licenses expandable up to 32 IP cameras; storage configurations available in 4TB, 8TB, or 12TB increments
-------------------	--

For more information, please visit lenelS2.com.



S2 VRx 1500

Overview

S2 VRx 1500 video management system supports up to 64 IP cameras and up to 48TB of video storage, making the system well suited for mid-sized deployments. Real-time video monitoring and recorded video playback are accessible through the S2 VRx web interface, S2 Magic Monitor® client or S2 Mobile Security Professional® mobile app.

S2 VRx 1500 is available as a stand-alone system and also tightly integrates with S2 NetBox® access control systems. Real-time video surveillance and recorded video playback are unified with the activity log in the user interface. By clicking on an icon in the activity log, users can instantly play back recorded video associated with an event and save it to the case library. Additional features include on-screen PTZ controls and integration of live video views into floor plan graphics in S2 Magic Monitor.

S2 VRx 1500 includes the capability to manage and display crowdsourced video. Video footage submitted to the security team can be stored on the S2 VRx 1500 server and made available for forensic investigation.

Multiple S2 VRx 1500 servers can be managed with the S2 Magic Monitor client or connect to a single S2 NetBox controller, allowing the system to easily scale with organizational growth.

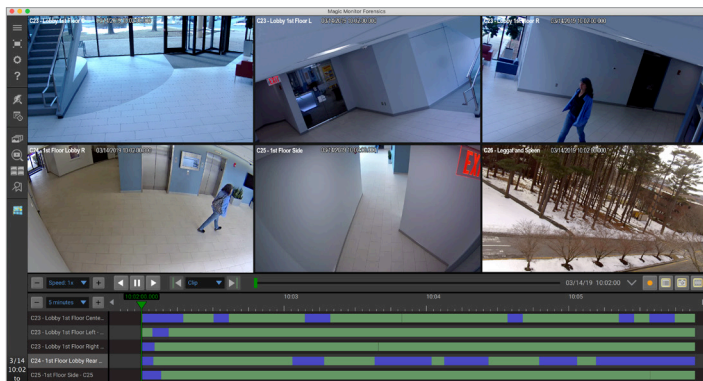
Key Features

Video Management

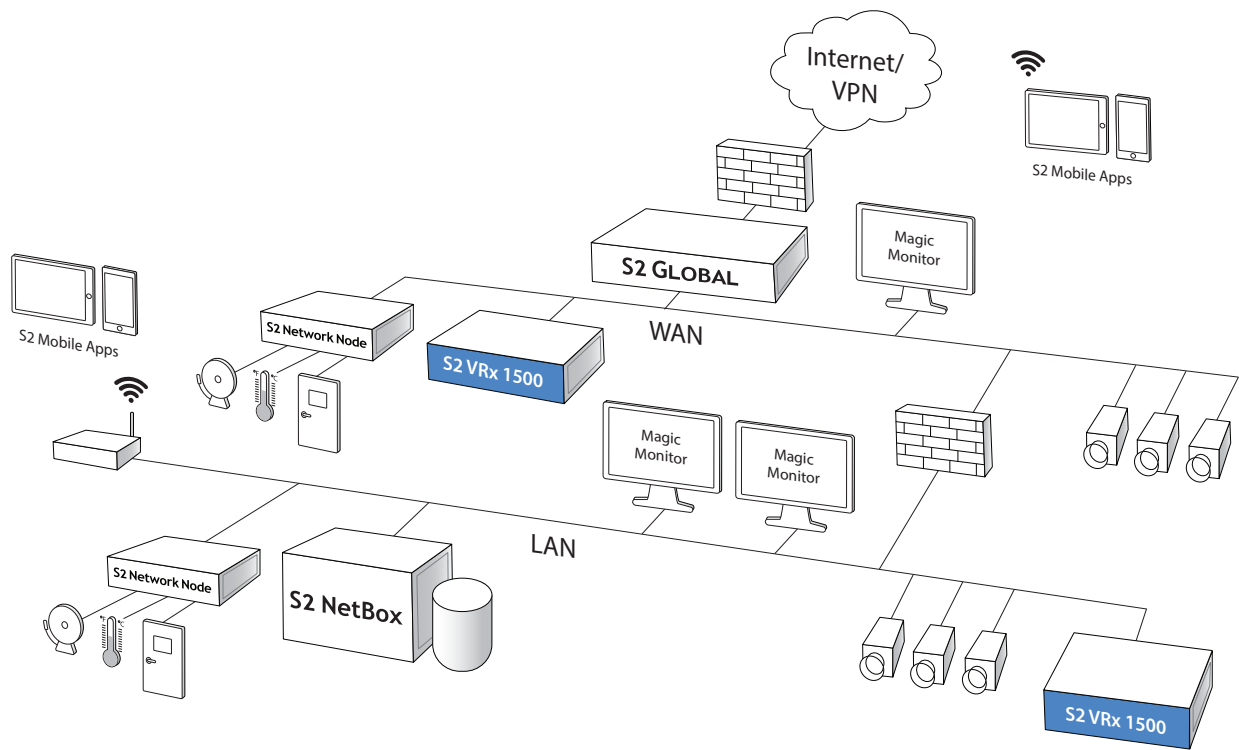
- **Cameras:** Supports up to 64 IP cameras
- **High Quality Video:** Supports 4K cameras and H.265 storage
- **Crowdsourced Video:** Manages video submitted from the organizational community, making it available for playback during forensic investigation
- **Real-Time Surveillance:** Allows for live video tours and on-screen PTZ controls using S2 Magic Monitor
- **Forensic Search:** Locates recorded video of interest with a single click and saves it to the case library
- **Storage:** Supports up to 48TB of internal RAID 5 or RAID 6 video storage
- **Storage Management:** Provides a simple user interface to add or replace media drives in the field

System

- **IP Video Server:** Delivers real-time and recorded video to client
- **Access Control Integration:** Integrates with S2 access control systems for unified system management and administration
- **Customizable Monitoring Displays:** Provides customization of real-time monitoring displays, with single or multi-camera views
- **Mobile App:** Allows for mobile security management using S2 Mobile Security Professional



Easily search, review and catalog video with Magic Monitor Forensics.

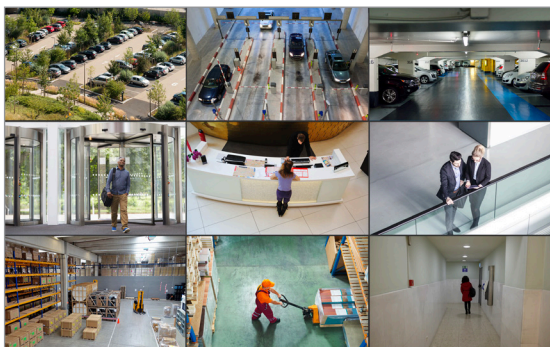


Schematic only. Not a network diagram.

Specifications – S2 VRx 1500

Video Management	
IP Camera Streams	Up to 64
IP Camera Resolution	IP camera dependent
IP Camera Frame Rate	IP camera dependent
Compression Type	H.264 or H.265 (camera dependent)
Appliance	
Video Storage	48TB maximum capacity using 4TB, 8TB, or 12TB hot swappable 3.5in drives
Storage Configuration	RAID 5 or RAID 6
Processor	Intel Xeon E3-1220v5
Memory (RAM)	8GB
Operating System	Ubuntu Linux
OS/Application Storage	80GB SSD minimum
Ethernet Ports	2, expandable to 4
Max Video Throughput (Aggregate Inbound)	400 Mbps
MTBF	45,600
Chassis	Standard 1U rack mount, rail kit included
Dimensions (H, W, D)	1.75in x 19.0in x 21.8in (44.45mm x 482.60mm x 553.72mm)
Appliance (continued)	
Weight	23 lbs (10.4 kg) maximum
Operating Temperature	50° – 95°F (10° – 35°C)
Storage Temperature	-40° – 158°F (-40° – 70°C)
Operating Environment	Humidity 85%, non-condensing 35°C
AC Input	100 – 240 VAC, 50/60 Hz, 6A/3A
BTU Maximum	1,075 per hour
Regulatory Approvals	UL, CE, FCC, RoHS
Warranty	3 years, hardware; 3 years, software
Client Requirements	
Operating System	Windows 10 (64 bit), macOS High Sierra and later
Processor	Intel Core i3 or higher
Memory (RAM)	8GB minimum
Hard Drive	100GB minimum
Part Numbers	
S2-VRX1500	IP camera licenses expandable up to 64 IP cameras; storage configurations available in 4TB, 8TB, or 12TB increments

For more information, please visit lenelS2.com.



S2 VRx Virtual Machine

Overview

S2 VRx Virtual Machine is a high-performance enterprise video management system that can be installed on user-preferred hardware. Supporting up to 128 IP cameras, the system is well suited for large security deployments. Real-time video monitoring and recorded video playback are accessible through the S2 VRx web interface, S2 Magic Monitor® client or S2 Mobile Security Professional® mobile app.

S2 VRx Virtual Machine tightly integrates with S2 NetBox® access control systems. Real-time video surveillance and recorded video playback are unified with the activity log in the user interface. By clicking on an icon in the activity log, users can instantly play back recorded video associated with an event and save it to the case library. Additional features include on-screen PTZ controls and integration of live video views into floor plan graphics in S2 Magic Monitor.

S2 VRx Virtual Machine includes the capability to manage and display crowdsourced video. Video footage submitted to the security team can be made available for forensic investigation.

S2 VRx Virtual Machine is ideal for organizations that choose to implement a video management solution on their preferred hardware platform. Multiple S2 VRx Virtual Machine systems can be managed with the S2 Magic Monitor client or connect to a single S2 NetBox controller. For distributed installations, multiple S2 NetBox controllers and S2 VRx Virtual Machines can be centrally managed with S2 Global®, allowing for nearly unlimited scalability.

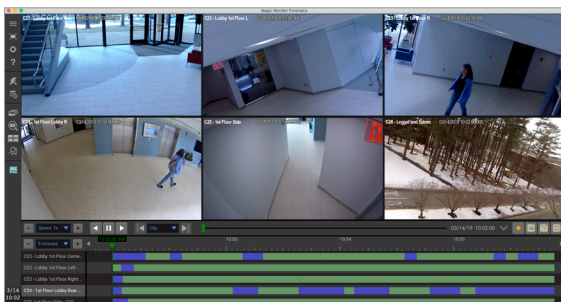
Key Features

Video Management

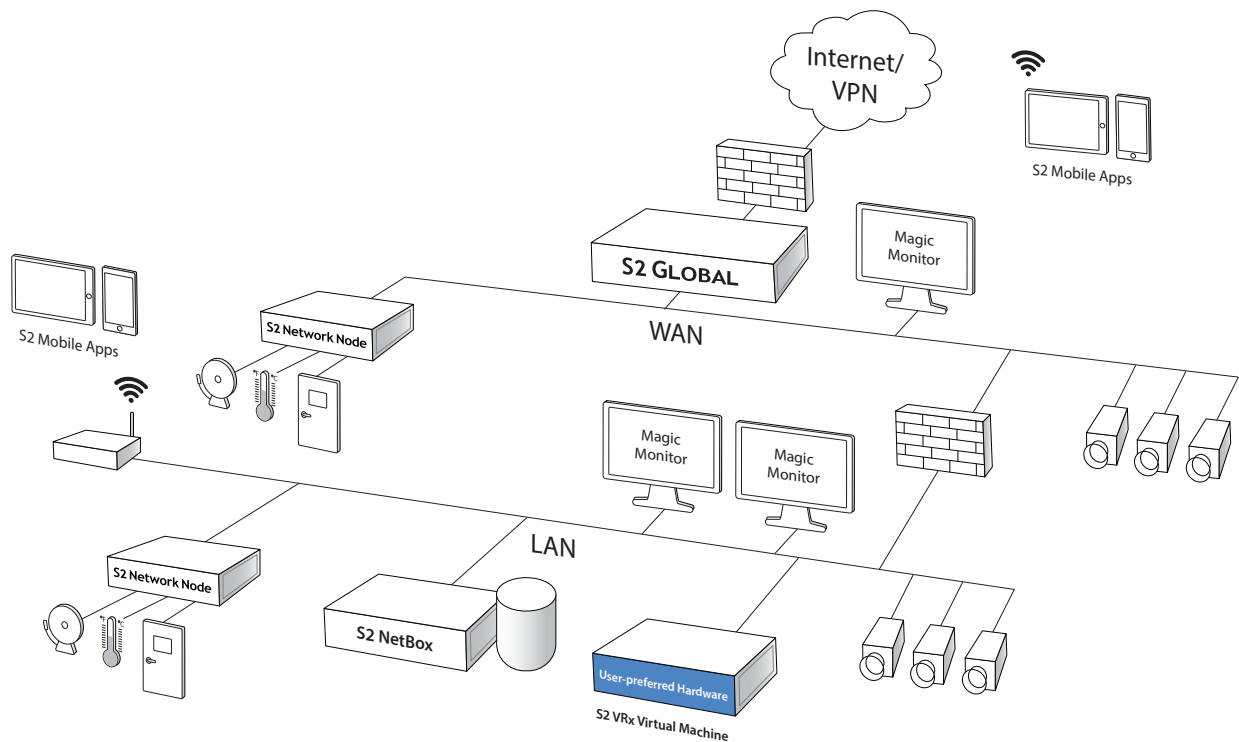
- **Cameras:** Supports up to 128 IP cameras
- **High Quality Video:** Supports 4K cameras and H.265 storage
- **Crowdsourced Video:** Manages video submitted from the organizational community, making it available for playback during forensic investigation
- **Real-Time Surveillance:** Allows for live video tours and on-screen PTZ controls
- **Forensic Search:** Locates recorded video of interest with a single click and saves it to the case library

System

- **IP Video Server:** Delivers real-time and recorded video to client
- **Access Control Integration:** Integrates with S2 access control systems for unified system management and administration
- **Customizable Monitoring Displays:** Provides customization of real-time monitoring displays, with single or multi-camera views
- **Mobile App:** Allows for mobile security management using S2 Mobile Security Professional



Easily search, review and catalog video with Magic Monitor Forensics.



