FlySense® Network Installation Checklist & Best Practices

Introduction

The innovative FlySense® Vaping and Elevated Sound Detector is a device that can be installed in private areas where cameras and microphones are not allowed. The cloud-based system sends real-time alert notifications to designated officials. This provides situational awareness that enables officials to address potentially dangerous or harmful incidents swiftly and appropriately.

We know all-too-well that vaping in schools is a pervasive problem and we are committed to ensuring that FlySense® is an effective detection and deterrence tool. This will help ensure healthier and safer schools.

We focus on using advanced sensor and software technology to detect and deter potentially dangerous or harmful situations before they escalate. Thank you for using our solutions for a safer world – achieving one healthier and safer school and workplace at a time.

The purpose of this document is to implement the best practices to maximize the effectiveness of a successful FlySense® solution. By following these best practices, the FlySense® system will be an effective detection and deterrence tool.

Pre-Installation / Network Checklist

1. Get an estimate of the location dimensions. Each unit typically covers 10 ft by 10 ft.
2. Determine if the school has a DHCP server for dynamically assigning IP addresses. If not, Static IP addresses can be supported.
3. Network administrators should be aware of the requirement for multiple communication ports to be available for the devices and overall system to properly operate:
    - a. Device Communications (alert notifications): Port 11086 (outbound) to:
        - emq.sotertechnologies.com
    - b. Device Over-the-Air (OTA) Updates: Port 22 (outbound) to:
        - ota.sotertechnologies.com
    - c. General Internet Access: Ports 80 and 443 (outbound)
4. Confirm the firewall/content filter on the network is not blocking devices.

5. Confirmation of power source – i.e., PoE (802.3af) or AC/external. If external power, make sure you have secured the appropriate 24V @ 0.5A AC/DC transformers.

    a. Choose one power source for a single FlySense® device (1 unit).

        i. DO NOT use BOTH PoE and WiFi connectivity for a single FlySense® device.

    b. For FlySense® devices using WiFi: We offer AC/DC transformers on our website at: https://www.sotertechnologies.com/product-page/ac-power-adapters-for-flysense

6. Record the MAC address **AND** serial number of each device prior to mounting. Record which MAC is going into which location

    a. Register your organization into the FlySense® portal at https://sense.sotertechnologies.com.

    b. Please use the serial number you recorded. After registering, you will be prompted to schedule an onboarding session at sotertechnologies.com/onboarding.

    c. You will then receive an email that will allow you to create a password (be sure to check Spam Folder too).

        i. **REQUIRED:** You will receive an email to set-up your password and then you will need to register for your Onboarding session. Once your Onboarding session is completed, you will then be able to add your devices to the portal.

7. Stage the devices by plugging them in and making sure they complete the normal boot sequence.

8. Coordinate availability of Soter personnel for onboarding and installation prep call with the appropriate school or security partner resources.

Installation Checklist

1. Run the cables – Cat 6 cable preferred from network switch to FlySense® device.

2. Installation should be scheduled when school is not in session.

3. Mount each device (use the 'Cut Out Template' provided with the device User Guide), plug in power, confirm the device completes the normal boot sequence (refer to the device User Guide for details on LED sequence).

Best Practices

Number of Devices and Coverage

In general, each FS device will cover a 10' x 10' area for a bathroom with 9' ceilings. In large school bathrooms (3+ stalls) - we recommend placing the devices in the middle of the stalls to cover the 10' x 10' area – **NOTE**: please be mindful of the airflow within the bathroom as vents and open doors/windows can cause the vape to blow away from the sensor(s).

To maximize the effectiveness of the tool as a deterrent, FlySense® detectors should be deployed throughout the school – with the right response system process in place. A couple of isolated units – one in a boy's bathroom and one in a girl's bathroom – are not going to provide a good indication of the effectiveness of the system and are not going to constitute an effective deterrent.

Preparing for Installation - Organization and Device Registration

Per the Installation and User Guide, the installation and activation process begins using the cloud-based FlySense® portal to register your organization and devices at sense.sotertechnologies.com. This requires information found on the manufacturing label affixed to the bottom plate of each device.

Before physically installing/mounting the devices:

- Take a picture of each device's manufacturing label (MAC address **AND** serial number) & note the location it will be installed. Record which MAC is going into which location.
- Register your organization; you will need to use a valid device serial number to do this.

REQUIRED: You will receive an email to set-up your password and then you will need to register for your Onboarding session. Once your Onboarding session is completed, you will then be able to add your devices to the portal.

- Register your devices; you will need each device's MAC address **AND** serial number for this. Record which MAC is going into which location.
- Stage the devices by plugging them in and making sure they complete the normal boot sequence and reflect 'Online' status on the Devices tab of the portal. **NOTE:** please reference 'Communications' below prior to applying power to the devices.

Communications - Open Outbound Ports and Potential Whitelisting

Network administrators should be aware of the requirement for multiple communication ports to be available for the devices and overall system to properly operate. You must configure a whitelist if your security policy denies access to most or all external IP addresses and websites.

- Device Communications (alert notifications): Port 11086 (outbound) to IP addresses associated with:
    - emq.sotertechnologies.com
- Device Over-the-Air (OTA) Updates: Port 22 (outbound) to IP address associated with:
    - ota.sotertechnologies.com
- General Internet Access: Ports 80 and 443 (outbound)

The fact that these ports are open for outbound communications only – initiated only by the FlySense® devices behind the firewall and never initiated from outside the firewall –means that the security risk associated with the FlySense® system is absolutely minimized.

