OpenEye® | The Cloud Video Platform

WEB SERVICES SECURITY HARDENING AND BEST PRACTICES

Contents

INTRODUCTION

Security is a top priority for companies doing business in the cloud. As the number of cloud connected devices continues to grow, so does the risk of data breaches and the potential for unwanted access to vital information. In order to mitigate these risks, organizations need a video surveillance platform that leverages the latest in network security, pro-actively protecting against people or programs that might cause harm.

OpenEye Web Services (OWS) is a scalable and highly-secure cloud managed video surveillance solution that simplifies operations and management by moving these functions to the cloud. It is important to identify and mitigate security issues that can occur as a result of installation or operation of the OWS platform. This guide provides recommendations for secure installation, configuration and operation of the platform to ensure it is secured against all attack vectors.

SYSTEM COMPONENTS OVERVIEW

There are several components that should be considered when planning installation and configuration of your security solution to ensure optimal protection.

PHYSICAL ENVIRONMENT

The physical security of your system is just as important as the cyber security of your system. Make sure to take this into consideration when planning where you will place your recorder. This should begin early in the design process as it may dictate where your power is installed and network cables are run.

NETWORK ENVIRONMENT

The OWS platform is designed to work seamlessly with most network environments, but precautions should still be taken to ensure the network is properly secured.

Follow the recommendations in this guide and any guide available from IT equipment vendors to ensure optimal security.

RECORDER

As the hub of your surveillance solution it is critical to ensure the recorder is secure. The recorder is comprised of multiple sub components, such as the operating system and recording software, which must be addressed independently to ensure its security.

REMOTE CLIENTS

Remote Clients are the primary method for users to interface with their surveillance system. It is important that these remote connections are secure and that the systems they are running on are also secure.

CLOUD

Cloud managed services provide a great amount of utility and convenience for both users and administrators of video surveillance systems alike. But proper care must be taken to protect users accounts, credentials, and lock down remote access.

STANDARD PROTECTION STEPS

There are a number of standard steps that can be taken to ensure protection against the most common attack vectors with little investment of time and effort. It is highly recommended that ALL of these steps be taken to ensure integrity of the platform.

PHYSICAL SECURITY

Any networked device is only as secure as its physical environment. Anyone with physical access and enough time can compromise almost any device, so it is important to ensure the recorder is only accessible to authorized individuals.

Keep the Recorder in a Secure Location

- The recorder should be secured in a locked room which restricts access to the recorder to only those users who need access.
- If a secure room is not available, consider a locking cabinet or enclosure.
  CAUTION: When using a cabinet or enclosure ensure proper ventilation exists to prevent overheating.

Restrict Use of Removable Media

- Malware can often spread between systems via removable media such as USB flash drives.
- For optimal protection, use WS to back up video clips or apply updates from the cloud. Video clips can be safely shared or downloaded and copied to removable media once they have been uploaded to Web Services.
- If removable media must be used, consider dedicated media that is only used for recorder file or video transfer, and format the media after each use.

NETWORK SECURITY

Most modern cyberattacks focus on the theft of either information or device resources. Aside from physical access, the network is the only way for anything to enter or leave the local system, so proper network configuration is critical. Exact configuration steps for routers and switches vary widely between devices, so refer to any available security guide from the vendor, as well as device documentation, for exact steps on these recommendations.

Secure the Network Gateway

- The gateway device (usually a router or modem that provides access to the Internet) has a firewall that protects against cyberattacks. Verify that the firewall is on, and that exceptions exist to allow outbound traffic on the ports used by WS enabled recorders (80 & 443 by default).
- Change the password of the gateway device. Most modems and routers have a widely published or easily guessed default password. Even if remote configuration of the gateway device is disabled, the password should be changed to help ensure protection.
- Audit the open inbound ports on your gateways firewall. OWS includes networking features which eliminate the need to open inbound ports on your firewall to enable remote access.

Isolate Your Camera Network

- Install cameras on an isolated network Exposing cameras to the Internet or any devices beyond the recorder adds risk and should be avoided whenever possible
- Connect cameras either to a PoE switch connected to the Camera port on the recorder or directly to the recorder's internal PoE ports (available on PoE integrated models).
- The Recording software includes a Camera Link feature to allow direct access to the camera's web interface through a proxied tunnel, in the case where advanced configuration is needed, eliminating the need for unnecessary exposure.

Audit All Devices on Your Network

Every device on a network is a potential security risk if improperly configured. Ensure default passwords have been changed on all devices on your network, firmware and software are up to date, and anti-virus software is installed where applicable.

CAMERAS

Cameras are configured in a secure manner as shipped from the factory. Do not enable features networking features such as xxx unless you know what you are doing or have s specific need for them.

Change your Default Password

- One of the simplest ways to reduce vulnerability of a camera is to change the password of the default admin account.
- Passwords of at least 12 characters including numbers and both lower and upper-case letters are recommended.
- Avoid the use of real words or names in the password.

Select a Secure Camera

Ask the camera vendor for their security policy and recommendations, avoid vendors who do not conduct security audits against their cameras or provide guidelines on secure configuration.

Protect Against Physical Tampering

Physical tampering with a camera is the easiest way to compromise it. Consider using vandal resistant cameras where applicable and when possible mount cameras so they are out of reach without the aid of a ladder.

Keep Firmware Up To Date

An important part of preventing cyberattacks is keeping firmware updated to ensure the latest security patches are applied.

RECORDER

The recorder is designed to provide a secure recording environment out of the box, but there are a few steps that can be taken to further ensure security.

