Security Hardening Guide

Version 1.4

Overview

Speco Technologies, a family-owned and operated manufacturer of video surveillance, audio solutions, and access control, is dedicated to providing the highest quality products. This guide offers best practices for securing Speco Technologies' network-based devices, including IP cameras, DVRs, NVRs, Access Control Panels, servers, and networking equipment. Following these guidelines, you help safeguard your equipment, networks, and sensitive data. In today's interconnected digital landscape, maintaining the safety and integrity of the networks that support our lives and livelihoods is a shared responsibility.

The Physical Device

Ventilation

• Network devices should be housed in adequately ventilated servers or equipment rooms to prevent overheating, which can degrade performance and lead to failures.

• Adhere to recommended operating temperatures in product specifications to ensure optimal performance and longevity.

Perimeter Security

• Restrict physical access to equipment rooms to authorized personnel only, with entryways secured by locks.

• Use Speco surveillance devices to monitor and/or Speco Access Control to monitor access.

• Disconnect and isolate any suspected failing devices for evaluation, repair, or replacement to prevent network disruption.

• When necessary, laptops and smartphones should only connect to a single network device via a wired or wireless Ethernet connection. Failure to manage this properly can expose the entire network to software vulnerabilities, potentially causing widespread damage. For example, a single compromised device can spread harmful malware, such as the WannaCry ransomware, which may lead to irreparable harm to the network.

• Therefore, the configuration and operation of equipment in the room should always be handled by trained professionals. Additionally, utilizing Speco Technologies video surveillance devices to monitor and Speco access control to the room is strongly recommended.

• If any device in the equipment room is suspected of failure (whether due to hardware or software issues) it should be promptly disconnected from the network. The device must then be removed from the room for evaluation, repair, or replacement by qualified personnel to prevent further disruption or compromise.

Network Infrastructure

Network security is not a matter to be taken lightly. Securing your network infrastructure is the foundation of protecting your investments from breaches or sabotage by criminals and hackers. At the same time, earlier chapters addressed the importance of safeguarding physical network devices, which is insufficient in today's evolving threat landscape. Equal attention must be given to securing the software running on these devices. This includes enabling one or more firewalls and ensuring their rules and filters are correctly configured to protect your network.

Over the decades, network device manufacturers have invested billions of dollars in advancing and refining security measures to safeguard governments, businesses, and consumers. As new threats emerge daily, even more significant investments are being made to stay ahead of potential vulnerabilities. Whether you operate a small, medium-sized, or enterprise-level business, prioritizing network security is critical.

Network infrastructures are often composed of equipment from a single manufacturer or a mix of many. Each manufacturer provides security recommendations and guidelines, which must be carefully reviewed and implemented promptly. Neglecting these measures leaves your network exposed to unnecessary risks.

For Speco Technologies' line of network, access, and video devices, this guide is a comprehensive resource to ensure end-users have the necessary tools and knowledge to keep their Speco Technologies equipment secure. Follow these steps to maintain a robust and resilient network infrastructure:

1. **Regular Updates**: Ensure all firmware and software are updated to the latest versions to mitigate vulnerabilities.

2. **Access Controls**: Implement robust access controls, including multi-factor authentication, to restrict unauthorized access.

3. **Monitoring**: Utilize Speco Technologies' video surveillance systems to monitor network activity and physical access points for anomalies.

4. **Firewall Configuration**: Regularly establish and review firewall rules to ensure they are optimized for current threats.

5. **Device Segmentation**: Segment the network to isolate sensitive de vices and data, limiting the spread of potential breaches.

6. **Adherence to Guidelines**: Follow the specific security guidelines provided by Speco Technologies and other manufacturers in your network to maintain a unified defense strategy.

By investing the time and effort to secure both the hardware and software components of your network infrastructure, you protect your equipment and the sensitive data and operations vital to your business.

Firewall Configuration

Modern routers have built-in firewalls, which serve as the cornerstone of network security. While no firewall can offer absolute protection (especially with persistent threats from malicious actors) it remains the most effective first line of defense. Behind this firewall lies your network's core: switches, appliances, and devices like Speco Technologies products, all shielded from external threats.

It's important to note that many IP cameras, DVRs, and NVRs typically do not feature built-in firewalls. This makes the primary router's firewall essential for safeguarding your network. The router's firewall not only filters incoming and outgoing communication with the outside world but also manages and secures communication between devices within the network.

