Security Hardening Guide

Version 1.3

November 13, 2020

speco technologies®

Giving You More.

Security Hardening Guide v1.3

Table of Contents

Overview

Speco Technologies is a family owned and operated video surveillance, audio, and accessories manufacturer. We pride ourselves in delivering the highest quality products to you, our customers; our extended family. Speco Technologies has developed this security hardening guide to advise and recommend on best practices for securing your Speco Technologies network based devices. These are our line of IP Cameras, DVRs, NVRs, Servers and networking equipment. By following our guidelines for securing your valuable equipment, you are also doing due diligence to protect yours and your end-user's property and interest. As we are all intertwined in this age of digital highways, each one of us must take responsibility to preserve the safety and integrity of the highways by which we all depend on as our way of life and for our livelihoods.

The Physical Device

Security not only concerns threats from outside, but also threats from within. Security starts in the home and in the server room.

Ventilation

Network devices should be contained within properly ventilated server or equipment rooms. An improperly ventilated area is the leading cause of degradation of electronic equipment leading to component failures and ultimately catastrophic failure of the equipment. Gradual degradation of components also leads to non-optimal performance of devices and its software resulting in increased risks of physical injuries and security breaches. Moreover, equipment and component failures are the leading causes of data loss. Please refer to each device's product specification to obtain recommended operating temperatures.

Perimeter Security

The other aspect of the equipment room is perimeter security. Only authorized persons should be allowed to enter the equipment room. Secure the room with locked entryways. Outside electronic and smart devices such as notebook laptops, mobile/smart phones, digital probes and readers should not come in contact with any devices in the equipment room and if need be, only by a trained personnel. Probes, readers and other electronic devices can cause shorts in components. Devices such as laptops and smart phones need only to connect to a single device on the network via an Ethernet wired or wireless connection causing crippling software damage to all other devices on the network. A single device can spread harmful viruses like the Ransomware WannaCry causing irreparable damage. Therefore, the configuration and operation of devices in the equipment room should only be done by trained personnel. And last but not least, utilize your Speco Technologies video surveillance devices to monitor access.

Should a device be suspected of being in a state of failing due to any number of reasons, including software and/or hardware related ones, it should be disconnected immediately from the network and moved outside of the equipment room where it can be evaluated, repaired or replaced by a trained personnel.

Network Infrastructure

Don’t take your network security for granted. Invest the time and effort into securing your network infrastructure. This is the most important step in protecting your investments from being breeched or sabotaged by criminals and hackers. We discussed securing the physical network devices in earlier chapters, but is it enough? It is not. Care and considerations must also be given to securing the software running on these devices by ensuring that one or more firewalls are enabled and their rules and filters have been properly configured. For decades, network device manufacturers have invested billions of dollars to evolve and improve security measures on their products to protect governments, businesses and consumers. And with new threats appearing every day, billions more are being invested. Whether a small, medium-size or enterprise level business, focus on security should be your number one priority. It’s important to keep in mind that network infrastructures can be made up of many pieces of equipment either from a single manufacturer or a combination of many different manufacturers. Each manufacturer will have their own set of security recommendations and guidelines. Those guidelines should be followed and implemented in a timely manner. For Speco Technologies’ brand of network and video devices, the main scope of this document is to ensure our end-users have all the necessary information to keep their Speco Technologies equipment secure and safe.

Firewall

All routers today have built in firewalls. This firewall is perhaps the most important tool for securing your network. The best firewall is not foolproof so long as there are bad people wanting to breach your network; however, it is your best option as a first line of defense. Behind the firewall and protected from the rest of the world are the rest of your network switches, appliances and Speco Technologies products.

It is normal for IP cameras, DVRs and NVRs to not have a built in firewall which is the reason for the importance of the primary router's firewall. The primary router's firewall not only filters communication from the outside world but it also directs and monitors communication between all devices in the network. Network ports are individual channels of the network through which devices communicate with one another. The router is the gate keeper of all such ports and directs communication from one port to another.

Network Ports

There are a total of 65536 ports within a network and the router manages communication between all 65536 ports. However, most of the ports are locked down and only a selected few need be enabled. For every device on the network, there are certain ports which are assigned by default because they are commonly used ports for specific applications and should not be changed. The individual device's configuration tool often allows the choosing of alternate port numbers to use, but this is not recommended unless to avoid conflicts between devices. Again, this would be a task for trained network personnel. Take steps to secure non-essential network ports; those which are not needed to be opened in order for communication with other devices on the network. When network ports are needed to be enabled, it's expected that all devices that are connected to those ports have implemented the necessary safeguards to deflect irrelevant data as well as thwart attempts to hack into the devices. Even so, each device manufacturer's security recommendation should be given serious consideration and followed through for each device. As mentioned earlier, there are a number of so-called well-known network ports that are usually enabled and are necessary for all devices to establish communication. Well-known ports can be normally enabled or disabled depending on your needs and the manufacturer's discretion.