Specifications – S2 VRx Virtual Machine

Video Management	
IP Camera Streams	Up to 128
IP Camera Resolution	IP camera dependent
IP Camera Frame Rate	IP camera dependent
Compression Type	H.264 or H.265 (camera dependent)
Client Requirements	
Operating System	Windows 10 (64 bit), macOS High Sierra and later
Processor	Intel Core i5 or higher
Memory (RAM)	8GB minimum
Hard Drive	100GB minimum
Minimum Provisioning Requirements	
Storage Capacity	8TB minimum
Processor	Intel Xeon Quad Core (3.1 GHz)
Memory (RAM)	16GB minimum
Gigabit Ethernet Ports	2 minimum
Server Host	VMWare ESXi v6.5 or later
Warranty	3 years, software
Part Numbers	
S2-VRX-VM	IP camera licenses expandable up to 128 IP cameras

For more information, please visit lenels2.com.

S2 Magic Monitor[®]

Unified security management



Everything you need, all in one stunning user interface. S2 Magic Monitor provides an unsurpassed user experience, unifying access control, video surveillance, forensics, digital signage and live Internet feeds.

Solve a wide range of security challenges with S2 Magic Monitor.



Empower your security operations center

Operators focus on critical tasks without becoming overwhelmed. Magic Monitor allows them to handle incidents according to your policies and procedures.

Direct public response to events and alarms

Video and digital signage appear on Magic Monitor in response to events and alarms, guiding staff and visitors to safety.



Unify all of your security needs in a single client

Whether you have a single display, a command center workstation or expansive video walls, Magic Monitor allows you to manage access control and video in one place.



Enhance situational awareness and operational efficiency

Integrated access control, video and live Internet feeds give you a 360° view of what's happening. Design the interactive content and layouts you need to create the ideal workflow.



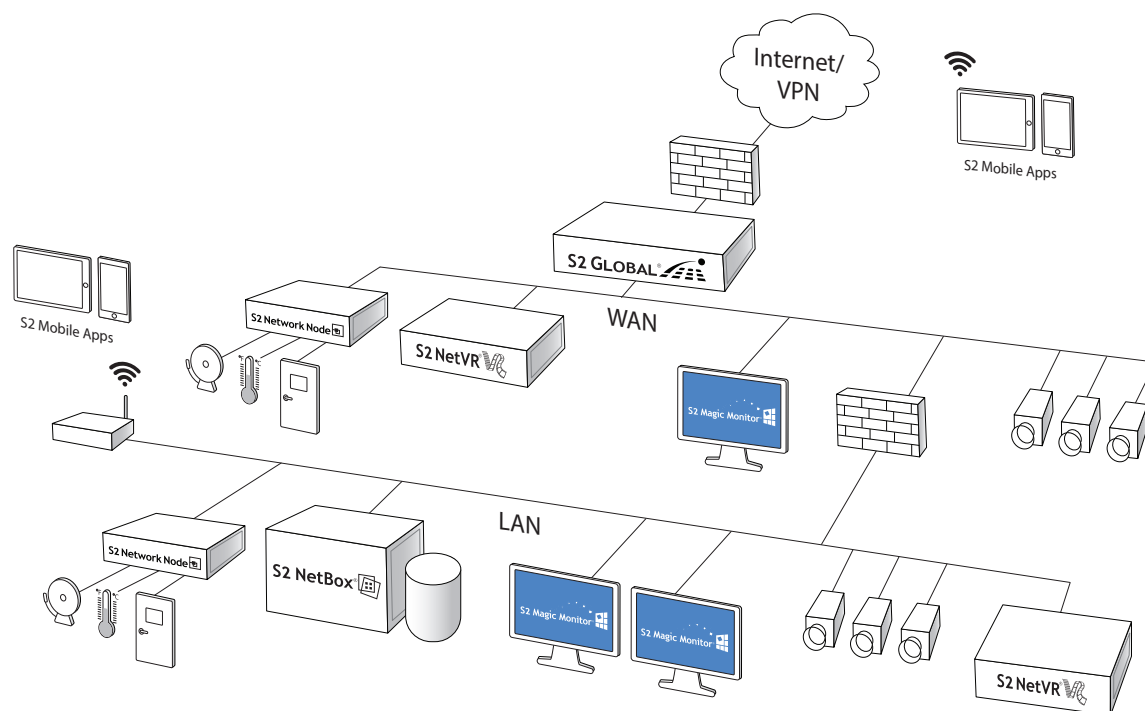
Search, review, and catalog video with amazing ease

Quickly locate the evidence you need to address situations more effectively. With Magic Monitor Forensics, recorded video from any camera is at your fingertips.

Control messaging across your facility

Magic Monitor presents dynamic digital signage, promotional videos and camera feeds in environments ranging from corporate lobbies to campuses to retail.





Schematic only. Not a network diagram.

Specifications – S2 Magic Monitor

Video Management

Maximum Total Bitrate	100 Mbps
Maximum Camera Resolution	IP camera dependent
S2 NetVR® Software	Version 1.5 and later

Access Control

S2 NetBox® Software	Version 4.9.13 and later
----------------------------	--------------------------

Tablet Requirements

Hardware	Any tablet running Windows 10
Operating System	Windows 10
Processor	Intel Core i5 or higher
Memory (RAM)	4GB minimum
Simultaneous Camera Views	9 cameras: 1080p, 15 fps 16 cameras: 720p, 15 fps

Minimum Client Requirements

Operating System	Windows 10, 64-bit Mac OS X Sierra
Processor	Intel Core i3 or higher
Memory (RAM)	4GB minimum
Hard Drive	500GB minimum
Video Card	Integrated Intel graphics
Simultaneous Camera Views	9 cameras: 720p, 15 fps 16 cameras: SD, 15 fps

Recommended Client Requirements

Operating System	Windows 10, 64-bit Mac OS X High Sierra
Processor	Intel Core i7
Memory (RAM)	8GB
Hard Drive	500GB minimum
Video Card	1GB RAM
Simultaneous Camera Views	16 cameras: 1080p, 30 fps

For more information, please visit s2sys.com.

© 2018 S2 Security Corporation. All rights reserved. S2 Security, S2 Magic Monitor, S2 NetBox and S2 NetVR are registered trademarks of S2 Security Corporation. Third-party trademarks are the property of their respective owners. Data subject to change without notice.

S2040418



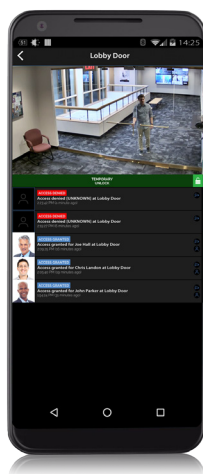


S2 Mobile Security Professional™

Overview

S2 Mobile Security Professional is an app for iOS and Android devices that allows both management and staff to operate their S2 access control and video management systems from anywhere. Users can switch between separate S2 systems or partitions directly in the app. S2 Mobile Security Professional is administered from a central location, and all actions are instantly displayed at the command center.

With S2 Mobile Security Professional, mobile staff can review surveillance video, monitor events and alarms in real time and manage evacuations. Cameras are accessible on demand, displaying high-quality, high frame rate video. Video snapshots can be shared as needed. In response to event activity, staff is able to take immediate action such as remotely opening related doors and identifying a person of interest in video. Mustering for evacuations is effortless, with multiple mustering points coordinated right on the screen. S2 Mobile Security Professional dramatically improves productivity, decision making and response time.



Door Controls: Users can momentarily unlock doors as well as view live video and recent access history associated with portals.

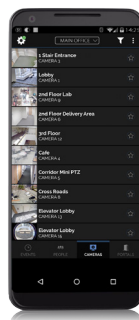
Key Features

System

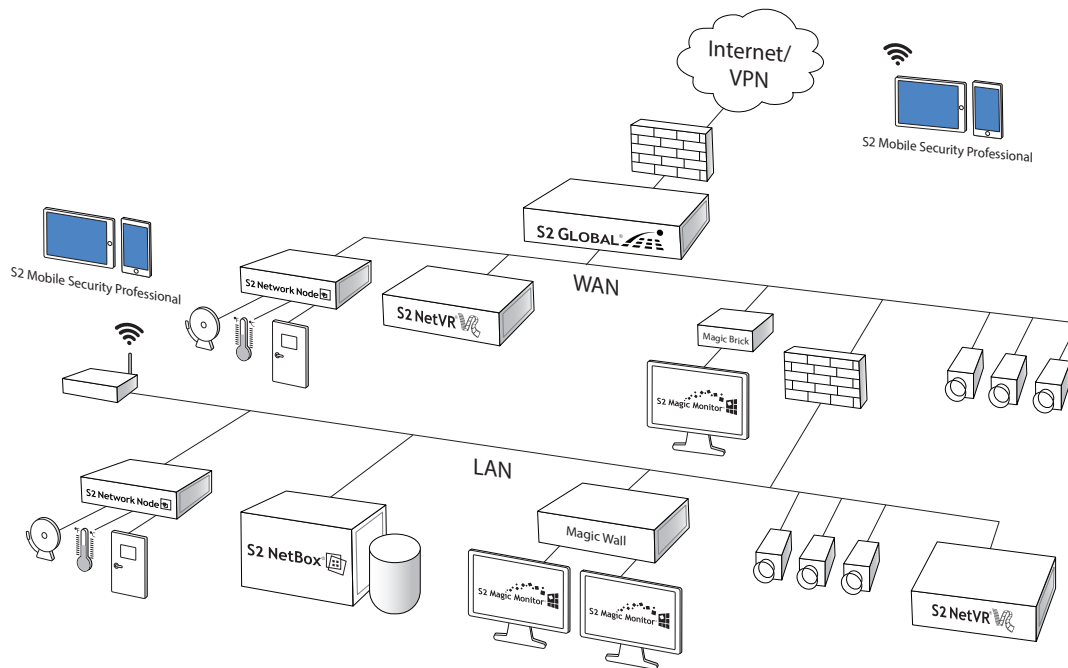
- **Mobile App:** Allows for operation of distributed S2 access control and video management systems on iOS or Android devices
- **Multi-System Control:** Includes the ability to switch between separate S2 systems or partitions
- **SSL Support:** Provides encrypted communications between S2 Mobile Security Professional and the S2 NetBox® controller

Mobile Security Management

- **Video Surveillance:** Delivers live video and event-based video recording from any S2 NetVR® camera
- **Video Snapshot:** Allows sharing of critical images via email or text message
- **Event Monitoring:** Displays event activity and video of interest, both real time and recorded
- **Person Detail:** Provides person identification and their access history log in one touch
- **Door Controls:** Enables momentary unlock of any door in the system
- **Photo ID Capture:** Takes an ID photo directly from the app
- **Evacuation Management:** Tracks evacuations and allows for management of multiple mustering points



Video Surveillance: Mobile users can access S2 NetVR cameras on demand and view live video in full screen mode.