Here are updated guidelines for firewall management in 2024:

1. **Configure Firewall Rules**: Set up customized rules to filter and control traffic based on protocols, IP addresses, and ports—Disable unused or unnecessary ports to minimize exposure to potential threats

2. **Network Port Management:** Network ports act as communication channels between devices. Your router serves as the gatekeeper, directing traffic between these ports. Regularly audit open ports to ensure only essential ones are active, reducing the attack surface for cyber threats.

3. **Enable Intrusion Detection and Prevention:** Modern routers offer built-in intrusion detection and prevention systems (IDS/IPS). Enable these features to identify and mitigate suspicious activities on your network automatically.

4. **Secure Remote Access:** If remote access is necessary, ensure it is encrypted and protected with multi-factor authentication (MFA). Consider using virtual private networks (VPNs) for added security when accessing your network remotely.

5. **Update Router Firmware Regularly:** Keep your router's firmware current to address vulnerabilities and enhance security features. Many manufacturers release regular updates to combat emerging threats.

6. **Segment Your Network:** Use VLANs or subnets to separate devices based on their function or level of sensitivity. For instance, isolate Speco Technologies products from other general-use devices to add an extra layer of protection.

7. Use **Next-Generation Firewalls (NGFW)** for advanced threat detection and mitigation.

8. Regularly review and update firewall rules to ensure they align with current threats.

9. Disable unused ports and enable only those necessary for operation.

By implementing these best practices, you can maximize your firewall's effectiveness and ensure your network infrastructure's security. A properly configured router firewall blocks unauthorized external access and maintains order and security within the network, directing and monitoring communication between devices to safeguard your operations.

Device Segmentation

• Segment networks to isolate sensitive devices, limiting the spread of potential breaches.

• Use VLANs or subnets to separate devices based on their function or sensitivity level.

Regular Updates

• Ensure all firmware and software are updated to the latest versions to mitigate vulnerabilities.

Network Ports

A network consists of 65,536 ports, with the router responsible for managing communication between them. Most of these ports are locked down by default, with only a few enabled for specific purposes. Proper management of these ports is essential for maintaining a secure and efficient network.

Key Guidelines for Managing Network Ports in 2024:

1. **Default Port Assignments:** Each device on the network typically uses specific default ports based on the application or service it supports. These ports are standardized and should not be changed unless necessary to avoid conflicts. If changes are required, trained network personnel should only handle this task.

2. **Non-Essential Ports:** Non-essential network ports (those not required for device communication should) be secured and disabled. Leaving unnecessary ports open increases the risk of unauthorized access and other vulnerabilities.

3. **Port Security Measures:** Ensure that all connected devices have implemented robust security measures when enabling network ports. This includes filtering irrelevant data and blocking unauthorized access attempts. Devices should have firewalls, intrusion detection systems (IDS), or other safeguards to protect these entry points.

4. **Manufacturer Guidelines:** Always consult and adhere to the security recommendations provided by the device manufacturer. These guidelines are tailored to ensure optimal functionality and security for their products.

5. **Advanced Port Management:** Consider using advanced router features like port forwarding and port triggering sparingly and only for specific applications. Monitor open ports regularly to detect any unauthorized activity.

Additional Best Practices:

• **Audit Regularly:** Conduct routine audits to ensure that only the necessary ports are open and that unused ports remain securely closed.

• **Monitor Traffic:** Use network monitoring tools to track traffic through open ports and identify unusual patterns that could indicate a security breach.

• **Training and Expertise:** Port configuration and management should only be performed by trained network professionals to minimize the risk of errors.

By following these updated guidelines, you can effectively manage network ports to maintain a secure and efficient network environment. Proper port management ensures that essential communication remains seamless while protecting your network from potential threats.

Well-Known Ports

Well-known ports are standardized network ports used by specific applications or services. These ports are widely recognized and often enabled by default for their respective purposes. Understanding their functions and proper usage is crucial for maintaining secure and efficient network operations.

Commonly Used Well-Known Ports:

• **TCP 20 and 21: File Transfer Protocol (FTP)** Used for transferring files between computers.

• **TCP 22: Secure Shell (SSH)** Provides secure remote login and other secure network services.

• **TCP 23: Telnet** Used for remote text-based communication, though considered insecure and often

• **TCP 25: Simple Mail Transfer Protocol (SMTP)** Used for sending email.

• **TCP and UDP 53: Domain Name System (DNS)** Resolves domain names to IP addresses, essential for internet communication.

Commonly Used Well-Known Ports:

• **UDP 69: Trivial File Transfer Protocol (TFTP)** A simplified file transfer protocol, typically used in boot and network configuration environments.

• **TCP 79: Finger** Used to retrieve information about users, though rarely used today due to security concerns.

• **TCP 80: Hypertext Transfer Protocol (HTTP)** Enables browsing the web via unencrypted communication.