Well-Known Ports

- TCP 20 and 21 (File Transfer Protocol, FTP)
- TCP 22 (Secure Shell, SSH)
- TCP 23 (Telnet)
- TCP 25 (Simple Mail Transfer Protocol, SMTP)
- TCP and UDP 53 (Domain Name System, DNS)
- UDP 69 (Trivial File Transfer Protocol, tftp)
- TCP 79 (finger)
- TCP 80 (Hypertext Transfer Protocol, HTTP)
- TCP 110 (Post Office Protocol v3, POP3)
- TCP 119 (Network News Protocol, NNTP)
- UDP 161 and 162 (Simple Network Management Protocol, SNMP)
- TCP 443 (Secure Sockets Layer over HTTP, https)

Speco Video Devices

Speco Technologies devices also requires the use of various ports that may or may not be well-known ports and may need to be open in order to fully utilize all features of the devices. The following are the default port values and Speco Technologies recommends the ports to be forwarded and accessible through your firewall if accessed over a WAN.

Speco IP Camera Ports

- HTTP: 80
- HTTPS: 443
- Data: 9008
- RTSP: 554

NX Series NVR Ports

- TCP: 37777
- UDP: 37778
- HTTP: 80
- HTTPS: 443
- RTSP: 554

HS/HT/HU/NS/VT/VX Series DVR/NVR Ports

- TCP: 5445
- HTTP: 80
- Audio: User Assigned + 1

- IP Camera Setup through web viewer: Forward ports 59011 ~ 59254 to the NVR (**NS series only**)

NR/NRL/NRE/NRN/NRP/HRL Series NVR/HVR Ports

- HTTP: 80.
- HTTPS: 443.
- Server: 6036
- RTSP: 554.

JLA Series

- TCP: 9000 for proprietary protocol.
- UDP: 9333 for proprietary protocol.
- HTTP: 80.
- HTTPS: 443.
- RTSP: 554.

SecureGuard® Server/NVR Ports

- Server: 7312
- Video: Server + 1 (7313)
- Mobile App: Server + 2 (7314)
- DDNS: 7312-7314
- Outgoing/Incoming TCP and UDP: 50192, 44210

SecureGuard® Server Firewall

SecureGuard® Servers run a Windows based operating system which comes with its own firewall. The SecureGuard® Server is the only Speco Technologies device which has its own firewall. Although the SecureGuard® Server itself has a firewall, its firewall should not be used as a primary layer of protection. The SecureGuard® Server should be located behind a primary network router that has an adequate firewall as a first line of security. The SecureGuard® Server's firewall serves well as a second line of protection.

Credentials

Every device on the network is password protected and preconfigured at the factory with a default username and password. Speco Technologies' devices are no different. They are assigned a default username and password at the factory which is only used to gain access to the devices for initial setup and configuration. However, these passwords offer virtually no protection if they are not changed to strong passwords. Assigning strong passwords from the onset greatly minimizes the risk of someone being able to gain access and sabotaging the devices. It's important to note that default usernames and passwords for any device albeit Speco Technologies or other brands are widely published on the internet and are easily searchable with a few simple keywords. For example, Google "IP camera password" and topping the list of results is this web site which lists common default username and passwords for practically every manufacturer of IP video cameras.

Strong Passwords

Passwords that are considered strong contain all of the following elements:

- 12 or more characters.
- 1 or more lower case letters
- 1 or more upper case letters
- 1 or more numbers
- 1 or more special characters (i.e. *,!,&#)
- Does not contain common words

It is also important to change passwords every 3 months and not reuse any passwords that have been used in the past.

IP Cameras, DVR, NVR Default Username/Password

In most cases, the following are the default administrative login credentials:

- Username: "admin"
- Password is "1234" or "asdf1234#"

The password should be changed to a strong password at initial startup.

SecureGuard® Default Username/Password

SecureGuard® leaves the factory with 3 pre-defined users and 3 different login credentials with each having an administrator, a user and a guest role. Please refer to the SecureGuard® User's Guide:

Administrator:

- Username: "admin"
- Password: "admin"

User:

- Username: "user"
- Password: "user"

Guest:

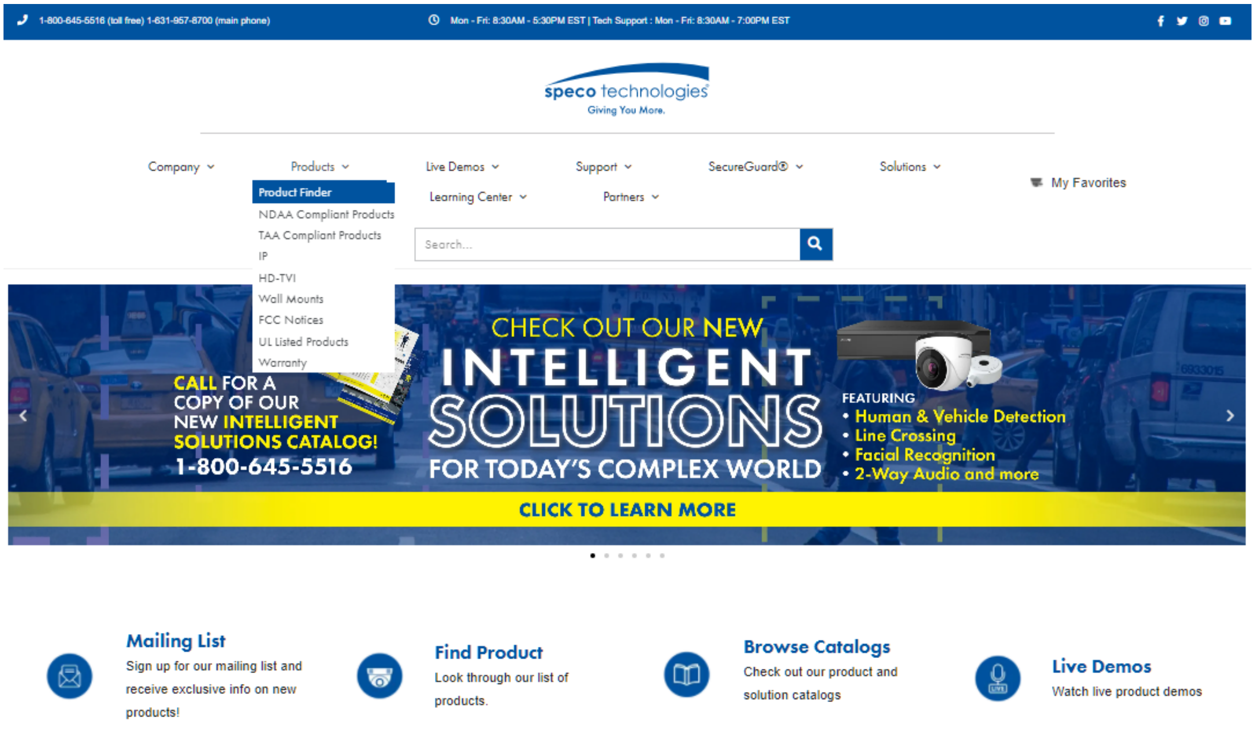
- Username: "guest"
- Password: "guest"

Software/Firmware Updates

Ensure that every device on the network is running the most updated software and firmware available. This should be done on a regular basis. As new security threats emerge, manufacturers are continually implementing safeguards within their software to protect their devices from such threats. This is why it's good practice to continually check for new updates from the manufacturer's web site.

IP Cameras, DVR, NVR

The latest Speco Technologies IP Camera, DVR and NVR firmware can be found on our web site: www.specotech.com. From our web site, find your IP Camera, DVR or NVR web page from our "Product Finder" web page or enter the model number in our web site search tool and click "Go" to locate your camera.



1-800-645-5516 (toll free) 1-631-957-8700 (main phone)

Mon - Fri: 8:30AM - 5:30PM EST | Tech Support : Mon - Fri: 8:30AM - 7:00PM EST

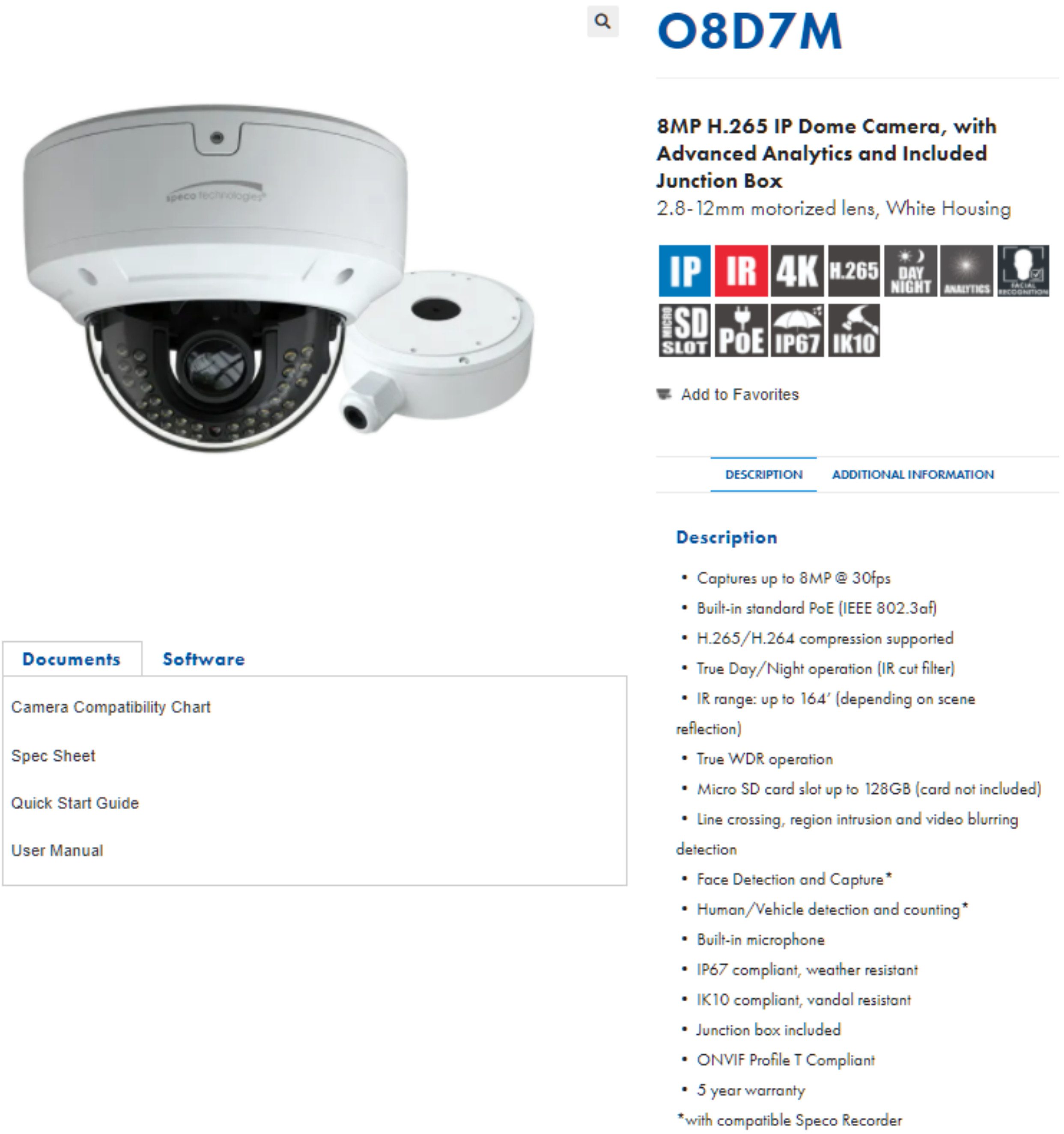
Mailing List
Sign up for our mailing list and receive exclusive info on new products!

