WHITEPAPER

Integration with Google for Education Bringing secure Wi-Fi authentication to K-12 classrooms

Table of Contents

INTRODUCTION

Technology is significantly transforming the way students learn and teachers teach, making Wi-Fi one of the most important components of modern digital learning initiatives. According to Deloitte, 42% of teachers say that at least one digital device is used in the classroom every day and 75% of teachers believe that digital learning content will replace printed textbooks within the next 10 years. Technology impacts everyone involved in education, but as Wi-Fi's popularity grows 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 Wi-Fi 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 Wi-Fi networks, with PSK being used most predominantly. 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 Wi-Fi network.

With 802.1x, though each user has unique credentials, there is really no way to keep 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 K-12 Wi-Fi 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, WatchGuard introduced a new feature within the Wi-Fi Cloud that, together with Google, takes advantage of the registered device list in the Google Cloud and ensures that only authorized devices connect to the network. Beyond this, WatchGuard can also ensure that appropriate network access policies (roles) are applied based on device OU (Organizational Unit) membership defined in Google.

41%

of teachers believe there is a lack of education technology training[1]

90%

90% of kids use digital learning materials at home[2]

57%

of teachers regularly use technology to make learning more interesting[3]

[1, 2, 3] 2016 Digital Education Survey, Deloitte

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 many countries, 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 Organizational Units are core services offered as part of Google for Education that allow admins to create organizational structure and control over 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.

Benefits of Integrating with Google for EDU

- Finally control which digital devices can connect to the school Wi-Fi network
- Absolutely no additional hardware, software or license is required (when access point is Wi-Fi Cloud enabled)
- WatchGuard pulls the registered device list regularly and automatically distributes that information to every access point
- The solution is resilient to WAN outages and ensures that clients can get authenticated even if connectivity to cloud is unavailable

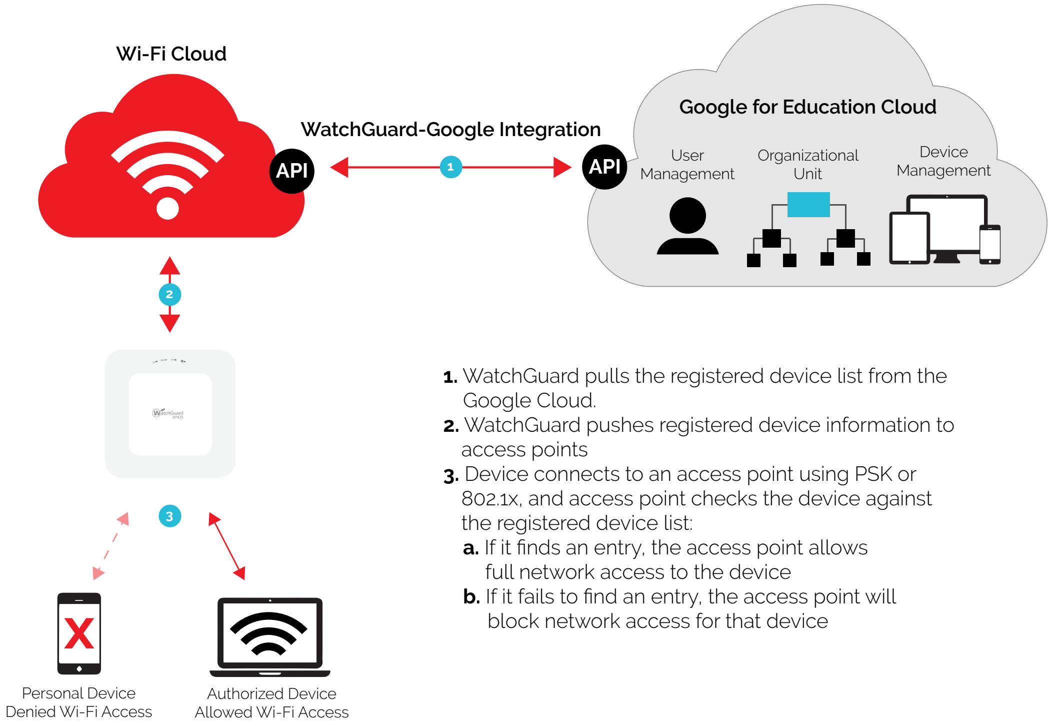
Wi-Fi Network Requirements	PSK	802.1x (UN/PW)	WatchGuard Wi-Fi Cloud
Enforce user access based on Google accounts	x	✓*	✓
Enforce which device can connect to the network	x (Cannot be enforced using the registered device list)		✓
Enforce network access rights based on OU membership	x (Cannot be enforced using the registered device list)		✓