Schematic only. Not a network diagram.

Specifications – S2 Mobile Security Professional

Access Control

S2 NetBox Software Version 4.9.10 and later

Video Management

S2 NetVR Software Version 1.8 and later

Camera Stream Layout Single cell

IP Camera Resolution IP camera dependent

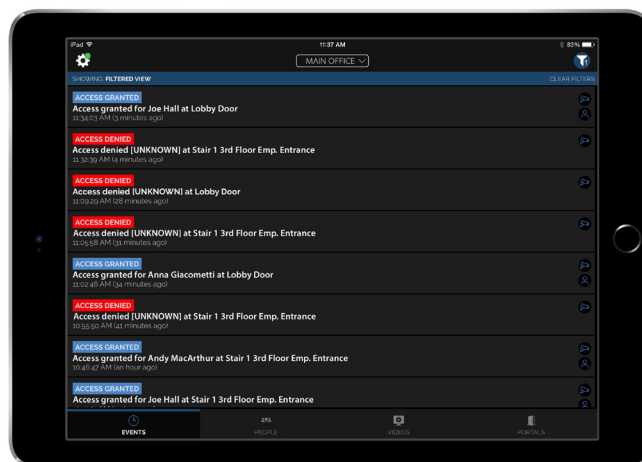
IP Camera Frame Rate IP camera dependent

Client Requirements

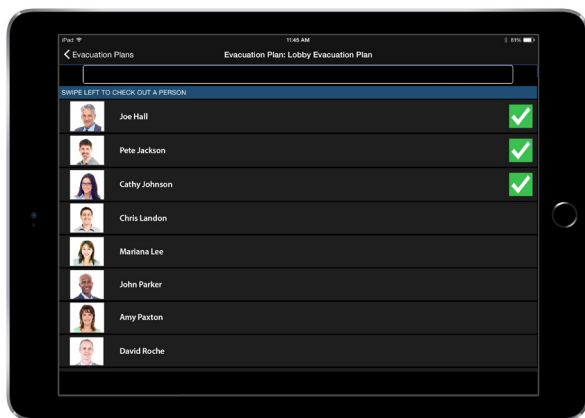
Operating System iOS 10 and later
Android 4.4 and later

Product Sourcing

Free download from Apple App Store and Google Play



Event Monitoring: S2 Mobile Security Professional displays all event activity and allows users to view video of interest with one touch.



Evacuation Management: With one touch, mobile staff can account for individuals at mustering points.

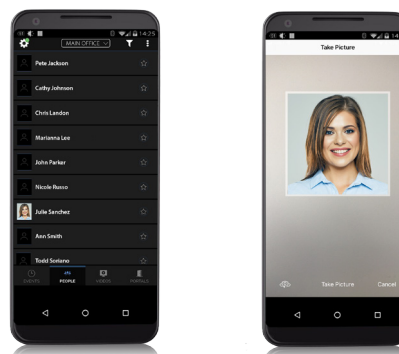


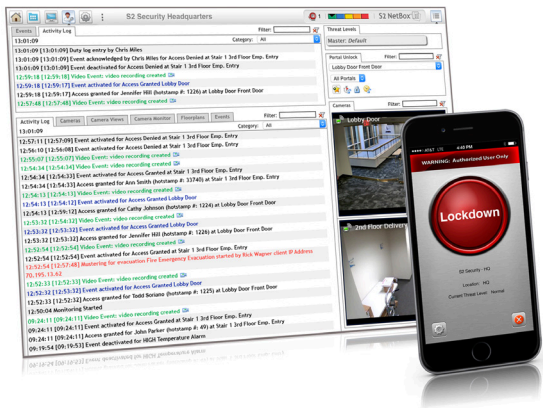
Photo ID Capture: Allows users to take photos and add them to person records using a camera on an iOS or Android device.

For more information, please visit s2sys.com.

© 2017 S2 Security Corporation. All rights reserved. S2 Security, S2 Mobile Security Professional, S2 NetBox and S2 NetVR are registered trademarks or trademark applications of S2 Security Corporation. Third-party trademarks are the property of their respective owners. Data subject to change without notice.

52010118





S2 Threat Level Escalator

Overview

S2 Threat Level Escalator is an app that enables security personnel and general users such as school and hospital staff to instantly change the threat level status of a location in their S2 access control system from a mobile device. The one-button user interface is optimized for rapid response to emergency situations. When tapped, the button initiates a pre-programmed response protocol, for example, a facility lockdown. It can also dial an emergency phone number or initiate communications to a command center if needed.

All users and mobile devices are managed by the S2 access control system administrator and assigned specific threat level and location credentials. The app is password protected on the device, ensuring only authorized personnel and devices can escalate the system threat level.

S2 Threat Level Escalator is especially applicable for high-risk organizations such as educational institutions, hospitals and industries working in hazardous environments. S2 Threat Level Escalator works with S2 NetBox® and S2 NetBox VR series products.



A facility-wide lockdown and emergency response protocols can be initiated with the tap of a button.

Key Features

System

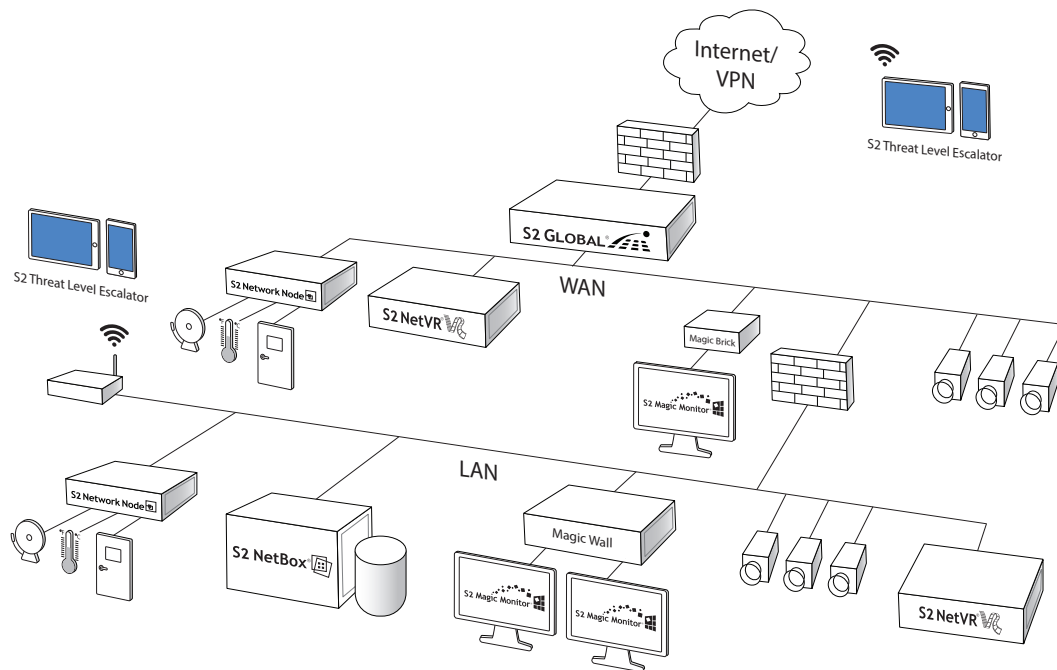
- **Mobile App:** Allows authorized security personnel and general users to instantly change facility threat levels from a mobile device
- **User Management:** Enables assignment of users, devices and credentials according to an organization's policies and procedures

Mobile Security Management

- **Access Control:** Restricts access to locations specified by the user's credentials
- **Simple User Interface:** Provides one-button operation for security personnel and general users as such school and hospital staff
- **Emergency Call Option:** Automatically or manually initiates a call to first responders or a command center



Authorized security personnel and general staff can restrict access to specified locations within their facility.



Schematic only. Not a network diagram.

Specifications – S2 Threat Level Escalator

Access Control

S2 NetBox Software Version 4.4.04 and later

Client Requirements

Minimum Operating System iOS 6.1 and later (iPhone, iPad and iPod Touch)

Product Sourcing

Free download from Apple App Store

Threat levels are customizable in the S2 access control system according to organizational policies and procedures.

Registered Devices:						
☐	Person	Device Name	Location	Threat Level	Phone Number	Phone Option
☐	Superintendent	District iPad	All v	Unscheduled Closing v		None v
☐	High School Principal	iPhone	High School v	Lockdown v	911	Auto Dial v
☐	High School Administrator	Main Office iPad	High School v	EMT Response v		None v
☐	High School Teacher	Classroom iPad	Classroom v	Restricted Access v	555-555-5555	Manual Call v
☐	Middle School Principal	iPhone	Middle School v	Lockdown v	911	Auto Dial v

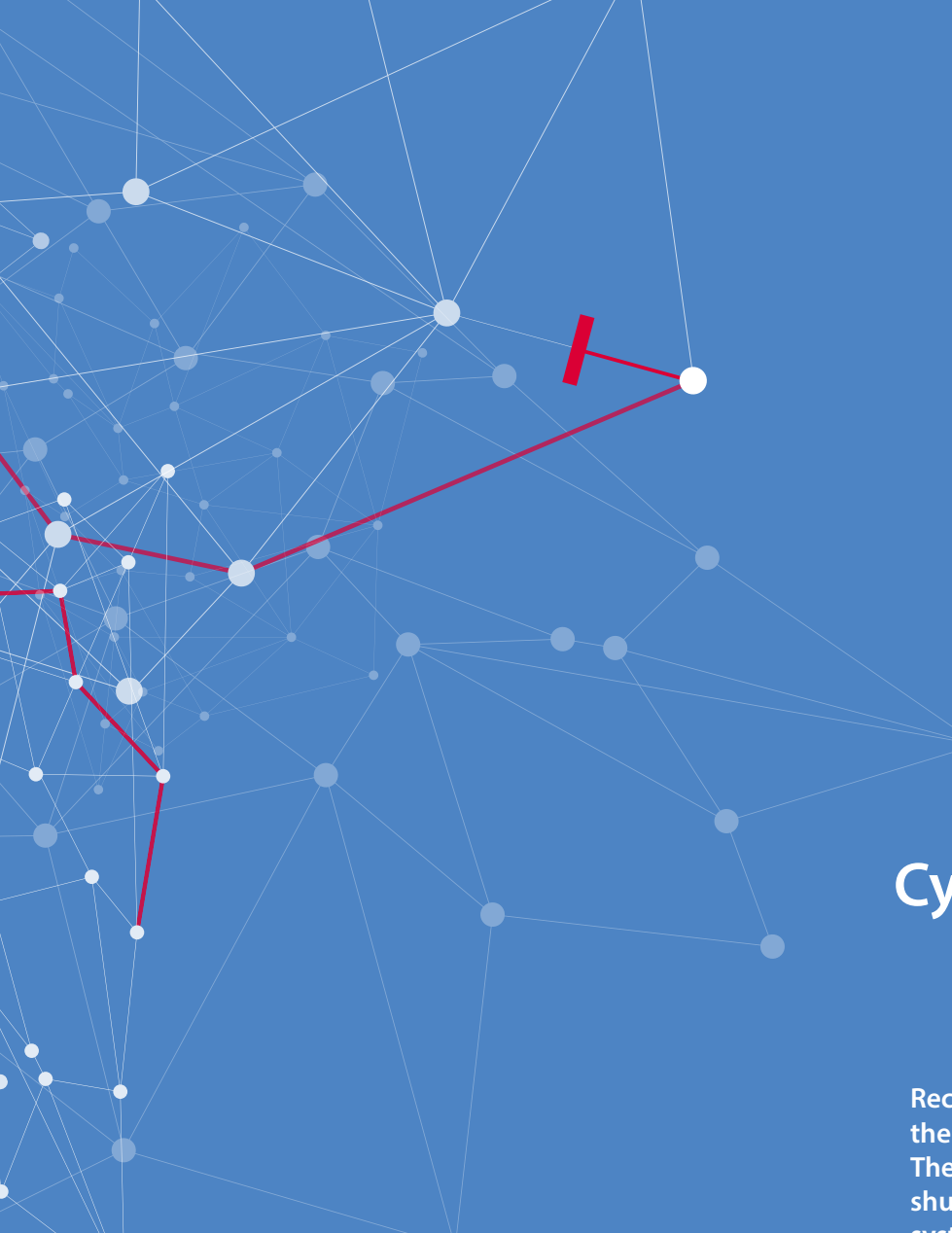
S2 Threat Level Escalator enables assignment of users, devices and credentials.