• **TCP 110: Post Office Protocol v3 (POP3)** Retrieves email from a server to a local client.

• **TCP 119: Network News Protocol (NNTP)** Facilitates reading and posting articles on Usenet.

• **UDP 161 and 162: Simple Network Management Protocol (SNMP)** Used for managing devices on IP networks.

• **TCP 443: Secure Sockets Layer over HTTP (HTTPS)** Provides secure web browsing using encryption.

Best Practices for Well-Known Ports:

1. **Enable Only When Necessary:** Avoid enabling ports unless their associated services are required. This minimizes the network's attack surface.

2. **Use Secure Alternatives:** Replace outdated or insecure protocols like Telnet (TCP 23) and Finger (TCP 79) with secure alternatives such as SSH (TCP 22).

3. **Monitor Traffic:** Continuously monitor activity on open ports to detect unauthorized access or abnormal traffic patterns.

4. **Restrict Access:** Implement firewall rules to restrict access to well-known ports based on IP addresses or network zones.

5. **Encrypt Communication:** Where applicable, prefer secure versions of protocols (e.g., HTTPS over HTTP) to protect data during transmission.

6. **Regular Updates:** Ensure firmware and software associated with services using these ports are kept up to date to address vulnerabilities.

By properly managing well-known ports, you can balance functionality with robust security, ensuring your network is protected against potential threats.

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 device. 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

NR/NRL/NRE/NRN/ NRP/HRL Series NVR/ HVR Ports
• HTTP: 80
• HTTPS: 443
• Server: 6036
• 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)

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

Speco Blue Ports

Default Ports for Inbound Traffic

Port Number	Description
80	HTTP Port
443	HTTPS Port
554	RTSP Port (Recorder)
9008	RTSP Port (IP Camera)
6036	Server Port (Recorder)
554	Server Port (IP Camera)
7681	WebSocket Port (IP Camera)
8080	API Port (IP Camera)

Speco utilizes P2P servers hosted by AWS. The table below lists the domain names (if applicable), IP addresses, and ports that may be used by Speco Blue recorders for outbound traffic. Note that when a user logs into a recorder via the P2P server, a direct connection from the recorder to the end user may be established.

Additional Services

Service	Domain/IP	Port (TCP/UDP)
Speco DDNS	specoddns.net	80 / None
Dashboard Email	specodash.cloud	587 / None
Configured DNS Servers	Various	None / 53

Outbound Traffic Information

Domain Name	IP Address	TCP Ports	UDP Ports
nat.specotech.cloud	184.73.47.149	80, 6071, 8991-8993, 10001-10010	8989-8999
nat.specotech.cloud	3.220.216.155	80, 6071, 8991-8993, 10001-10010	8989-8999
nat.specotech.cloud	54.157.148.117	80, 6071, 8991-8993, 10001-10010	8989-8999
nat.specotech.cloud	54.175.119.152	80, 6071, 8991-8993, 10001-10010	8989-8999
dev-push20.specobluep2p.com	47.88.104.253	7010, 7023	None
dev-push20.specobluep2p.com	47.88.102.123	7010, 7023	None
dev-nat20.specobluep2p.com	44.206.166.226	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	3.216.131.161	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	3.230.140.78	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	3.230.168.129	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	18.205.15.180	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	23.21.160.17	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	34.235.194.112	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	44.206.166.226	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	54.236.113.131	80, 443, 446, 9971	11001, 11101
dev-nat20.specobluep2p.com	100.24.188.209	80, 443, 446, 9971	11001, 11101

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

Password Policies

- Password must:
    - Be at least **16 characters** long.
    - Include uppercase, lowercase, numbers, and special characters.
    - Avoid dictionary words or predictable patterns.
- Change passwords every **90 days** and do not reuse previous passwords.
- Use **Multi-Factor Authentication (MFA)** wherever possible.

Default Credentials

- Devices must ship with **randomized default credentials** to reduce unauthorized access risks.
- Setup wizards should prompt users to:
    - Configure unique, strong passwords.
    - Enable security features during the initial setup.

Encryption Standards

Transport Layer Security (TLS)

- Enforce **TLS 1.3** as the default encryption protocol for all communications.
- Deprecate and avoid using older protocols like SSL 3.0.

Data Encryption

- Use **AES-256 encryption** for all stored and transmitted data.
- Encrypt user credentials, video data, and sensitive logs.

Software and Firmware Updates

Automatic Updates

- Download the latest firmware from Speco Technologies' website.
- Follow update instructions provided in the user guide.

