Technology Overview

2024

This guide is designed to help you understand the technology behind **NextGrad** and outline the key steps we take when partnering with a school district. It covers:

1. District Approval Process
2. Installation Process
3. Continued Maintenance

We want to remain as transparent as possible to make sure any concerns you have are addressed. Our goal is to ensure a smooth integration with your district's network while maintaining strong security protocols and efficient communication.

1. District Approval Process

The district approval process helps ensure that **NextGrad** is compatible with your network and meets your security standards. Below are details to assist your network administrators in evaluating **NextGrad**:

Operating System

- **NextGrad** uses a custom **Linux image** built on **Ubuntu 22.04 LTS** called **VistarOS**.
    - The image was developed by *VistarMedia* (*vistarmedia.com*)
- This image only includes the **Cortex Media Player** and access to a secure terminal for initial setup and troubleshooting. This creates a sandboxed environment and offers **greatly improved security and privacy** compared to a kiosk running Windows, more details outlined below.
- **NextGrad** only communicates with the kiosk through **HTTPS** for secure data transmission (Media, online status, operational logs).

Serving Content

- Content is pushed from **Cortex Fleet** (Fleet), our Content Management System (CMS) built by *VistarMedia*.
- All data transferred between Fleet and the kiosks is encrypted via **HTTPS**.
- **No personal information** is collected nor transferred, only school-approved content (e.g., imagery and videos).

Information Gathered and Locally Stored Content

- **NextGrad** does not collect any data on students, staff, or visitors. There are no cameras nor data collection processes of any kind.
- Each kiosk has a **local cache** that is used to store recent media it has received. If the network goes down, cached content will continue playing until the connection is restored.
- The only information and data stored in this cache is the following:
    - Media content
    - The Cortex Media Player application
    - Kiosk location
    - Operational status (e.g. up/downtime)
    - Operational logs (e.g. crash reports and error logging)

Network Requirements

Network Connection Information

- Our kiosks support both **wired** and **wireless connections** (WPA2-Personal, WPA2-Enterprise, Hidden Networks, and EAP-TLS).
- There are several types of networks that our kiosks are capable of connecting to, please look below and see which network description best matches your needs.
    - **Hidden Network:** A network where the SSID is not broadcasted at all, but still allows devices to connect given they have the correct credentials.
    - **Personal Network (WPA2)**: A standard network connection, all that's needed to connect is the SSID of the network and the password.
    - **Enterprise Network (WPA2 802.1x):** A network requiring a username and password for a connection to be established.
    - **EAP-TLS:** A network without credentials. The kiosk and the network's CA server have asymmetrically encrypted certificates to verify one another.
        - **NextGrad** kiosks are incapable of reading "**.p7b**" formatted certificates. If possible, please use "**.pem**", "**.cer**", and "**.key**" formats for certificates.

Network Configurations and Whitelisting

If your network involves **DHCP**, we recommend setting up our kiosk with a **static IP within your reserved IP range** and/or **registering the kiosk's MAC address**. In addition to this, we want to ensure the following site origins are whitelisted and ports are opened so that there is no issue when serving content.

These are the site origins our kiosks communicate with:

- **api.vistarmedia.com**
- **fleet.cortexpowered.com**
- **stem.cortexpowered.com**

These are the ports used by **NextGrad** kiosks:

- **Port 443**
    - HTTPS outbound
- **Port 80**
    - HTTP outbound

Note: *No inbound ports are required.* Ports 80 and 443 must be open for outbound traffic to facilitate secure communications and remote management.