Find Product
Look through our list of products.

Browse Catalogs
Check out our product and solution catalogs

Live Demos
Watch live product demos

At the middle of the camera web page, click on the "Software" tab and the latest firmware available for download will be listed.



O8D7M

8MP H.265 IP Dome Camera, with Advanced Analytics and Included Junction Box

2.8-12mm motorized lens, White Housing

Add to Favorites

DESCRIPTION | ADDITIONAL INFORMATION

Description

- Captures up to 8MP @ 30fps
- Built-in standard PoE (IEEE 802.3af)
- H.265/H.264 compression supported
- True Day/Night operation (IR cut filter)
- IR range: up to 164' (depending on scene reflection)
- True WDR operation
- Micro SD card slot up to 128GB (card not included)
- Line crossing, region intrusion and video blurring detection
- Face Detection and Capture*
- Human/Vehicle detection and counting*
- Built-in microphone
- IP67 compliant, weather resistant
- IK10 compliant, vandal resistant
- Junction box included
- ONVIF Profile T Compliant
- 5 year warranty

*with compatible Speco Recorder

Documents | **Software**

Camera Compatibility Chart

Spec Sheet

Quick Start Guide

User Manual

Download the firmware and follow the firmware update instructions in the camera's user guide to apply the new version.

SecureGuard® Server

With SecureGuard® Server version 2.2 and newer, when enabled, the server will check for new software updates on a daily basis at the administrator's specified time. We recommend leaving this auto update feature on if the server is connected to the internet and can reach Speco Technologies' software update server. However, in the situation where the server does not have internet access, the auto update feature can be disabled. A "Check Now" button is also available to allow the administrator to manually check for software updates whenever an internet connection is present. If an update is available, the latest Windows and Mac SG installer files will be downloaded automatically. After the download is completed, a gear icon will be displayed in the lower right side of the Configuration Tool and an administrator's Client notifying them that an update is ready to be installed. Please refer to the SecureGuard® User's Guide for in-depth instructions on updating the server's software. All SecureGuard® servers running software version 2.1 and older must be updated to the latest version in order to take advantage of the auto software update feature along with other new features and improvements.

Speco Cloud

Speco cloud-enabled cameras and the servers which these cameras record to brings a new dimension to cyber security. Video storage is no longer confined to a closed network of IP cameras and recorders, but can now be transmitted across the internet to be stored on remote servers in the cloud. With the emergence of recording to the cloud technology, video packets are primarily transmitted across a wide area network (WAN) that traverses many networks some of which are tightly controlled, some not so much. Speco understands the vulnerabilities and risks to our customers' video data and have deployed the latest cryptographic protocols to ensure that the data transmitted between our cameras and Speco Cloud servers are secure and safe from cyber crime. Video data is encrypted in accordance to internet communication security standards, TLS and SSL, which are regulated by the Internet Engineering Task Force (IETF).

Transport Layer Security (TLS)

RFC 5246 of the IETF states: "This document specifies Version 1.2 of the Transport Layer Security (TLS) protocol. The TLS protocol provides communications security over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery.

Secure Socket Layer (SSL)

RFC 6101 of the IETF states: "This document specifies version 3.0 of the Secure Sockets Layer (SSL 3.0) protocol, a security protocol that provides communications privacy over the Internet. The protocol allows client/server applications to communicate in a way that is designed to prevent eavesdropping, tampering, or message forgery."