Communications - Network Switches and IP Addressing

If you are using a POE capable switch, please ensure that each switch port connected to a FS device is configured or hard-set to 100 Mbps full duplex communications.

For IP addressing, you have a choice of assigning dynamic (via DHCP) or static IP addresses. To avoid dependency on DHCP, as well as reduce the risk of an address conflict, we recommend reserving static IP addresses for devices on your network – similar to IP security camera set-up. A good approach is to put all FS devices on a separate VLAN using static IP addresses.

Mounting Devices

These devices are typically ceiling mounted in school bathrooms and locker rooms. In each bathroom, the device(s) should be located directly over the stalls.

Room ventilation is a key factor. Detection is going to be degraded when vaping is done close to open windows or active ventilation such as exhaust fans. An HVAC system could impact the ability to properly detect vaping. If there is consistent air flow in a particular direction, locate the device in the path of the air

flow. Devices should be installed when students are not in school. See 'Tips Related to Potential Tampering' below for additional info.

Alert Notifications

The FlySense® system sends alert notifications in the form of SMS text messages and/or email. SMS text messages consistently provide the best performance in terms of notification latency. Be sure that the subscriber device associated with SMS alert notifications is indeed capable of receiving SMS text messages – i.e., a device with a carrier data plan and LTE wide-area radio. Some customers prefer email because the designated responders are using Wi-Fi tablets and cannot receive SMS text messages without a carrier data plan. However, there can be unpredictable latency associated with email notifications – for reasons beyond Soter's control.

Alert Notifications - Please Be Aware…

- A device will not send any incident notifications if there are no subscribers associated with that specific device.
- After a vaping or elevated sound incident and corresponding alert notification occurs, you will not receive another alert notification for the same incident category – vaping or sound – for a minimum of ten (10) minutes for that specific device location.

Need for Alert Monitoring and Response Processes

This is one of the most important considerations for overall vaping detection and deterrence. Prevention starts with detection and situational awareness. When an alert notification is received, it is imperative that a school official be onsite in less than a minute to confirm the alert and effectively address the situation.

Schools should have a well-defined process that includes team members assigned to receive alert notifications and follow up on them – for specific locations during specific times of day. This is highly recommended even if schools have cameras installed outside bathrooms that allow school officials to use the alert notification timestamp to 'go to the video' and see who entered and left the bathroom around the time of the reported incident.

For larger schools with many bathrooms, you may want to consider having multiple subscribers with multiple windows to receive alerts during different times of the day.

Examples:

- Scenario 1: A male health science teacher is one of the individuals assigned to cover 2 boys bathrooms located on the 2nd floor west wing between 9:00-10:00am and then again from 1:00-3:00pm

- Scenario 2: A female assistant principal is one of the individuals assigned to cover 3 girls bathrooms on the 1st floor between 7:00-9:00am and then again from 12:00-2:00pm.

- Scenario 3: it is recommended that subscriber alert notifications be enabled during school hours (i.e. 7:00am-4:00pm) and during extracurricular activities (i.e. 6:00-8:00pm)

Use of Web Portal for Confirming and Classifying Incidents

The FlySense® web portal provides the ability to classify incidents. This is extremely valuable for reporting and analytics.

The web portal, accessible on any device with a web browser, ensures that incidents are classified accurately in a timely and efficient manner. The user will be able to:

- Confirm receipt of alert notification and ability to respond/investigate right away.

- Confirm a true vaping or elevated sound incident and add comments.

An incident should not be classified as a false positive unless it is truly confirmed to be a false positive.

Refer to the Installation and User Guide for more information on classifying incident alerts.

Tips Related to Potential Tampering by Students

- Install units when students are not in school. Make sure units are registered on the network and active before students return to school.

- The actual FlySense® unit does not have any identifying logo on an exposed surface because it is meant to be discrete.

- The basic warranty does not cover tampering before or after the product is installed. 1-year limited hardware warranty covers defects in workmanship and materials. 3-year and 5-year extended service options available at time of purchase.

FlySense® Liability and Performance Disclaimer

FlySense® is a multi-sensor device that detects:

- Elevated sound or noise that may suggest bullying or fighting.
- Vaping signatures®, THC and cigarette smoke (note: the device does not differentiate chemical composition)

This is a quality engineered solution that has been extensively tested. However, there are detection limitations driven by external factors and countermeasures. More specifically…

- Vaping detection is likely to be impaired in the following circumstances:
- Vaping is done close to open windows or active ventilation.
- Individuals are taking countermeasures to avoid system detection – such measures include, but are not limited to:
    - exhaling vapor inside a jacket or coat;
    - exhaling vapor close to a toilet or urinal, and then flushing.
- There is a wall or high door located between the vaping source and the sensor device.
- Vaping detection will be degraded in the following circumstances:
    - If the sensor is mounted to a ceiling or ceiling tiles higher than 9 feet above the floor. As the ceiling height increases, the effectiveness of the detector will decrease.
    - If the vapor is being emitted from a horizontal radius distance of more than 5 feet from the sensor. As the distance from the sensor increases, the effectiveness of the detector will decrease.
- Soter Technologies is not responsible for any personal or property damage that results from:
    - Tampering with the sensor device before or after installation by a qualified professional.
    - Improperly installing the device that is not consistent with the product installation guide.
    - Using the device in any fashion that is not recommended by Soter or is not consistent with its intended use.

SOTER TECHNOLOGIES

If you have any questions or issues, please contact Soter Support at 1-877-363-8273 or support@sotertechnologies.com