For more information, please visit www.s2sys.com.

© 2017 S2 Security Corporation. All rights reserved. S2 Security, S2 NetBox, S2 NetVR, S2 Magic Monitor and S2 Global are registered trademarks of S2 Security Corporation. Third-party trademarks are the property of their respective owners. Data subject to change without notice.

S2072617





Cybersecurity at Every Product Phase

Recent high-profile cyber attacks have exposed the world to the magnitude of their impact. The WannaCry ransomware attack effectively shut down the United Kingdom's healthcare system and affected many other organizations in over 150 countries. Target's extensively covered cybersecurity disaster in 2014 resulted in the theft of more than 70 million customers' personal financial information. The company continues to pay fines to the US government, and was even forced to reverse its planned expansion into Canada.

When it comes to physical security, the complexity and interconnectedness of today's systems provide multiple potential entry points for would-be attackers. This is why S2 Security incorporates information security into every phase of our products. Our comprehensive approach also empowers our customers to implement cybersecurity best practices while remaining vigilant.

Design



At S2 Security, we design secure products from the ground up. This means designing within a secure environment and reviewing all of our code to minimize potential vulnerabilities. The entire S2 system architecture is protected from cloud to network to server to panels using the TLS 1.2 protocol. Inaccessible from outside our facility, our design process ensures that would-be attackers cannot gain an early advantage. Our teams operate within a series of firewalls and antivirus redundancies, and access to these systems is also highly restricted within the company.

Development and quality assurance



Our developers follow coding best practices so that no shortcuts are taken which could result in a product weakness. Both the development and quality assurance teams run a variety of scans to detect any potential vulnerabilities along the way. These scans range from static scans to dynamic scans, each of which detect different types of vulnerabilities. Our teams also run daily scans on new and existing codebases to ensure no vulnerabilities have cropped up over time.

Manufacturing



Once development and quality assurance have signed off on the product code, a golden copy – verified to be secure and virus free – is provided to manufacturing.

As in the other stages of the process, manufacturing does its job almost entirely offline and always behind a series of firewalls. When manufacturing is “online,” it is on a closed network. In fact, no product spends more than approximately five minutes connected to any sort of intranet. These brief periods are used for quick testing and licensing to make sure the product is working as intended.

Installation and deployment



The installation and deployment phase involves collaboration between S2 Security, systems integrators and end users. Once systems are installed or in use, they run the risk of being compromised if appropriate measures are not taken to secure the operating environment. To mitigate this risk, we provide cybersecurity best practices training to our installation experts. Our product requirements and guidelines – from forced default credential changes to networking recommendations – help secure systems in the field.

When an installation is complete, we suggest the systems integrator perform a survey that reviews safe computing practices with the end user. This empowers the end user to employ best practices while monitoring for potential vulnerabilities.

Maintenance



Following deployment, integrators receive timely updates with the information and tools they need to keep systems secure. We conduct daily scans for vulnerabilities and monitor for generalized cybersecurity threats. The S2 Technical Support team also immediately reports issues to our customers.

If a vulnerability or exploit is found, we systematically determine the best course of action – be it an immediate patch within 24 hours, or a notification to raise awareness.

We also receive bi-annual feedback from end users on our Cybersecurity Advisory Council to address emerging concerns.

Security at every product phase

- Series of firewalls
- Antivirus redundancies
- Highly restricted employee access
- Entire system architecture secured with TLS 1.2



Design

- Static scans
- Dynamic scans
- Daily scans across codebases



Development and quality assurance

- Testing in secure environment
- Licensing in secure environment



Manufacturing

- Best practices training
- Installation checklist
- Required credential changes



Installation and deployment

- Vulnerability monitoring with daily scans
- Notification of issues
- Software updates and patches
- Feedback from Cybersecurity Advisory Council



Maintenance

Our Cybersecurity Responsibility

Cybersecurity is an ongoing process. The landscape of threats is always evolving, and so are our efforts to meet high cybersecurity standards. To provide you with the best, safest possible solutions, we design and manufacture secure software and hardware products, monitor for vulnerabilities and empower you to remain vigilant. We are committed to working with our customers and partners to support the security of their S2 systems and remain alert for what the future brings.

s2sys.com

© 2017 S2 Security Corporation. All rights reserved. S2 Security is a registered trademark of S2 Security Corporation. Third-party trademarks are the property of their respective owners.



BlueDiamond Multi-technology Readers



Overview

The BlueDiamond™ platform offers a complete, next-generation access control experience. With multi-technology readers, a feature-rich mobile app and the ability to support mobile and physical credentials, organizations can upgrade to the BlueDiamond experience at their own pace.

BlueDiamond multi-technology readers are among the most versatile access control readers on the market, work seamlessly with existing infrastructures and leverage open credentialing standards. The readers are non-proprietary, access control platform agnostic and support standard output protocols including Supervised F/2F (SF/2F), Wiegand, OSDP™ and OSDP V2. When utilizing LenelS2 OnGuard® and NetBox™ access control systems, users can conveniently manage mobile credentials through a single system.

Simultaneous support for a wide range of smart cards – including HID® iCLASS®, MIFARE® and DESFire® EV1 and EV2 – in addition to support for standard proximity cards means BlueDiamond multi-tech readers provide a seamless migration path from less secure card technologies to a more secure, open standard with DESFire EV2 and BlueDiamond mobile credentials.

With both mobile-ready and mobile-enabled versions available within the BlueDiamond multi-tech reader portfolio, organizations can achieve enhanced security at their own pace. For organizations that are not ready for mobile credentialing, but want to have the flexibility to add it in the future, the BlueDiamond mobile-ready readers provide flexibility without the need to replace or add hardware. Mobile credentialing can be enabled within these readers through the purchase of a license. The BlueDiamond mobile-enabled readers are ready out of the box to support mobile credentials.

Features & Functionality

- Support for BlueDiamond mobile credentials via Bluetooth
- Multi-tech readers offer simultaneous support for:
 - **125kHz proximity cards**
 - HID Proximity
 - AWID® Proximity
 - CASI/GE Security ProxLite
 - **13.56MHz smart cards**
 - MIFARE DESFire EV1/EV2
 - MIFARE Classic - ISO 14443
 - Vicinity Card Serial Number - ISO 15693
 - HID iCLASS**
- Mobile-ready readers can be upgraded to read mobile credentials through the purchase of a license without the need to add or replace hardware
- Mobile-enabled readers support mobile credentials out of the box
- Wiegand, SF/2F or OSDP with or without secure channel encryption, auto-configuring with LenelS2™ access panels
- Firmware updates, custom key loading and configuration changes via OSDP file transfer when BlueDiamond multi-tech readers are paired with the OnGuard access control system version 7.5 or greater, Mercury xSeries Controllers and Mercury Series 3 i/o boards
- Slim profile
- Fingerprint-resistant black textured finish
- Optical tamper switch

BlueDiamond Multi-technology Readers

Specifications

Specifications				
				
Mobile-ready Readers	Multi-technology Mini-mullion Reader LNL-R10330-05TB S2-R10330-05TB	Multi-technology Standard-size Reader LNL-R10320-05TB S2-R10320-05TB	Multi-technology Standard-size Reader with PINpad LNL-R10325-05TB S2-R10325-05TB	N/A
Mobile-enabled Readers	Multi-technology Mini-mullion Reader LNL-R11330-05TB S2-R11330-05TB	Multi-technology Standard-size Reader LNL-R11320-05TB S2-R11320-05TB	Multi-technology Standard-size Reader with PINpad LNL-R11325-05TB S2-R11325-05TB	Multi-technology Prox + Mobile Mini-mullion Reader LNL-R11030-85TB
Mechanical				
Dimensions	3.8 x 2.1 x 0.8 in 96 x 52 x 21mm	4.2 x 3.0 x 0.8 in 120 x 76 x 21mm		3.8 x 2.1 x 0.8 in 96 x 52 x 21mm
Housing	Molded polycarbonate/ABS			
Finish	Black, textured, fingerprint resistant			
Mounting	Wall surface or standard US, UK, or EU switchbox			Anywhere within 10ft/3M of legacy reader
Environmental				
Operating Temperature	-31° - 149°F (-35° - 65°C)			
Humidity	0 - 100% RHNC			
Ingress Protection Rating	IP65			
Electrical				
Voltage	10Vdc to 16Vdc			
Average Current draw at 12 VDC	35mA	35mA	67mA	12mA
Peak Current draw at 12 VDC	67mA	73mA	105mA	21mA
Data Voltage	Rest >4Vdc / Active <1Vdc			
Reader Interface	Supervised F/2F***, OSDP, Weigand			Weigand
Indication	1 RGB LED		1 RGB LED + illuminated keypad	1 RGB LED
Sounder	Integral speaker			
Read Range	Up to 4 in. (10cm) for RFID cards, up to 30 ft. (9m) for Bluetooth			
Warranty				
Warranty	5-year limited warranty			
Certifications				
FCC Part 15 UL294 CE Marked RoHS WEEE				

* The BlueDiamond mobile app is available for iOS® and Android® devices, as well as the Apple Watch®.

**Support for HID iCLASS Classic or Standard, not Elite Key, SE or SEOS.

***Support for Supervised F/2F protocol on a BlueDiamond reader is indicated by a label visible on the physical reader.

BlueDiamond Multi-technology Readers

Ordering Information

Mobile-ready Readers		
LNL-R10330-05TB	S2-R10330-05TB	Multi-technology Mini-mullion Reader
LNL-R10320-05TB	S2-R10320-05TB	Multi-technology Standard-size Reader
LNL-R10325-05TB	S2-R10325-05TB	Multi-technology Standard-size Reader with PINpad
Mobile-enabled Readers		
LNL-R11330-05TB	S2-R11330-05TB	Multi-technology Mini-mullion Reader
LNL-R11320-05TB	S2-R11320-05TB	Multi-technology Standard-size Reader
LNL-R11325-05TB	S2-R11325-05TB	Multi-technology Standard-size Reader with PINpad
LNL-R11030-85TB		Multi-technology Prox + Mobile Mini-mullion Reader
Pre-Encoded Credentials		
LNL-EV22KPP	S2-EV22KPP	DESFire EV2 ISO PVC 2K 13.56MHz
LNL-EV22KPPFOB	S2-EV22KPPFOB	DESFire EV2 2K 13.56MHz Keyfob
LNL-EV22KPPMG		DESFire EV2 ISO PVC 2K 13.56MHz with Magnetic Stripe (no encoding on stripe)
LNL-EV28KPP	S2-EV28KPP	DESFire EV2 ISO Composite 8K 13.56MHz
LNL-EV28KPXPP	S2-EV28KPXPP	DESFire EV2 ISO Composite 8K with Proximity Chip
LNL-EV28KPPMG		DESFire EV2 ISO PVC 8K 13.56MHz with Magnetic Stripe (no encoding on stripe)
Non-Encoded Credentials		
LNL-EV22KNP		DESFire EV2 ISO PVC 2K 13.56MHz
LNL-EV22KNPFOB		DESFire EV2 2K 13.56MHz Keyfob
LNL-EV22KNPMG		DESFire EV2 ISO PVC 2K 13.56MHz with Magnetic Stripe (no encoding on stripe)
LNL-EV28KNP		DESFire EV2 ISO Composite 8K 13.56MHz
LNL-EV28KPXNP		DESFire EV2 ISO Composite 8K with Proximity Chip
LNL-EV28KNPMG		DESFire EV2 ISO PVC 8K 13.56MHz with Magnetic Stripe (no encoding on stripe)
Licenses		
BDM-CRD-1		Required to create a BlueDiamond owner account
BDM-MERL		BlueDiamond mobile license upgrade to convert any mobile-ready reader to a mobile-enabled reader



LenelS2.com

(866) 788-5095

Specifications subject to change without notice.

©2020 Carrier. All rights reserved. All trademarks are the property of their respective owners.
LenelS2 is a part of Carrier. 2020/11





BlueDiamond™ Readers & Mobile Credentials

Welcome to the next generation
of access control.