In addition to securing the transmission of video data, the security of our customers' stored video is also top priority. For this reason, Speco Cloud utilizes all of the Amazon AWS infrastructure to store our customer data and limit video storage to only those servers that are kept and maintained in regions whithin the North American continent. Amazon AWS are trusted and proven servers utilized by many governmental, enterprise and educational bodies to store their customer data. Per Amazon: "The AWS infrastructure puts strong safeguards in place to help protect customer privacy. All data is stored in highly secure AWS data centers."

What steps does AWS take to protect customer privacy?

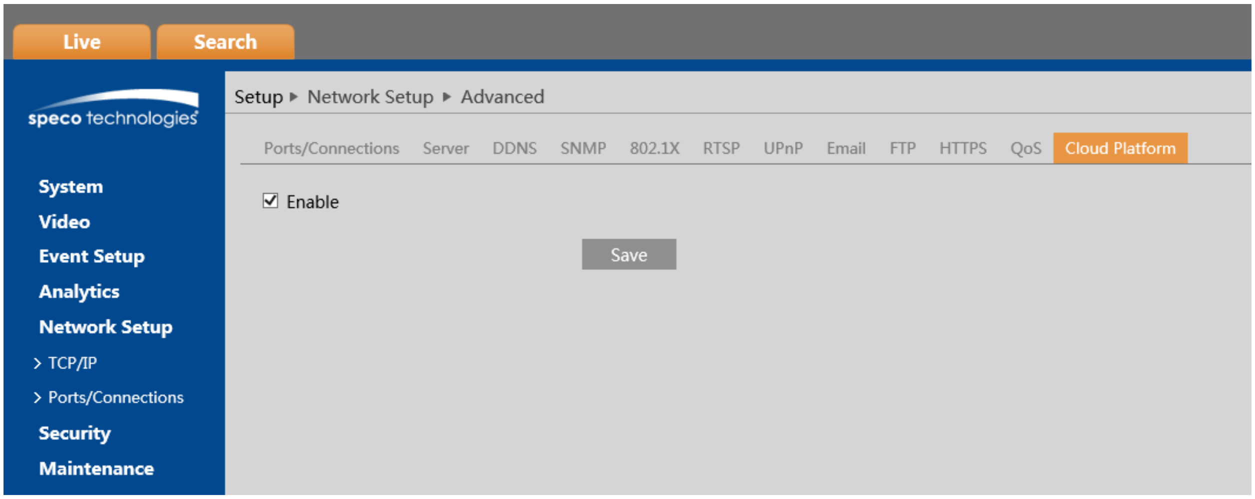
According the AWS data privacy web site: "AWS's alignment with ISO 27018 has been validated by an independent third party assessor. ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and provides implementation guidance on ISO 27002 controls applicable to Personally Identifiable Information (PII) processed by public cloud service providers. This demonstrates to customers that AWS has a system of controls in place that specifically address the privacy protection of their content."

Speco Technologies' and Amazon AWS commitment to data privacy and security are one of the same. We take our customers data seriously and safeguard it as if it were our own.

Disable Speco Cloud

Upon powering up a Speco cloud-enabled camera, the camera will begin sending periodic heart beats to the Speco Cloud server residing on Amazon AWS servers located in the United States. If within the first 2 hours of power up the camera does not successfully enroll/re-enroll onto Speco Cloud then all communication to Speco Cloud would cease and the camera will no longer communicate with Speco Cloud again until the camera is power cycled.

In the event the cloud-enabled camera is intended only for local recording, the entire communication process to Speco Cloud can be disabled from Settings menu (Settings->Network Setup->Ports/Connections->Cloud Platform, uncheck Enable (see image)).



☑ Enable

Speco Access – Cloud Based Access Control Appliances

Our controller is an embedded, browser managed network appliance that is designed to support physical security of a facilities via a fast and intuitive embedded HTML5 web interface it's primary use is to inform control who, what, where and when access events occur . The system manages any physical device that the system designer chooses to control such as door locking hardware, device management such as fans, pumps, pullies …. In addition the system is designed to monitor and inform the status of these devices. The hardware and software are configured and managed over a network using most internet browsers. The system can manage 60 transactions per second, using its Quad Core processor with 64 Bit processing. Speco offers additional system configurations that supports up to 120 transactions per second with significant system capacities for scaling options.

The access control software runs on an industry standard Linux Ubuntu operating system and requires no server or software to be installed on local PC's or other browser enabled devices. As a browser managed system, our technology ensures compatibility with network equipment, smart devices and computers. As a native IP network appliance, we do not require any additional gateways, communication wiring or add on adapters to be install. Our system's Gigabit auto sensing network connection is responsive while ensuring secure connectivity.

Our hardware is similar in design, using identical software and is uniquely designed to perform the function of a "server" or a "client". In this design each device contains all the capabilities of the system and with database redundancy. When installed, a controller is configured as a server or a client and no special hardware or software is required. Our market leading feature enhancement and system scaling allows you to grow or add capabilities when needed. It is fast and easy to turn an enhanced feature on or add additional clients to the system to manage more doors.

All communication between devices is encrypted and secure. Whether stored on the panel, SD Card and or FTP Server system data, event logs, user data are encrypted and secure.

Network Utilization

Many customers choose to leverage the company's network infrastructure to interconnect and manage their Physical Access Control System. Leveraging an existing network lowers the cost of installation and improves performance when compared to other communication methods.

