

mojo



Mojo Enforce

Integration with Google for
Education Delivers Secure School
WiFi Authentication

Let's be honest; WiFi is arguably one of the most important components to modern digital learning initiatives like classroom flipping, blended and online learning tools, and expanding online testing efforts. But as WiFi's prevalence expands throughout all levels of primary and secondary education, challenges around device management and access control persist.

IT organizations everywhere face the unfortunate decision to sacrifice security, control and even performance to lessen complexity and increase ease of use. Management and maintenance of the systems used today to help control access can be complex, and the need for extra appliances, software and licenses complicates this approach further. **The underlying problem remains: there is no way for schools to ensure that only authorized devices connect to their WiFi network.**

Problems with Existing Wireless Authentication Methods in Schools

Most schools use either PSK (Pre-Shared Key) or 802.1x (with username and password) as the primary authentication method for WiFi networks, with PSK being most predominantly used.

The challenge with PSK is that because there is a single key that is shared amongst all the devices, it is very easy for students (and teachers, for that matter) to use the same key on their personal device and connect to the WiFi network.

With 802.1x, though each user has unique credentials, there is really no way to enforce students from using these credentials on their personal devices. Also, using 802.1x requires schools to install on-premise RADIUS servers and maintain a local user directory, making deployments more complex and incurring extra cost.

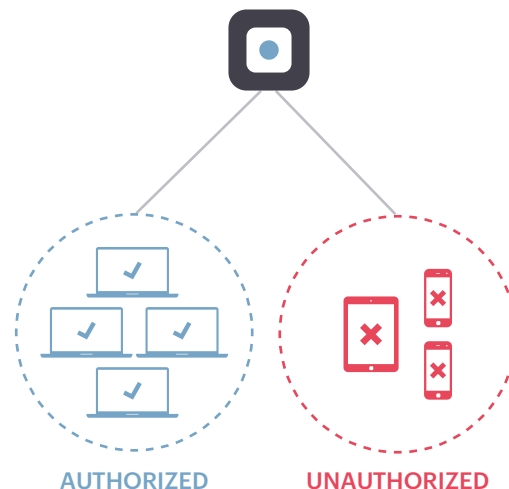
Though security is always top of mind when discussing unauthorized access, other issues can have an equally negative effect on the network.

Impacted Performance - The number one purpose of any K12 WiFi network is to support classroom activities. Too many devices attached to the network will consume more airtime and increase bandwidth consumption, effectively reducing the bandwidth available for student and teacher devices. This inevitably causes the network to slow down and hurts the digital learning experience.

Limited Visibility and Control -

Schools that invest in technologies that help them control application and content use on school-issued laptops do so for a variety of compliance and security reasons. But they have little to no knowledge of what unauthorized devices do and even less control. If a network policy allows access to a certain application or bandwidth allocation, it cannot distinguish between authorized and unauthorized devices.

IT Headache - The excess strain on the network can lead to unhappy users and in turn more support tickets, but when students and teachers inundate support with tickets concerning their unauthorized devices, this wastes precious IT resources and takes time away from new projects.



To solve the problem, Mojo has developed a new feature called Mojo Enforce that, with Google, takes advantage of the registered device list in the Google Cloud and ensure that only authorized devices connect to the network. Beyond this, Mojo Enforce can also ensure that appropriate network access policies (roles) are applied based on device OU membership defined in Google.