Unmatched Experience in Mobile Credentials

The BlueDiamond platform leverages Carrier's 20 years of experience developing mobile credential technology. With over 4,000,000 Bluetooth® locking devices deployed across multiple industries — including Energy, Financial, Hospitality and Real Estate — Carrier is well versed in cloud-based mobile credentials and has been a Bluetooth technology leader since 2010.



Next Generation Access Control

The BlueDiamond platform offers a complete, next-generation access control experience. With multi-technology readers, a feature-rich mobile app and the ability to support mobile and physical credentials, organizations can upgrade to the BlueDiamond experience at their own pace.

Whether an organization leverages a LenelS2™ OnGuard® or NetBox™ access control system, or a third-party solution, the BlueDiamond platform provides the features they need for a secure, seamless and mobile-ready access control experience.



Seamless Migration Path

The versatility of the BlueDiamond multi-technology readers enables a seamless migration to the latest technology. The readers can meet your credentialing needs today and tomorrow. Because they support physical and mobile credentials, it's easy to upgrade at your own pace and as budgets allow.

The BlueDiamond readers offer enhanced security, leveraging the industry's open standard, DESFire EV2 credential technology and BlueDiamond mobile credentials with 128-bit AES encryption.





Multi-technology Readers

Experience effortless access with your mobile phone, smart card or standard proximity card. BlueDiamond multi-technology readers are among the most versatile access control readers on the market, able to work seamlessly with existing infrastructure while leveraging open credentialing standards.

BlueDiamond readers provide advanced credential support, offering access control system choices. The readers are access control platform agnostic and support standard output protocols including Supervised F/2F (SF/2F), Wiegand, OSDP™ and OSDP V2. Users of LenelS2 OnGuard or NetBox access control systems can manage mobile credentials directly from the access control system user interface. With both mobile-ready and mobile-enabled versions available within the BlueDiamond reader portfolio, organizations can achieve enhanced security at their own pace.

Supported technologies include:

125kHz proximity cards

- HID Proximity
- AWID® Proximity
- CASI/GE Security ProxLite

13.56MHz smart cards

- MIFARE® DESFire® EV1/EV2
- MIFARE Classic - ISO 14443
- Vicinity Card Serial Number - ISO 15693
- HID iCLASS™*

Features

- Mobile-ready readers can be upgraded to read mobile credentials through the purchase of a license without the need to add or replace hardware
- Mobile-enabled readers support mobile credentials out of the box
- BlueDiamond mobile credentials
- OSDP file transfer**

**Support for HID iCLASS Classic or Standard, not Elite Key, SE or SEOS*

***Requires OnGuard access control system version 7.5 or greater, Mercury XSeries Controllers and Mercury Series 3 i/o boards*

The BlueDiamond Mobile App Experience



Tap to Unlock

Tap "Unlock" to send credential to reader

Phone as a Badge

Use a phone as badge to gain entry



Shake to Open + Turnstile Support

Gently shake phone to send credentials to turnstile or reader

Pathways™

Pre-load commonly accessed doors along a frequently-traveled route



Voice Commands

Ask Siri® to open a door or start a pathway

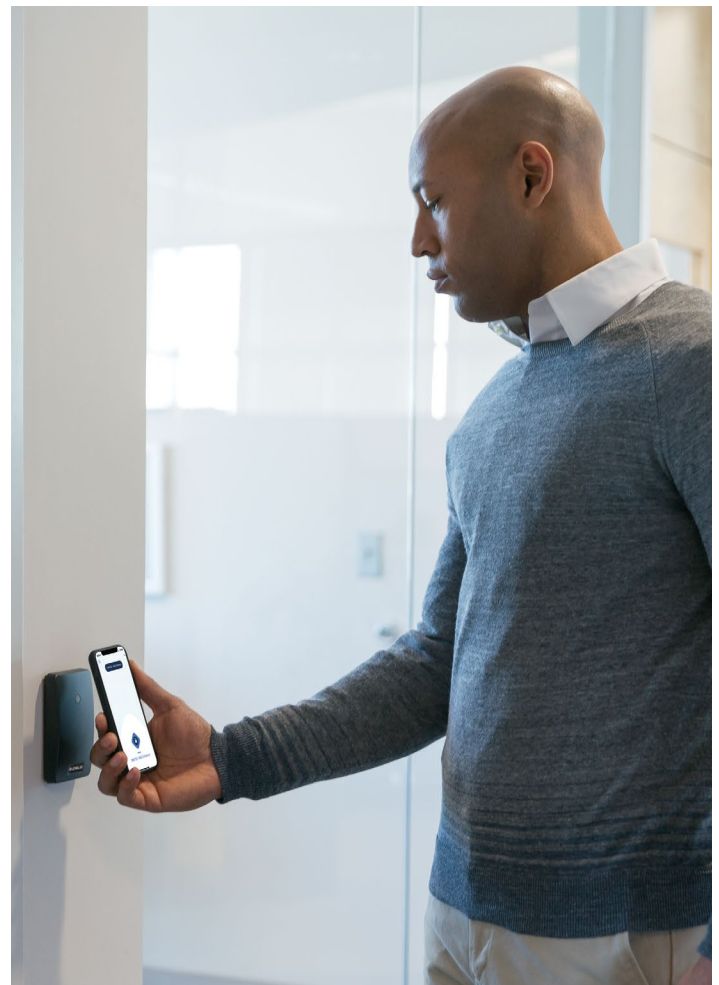
Favorites

Store commonly used doors for quick access



Two-factor Authentication

Confirm credentials for two-factor-enabled doors



Empower Your Phone to Open New Doors

The BlueDiamond mobile app delivers a smart alternative to plastic badges, offering convenience without compromising security. Available on both iOS® and Android® platform, the app is designed to provide a touchless, efficient and effortless credential experience. In addition to the app's feature-rich capabilities within a LenelS2 access control system, the BlueDiamond platform framework is also available to embed into an organization's current mobile application. LenelS2 provides assistance and the framework at no additional cost.*

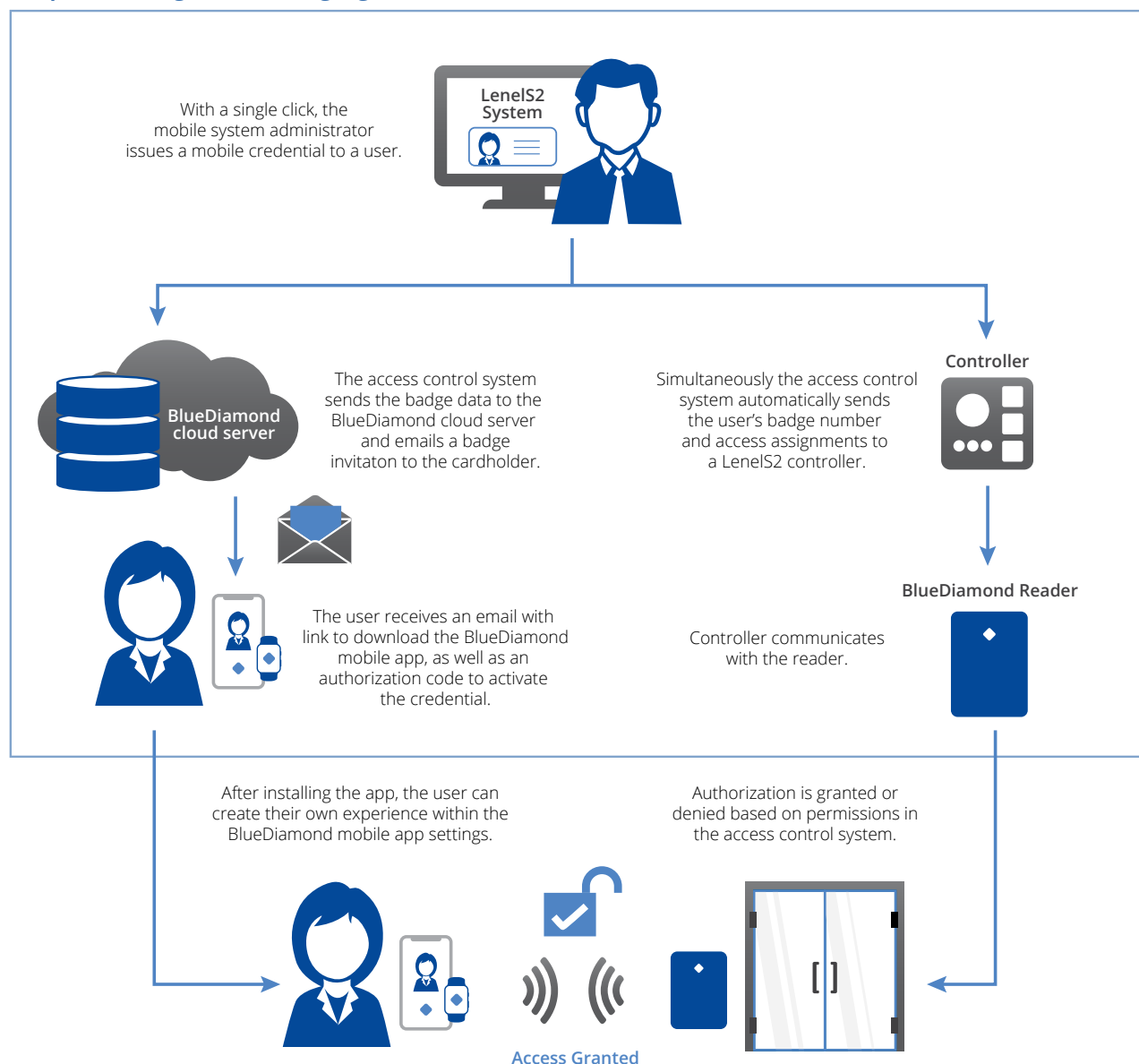
*terms and conditions apply

A comprehensive and open system for mobile credentials

LenelS2 Access Control Systems

The complete BlueDiamond platform includes the BlueDiamond mobile app, multi-technology readers and mobile credentials, all tied together by a cloud server. These components natively integrate with the LenelS2 OnGuard and NetBox security management systems allowing one-click issuance and management of mobile credentials.

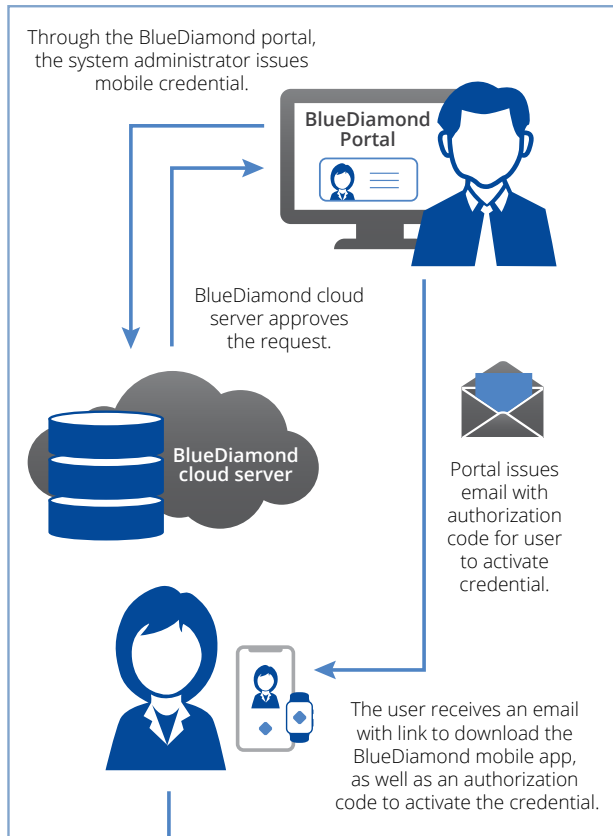
Step 1: issuing and managing credentials



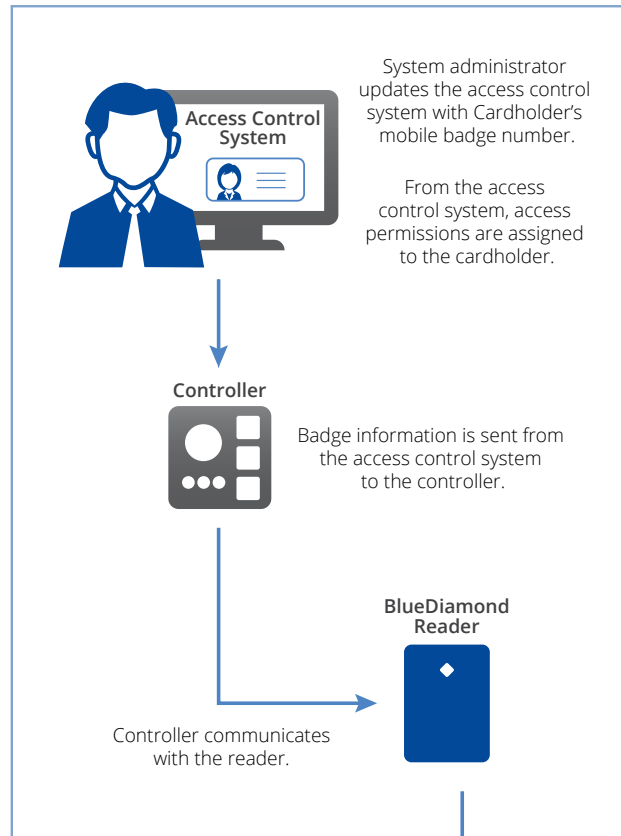
Third-party Access Control Systems

The BlueDiamond platform is access control system agnostic, allowing users to leverage their existing access control systems. Standard output protocols are supported along with open credentialing standards. Mobile credentials are issued through the BlueDiamond web portal and permissions are managed through the access control systems.