Access and Security

- The **Linux image** has no graphical user interface (GUI), and the terminal access is password-protected.
- If terminal access is needed for network configuration (e.g., WiFi setup), your **IT team will be provided access with the username and password** in order to **configure WiFi** according to their specifications during installation and for **followup maintenance**.
- **Subnet masking** can be manually configured by an IT staff member if desired with a **sudo user account**, but it is not a service that we at **NextGrad** directly support.
- All traffic, including managed content, logs, and current operational status, is sent via **HTTPS** on ports **80** and **443**. There is absolutely no personal information of students, staff, or any persons collected nor transferred.
- **USB information** is **not immediately read when plugged into** the kiosk, which is a default behavior of Linux. This means **no one can plug in a USB and tamper with the kiosk**.
- **All HID** (Human Interface Device, like a keyboard or mouse) would only be useful for accessing the secure terminal, which **will be inaccessible without the correct credentials**.
    - Additionally, well known keystrokes for Windows, Mac, and Linux will not do anything.
        - CTRL + ALT + DEL/HOME/END/ Etc.
        - CTRL + SHIFT + ESC/TAB/~
        - WIN + R/L/ENTER/DEL/ Etc.
        - ALT + F4/TAB
            - ***Note***: ALT + F4 does close the Cortex Media Player but the system software auto launches it immediately after closing/crashing to mitigate this.

2. Installation

Pre-Installation Checklist:

A. Location Selection

- Choose **2-3 high-traffic areas** for the kiosks (e.g., entryways, hallways, common areas). We will help finalize the locations during installation.
- Each location must be within **3 feet of a power outlet**.
- We avoid placing kiosks in areas like libraries, offices, or lunchrooms.
- The location must be within reach of either an **ethernet connection** or **WiFi access point**.

B. Network Information

- Please provide all network details for any WiFi connections.
    - We ask that the network password be provided beforehand if possible, to expedite installation.
- The kiosks are **incapable** of connecting to networks with **captive portals**
    - e.g. login portal or authentication portal of some kind.
- Make sure the network is configured for our needs.
    - Register the **MAC address** of the device on the network.
    - Ensure our necessary **site origins** are whitelisted.
    - Ensure our used **ports** are open.

C. IT Contact

- It is important to have **IT staff** present during installation to:
    - Enter any required network credentials, if needed.
    - Resolve any installation issues that may come up.
    - Familiarize themselves with the kiosk.

Installation Process

The installation is quick and simple, typically taking about **30 minutes** per kiosk.

1. Evaluate your pre-selected locations and choose the best spot.
    a. We want to ensure the location has **stable internet connectivity** and is in a **high traffic area**, while also being out of the way enough to **avoid tampering** or **accidental damage** to the kiosk.
2. Bring the kiosk inside, attach the base, and plug it in.
3. Connect the kiosk to the internet, ensuring it is properly integrated into the network.

3. Continued Maintenance

Ongoing maintenance is minimal and handled primarily by **NextGrad**.

Common Maintenance Tasks:

- **Reconnecting to the internet** or **changing content layouts** are simple fixes that your team can handle if necessary.
- If the kiosk malfunctions or needs replacing, a **NextGrad representative** will visit your school to resolve the issue at **no cost** to you.

NextGrad Commitment:

- All hardware is insured and maintained by **NextGrad**.
- No charges will ever be incurred by the school or district for broken or malfunctioning equipment.

Common Questions

1. How secure is the system?

- The custom Linux image provides a sandboxed, secure environment, and all data is transmitted via encrypted HTTPS.
- The password protected terminal is the only interface capable of allowing changes or additions to the software and behavior of the kiosk.

2. What kind of data do the kiosks collect?

- None. **NextGrad** kiosks do not track users, monitor internet activity, or collect any personal information. The only information tracked relates to kiosk uptime and the content being displayed.

3. What if we require specific network settings like subnet masking?

- We can accommodate custom network configurations. Subnet masking and other settings can be configured by your IT team during installation.

4. What if something goes wrong with the kiosk?

- Any malfunctioning or broken kiosks will be fixed or replaced by **NextGrad** at no cost to the district.
- Please reach out to us if there are issues with the kiosk either not displaying content or is malfunctioning for any reason and we will work to get it fixed.

If you have any further questions, please don't hesitate to contact us.

We look forward to partnering with you!