secureW2
next-gen wired & wireless security

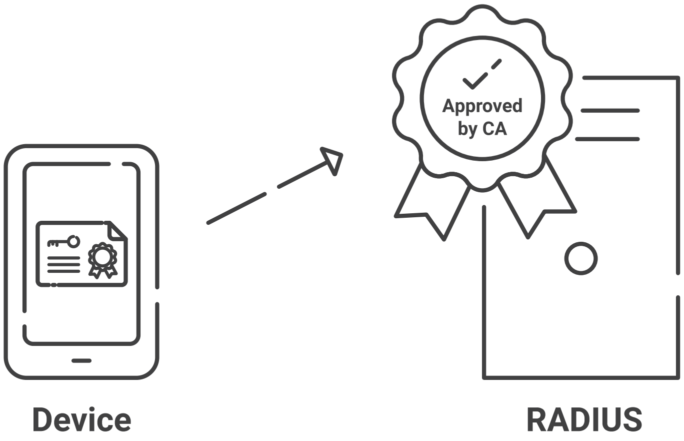
2021 State of Android Wi-Fi Onboarding

Google is constantly updating the Android Operating System (OS) with new features and changes for their mobile devices. These changes can vary from cosmetic touch ups to drastic security updates. A major change involves server certificate validation, which many Android users disable at the behest of the IT staff. Another issue we’ve seen involves Android users having difficulty connecting to Wi-Fi since the update.

In order to help educate organizations and individuals, we've created this guide to address what's new with Android 10-12 devices, how these changes will affect network security and connectivity, and how network administrators can enable WPA2-Enterprise Wi-Fi and connect every Android device.

Table of Contents

Google Mandates Server Certificate Validation for Android



In December 2020, Google released the Android 11 update to their users. One security update in particular has made a dramatic impact. Google is requiring server certificate validation for Android Pixel devices.

The security update has disabled the ability to select “Do Not Validate” for the “CA Certificate” dropdown in network settings for a given SSID. Essentially, this forces Android users to use server certificate validation in order to connect to their network. Many users historically omitted server certificate validation when configuring 802.1x, as it's no easy feat to manually configure. However, Google has deemed it too important for security to be disabled. Frankly, we agree.

Note: “Do Not Validate” will no longer be an option with WPA3-Enterprise. This implies that server certificate validation will be required for other operating systems in the future.

What is Server Certificate Validation?

Server certificate validation is a feature of a **WPA2-Enterprise** network that forces devices to check the identity of a server before they attempt to authenticate onto that network. A device is able to verify that the server is the intended one by checking the Certificate Authority (CA) and validating that it has been issued to the organization's domain.

Having users select the “Do Not Validate” option puts them at risk to leak their credentials by bypassing the server certificate validation process.

Let’s say it’s an employee’s first day on the job and they need Wi-Fi access. If the user notices that they connected to the wrong SSID, they hopefully would disconnect immediately, but relying on end users to maintain network security is never a good idea. Hackers can spoof SSIDs and trick users into sending over their credentials.

Web browsers can stop this from happening by verifying the server certificate. But when the user toggles the "Do Not Validate" option the web browser is prevented from properly verifying the server, leaving the network at risk.

Why was the option removed?

Many organizations instruct their users to use the "Do Not Validate" setting as a work around to avoid implementing proper EAP server certificate validation. It's not easy to configure for the average Android user, prompting many organizations to risk their network security rather than continue coaching end users at a dismal success rate. Google is sending a clear message by eliminating this option, putting an added emphasis on network security and urging others to follow suit.

Does this Affect all Android 10 Devices?

Due to the way Android chooses to update their software, it's possible to continue to use Android 10 devices that don't require server certificate validation, but that potentially opens up other avenues for security breaches so it is not recommended.

Does this Affect all Android 11 Devices?

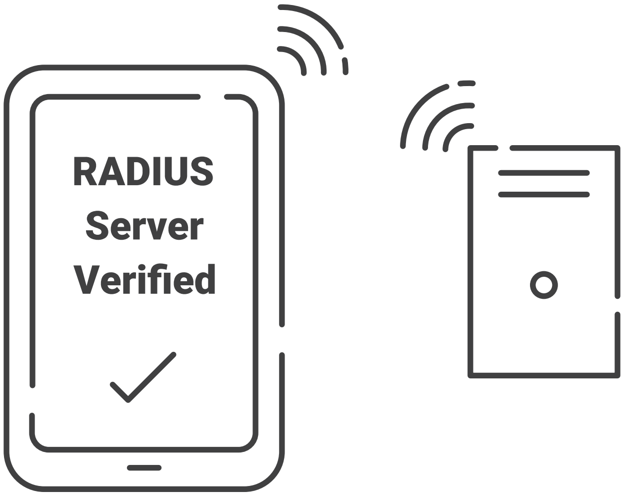
This Server Certificate Validation does affect Android 11 Devices. Of the cases we've observed in the field, we are specifically seeing Pixel 3 Models being affected by this mandate.