Step 1: issuing credentials



Step 2: managing credentials



After installing the app, the user can create their own experience within the BlueDiamond mobile app settings.

Authorization is granted or denied based on permissions in the access control system.





LenelS2 is a global leader in advanced physical security solutions, including access control, video surveillance and mobile credentialing. Our technology includes web-based and mobile applications enhanced by cloud-based services. Incorporating open architecture, LenelS2 provides scalable, unified security management solutions to customers ranging from global enterprises to small- and mid-sized businesses. Easy to install and use, LenelS2 products are supported by an experienced, responsive team dedicated to providing exceptional service. LenelS2 serves segments worldwide including corporate, education, healthcare and government. LenelS2 is a part of Carrier Global Corporation, a leading global provider of healthy, safe and sustainable building and cold chain solutions.

[LenelS2.com](https://www.LenelS2.com)

(866) 788-5095

Specifications subject to change without notice.

©2020 Carrier. All Rights Reserved. All trademarks are the property of their respective owners.
LenelS2 is a part of Carrier. 2020/12



School District Takes Proactive Approach to Security

Technology, team approach enable deterrence and rapid response across district

Summary

Organization

Granite Falls School District

Location

Granite Falls, Washington, United States

Industry

Education

Systems Integrator

LONG Building Technologies

Challenge

- Unify disparate security systems
- Adopt a proactive approach to security

Solution

- Deployed LenelS2 access control and video across District
- Integrated a range of security technologies

Results

- Standardized District-wide security
- Utilized technology to help deter potential incidents



Challenge

Granite Falls School District, located in Washington state, educates 2,000 students across two elementary schools, one middle school and two high schools. In light of the current threats faced by schools, Granite Falls reviewed its security infrastructure. The District found its setup to be not only expensive to maintain, but challenging to manage, with disparate systems at the five schools. For example, analog cameras and DVRs were not networked, so they had to be viewed separately. In addition, the elementary schools did not have video surveillance.

While Granite Falls needed a unified solution that fit its budget, the District was also determined to adopt a proactive approach to security with the help of technology. "We needed a partner who could provide a cost-effective, yet advanced system that would allow us to stay on top of potential threats," says Jeff Balentine, Capital Projects Manager, Granite Falls School District.

"Problems have significantly decreased, thanks to all the information and control we now have."

– Jeff Balentine, Capital Projects Manager,
Granite Falls School District



Solution

Granite Falls went to the public on a bond measure and asked for capital to improve security. Once the funding was secured, Granite Falls brought in its systems integrator, LONG Building Technologies, to assist with the project.

"By leveraging existing infrastructure, the LenelS2 solution enabled Granite Falls to come in under budget," observes Jim Jamison, Senior Account Executive, LONG Building Technologies. "The savings allowed us to explore additional, advanced capabilities that were important to such a forward-thinking school district."

The web-based NetBox™ access control system provides accessibility from anywhere, giving the District more flexibility and control. Integrations with Bosch intrusion alarm systems and 2N two-way intercoms at the front desk further enhance system capabilities. Although anyone with privileges can view events and video from a desktop or a mobile device, district-level management maintains Granite Falls' standards at each school. The budget surplus from the initial project made it possible to add capabilities such as custom-configured, discrete panic alarms (assistance, medical emergency, lockdown) which teachers can initiate from their computers.

LONG brought existing analog cameras into an IP network with a NetVR™ video management system and installed new IP cameras at schools without video surveillance. The District established a partnership with the local police department that enables close collaboration. The District provisioned the police with the Mobile Security Professional® app. Using the app, police can view video from all schools and even remotely lock or unlock doors – critical capabilities during active shooter or emergency response situations.

The Magic Monitor® unified client is used to power displays at the entrances to all five schools. The screens include information for the school community such as menus and events, and can provide critical messages during a lockdown. In addition, live camera views show each person entering the building video of themselves on camera, which acts as a form of deterrence.

Results

By leveraging a unified security approach, complemented by advanced integrations, Granite Falls has accomplished its goal of taking a proactive approach to security. Principals and school staff are confident in the system and enjoy a greater sense of security as a result. The police department is now able to enter any situation with far more information at their disposal.

"Problems have significantly decreased, thanks to all the information and control we now have," notes Balentine. "The team effort between LONG, LenelS2 and the District resulted in a well-thought-out security package that is cost-effective, and most importantly, raises the level of security for our students, teachers and staff."



For more information, please visit lenels2.com.

© 2019, 2021 Carrier. All rights reserved. All trademarks are the property of their respective owners. LenelS2 is a part of Carrier.

S2050521



Norwich Free Academy secures its open campus

S2 Security solutions control access while preserving campus environment

Summary

Organization

Norwich Free Academy

Location

Norwich, CT, United States

Industry

Education

Systems Integrator

Venture Communications and Security

Challenge

- Enhance security while maintaining an open campus
- Increase visitor management capabilities

Solution

- Integrated S2 system with other security functions
- Implemented credential-based system for control of each building

Results

- Streamlined campus security operations
- Controlled access while preserving campus environment



Challenge

Founded in 1854, Norwich Free Academy (NFA) is an independent high school with a student body of more than 2,300, housed on a 38-acre main campus and a nearby satellite campus. The school is also home to the Slater Memorial Museum, a nationally recognized fine and decorative art museum that is open to the public.

NFA wanted to enhance security and customer service, while preserving its open campus. "We needed to figure out a way to leave the doors open, but also lock them down quickly without going to a computer," explains Steve Bordua of Venture Communications and Security, the systems integrator for the project. "The school also wanted the ability to integrate with its existing video surveillance system."

"Community response to the S2 system is overwhelmingly positive."

- Al Fecteau
Director of Campus Safety
Norwich Free Academy



Solution

Venture Communications and Security designed the system with an S2 NetBox® Extreme and 14 S2 Network Nodes. The system is integrated with more than 125 IP cameras, several existing analog cameras linked to hybrid recorders, and other key security functions.

NFA wanted to allow public access to the Slater Memorial Museum while designating other floors as private. "We were able to integrate the S2 system with the elevator control," says Al Fecteau, Director of Campus Safety, Norwich Free Academy. "Now visitors can access the museum without special credentials but cannot reach other floors."

NFA also eliminated multiple access points to secure campus entry. New visitor check-in stations now provide service at two entry points, and an electronic gate integrated with the S2 system secures a third. The gate is kept closed, but is programmed to open automatically for those with access cards.

The real test was determining how to have an open campus while maintaining security over each building. Campus Safety staff carry multiple credentials, allowing them to lock and unlock doors as needed and to operate during after school programs and special events. In the event of an emergency, one of the credentials enables staff to lock down either an individual building or the entire campus from a single card reader.

Results

With the S2 solution, NFA is able to maintain its traditional open campus environment while enhancing safety and security for students, faculty and visitors. "We've managed access so we know who is on campus and why," explains Fecteau. "Community response to the S2 system is overwhelmingly positive."

For more information, please visit www.s2sys.com.

© 2014 S2 Security Corporation. All rights reserved. S2 Security and S2 NetBox are registered trademarks of S2 Security Corporation. Third-party trademarks are the property of their respective owners.





NetBox Solution Package for K-12 Schools

K-12 schools have one of the most important jobs: to provide children with the educational foundation for future success while keeping them safe and healthy. To fulfill that expectation, schools require security technology that gives students the confidence to focus on learning. With over 2,000 unique deployments in school districts, LenelS2 provides scalable solutions for K-12 schools' most critical security challenges. Our NetBox™ solution package offers a comprehensive approach to school security. With every new NetBox Extreme or NetBox Enterprise access control system purchase, it includes discounts on hardware, training and additional software support.

The NetBox system is part of Carrier's Healthy Buildings Program, a suite of solutions and services that help support building and occupant health.

Solution Package Details*

Access Control

5 years of software support with new NetBox Extreme or NetBox Enterprise access control system (S2-SUSP)

Active Directory integration (S2-AD)

Database Partitioning (S2-DBP)

Magic Monitor® Professional unified client (S2-MM-PRO)

10% discount on Network Nodes and Mercury Security hardware

25% discount on BlueDiamond™ readers

Video Management

5 years of software support with new VRx™ video management system (S2-SUSP)

10% discount on any VRx system hardware or camera licenses

Training

2 seats of NetBox virtual training for end users

For more information, please visit lenels2.com.

*Solution Package offer applies to new purchases of NetBox Extreme and NetBox Enterprise systems only. Offer valid on orders received by LenelS2 through September 30, 2022. All package components must be purchased in a single order. Offer may not be combined with any other offer.

©2021 Carrier. All Rights Reserved. All trademarks are the property of their respective owners. LenelS2 is a part of Carrier.

S2082021



HEALTHYBUILDINGS



NetBox Solution Package for K-12 Schools

K-12 schools have one of the most important jobs: to provide children with the educational foundation for future success while keeping them safe and healthy. To fulfill that expectation, schools require security technology that gives students the confidence to focus on learning. With over 2,000 unique deployments in school districts, LenelS2 provides scalable solutions for K-12 schools' most critical security challenges. Our NetBox™ solution package offers a comprehensive approach to school security. With every new NetBox Extreme or NetBox Enterprise access control system purchase, it includes discounts on hardware, training and additional software support.

The NetBox system is part of Carrier's Healthy Buildings Program, a suite of solutions and services that help support building and occupant health.

Solution Package Details*

Access Control

5 years of software support with new NetBox Extreme or NetBox Enterprise access control system (S2-SUSP)

Active Directory integration (S2-AD)

Database Partitioning (S2-DBP)

Magic Monitor® Professional unified client (S2-MM-PRO)

10% discount on Network Nodes and Mercury Security hardware

25% discount on BlueDiamond™ readers

Video Management

5 years of software support with new VRx™ video management system (S2-SUSP)

10% discount on any VRx system hardware or camera licenses

Training

2 seats of NetBox virtual training for end users

For more information, please visit lenels2.com.

*Solution Package offer applies to new purchases of NetBox Extreme and NetBox Enterprise systems only. Offer valid on orders received by LenelS2 through September 30, 2022. All package components must be purchased in a single order. Offer may not be combined with any other offer.

©2021 Carrier. All Rights Reserved. All trademarks are the property of their respective owners. LenelS2 is a part of Carrier.

