NextGrad

The high school opportunity network

Technology Documentation

2025

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

1. Specifications for Approval
    - Detailed information about our kiosks and the software they run.
2. Installation Process
    - Outline of the process for installing a new kiosk and important details.
3. Continued Maintenance
    - Quick overview of maintenance after install and common questions.

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. Specifications for Approval

This section covers all the specifications of our kiosks and their software to help 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 (NextGradOS)

- **NextGrad** uses a fully custom **Linux distribution** built on **Ubuntu 24.04 LTS**. It was developed by **NextGrad** to maintain full system control and ensure a high level of safety and security. *Don't hesitate to ask about it! (see end of document)*
- **NextGradOS** is very minimal. The environment it includes has the ***Cortex Media Player*** application (built by *VistarMedia* (*vistarmedia.com*)), the ***TeamViewer Tensor IoT*** application (inactive unless approved for use, more on this in a later section), and a **secure terminal** (tty) for initial setup and troubleshooting.

NextGradOS creates a sandboxed environment and offers **greatly improved security, privacy, and even power usage**, compared to a kiosk running Windows for example. All of this is discussed in greater detail in the *Access and Security* section below.

Serving Content

- Content is pushed from **Cortex Fleet** (Fleet), our Content Management System (CMS) built and maintained by *VistarMedia* (*vistarmedia.com*).
- 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 system logs and recent media content it has received. If the network goes down, cached content will continue playing until the connection is restored, for a seamless viewing experience.
- The **only** data stored in this cache is the following:
    - Media content
    - Operational status (e.g. up/downtime)
    - Operational system logs (e.g. crash reports and error logging)

Network Requirements

Network Connection Information

Our kiosks support both **wired** and **wireless connections** on all widely used types of networks running on *both* 2.4GHz and 5GHz channels.

- **Open Networks** (No Security): An open network connection, typically a guest network or for use with an authentication portal.
    - **NextGrad** kiosks **CANNOT interface with captive portals**, so we ask that the kiosk's MAC address be registered to bypass it or select a different network for us to use.
- **Personal Networks** (WPA2 or WPA3 (802.11)): A standard network connection to an SSID with a password.
- **Enterprise Networks** (WPA2 or WPA3 (802.1x)): A network connection to an SSID with *both* a username and password.
- **Enterprise EAP-TLS Networks** (WPA2 or WPA3 (802.1x)): A network connection to an SSID without standard credentials. The kiosk and the network's CA server have asymmetrically encrypted certificates to verify one another.
    - We ask that you provide us with "**.pem**", "**.crt**", "**.cer**", or "**.p7b**" formats for certificates and "**.key**" or "**.pem**" formats for keys.
    - **NextGrad** kiosks CANNOT read "**.p12**" and "**.pfx**" formatted certificates.

Required Network Configurations and Whitelisting

We **require** the following site origins (with all subdomains depending on network setup) to be whitelisted to avoid issues with serving content and remote management.

***Note**: If needed, we can provide you with a list of all the specific subdomains accessed by our kiosks if using the subdomain wildcard in the whitelisting is a concern.*

- ***.vistarmedia.com**
    - Contacted for requesting the ads targeted at the specific kiosk.
    - This is *VistarMedia*'s content host server where content is stored long-term.
- ***.cortexpowered.com**
    - Contacted for reporting uptime and logs.
    - This is *VistarMedia*'s content management service we use for monitoring kiosks.
- ***.teamviewer.com**
    - Contacted for remote connections via *TeamViewer IoT*. More on this in the next section.

Lastly, it isn't strictly necessary, but if your network utilizes **DHCP**, you are welcome to assign our kiosk to a **static IP within your reserved IP range** and/or **register the kiosk's MAC address**. This might help with whitelisting, especially if you whitelist by device rather than across the whole network, as well as assist in tackling any connection issues that may arise.

Access and Security

TeamViewer Tensor IoT

Check out TeamViewer's security guarantee on their website:

➔ https://www.teamviewer.com/en-us/products/tensor/security/

We use *TeamViewer Tensor (IoT)* for remote management if there are software updates that can be applied remotely, or if we have an issue arise on a screen and need remote access to check on kiosk system health. **TeamViewer is DISABLED by default unless explicitly allowed by your network security; TeamViewer has to be manually activated.**

- The kiosk software is configured to block ALL remote access unless attempted through our **NextGrad** admin account on *TeamViewer* for increased security.
- The connection is established through mutual certificate exchanges to ensure that **only authorized NextGrad staff can access the kiosks**.

General Information

- **NextGradOS** has no desktop environment or graphical user interface of any kind.
- Your **IT team** will be provided access to a secure terminal with the **guest username and password** in order to **configure the network** according to their specifications during installation and for any necessary followup maintenance.
    - The **guest account** has limited permissions in order to maintain a high level of security. The admin account is for authorized **NextGrad** use only.
- All kiosk traffic, managed content, remote connections, logs, and current operational status is sent via **HTTPS**. There is also an on-device firewall (UFW) that is configured to deny ***all*** incoming traffic by default and only allows outbound traffic on specific ports (standard HTTPS port 443).
- **USB information** is **never read or executed** on the kiosk, thus **no one can plug in a USB to tamper with a kiosk**. The kiosks have additional kernel hardening to protect against kill switches and auto executing USB drives.
- **All HIDs** (Human Interface Device, like a keyboard or mouse) can only be used for entering the secure terminal, which **will be inaccessible without the credentials**.
    - Additionally, well known keystrokes 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 protection is in place to launch it immediately after closing 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.
    - We typically avoid placing kiosks in areas such as libraries or offices since they don't have as much foot traffic.
    - We also recommend avoiding lunchrooms as there is a higher possibility of damage being inflicted on the kiosk or unplugging.
- Each location must be within **3 feet of a power outlet**.
    - We recommend using an outlet lock (provided by **NextGrad**) to secure the cable. This mitigates students unplugging the device.
- The kiosk must be close to either an **ethernet outlet** or **WiFi access point**.

B. Network Information

- Make sure your network is configured for our needs.
    - Ensure our necessary **site origins** are whitelisted.
    - Register the **MAC address** of the kiosk on the network, if needed.
- Please provide **all network details** we may need for any **WiFi** connections. (or ensure an IT staff member will be available to enter credentials for us)

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 **20-30 minutes** per kiosk.

1. Evaluate your pre-selected locations and choose the best spot.
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 local network and connected to our backend services.

3. Continued Maintenance

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

Common Maintenance Tasks:

- **Updating network information** in the event the network or its credentials change. This is a simple fix 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 the school or district.

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.

Frequently Asked Questions

1. How secure is the system?

- **NextGradOS** provides a heavily locked down, kernel hardened, sandboxed, and secure environment. It has been heavily secured and optimized for our use.
- All data is transmitted via encrypted HTTPS.
- The password protected secure terminal is the only method of configuring the behavior of the kiosk. Therefore, admin privileges are held only by **NextGrad**.

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 info kept relates to kiosk uptime and content.

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

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

4. What if something goes wrong with the kiosk?

- Any malfunctioning kiosks will be fixed or replaced by **NextGrad**.
- 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.

We look forward to partnering with you!

Camron Wilson is our *Director of IT* and developer of **NextGradOS**. He can help you with any and all further questions you may have, so please don't hesitate to reach out!

Email:

Camron@NextGrad.com

Alternatively, you can submit a form request with extra information here:

https://www.nextgrad.com/contact/