If you have Android 11 Pixel devices, you can expect to see end users having difficulty configuring themselves for 802.1X Wi-Fi. We highly recommend implementing 802.1x Onboarding Software, or at the very minimum having very detailed configuration instructions for Android 11 Pixel devices.

Will this Affect Android 12 devices?

Android 12 devices are set to continue the Android 11 tradition of mandating server certificate validation. The majority of Android devices are expected to be phased in over an undetermined length of time, most likely dependent on make/model/carrier of the device. Because of this, and the fact that Android 11 devices are already affected by this, we highly recommend adopting Onboarding Software or starting to document and train IT staff around Server Certificate Validation configuration.

How to Implement Server Certificate Validation on Android



Google has put a lot of people in a tough position as there is no real way to circumvent this issue. Public key cryptography is becoming essential for secure network authentication and Google is making a point in requiring it for their devices.

Organizations using WPA2-Enterprise network have two routes to consider:

1. Provide proper documentation and hire trained IT staff to assist their end users in configuring themselves.
2. Use a device onboarding solution so end users can self-configure with no risk of misconfiguration.

The first option can be done easily if you're a large corporation with endless amounts of money and resources to invest, but smaller IT organizations can be stretched thin in the job hiring and technical documentation process.

Auto-Configuring Devices for Server Certificate Validation

Creating documentations and relying on end users to configure their devices for server certificate validation runs the risk of misconfigurations and can lead to a pile of support tickets. With an onboarding software, users can be automatically configured for server certificate validation through digital certificates. Some onboarding software services come pre-configured with EAP-TLS authentication, using the certificates to authenticate users for

Certificates offer higher security, greater visibility, and better user experience when compared to traditional credential based networks. The tenants of public-private cryptography that are the framework for x.509 digital certificates renders a network impenetrable from both over-the-air attacks and phishing hacks, meanwhile the **EAP-TTLS/PAP protocol** sends unencrypted credentials strings for any hacker with skill to intercept.

Importantly, EAP-TLS eliminates the possibility for misconfiguring server certificate validation. End users are required to use the onboarding software to enroll for a certificate, simplifying user interaction to downloading an app and clicking a few buttons. Though it may seem inconvenient to set up, doing so prevents potential cyber attacks. The process is simplified with onboarding software pre-configured for EAP-TLS.

Onboarding Issues with Google Update

Due to the reasons we just discussed, onboarding applications have been the go-to solutions for many organizations. Unfortunately, Google made a change that broke the ability for onboarding applications to configure Wi-Fi. While Google has promised to fix this in Q1 of 2021, they haven’t specified if this fix will be an update for Android 10 or 11, or just something that's fixed in Android 12. Below we will highlight how things broke, and how we have worked with organizations to fix this.

Connect to Wi-Fi Prompts

Due to recent changes made to the Android 30 Software Development Kit (SDK), there are a few ways that third-party applications interact with the Android OS that have caused a lot of people to have trouble connecting to their Wi-Fi network. There have been numerous issues plaguing both Android 10 and 11, ranging from connectivity issues, first and third-party application bugs, UIs taking a long time to load, and batteries draining quickly.

