Streamline online classes during COVID-19 with Hexnode MDM

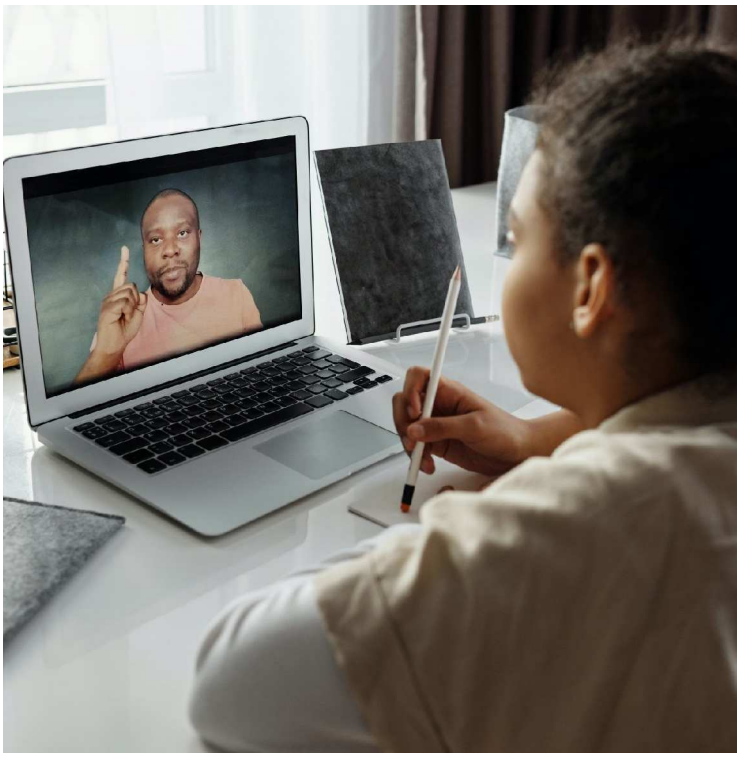
As the COVID-19 pandemic has affected 200+ countries, Schools and universities worldwide are being shut down indefinitely. Students need education and months of lockdown can impact the curriculum, there is only one way to utilize this time effectively, remote learning, or online classes.

But opting for remote learning is by no means a walk in the park, there are a lot of complications to be dealt with ranging from class timings to secure Internet access. Then comes the serious issue with the devices that students and teachers are going to use during these classes. How do you deploy so many devices in such a short span of time? How are you going to push the necessary content to these devices without making a hassle? How do you monitor the activity levels of each student during school timings? Another important decision is deciding which device you would allow the students and teachers to take home for online remote learning purposes. Would it be institution-issued devices or personal devices?

Finding the right solution to manage all your endpoints at a time of crisis like this, is nearly impossible.

After deciding what devices, the staff, and students should take home, then comes the herculean task of managing these devices. Using a mobile device management solution like Hexnode MDM is the right way to go in a scenario like this. Why? Let's see.

Institution issued devices



The first case is when the institution provides devices to the staff and students for attending the online classes. In most cases iPads, Android Tablets and Windows surface tablets or laptops are the preferred devices due to its power and flexibility as an educational tool. Since these devices are already provided to the students and staff, we can assume that they come pre-enrolled with device management software like Hexnode MDM. Out of the box. If that isn't the case, onboarding can be done pretty easily.

Automate device provisioning with volume deployment programs

For Apple devices, configuring the MDM server with the Apple Device Enrollment Program portal, devices can be automatically enrolled in the MDM solution during the initial setup. The preconfigured settings can be controlled by teachers/admin from a remote location. The device compliance can also be maintained wirelessly. Essentially, the management of devices over the air is made possible with the help of DEP.
For more help regarding DEP enrollment with Hexnode, click here.
The obvious alternative for Android regarding Apple's DEP enrollment would be Android Zero-Touch Enrollment. It is an onetime process for easy deployment of institution-owned devices. Similar to DEP it also provides an out-of-box experience to users where their device arrives enrolled and configured. A thing to keep in mind is, ZTE does not run on Samsung devices. Samsung Knox Mobile enrollment has to be used for enrolling those devices.
Are you still having trouble figuring out Android Zero-Touch Enrollment? Learn more here.
In the case of Windows devices, you can deploy them using Open enrollment methods such as through SMS and Email. For a more advanced form of enrollment, Active Directories can be used to deploy devices in a much more authenticated manner.