Google for Education

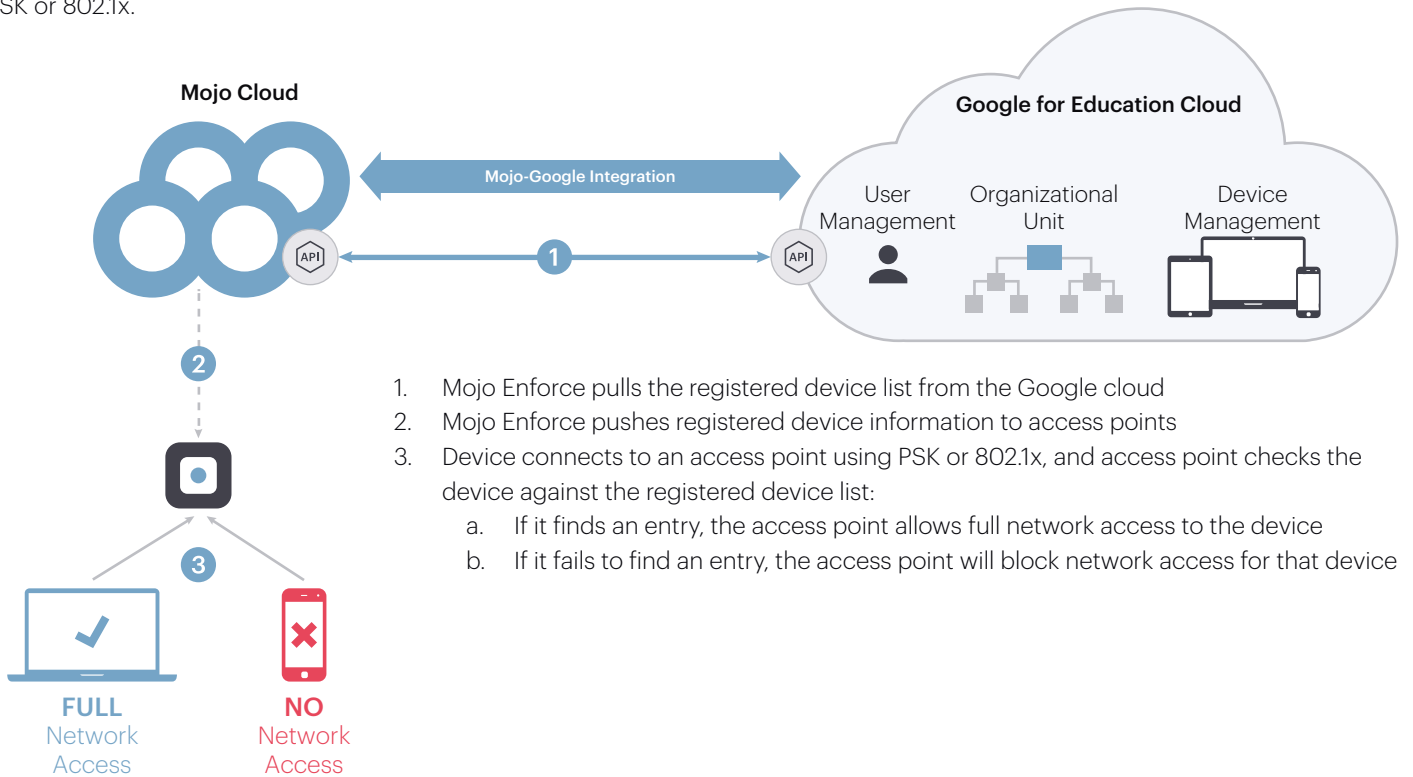
Google for Education is a collection of applications and services allowing students and teachers to engage anytime, anywhere and on any device. Google for Education is offered at no cost to schools along with 24x7 support and has been widely adopted within K-12 across the country and continues to grow. Google for Education broadly offers two class of services / applications to schools:

Collaboration tools include apps like Gmail, Classroom, Drive, Calendar, Vault, Docs, Sheets, Slides, Sites, and Hangouts. These allow teachers to effectively collaborate with students in and out of the classroom, keep classes organized and improve communication with students.

User & Device Management and Organization Units are core services offered as part of Google for Education allow admins to create organizational structure and control which settings and policies are applied to users and devices. User directory offers SSO for all Google applications, while device management allows admins to simplify deployment of chromebooks and remotely manage the student experience.