S2082021



HEALTHYBUILDINGS



Value-Added Resellers (VAR)

The following is a list of certified Value-Added Resellers (VARs) for Newport-Mesa Unified School District:

Nick Semolich - President Pacific Low Voltage 4532 Telephone Road #102, Ventura, CA 93003 nick@pacificlowvoltage.com 805.658.1PLV (1758) www.pacificlowvoltage.com	Jim Bernard Vice President of Sales Security Fire Life Safety Team Climatec 2150 S. Towne Centre Place Suite 200 Anaheim, CA 92806 Cell 949.431.8952 Fax 949.474.0956 www.climatec.com jbernard@climatec.com	Jeff Moormann Senior Director of Sales- AUTS West Allied Universal Technology Services W: 213- 267-8436 C: 714-913-3297 Jeff.Moormann@aus.com
Jeff Torok AM-TEC Security 4075 Schaefer Ave, Chino, CA 91710 909-573-9385 Cell 800-609-ALARM (2527) Office jeff@amtecsecurity.com	Yale Smith Maxim Security President 9064 Pulsar Ct., Suite F Corona, CA 92883 951-526-2979 yale@maximsecuritysystems.com	Angie Barnes NAVCO Security Executive VP 1335 Acacia Ave., Fullerton, CA 92831 O 714.399.3837 C 210.259.3104 abarnes@navco.com
Mariana Tejera West Regional Sales Director IES Communications, IES Communications 9211 Irvine Blvd, Irvine, CA 92618 Mobile 858.650.9625 mariana.tejera@iescomm.com www.iescomm.com	Randy Jara Chief Business Officer /Partner REDROCK Technologies (D) 949.860.0075 (C) 714.475.9230 (O) 949.900.3460 (F) 949.587.1428 RandyJ@ITREDROCK.com Corporate Office 15215 Alton Pkwy, Suite 200, Irvine, CA 92618 San Diego Operations 680 Fletcher Pkwy, Suite 204, El Cajon, CA 92020	Sam Deatherage Security and Life Safety Consultant Barton Integration Mobile (949) 701-3532 Main (866) 922-7866 Orange County Los Angeles San Diego Bay Area SamD@BartonIntegration.com www.BartonIntegration.com

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534



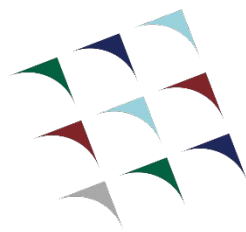
Jesse Martinez Western Audio Visual and Security M: 714-362-1057 E: JesseM@wav1.com W: https://www.wav1.com/security/	Eric Fiorino – Executive Vice President A.J. Kirkwood & Associates, Inc. 4300 N. Harbor Blvd. Fullerton, CA 92835 (714) 505-1977 ,318 (714) 936-3145 Cell	Denise Taylor Account Executive Netronix Integration 181 West Orangethorpe Ave, Ste E, Placentia, CA 92870 Office +1 714-993-1444 EXT 310 Mobile +1 714-599-4499
--	---	---

Jason Martin President Sonitrol Orange County & Sacramento 23 Mauchly #100, Irvine CA 92618 (949) 297-4355 Direct (949) 297- 4390 Fax (949) 293-3185 Mobile JMartin@SonitrolOC.com www.SonitrolOC.com	Stephanie Meurer Sales Manager Convergint Technologies 540 S. Jefferson, Placentia, CA 92870 O: 714-546-2780 M: 714.686.8612 stephanie.meurer@convergint.com www.convergint.com	Scott Hollis Vice President, Sales SSD Alarm 800-888-0444 shollis@ssdsystems.com www.ssdalarm.com
Marvin Barnes Stone Security 4 Latitude Way, Suite 103-104, Corona, CA 92881 (877) 888-0129 Office (310) 729-2481 marvin@stonesecurity.net www.stonesecurity.net		

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534

NEWPORT MESA UNIFIED SCHOOL DISTRICT



Newport-Mesa
Unified School District

REQUEST FOR PROPOSALS FOR INTEGRATED SECURITY SYSTEMS STANDARDS OCTOBER 13, 2022

**Proposals must be received by
4:00 p.m. PST on Thursday November 17, 2022**

With this Request for Proposals (“RFP”), the Newport-Mesa Unified School District (“District”) is requesting proposals (“Proposals”) from qualified integrated security system manufacturers (“Respondents”) for the following services:

INTEGRATED SECURITY SYSTEMS STANDARDS

The purpose of the Proposal is to demonstrate the qualifications, competence and capacity of Respondent to perform the work or provide the services described in this RFP. The Proposal should demonstrate the qualifications of the Respondent and of the particular staff to be assigned to this project.

The successful Respondent will be expected to execute the Agreement included with this RFP without modification of the terms.

1. Introduction

1.1 About Newport-Mesa Unified School District.

The Newport-Mesa Unified School District (“NMUSD” or “District”) was Unified on July 1, 1966, in the County of Orange California and covers 58.83 square miles including, Newport Beach, Costa Mesa and Corona del Mar. The District consists of (32) thirty-two schools and approximately (19,000) nineteen thousand students. The District employs approximately (3200) three thousand two hundred employees including teaching and non-teaching positions.

1.2 Project Description.

- (a) Newport Mesa Unified School District (District) is selecting a new security system to deploy at facilities throughout the District. The District has completed a Request for Information process to identify security system manufacturers that meet the District’s integrated security system requirements. This RFP process is intended to allow the District to further evaluate security systems and select finalists.
- (b) Pricing provided in response to this RFP is intended to allow the District to determine Total Cost of Ownership (TCO) and establish consistent pricing to the District from the integrated security system manufacturer that will be applicable to all integrators/partners that will install the integrated security system at the District’s facilities. Pricing shall include software, licenses, and other products and services that must be purchased through the manufacturer. Pricing may also include products and services available through the manufacturer (e.g., card readers, pre-configured computer hardware, partner products, etc.). Submitted pricing shall be the price to the District through the manufacturer’s integrators/partners.

1.3 Project Schedule.

This RFP is intended to assist the District in determining a standard for an integrated security system as outlined in these documents. Therefore, there will not be a direct award of any contract for the procurement of labor or materials as a result of this RFP. Rather, awarded

manufacturer(s) will be presented to the Board of Education to determine a standard for future NMUSD security projects.

1.4 Pre-Proposal Meeting.

District will conduct a **mandatory** pre-proposal meeting, this meeting will be held virtually via Zoom to ensure all candidates have the ability to attend. The meeting will occur at **10:00 AM PST on Monday October 24th**. A Zoom link will be provided 24hrs prior to the meeting to all those vendors whom received RFP documents via the PlanetBids web portal.

2. Scope of Required Services

2.1 Summary of Services.

A detailed description of the required services and technical requirements described in the Scope of Services attached hereto as Attachment "1".

3. Qualifications

The following integrated security system manufacturers have been prequalified for this RFP through the previously conducted RFI process:

- Genetec – Unified access control and video system
- Lenel/S2 – S2 NetBox access control and S2 VRx video
- Motorola – Avigilon Control Center and Access Control Manager
- Open Options – Access control, integrated video and intrusion systems must be submitted with the RFP response.
- RS2 Technologies – Access control, integrated video and intrusion systems must be submitted with the RFP response.

Milestone has been prequalified as a video system manufacturer that may be integrated with access control and intrusion systems from other manufacturers.

To qualify, respondents must prepare and include responses to the District's original Request for Information (included in Attachment 3). Proposals from vendors that have not been pre-approved and that do not include the RFI response information will be considered non-responsive and will receive no further consideration.

4. Schedule of Events

Estimated Timetable for Reviewing and Evaluating Proposals:

- | | | |
|----|---|------------|
| 1. | RFP Release | 10/13/2022 |
| 2. | Pre-Proposal Meeting Zoom 10:00AM PST | 10/24/2022 |
| 3. | Pre-Proposal Requests for Clarification | 11/07/2022 |
| 4. | Proposal Due Date | 11/17/2022 |
| 5. | Anticipated Final Selection | 12/16/2022 |

6. Award by Board of Trustees
7. Notice to Proceed

1/10/2023
1/11/2023

The dates listed above are estimates only and are subject to change in District's sole discretion.

5. Proposal Requirements

5.1 Proposal Format.

Respondent's Proposal shall be clear, accurate, and comprehensive. Excessive or irrelevant materials will not be favorably received. Respondents are directed to make their Proposals as concise as possible. The Proposal shall be signed by an individual or individuals authorized to execute legal documents on behalf of the Respondent.

The following items shall be packaged into a single electronic file in ".pdf" format:

A. Arrange information in the following order.

1. A Title page that indicates:
 - a. The name, address, and telephone number of the Vendor
 - b. The date of the submission
 - c. A statement that the information is in response to this RFI
 - d. The name, title, telephone number and e-mail address of the contact person responsible for the Vendor's response.
2. 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.
3. Executive Summary not exceeding three pages, including overviews of:
 - a. The Respondent's perspective of what major solution attributes differentiate their offering from that of competing solutions.
 - b. The Respondent's strategy to provide direct training, certification, and support to the District's staff necessary to maintain the system.
 - c. The Respondent's ability to provide products and services to the District including the manufacturer's responsibilities and the integrator/partner responsibilities.
4. A Solution Narrative to explain the system elements, roles, integration, proposed deployment, and manufacturer support. The narrative shall demonstrate compliance with the District's security system goals and expectations.
5. A System Diagram to illustrate the primary components (e.g., servers, workstations, panels, etc.) included in the proposed system deployment.
6. System requirements for off-the-shelf computer equipment utilized by the system.

7. Cyber security program information to illustrate how the manufacturer recognizes and adapts to evolving threats, compliance, and regulation.
8. An itemized price proposal (manufacturer-provided integrated access control, video surveillance and intrusion system products and services only) by facility type that includes all software, licenses, and manufacturer-specific hardware identified in the proposed Solution Narrative and System Diagram.
9. Product data for each of the system elements.
10. A list of certified integrators where the District can purchase the Respondent's products based on the proposed pricing. Include contact information for each with a preference for providers in Orange County or surrounding areas.
11. A complete and detailed copy of the RFP, including all information and binding signatures as indicated.
 - a. To the extent clarifications to this RFP are issued by the District (typically via email), printed copies of each and every such clarification shall also be included within this section.
12. A summary of at least one similar and completed solution deployment with similar direct end user support as required by the District, preferably from a comparable K-12 school district. Include project references and contact information.
13. Any other documentation as required by the RFP.
14. Supplemental data as desired by the Respondent to supplement the RFP response.

5.2 No Deviations from the RFP. District will not consider any deviation from this RFP. In submitting a Proposal in response to this RFP, Respondent is certifying that it takes no exceptions to this RFP.

5.3 Submittal Instructions.

To be considered, District must receive the Proposal no later than **4:00 p.m. PST on Thursday November 17, 2022**

Proposals must be submitted through PlanetBids for consideration. No other method of submitting proposals will be accepted. Respondents may not submit bids by fax, email, telephone or other means; any proposals received through any other means than PlanetBids will be returned unopened.

Respondents are solely responsible for the "on time" submission of their electronic Proposal. District will only consider Proposals that have transmitted successfully and have been issued a confirmation number with a time stamped from PlanetBids indicating that the Proposal was submitted successfully. Transmission of Proposals by any other means will not be accepted. Respondents shall be solely responsible for informing themselves with respect to the proper utilization of the online bid management system, for ensuring the capability of their computer system to upload the required documents, and for the stability of their internet service. Failure of

the Respondent to successfully submit an electronic Proposal shall be the Respondent's sole risk and no relief will be given for late and/or improperly submitted Proposals.

6. Evaluation Process

6.1 Evaluation Criteria.

Proposals that meet the submittal requirements will be evaluated by District based on the following criteria (in no particular order):

- (a) Quality and comprehensiveness of the Proposal.
- (b) System Maturity: Points will be awarded to manufacturers with extensive experience in security systems. Preference is given to products with a long track record of success in similar applications over new or developing technologies.
- (c) Pricing: Points will be awarded to the respondent's price based on the sample scenario included in the RFP.
- (d) Integrators: The District desires to standardize security systems for specifications on future publicly bid projects. It is desired to have multiple qualified integrators within fifty miles of the District that can participate in future bids for the purchase and installation of equipment as identified in this RFP.
- (e) Direct Support to the District: All points awarded to manufacturers who clearly define a direct support agreement with the District. These criteria must be addressed in the response and will be evaluated to ensure that the response supports the District's criteria.
- (f) Intangibles: Each manufacturer may submit details that provide additional value to the District (e.g., discounts over an extended time, inclusion of features especially useful to the District, etc.). These are discretionary and should be discussed by all reviewers before awarding points to ensure that the responses are appropriately and consistently assigned. This category may also be used to award points to manufacturers who provide additional technical value based on the initial manufacturer RFI evaluations.

Respondents should note that the lowest cost proposal is not the sole determining factor in District's evaluation.