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

Easily Connect Students and Teachers

Allowing Only Registered Devices to Connect to the Wi-Fi Network

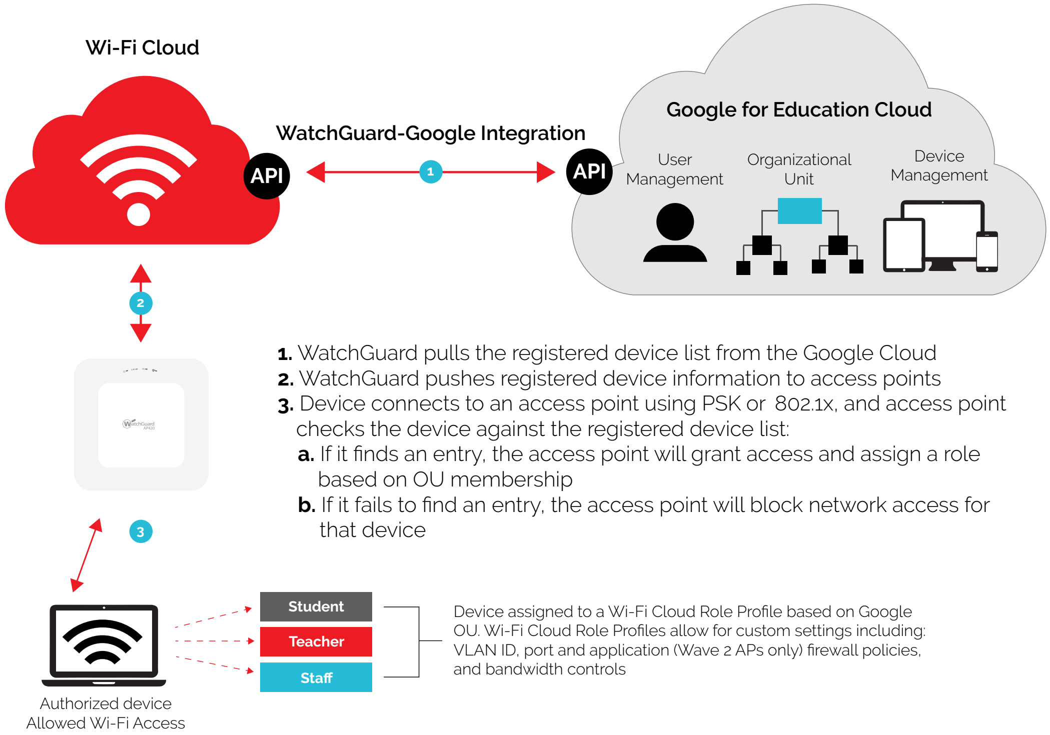
WatchGuard makes use of the registered device list on the Google Cloud to validate the authentication session above and beyond PSK or 802.1x.


Wi-Fi Cloud
API
WatchGuard-Google Integration
1
API
Google for Education Cloud
User Management
Organizational Unit
Device Management
2
3
Personal Device Denied Wi-Fi Access
Authorized Device Allowed Wi-Fi Access

1. WatchGuard pulls the registered device list from the Google Cloud.
2. WatchGuard pushes registered device information to access points
3. Device connects to an access point using PSK or 802.1x, and access point checks the device against the registered device list:
   - **a.** If it finds an entry, the access point allows full network access to the device
   - **b.** If it fails to find an entry, the access point will block network access for that device

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, bandwitdth limit and more.


Wi-Fi Cloud
API
WatchGuard-Google Integration
1
API
Google for Education Cloud
User Management
Organizational Unit
Device Management
2
3
Student
Teacher
Staff
Authorized device Allowed Wi-Fi Access

1. WatchGuard pulls the registered device list from the Google Cloud
2. WatchGuard pushes registered device information to access points
3. Device connects to an access point using PSK or 802.1x, and access point checks the device against the registered device list:
   - **a.** If it finds an entry, the access point will grant access and assign a role based on OU membership
   - **b.** If it fails to find an entry, the access point will block network access for that device

Device assigned to a Wi-Fi Cloud Role Profile based on Google OU. Wi-Fi Cloud Role Profiles allow for custom settings including: VLAN ID, port and application (Wave 2 APs only) firewall policies, and bandwidth controls

Your Business + Our Wi-Fi = Endless Possibilities

WatchGuard's Cloud-Managed Wi-Fi delivers the strongest security, performance, and manageability package.

- Patented Wireless Security
- Management that Scales
- Business-driven Analytics
- Powerful Engagement Tools

To learn more visit www.watchguard.com/wifi

ABOUT WATCHGUARD

WatchGuard® Technologies, Inc. is a global leader in network security, endpoint security, secure Wi-Fi, multi-factor authentication, and network intelligence. The company's award-winning products and services are trusted around the world by over 18,000 security resellers and service providers to protect 250,000 customers. WatchGuard's mission is to make enterprise-grade security accessible to companies of all types and sizes through simplicity, making WatchGuard an ideal solution for midmarket businesses and distributed enterprises. The company is headquartered in Seattle, Washington, with offices throughout North America, Europe, Asia Pacific, and Latin America. To learn more, visit WatchGuard.com.

For additional information, promotions and updates, follow WatchGuard on Twitter @WatchGuard, on Facebook, or on the LinkedIn Company page. Also, visit our InfoSec blog, Secplicity, for real-time information about the latest threats and how to cope with them at www.secplicity.org.

U.S. SALES 1.800.734.9905 INTERNATIONAL SALES +1.206.613.0895 www.watchguard.com

No express or implied warranties are provided for herein. All specifications are subject to change and expected future products, features or functionality will be provided on an if and when available basis. WatchGuard and the WatchGuard logo are trademarks or registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No WGCE67038_071221