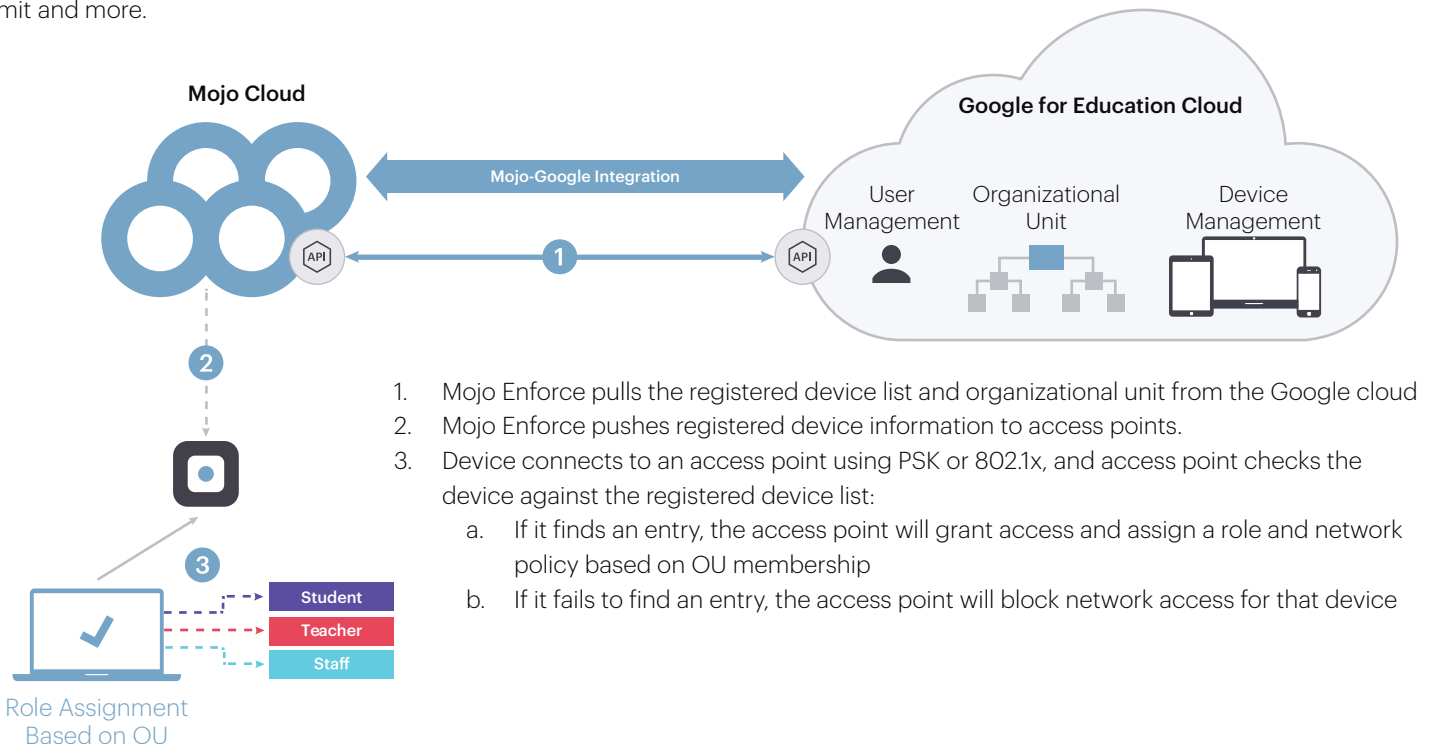
Allowing Only Registered Devices to Connect to the WiFi Network

Mojo Enforce makes use of the registered device list on the Google Cloud to validate the authentication session above and beyond PSK or 802.1x.



Assigning Network Access Policies / Roles based on OU Membership

In addition to enforcing access based on the registered device list, roles can be assigned to devices based on the organizational unit membership of the device defined in Google. Roles can control various settings like application access, firewall rules, QoS, bandwidth limit and more.



Benefits

Schools that have adopted Google for Education can very easily take advantage of Mojo Enforce.

- Absolutely no additional hardware, software or license is required
- Mojo Enforce pulls the registered device list regularly and automatically distributes that information to every single access point
- The solution is resilient to WAN outages and ensures that clients can get authenticated even if connectivity to cloud is unavailable

WiFi Network Requirements	PSK	802.1x (UN/PW)	Mojo Enforce
Enforce user access based on Google accounts	✘	✔*	✔ (Works on top of both PSK and 802.1x)
Enforce which device can connect to the network	✘ (Cannot be enforced using the registered device list)		✔
Enforce network access rights based on OU membership	✘ (Cannot be enforced using the registered device list)		✔

*Requires on-prem RADIUS and user directory replication from Google

About Mojo Networks, Inc.

Mojo Networks is redefining the modern enterprise WiFi infrastructure with a high-performance, highly automated and secure WiFi software architecture. Powering Fortune 500 and Global 2000 environments and trusted in the highest levels of the government, Mojo Networks is the choice for smart CIOs looking to implement an enterprise, cloud-first solution with the scalability, cost-savings and smarter hardware pricing. Mojo Networks is changing the industry to a new era of prolific WiFi connectivity. Request a free trial and learn more about Mojo Networks at www.mojonetworks.com.