Configure acceptable use policies and security restrictions

Managing the devices which were given out to the staff and students is a challenge on its own. Some levels of advanced restriction have to be applied to these devices to ensure efficiency and productivity. As of now, Apple has announced that advanced levels restrictions may only be applied in supervised devices. These advanced-level restrictions include web- content filtering, which is basically whitelisting and blacklisting of websites on the targeted devices. Restrictions can also be placed on the Safari browser so that students don't waste their time surfing the internet. Other restrictions also include blocking explicit content on devices that are used by the students.
As far as Android devices are concerned, restrictions can be placed on any android device. Other than that, the restrictions provided for Android as well as Apple are quite similar.

Blacklist non-essential applications and distribute educational apps & content

App management is streamlined in Apple devices with the Volume Purchase Program. It enables schools to purchase apps in bulk and distribute them to users. With Apple VPP

and Hexnode MDM integration, the admin/teacher can send apps or content or apps to connected devices.
With VPP, you can also securely distribute custom-made in-house apps to the students. For example, if you have an in-house app for marking attendance for online remote learning classes and pushing announcements, then that app can be distributed among the students using VPP.
The teacher or the admin can deploy the mandatory apps and content that are required by the students through VPP and Hexnode. These can be done on the basis of the different course material and curriculum by employing device grouping functionality provided by Hexnode. Furthermore, utilize Hexode's App catalog feature to add any complementary apps that might be useful to the students during their online classes.
Didn't understand how VPP works? Learn more about it here.
For Android devices, all the necessary apps can be pushed to targeted devices by setting these apps as mandatory. This can be done by creating a custom policy in the Hexnode MDM console. Under this policy, you can list all the apps that would be necessary during remote learning. You can also create app groups and app catalogs. App groups can help to accumulate all the apps required for a certain group of students on the basis of subjects, for example.
Having trouble getting started with Android App management, let us get that fixed here!

Enforce kiosk lockdown to enable a fully-managed device experience

Kiosk lockdown feature has several uses in an online class situation. One of the most important of them being, conducting class tests. Single autonomous lockdown mode, which is available only on supervised devices with iOS 7.1+, can be leveraged here to conduct a test. In single app autonomous mode, the device only shows the particular app or page. The student cannot go beyond this and hence is perfect for tests. There are two more lockdown modes, single app lockdown which is available on devices with iOS 6+ and Multi app kiosk mode for a device with iOS 9.3 +.
Learn how to set up an iOS device lockdown here.
In the case of Android devices, by enrolling a device owner the admin or the teacher could push a Kiosk lockdown mode on to the device. Options like single app kiosk mode and multi-app kiosk mode are there for Android devices. The single app kiosk mode is ideal for conducting tests or evaluations of any kind.
Learn more about Android kiosk management, here.

Personal Devices

The second case is obviously the case of personal devices that the students and staff

can use. These devices may hail from a plethora of platforms including Android, iOS, Windows, iPadOS, macOS, etc. The easiest way of enrolling these devices is through open enrollment.

With Hexnode as your device manager, students using Android, iOS or macOS devices can enroll their personal devices with Email or SMS. This makes their personal device; a BYOD-ready device is less than two minutes.

Enable secure access to school networks without impacting student privacy

If the students are planning to use their own devices for remote learning, the teacher or the admin should make sure that the data they share is secure without compromising the student's privacy. Hexnode MDM can help you with that.

Deploy Android for Work profiles to isolate schoolwork and personal data

As an admin/teacher, the decision you should make here is whether you would like to control the device as a whole or create a work container for the online classes.
If you want to control the device as a whole, you can enroll it as the device owner. It gives you access to advanced restrictions and it would even provide you with Kiosk lockdown capabilities.
The other option is to enroll the device as a profile owner. This allows the creation of separate work container. In this case, only the work container section of the device would be managed and the personal section would be left unmanaged. This is more desirable in the case of a BYOD scenario regarding online classes because students would still be able to use their personal device whichever way they please when not attending classes.

Setup Managed open-ins to prevent workspace data from shared across personal apps

Hexnode MDM can help in controlling the flow of data between the personal and workspace in an iOS device by employing a business container. Though this sounds a bit corporate, it works well on school-issued devices too. It creates a discrete partition among the apps and content that is meant for school and personal apps and content. These BYOD management restrictions can be applied by creating custom policies on the MDM portal for different platforms and associating them with the target devices. You can select the time frame in which these restrictions need to be active, say you follow a school hour criterion.