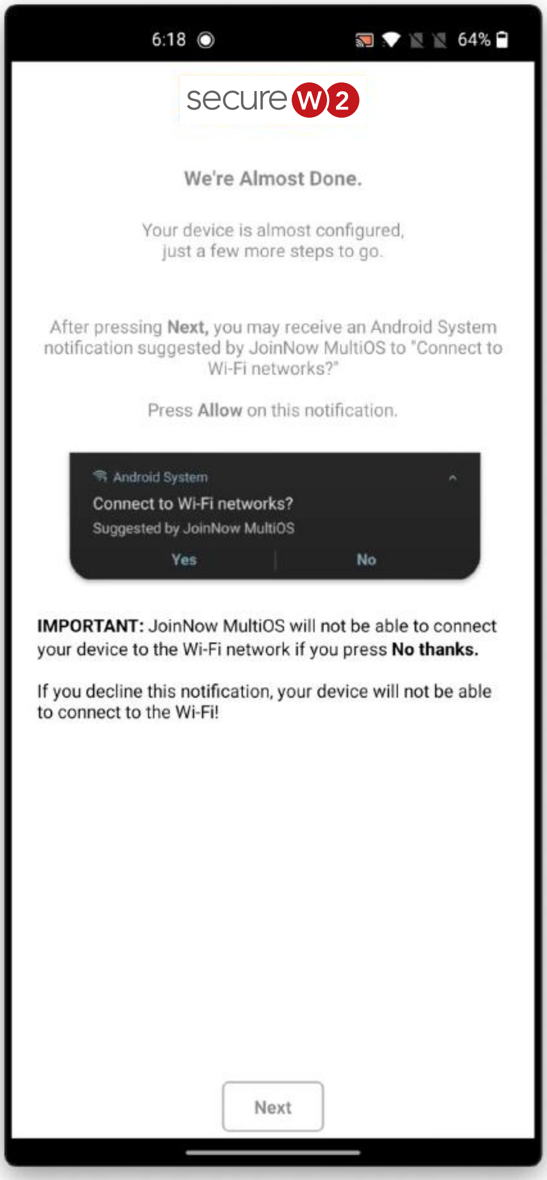
Changes to Android 10 Devices

One common bug we've been seeing is Android 10 devices not receiving the Wi-Fi networks notification, or the notification delaying for up to 5 minutes. This is a confirmed bug by Google, and it will require Android 10 users to manually connect to their organization's secure Wi-Fi network.

Does the SecureW2 App Accommodate for this Android 10 Bug?

Absolutely! Even though the prompt issue will prevent you from connecting to Wi-Fi, it doesn't stop the JoinNow App from configuring your device. You can easily rectify this by following these few simple steps below:

1. Navigate to your Wi-Fi Settings
2. Select the secure Wi-Fi network your organization uses.
    a. Eduroam is a real-world example of this feature.
3. If prompted, select your Certificate that was generated by the SecureW2 Android Application.



6:18 64%

We're Almost Done.

Your device is almost configured, just a few more steps to go.

After pressing **Next**, you may receive an Android System notification suggested by JoinNow MultiOS to "Connect to Wi-Fi networks?"

Press **Allow** on this notification.

Android System

Connect to Wi-Fi networks?

Suggested by JoinNow MultiOS

Yes | No

IMPORTANT: JoinNow MultiOS will not be able to connect your device to the Wi-Fi network if you press **No thanks.**

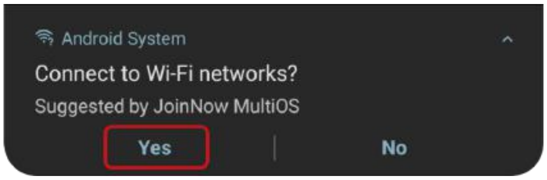
If you decline this notification, your device will not be able to connect to the Wi-Fi!

Changes to Android 11 Devices

Much like the Android 10 devices, Android 11s have been facing **connectivity issues** with Wi-Fi networks and third-part applications.

What are these requirements?

Google made it so that any time an Android app tries to connect you to the Wi-Fi, they must consent on this new notification below that pops up.

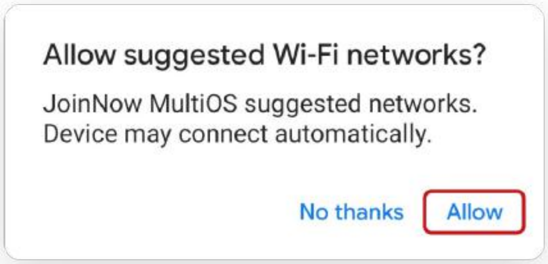


Android System

Connect to Wi-Fi networks?

Suggested by JoinNow MultiOS

If the user does not consent, by pressing **No,** then the app is forbidden from configuring anything involving Wi-Fi configurations for that device. This can be a major pain for onboarding applications and network administrators.