At the conclusion of the Proposal solicitation period, District will review each submission and perform any other investigation it deems appropriate, and then rank the Proposals according to evaluation criteria. Based on the rankings, District may, at its sole discretion, invite a short list of Respondents to participate in interviews and/or demonstrations. If interviews and/or demonstrations are conducted, the evaluation panel will evaluate the short listed Respondents based on the information provided in the Proposal, the results of District's research and investigation, and the interview and/or demonstration and recommend the Respondent who

ranked highest. No Respondent shall be entitled to or otherwise guaranteed an interview with District.

6.2 Award of Contract.

Upon determination of the highest ranked firm, District will endeavor to negotiate a mutually agreeable scope of services and fee with the selected firm. In the event that District is unable to reach agreement, District will proceed, at its sole discretion, to negotiate with the next firm selected by District.

If awarded, the contract will be awarded to the firm selected on the basis of information provided in the Proposal, the results of District's research and investigation, and, if conducted, oral interviews.

District reserves the right to reject all proposals and to contract for services in the manner that most benefits District, including awarding more than one contract if desired.

7. Requests for Clarifications

All questions and requests for interpretations or clarifications, either administrative or technical must be submitted in writing to District through PlanetBids by selecting the Q&A Tab. Questions sent directly to District Staff will not be addressed and you will be directed to submit your question(s) online.

All questions properly submitted will be answered in writing through PlanetBids. Verbal statements regarding this RFP by any persons should be considered unverified information unless confirmed in writing. To ensure a response, questions must be received through PlanetBids by **4:00 p.m. PST on Monday November 7, 2022**

8. General Provisions

Respondent is encouraged to review this RFP carefully in its entirety prior to preparation of its Proposal. District reserves the right to reject any or all Proposals or to select the Proposal most advantageous to District. District reserves the right to verify all information submitted in the Proposal which includes but is not limited to any other investigation it deems appropriate.

8.1 Addenda to RFP. District reserves the right to amend the RFP or issue addenda to answer questions for clarification.

8.2 No Commitment to Award. Issuance of this RFP and receipt of proposals does not commit District to award a contract. District expressly reserves the right to postpone the proposal for its own convenience, to accept or reject any or all proposals received in response to this RFP, to negotiate with more than one Respondent concurrently, or to cancel all or part of this RFP.

8.3 Amendments to Proposals. No amendment, addendum or modification will be accepted after the deadline stated herein for receiving Proposals. Respondent may modify or amend its Proposal only if District receives the amendment prior to the deadline stated herein for receiving Proposals.

8.4 Non-Responsive Proposals. A Proposal may be considered non-responsive if incomplete or if it contains conditions, alterations of form, additions not called for, or other irregularities that may constitute a material change to the Proposal.

8.5 Late Proposals. District will not be responsible for delinquent Proposals. Respondent is solely responsible for submitting the Proposal before the closing date and time.

8.6 Costs for Preparing. District will not compensate any Respondent for the cost of preparing any Proposal, and all materials submitted with a Proposal shall become the property of District. District will retain all Proposals submitted and may use any concept or information in a Proposal regardless of whether that Proposal is selected.

8.7 Alternative Proposals. Only one final Proposal is to be submitted by each Proposer. Multiple proposals will result in rejection of all proposals submitted by the Respondent.

8.8 Public Documents. All Proposals and all evaluation and/or scoring sheets shall be available for public inspection at the conclusion of the selection process. If any information in a Proposal is claimed to be confidential by the Respondent, and such information is clearly identified in the Proposal as confidential, along with a statement of the basis of the claim, then a copy of any Public Records Act request or other request for disclosure of the information will be sent to the Respondent. At its sole cost and expense, the Respondent may seek, within the required timeframe for disclosure, to enjoin the production of the information it claims to be confidential. The Respondent must defend, indemnify, and hold harmless District for any costs associated with withholding the information.

8.9 No Exceptions. Submission of a Proposal constitutes acceptance by Respondent of the conditions contained in this RFP. No exceptions will be considered.

8.10 Withdrawal. Respondent's authorized representative may withdraw its Proposal by notifying the District in writing before the Submittal Deadline. After the Submittal Deadline, if it is in the best interest of District, the District, in its sole discretion, may consider whether to grant a Respondent's request to withdraw its Proposal and will evaluate any impact on the Respondent's bid bond, if applicable.

ATTACHMENT 1

SCOPE OF SERVICES

SECURITY SYSTEM REQUEST FOR PROPOSAL (RFP)

SECTION 1 - TECHNICAL REQUIREMENTS

1.02 Proposed System Solution

- A. The District will select a new security system to provide integrated access control, video surveillance, and alarm monitoring for the District's facilities. The District's expectations for the new security system and manufacturer include:
 - 1. A mature, reliable, and scalable system that has been successfully deployed in multiple projects of similar size, complexity, and integration to the District.
 - 2. A manufacturer partner with the District to support and maintain the system.
 - 3. Web-based applications to minimize software installation and maintenance.
 - 4. Flexibility to support the District's varying facility types and requirements.
 - 5. Support for Mercury Security and other access control hardware supported by multiple system manufacturers.
 - 6. Product availability and support through multiple local certified integrators that can respond to calls for service in a timely manner.
- B. Submit system narrative and manufacturer support narrative to demonstrate compliance with the District's security system goals and expectations.

1.03 Software and License Pricing

- A. The District has developed the following criteria to demonstrate the anticipated security system size and capacities.
 - 1. Simultaneous Users: 40
 - 2. Workstation Locations: 50
 - 3. Badge Enrollment Workstations (including portrait camera, flash, backdrop, and badge printer): 1
 - 4. Video Recorders: 30 (1 per facility)
- B. Provide Active Directory integration to populate employee user and cardholder information in the security system.
- C. Submit proposed manufacturer pricing as follows based on the anticipated system capacities.
 - 1. Unit prices and quantities for system software and licenses.

2. Badge enrollment workstation including the following:
 - a. Workstation software and licenses.
 - b. Portrait camera with direct controls from workstation, tripod, and flash unit.
 - c. Portrait backdrop.
 - d. Fargo DTC5000 or equal badge printer with simultaneous dual sided, over-the-edge printing and printer cleaning kit.
 - e. Printer materials to print 2,000 badges.
3. Software and licenses to support the anticipated facility equipment as indicated in the attached Security System Quantities Summary. The summary indicates the types of facilities and the quantity of each, card readers, cameras, intrusion panels, and security equipment locations (where access control equipment will be located).
4. Total cost to implement the anticipated system. The total cost shall not include off-the-shelf hardware such as servers, workstation computers, monitors, and other equipment that can be purchased by the District, through typical technology contracts.
5. Unit prices to add software licenses and capacity after the initial purchase where different from proposed initial system prices (e.g., escalation, renewal, etc.).
6. Unit prices for each manufacturer-provided Mercury access control hardware element.
7. Unit prices for each hardware element necessary to implement the system that must be purchased from the manufacturer.
8. Unit prices for other hardware and equipment that can be purchased through the manufacturer (e.g., card readers, access cards, printers, etc.).

1.04 Integrators

- A. The number and quality of integrators that can support the manufacturer's product for the District will be evaluated.
- B. Submit a list of certified integrators that can provide services and support to the District. Include contact information and address for each.

1.05 Support to the District

- A. Direct manufacturer support is essential to the District. The District will train and certify their personnel who will service and support the security system.
- B. Submit proposed manufacturer pricing to support the District's maintenance staff as follows.
 1. Annual software support and maintenance agreement to provide direct support to the district. Provide costs for a minimum of five years.]
 2. Training and certification for installation and maintenance technicians.
 3. Training and certification for system administrator and configurator staff.

4. Training and certification for system operators.
5. Include individual and group package pricing for each of these programs as applicable.

1.06 Video System Integration

- A. Include in the system narrative a detailed explanation of video system integration with access control and intrusion detection functions. Provide details for the following:
 1. Integrated video system manufacturer.
 2. Relationship between the manufacturers.
 3. Manufacturer roles and responsibilities including integration support.
 4. Integrated user interface and system functions available through the integrated user interface.
- B. Provide software, licenses, professional services, and other costs necessary to implement the video system integration.

1.07 Video Analytics

- A. Include in the system narrative a detailed explanation of video analytics supported by the system. Provide details for the following:
 1. Video analytics integrated into the video surveillance system.
 2. Partner manufacturers providing video analytics.
 3. Key video analytics provided through partner manufacturers.
 4. Operational differences of partner manufacturers versus integrated video analytics.
 5. Integration of partner manufacturer video analytics into the user interface.
- B. Included in the itemized pricing a detailed unit price list for video analytics. Include the following:
 1. Integrated video analytics licenses and licensing scheme.
 2. Primary partner video analytics licenses and licensing scheme.
 3. Optionally, provide secondary partner video analytics licenses and licensing schemes.

1.08 Intrusion Detection Integration

- A. Include in the system narrative a detailed explanation of intrusion detection system integration with access control and video surveillance functions. Provide details for the following:
 1. Integrated intrusion detection system manufacturer.
 2. Relationship between the manufacturers.
 3. Manufacturer roles and responsibilities including integration support.

4. Integrated user interface and system functions available through the integrated user interface.
- B. Provide software, licenses, professional services, and other costs necessary to implement the intrusion detection system integration.

ATTACHMENT 2

SECURITY SYSTEM QUANTITIES

Facility Type	Number of This Type	Card Readers		Cameras		Intrusion Panels		Equipment Locations	
		Each	Total	Each	Total	Each	Total	Each	Total
Elementary Campuses+Back Bay/Monte Vista+Early College	23	3	69	14	322	12	276	1	23
Middle School Campuses+Lincoln	3	7	21	12	36	5	15	1	3
7-12 (CdM & Costa Mesa) and 9-12 (Estancia & Newport Harbor) Campuses	4	10	40	12	48	10	40	6	24
			0		0		0		0
			0		0		0		0
			0		0		0		0
			0		0		0		0
Total Quantities	30		130		406		331		50

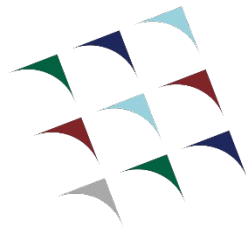
ATTACHMENT 3

Request for Information #104-21

For the purpose of this RFP #104-23, proposers that did not previously submit a response to the RFI #104-21 and are not listed in Section 3. Qualifications on this RFP as a pre-qualified systems manufacturer, all deadlines and dates included in the RFI below shall be negated. Proposers that did not previously submit a response to this RFI shall include a full and complete response to the RFI below with the current RFP #104-23 response.

THE REST OF THIS PAGE LEFT INTENTIONALLY BLANK

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

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.
 - 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. Consideration for future Cloud deployment
 - 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

- 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
 - 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 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	
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.

- 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
- 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, April 5, 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



Newport-Mesa
Unified School District

NEWPORT-MESA UNIFIED SCHOOL DISTRICT

ADDENDUM NO. 1

Integrated Security Standards

RFP No. 104-23

NEWPORT MESA UNIFIED SCHOOL DISTRICT
2985 BEAR ST., BLDG.-A
COSTA MESA, CALIFORNIA 92626

October 17, 2022

The following revisions and/or clarifications shall be made to the RFP documents for the above-named work. All work described in the original RFP documents and all applicable Sections of the original RFP documents shall be included in the contract, except as herein modified:

Acknowledgement of this Addendum shall be made below and submitted with the RFP submission. If acknowledgement is not made the proposal may be considered non-responsive.

1. **Change:** Change RFP Submitters Meeting date to October 24, 2022, at 1:00 PM

All other provisions of the RFP remain unchanged.

BELOW, PLEASE ACKNOWLEDGE RECEIPT OF THIS ADDENDUM AND SUBMIT IT WITH YOUR PROPOSAL.

Name:

ERIC MARTIN

Signature:

Firm Name:

LENEL SZ

Address:

1212 PITTSFORD VICTOR RD, PITTSFORD, NY

Telephone #:

Fax #:

(END OF ADDENDUM NO.1)



Similar Deployment

LenelS2 NetBox solution has been deployed at more than 1,000 schools throughout the United States. Below is the full contact information for three school districts who have deployed the LenelS2 NetBox solution.

Mark Anderson
Rockford Public Schools
Cell: 815-378-4526
mark.g.anderson@rps205.com

A Carrier Company

1212 Pittsford-Victor Road, Pittsford, NY 14534