Multiple Panels Interconnection

Our controllers are designed to interconnect and control access for one or many doors or devices. When controllers are added to a network / system the hardware automatically sets itself an IP address in the zeroconf address space. The expansion controller then multicasts for a server controller at a specific IP address and port and presents our Unique Identifier (UID) to let it be known as an expansion controller. The Server controller then responds to establish the system interlink.

Expansion controllers can be statically or dynamically addressed. Typically, the server is assigned a static IP address and clients are configured for DHCP. However, the systems clients could be configured statically should the network administrator prefer.

These panels are typically interconnected on a local LAN or WAN but also can be securely interconnected via public internet.

Encryption Standards and Protocol

Network security and encryption is something we do not take lightly. We deploy the latest security encryption and protocols available. We have had and will continually perform PEN tests to ensure our standards and cyber protection practices are sound and up to date.

- SSL Encryption and Authentication for the browser to the controller
- HTTPS - Hypertext Transfer Protocol Secure
- SSH Authentication and Encryption between the server and the expansion hardware "clients". The system administrator has the option to upload a private / corporate key.
- AES 256 Advanced Encryption Standard – data packets Users, Logs, Systems settings…
- In addition to the use of industry IT security standards, our system adds a secondary encryption require that only our hardware / ecosystem is capable of decoding and visually displaying the data that is produced and communicated by our system. This is proprietary to our system and is an added protection because the data is specific to our system use only.

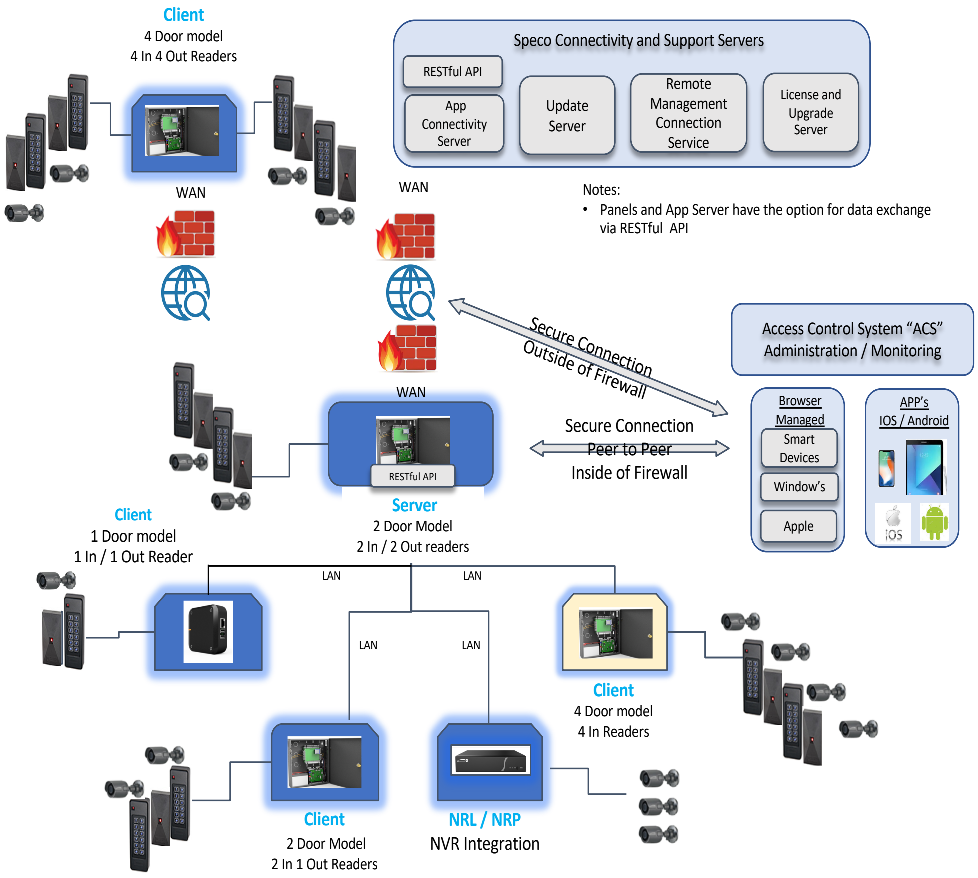
To ensure our systems are secure we perform and utilize a variety of services to test the product for Cyber Security (PEN Testing). As a security provider, we take network security seriously and will provide periodic security updates as required.