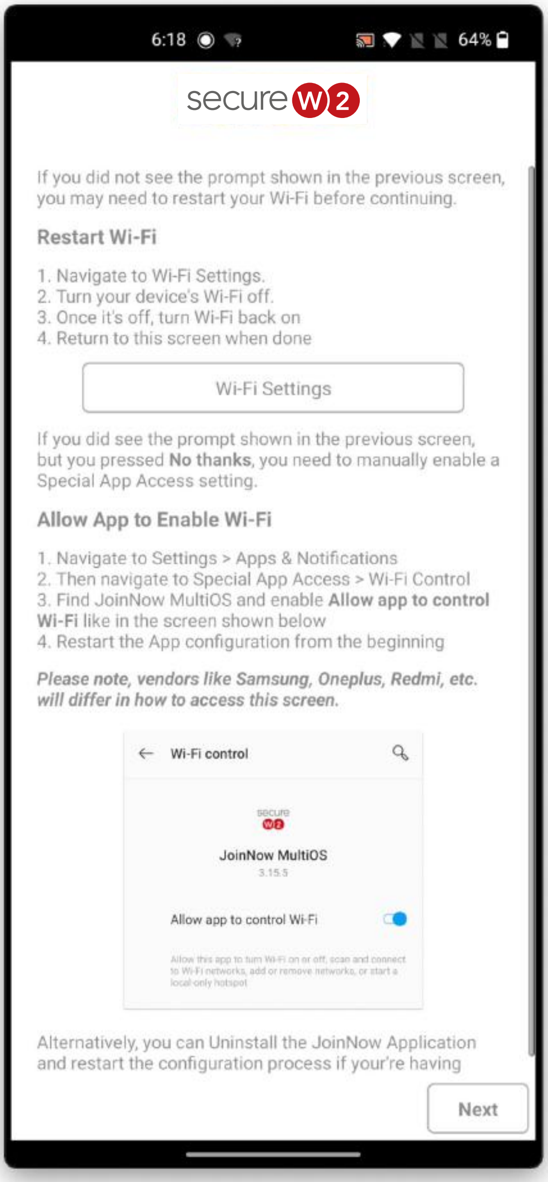


Allow suggested Wi-Fi networks?

JoinNow MultiOS suggested networks. Device may connect automatically.

By clicking **Yes** and **Allow,** the user is able to self-configure their device and automatically and securely connect to the Wi-Fi.

What Can I Do If I Hit “No” on the Wi-fi Prompt?



If you did not see the prompt shown in the previous screen, you may need to restart your Wi-Fi before continuing.

Restart Wi-Fi

1. Navigate to Wi-Fi Settings.
2. Turn your device's Wi-Fi off.
3. Once it's off, turn Wi-Fi back on
4. Return to this screen when done

If you did see the prompt shown in the previous screen, but you pressed **No thanks**, you need to manually enable a Special App Access setting.

Allow App to Enable Wi-Fi

1. Navigate to Settings > Apps & Notifications
2. Then navigate to Special App Access > Wi-Fi Control
3. Find JoinNow MultiOS and enable **Allow app to control Wi-Fi** like in the screen shown below
4. Restart the App configuration from the beginning

Please note, vendors like Samsung, Oneplus, Redmi, etc. will differ in how to access this screen.

Allow app to control Wi-Fi ●

Allow this app to turn Wi-Fi on or off, scan and connect to Wi-Fi networks, add or remove networks, or start a local-only hotspot

Alternatively, you can Uninstall the JoinNow Application and restart the configuration process if your're having