SERVER SOFTWARE

Change Your Default Password

- One of the simplest ways to reduce vulnerability of a recorder is to change the password of the default admin account.
- Passwords of at least 12 characters including numbers and both lower and upper-case letters are recommended.
- Avoid the use of real words or names in the password.

Avoid Local User Accounts

- Adding user accounts to local recorders increased the probability of orphaned or outdated user accounts remain on systems and potentially compromising them
- User account management via OWS is recommended as it allows for a single point of control for multiple recorders and easy configuration at a platform level.

Keep Software Up To Date

- An important part of preventing cyberattacks is keeping software updated to ensure the latest security patches are applied, the recording software is no exception.
- Software updates are digitally signed and can easily be installed from a secure cloud server from within the setup menu.

OPERATING SYSTEM

The recording software is available on both Linux and Windows based operating systems. Linux-based recorders are designed to run the operating system silently with no direct user interaction. Windows recorders are designed with flexibility in mind, giving installers several options during initial configuration to ensure platform security and compatibility within their existing IT infrastructure.

Change The Windows Password

The default Administrative password is static, so changing it to a secure custom password is strongly recommended.

1. To change the password, do the following: **Click Start > Control Panel > User Accounts**
2. Select **Manage another account**
3. Enter the **NVRAdmin default password** (found in the software manual)
4. Click on the **NVRAdmin account**
5. Click **Change the Password**
6. Enter the current password, the new (secure) password, then click **Change password**

   CAUTION: The OS administrative account password cannot be retrieved; if lost the only way to regain access is to run the factory recovery media, which will reset all settings to default (video is preserved).

Turn On Windows Updates

Enable Windows Updates for critical security updates to ensure operating system vulnerabilities are quickly patched.

To enable, click **Start > Control Panel > Windows Update > Change Settings** and enable **Install updates automatically.**

NOTE: It is recommended to set updates to install outside of critical operating hours for the site as some require a restart, which will result in several minutes of down-time [no video recording].

Install Anti-Virus Software

- Installing anti-virus software is an important part of mitigating security vulnerabilities. In addition to preventing infections on the recorder, anti-virus software also offers quick, automated mitigation to many security threats.
- Windows Defender and solutions from Kaspersky have been determined to work on recorders with no custom configuration.
- If the anti-virus solution includes a firewall, be sure to add exceptions for the Apex services and ports.
- If the anti-virus solution includes active network monitoring, be sure to filter out the recording software traffic to prevent video data transmission problems resulting from routing through anti-virus software.

REMOTE CLIENTS

Avoid Untrusted Networks

When connecting to the recorder outside of the local network, be aware that not all networks are secure and it is usually not possible to know if a public network has been compromised.

Connect Through Web Services

Use OWS whenever connection to the recorder from outside the local network is necessary to ensure a secure connection.

Use Only Trusted Devices

Client systems that are infected with malware can have unpredictable results. Ensure all devices that connect to the recorder are running Antivirus software, updated OS environment and follow established security practices.

CLOUD

Use Multi-Factor Authentication

Turn multi-factor authentication on in OWS for all users for an additional layer of protection

Create A User Account For Each User

Avoid sharing accounts between multiple users as this makes it difficult to restrict access to one of the users should the need arise.

Manage User Access with Groups

Set up user groups to manage your users by job description and level of access. Instead of setting up every user individually, user groups will not only save you time during initial setup and when making changes but will also improve security by ensuring that a single individual doesn’t get left out of updates or changes.

Manage Remote Client Access

User access to remote clients should be restricted by need and location. Access to clients is managed in User Groups and can be restricted both by client type and by IP range. This gives Administrators the flexibility to enforce policies such as preventing Users from accessing video using the mobile app or to prevent access to clients when a user is not on the corporate network.

ADVANCED PROTECTION STEPS

There are a variety of more complex steps that can provide additional layers of security. These steps focus on further protecting the network environment and may be difficult to configure, so consulting an experienced IT professional is recommended.

PHYSICAL SECURITY

Keep The Recorder In An Access Controlled Location

Physical keys can be copied and do not leave a complete audit trail of who used them. An access controlled door provides a clear audit trail of what users’ card accessed a door.

NETWORK SECURITY

VLANs

- Consider configuring a VLAN with network access restricted to authorized users and hosts on the local network to prevent unauthorized access to recorders.
- If cameras cannot be installed on an isolated network, consider configuring a VLAN to isolate camera traffic from the rest of the network.

Proxy

- A network proxy exists as an additional layer of protection between the Internet and local network.
- Recorders running Apex Professional support remote access via proxy.
  To configure, go to **Setup > Network Configuration,** enter proxy settings and click **Save.**

VPN

- A VPN creates a secure connection between two points over the Internet, effectively creating a virtual extension of the local network.
- Use of a properly configured VPN is highly secure, but adds additional network overhead that may decrease performance for client connections.

Port Forwarding

- Port forwarding may be required in some network configurations in order to allow remote access to the Apex recorder.
- Port forwarding can reduce video latency in remote connections, but introduces greater risk as it exposes the recorder directly to the Internet.
- When using port forwarding, users should refrain from using the default ports whenever possible and switch to ports that are infrequently used and not IANA registered.

Vulnerability Scanner

- Network vulnerability scanners can be used to automate scanning of the network for any devices with known security vulnerabilities. This helps ensure any newly discovered vulnerability on the network can be quickly identified and mitigated. Commercial solutions are available from vendors such as Rapid7 or Tenable, and a free open-source scanner called OpenVAS is available, but requires an IT professional proficient in Linux administration for proper configuration.