Manual Updates

- Use **AES-256 encryption** for all stored and transmitted data.
- Encrypt user credentials, video data, and sensitive logs.

Remote Access Security

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"

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 is "admin"

User:

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

Guest:

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

Speco Blue VMS Username/Password

Speco Blue VMS has a pre-defined administrative login. After initial installation, the system will prompt you to change the default password.

Administrator:

- Username: “admin”
- Password is “1234”

PCI Compliance

Updated Practices

- Encrypt all sensitive data in transit and at rest.
- Implement **audit logging** to track access to video, payment, or sensitive data.
- Perform annual penetration testing and quarterly vulnerability scans.

Device Recommendations

- Disable unused user accounts.
- Enforce unique, strong passwords for all active accounts.

Cybersecurity Awareness

Personnel Training

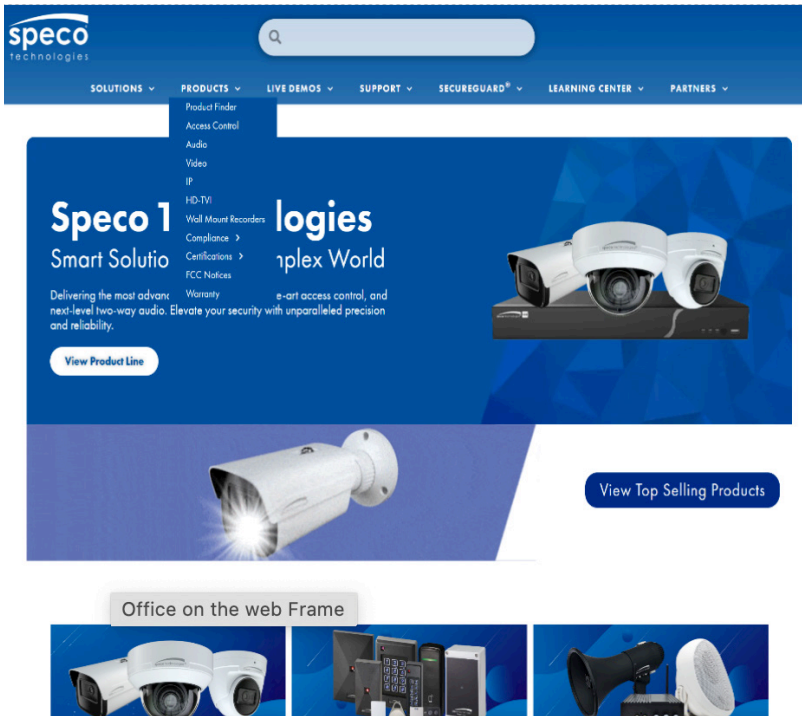
- Provide ongoing training for administrators and end users on cybersecurity best practices.
- Educate staff on recognizing phishing attempts, ransomware, and social engineering threats.

Incident Response Plan

- Develop and document a clear incident response plan.
- Include steps for isolating compromised devices and mitigating damage.

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.

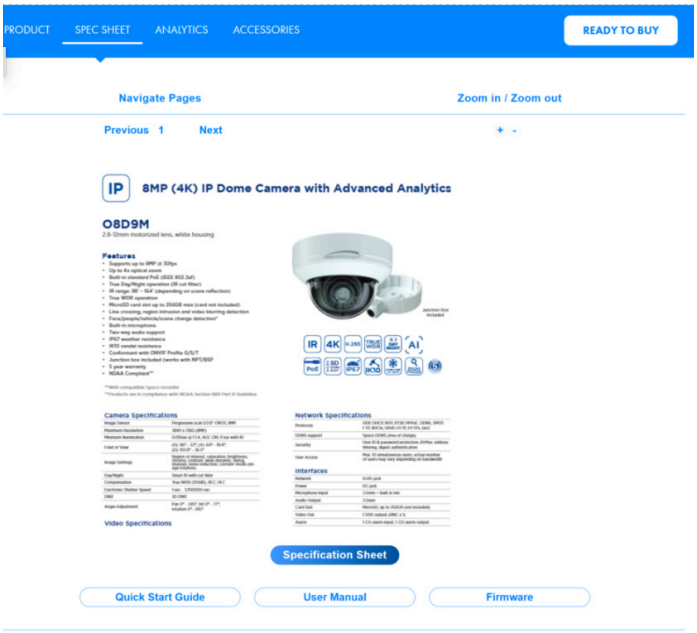


IP Cameras, DVR, NVR

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.

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

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.

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?