Network Port Usage

TCP Port	Description and Function
80	HTTP - Open to Controller for Browsers to access the Security Application, Can be configured on a different port.
443	HTTPS (SSL) - Open to Controller for Browsers to access the Security Application, Can be configured on a different port.
554	RTSP Port for NVR
1022	SSH Communications
2000	FTP Server System Back up
6000 / 6001	Server / Client configuration and set up - Once configured the system does not use.
8081	RESTful API
9000	Mobile App
9000~9100	FTP Data Backup
9500	Update Server (Link Server)
9900	Remote Management Connector RMC
2021	Software Update FTP Server

Security Hardening Guide v1.3

Eco System Overview



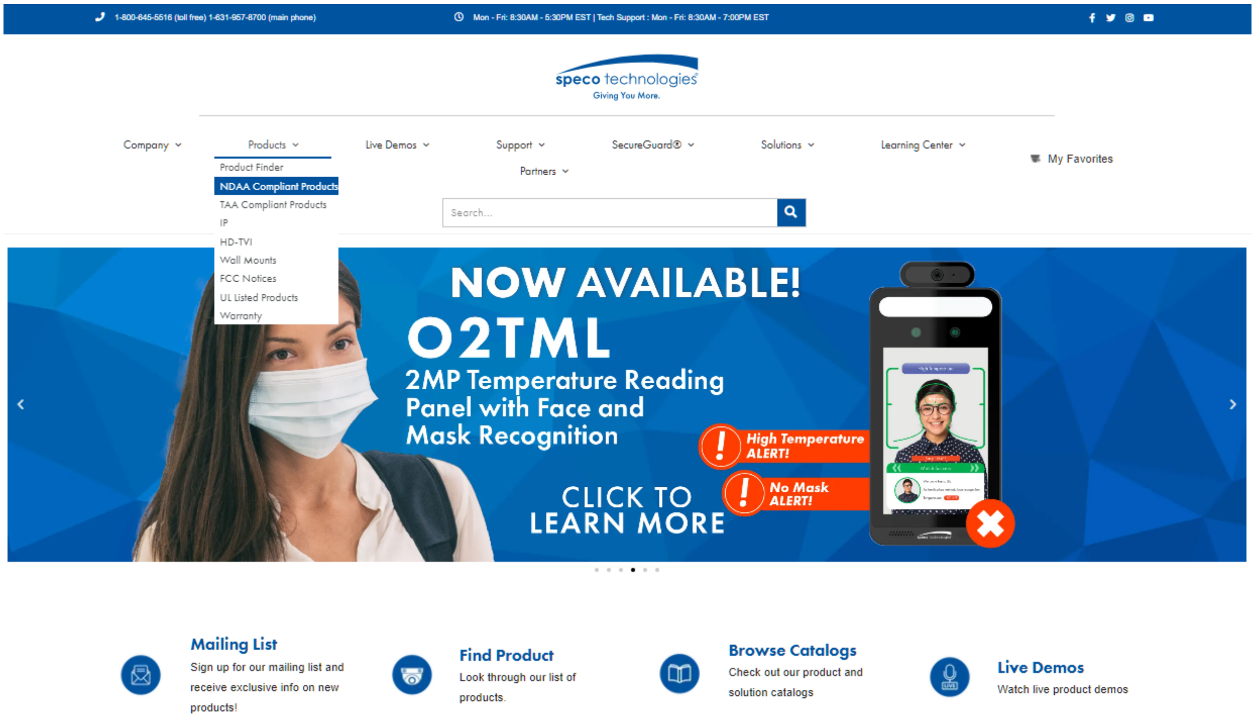
System Setup Requirements

- DNS (Domain Name Server)
- IP address(es)
- Gateway IP Address, if any
- Subnet mask and IP addresses for the server and clients
- E-Mail relay server address or name
- E-Mail address name and setup on the email server to accept the mail for the eNc relay
- NTP (Network Time Protocol) server name (s) if the network has no internet access

NDAA Compliance Statement

The John S. McCain National Defense Authorization Act for Fiscal Year 2019 (NDAA 2019) is a United States federal law which specifies the budget, expenditures and policies of the U.S. Department of Defense (DOD) for fiscal year 2019. It was signed by President Donald Trump during a ceremony in Fort Drum, New York on August 13, 2018. **NDAA bans the federal government from purchasing equipment from certain Chinese suppliers due to security concerns**, including Huawei and ZTE, as well as any surveillance equipment for the purposes of national security from Dahua Technology, Hytera, and Hikvision.

Speco is actively moving to exclude components from these banned companies. Please find a list of current models from Speco Technologies that **DO NOT CONTAIN ANY COMPONENTS** from (NDAA Section 889 Part B) banned companies on our web site: www.specotech.com. From our web site, navigate to the "NDAA Compliant Products" web page from the products drop-down menu.



1-800-645-5516 (toll free) 1-631-957-8700 (main phone)

Mon - Fri: 8:30AM - 5:30PM EST | Tech Support : Mon - Fri: 8:30AM - 7:00PM EST

Sign up for our mailing list and receive exclusive info on new products!

Look through our list of products.