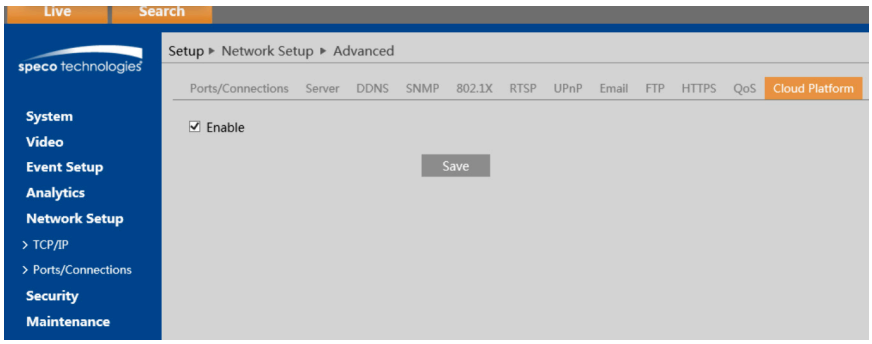
According the AWS data privacy web site: "AWS's alignment with ISO 27018 has been validated by an independent third party assessor. ISO 27018 is the first International code of practice that focuses on protection of personal data in the cloud. It is based on ISO information security standard 27002 and 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).



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.

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.

- SSL Encryption and Authentication for the browser to the controller
- HTTPS - Hypertext Transfer Protocol Secure
- AES 256 Advanced Encryption Standard – data packets Users, Logs, Systems settings
- SSH Authentication and Encryption between the server and the expansion hardware “clients”. The system administrator has the option to upload a private / corporate key.
- 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.

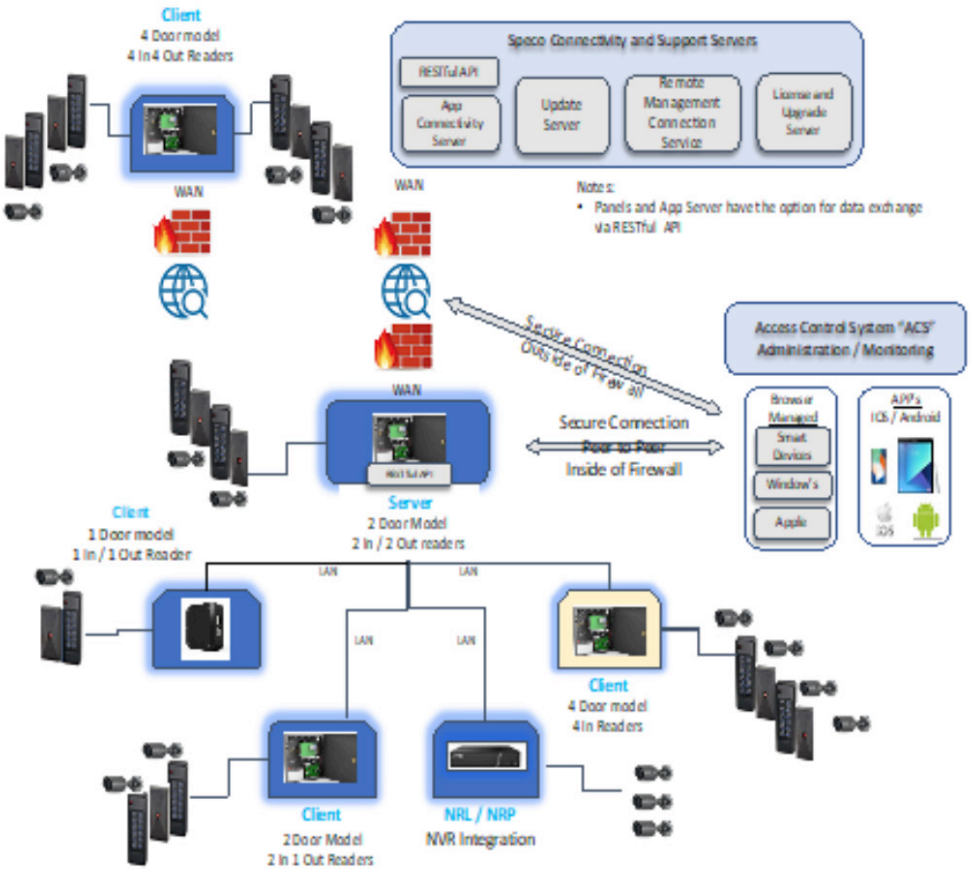
To ensure our systems are secure we perform and utilize a variety of services to test the product for Cyber Security (PEN Testing). As a security provider, we take network security seriously and will provide periodic security updates as required.

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

Encryption Standards and Protocol

Domain Name	Description & 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



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.

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."

Periodic Testing

- 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.