Check out our product and solution catalogs

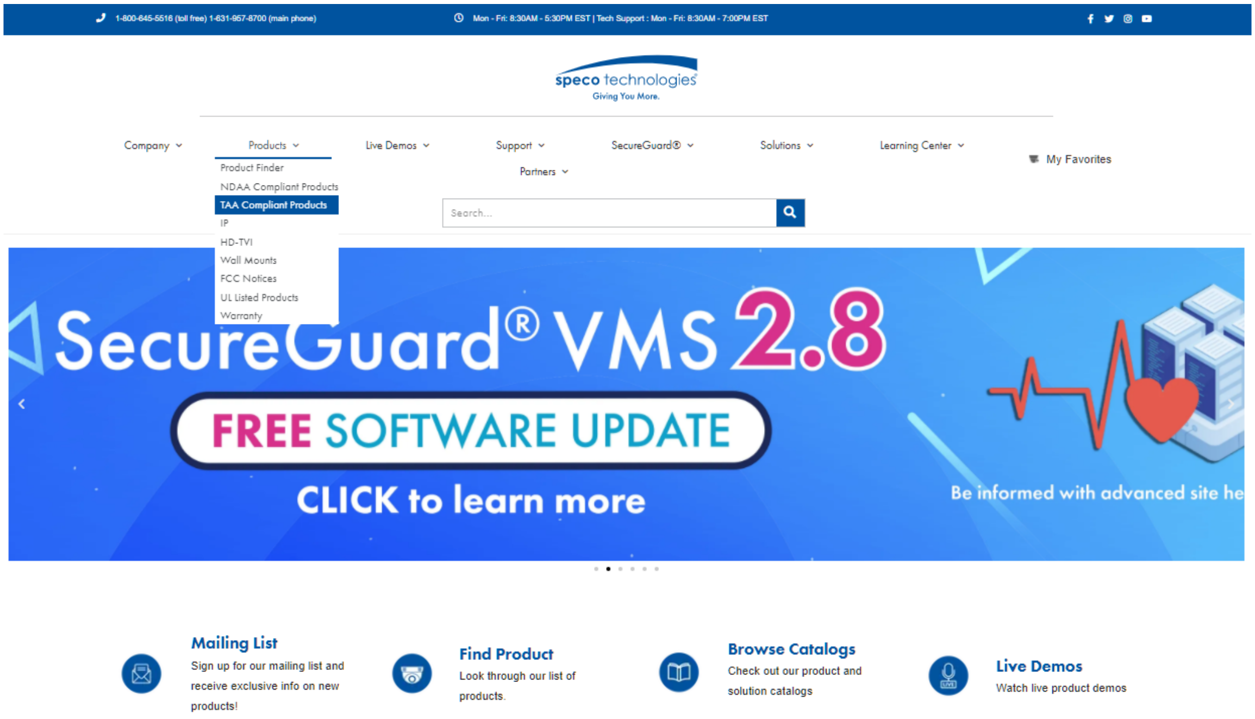
Watch live product demos

TAA Compliance Statement

Speco Technologies is proud of our rich history of providing TAA compliant products to the security industry. The Trade Agreement Act (TAA) (19 U.S.C. &

2501-2581) was created in 1979 and is intended to foster the growth and maintenance of a fair and open trading system.

Please find a list of current models that are TAA compliant on our web site: www.specotech.com. From our web site, navigate to the "TAA Compliant Products" web page from the products drop-down menu.



PCI Security Requirements

The past few years saw an explosion in the use of digital data to handle money transactions, from debit cards to now Apple Pay and Google Wallet. As part of this growing trend, protocols were established and enhanced to protect this data from those who would seek to exploit it.

A group of transaction processors got together and formed an industry group. They named themselves the Payment Card Industry (PCI). This group put together a series of protocols to follow for securing the storage, transmission and processing of data that includes payment information (i.e. credit cards, debit cards, gift cards, etc.).

Speco Technologies' DVR, NVR and video servers are specifically designed to only use and process either proprietary information or ONVIF protocols to record and transmit video and audio data. With this, requirements for PCI Security have mostly been met. What is required from the user when placing a Speco DVR into a network that will transmit and receive PCI data are the following steps:

- Disable user accounts in the DVR that will not be used.
- Change the passwords of the user accounts that will be used for video/audio access.

Updates to Speco's Privacy Policy

As part of our continual commitment to update our products and services to meet regulations in safeguarding the personal data of all our customers, we have made some changes to our Privacy Policy. Please take time to review our Privacy Policy and understand how we collect and use personal data that may be shared with us. In particular to citizens of the European Union, any information you share with us are protected as mandated by the EU GDPR and we respect your right to opt out by contacting salessupport@specotech.com. Speco Technologies looks forward to continuing relationship with our customers from around the world and reaffirm our commitment to upholding the highest standards in security and privacy.

The Fight against Cyber-Attacks

Speco Technologies is taking the lead in fighting Cyber-Attacks in the Video Surveillance Industry. We are working toward UL 2900 certification with all our video surveillance products and software.

We are proactively working with Underwriters Laboratory (UL) to obtain a UL 2900 certification for all of our video surveillance products and software. In April 2016, UL launched its new Cybersecurity Assurance Program to assess software vulnerabilities and weaknesses, minimize exploitation, address known malware, review security controls and increase security awareness. Based on UL testing, we have improved the cyber posture of our cameras, recorder, and SecureGuard® VMS and are working closely with their team to get our products UL 2900 certified.

Speco Technologies is aware that cyber-attackers are becoming increasingly sophisticated and is proactively working toward safeguarding the privacy and security of our customers. Speco Technologies' President, Todd Keller, stated "By identifying vulnerabilities, we are able to alleviate those risks and work with our product development team to continue to innovate and manufacture more secure products to stay ahead of any possible cyber-attacks."