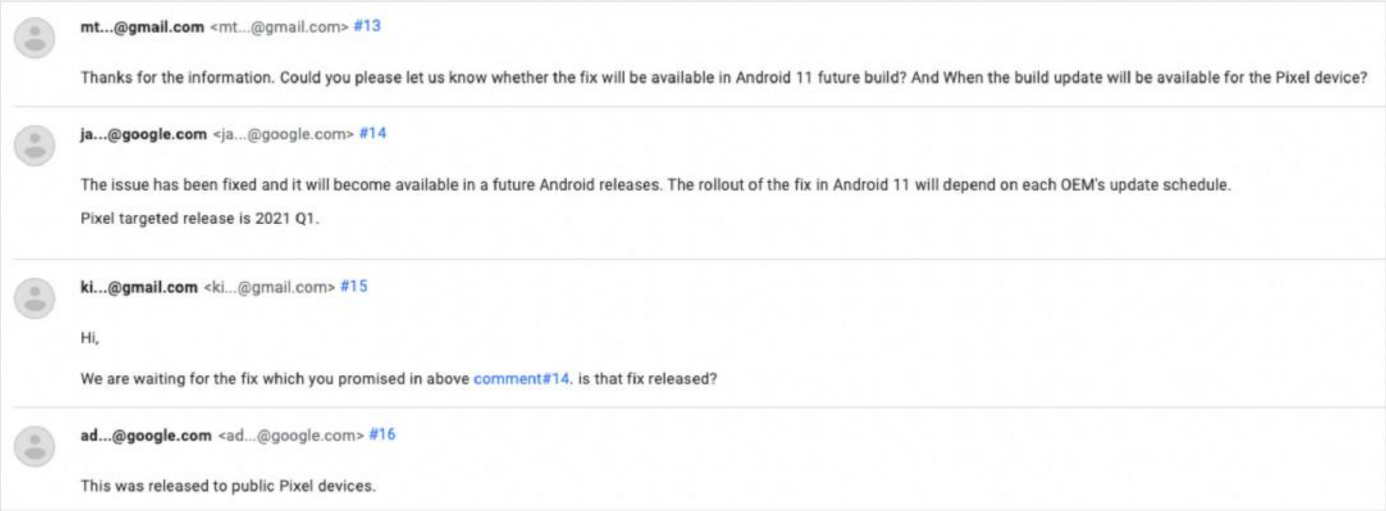
Reinstall the SecureW2 App

SecureW2 added new and improved messaging for Android device onboarding. Users will now see detailed instructions around navigating new Android system prompts that are required in order for the JoinNow application to properly configure devices.

Configure the Android System Settings

We’ve provided a message warning users that their devices will be unable to connect to Wi-Fi if they deny suggested Wi-Fi networks. This improved messaging has been implemented in response to the new processes required to navigate Google’s recent changes made to Android.

Is it fixed for Android 12 Devices?



mt...@gmail.com <mt...@gmail.com> #13

Thanks for the information. Could you please let us know whether the fix will be available in Android 11 future build? And When the build update will be available for the Pixel device?

ja...@google.com <ja...@google.com> #14

The issue has been fixed and it will become available in a future Android releases. The rollout of the fix in Android 11 will depend on each OEM's update schedule.
Pixel targeted release is 2021 Q1.

ki...@gmail.com <ki...@gmail.com> #15

Hi,

We are waiting for the fix which you promised in above comment#14. is that fix released?

ad...@google.com <ad...@google.com> #16

This was released to public Pixel devices.

Google confirmed this issue will be **addressed in Quarter 1 of 2021.** A follow-up post confirmed that Google had fixed the issue for both Android 11 and 12 and has been released to public schedule.

Android 11 Deep Sleep Prevents Network Configuration

What is "Deep Sleep"?

Android has been testing different ways to preserve a device's battery life and a more recent feature is deep sleep, introduced in Samsung's One UI overlay. The purpose is to save battery life by putting apps that aren't used often into a sleep mode and not using any battery.

The unintended consequence is that many apps are designed to be set up and forgotten, actively working in the background. Android will automatically assume these are unused devices, place them in deep sleep and have them deactivated.

This **page provides good insight** into why the deep sleep feature can be considered an "app killer".

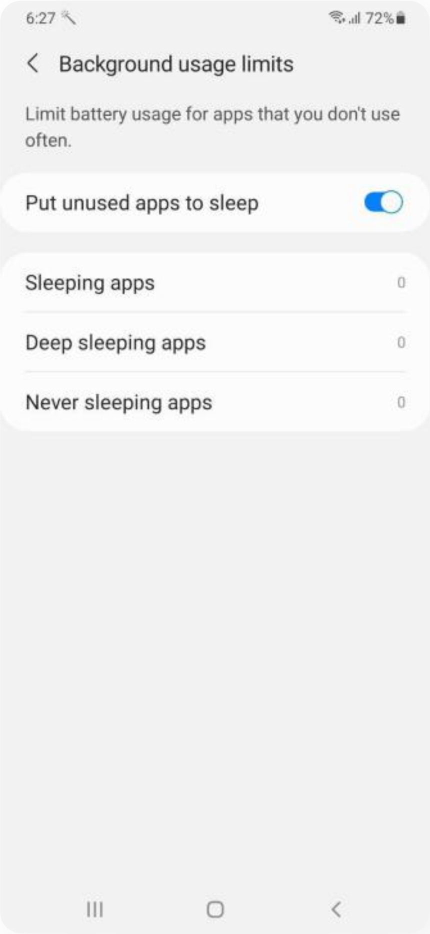
How to Check What Apps are In Deep Sleep

Follow the sequence below:

Settings ⟶ Device Care ⟶ Battery ⟶ App Power Management

Wi-Fi Will Disconnect if Onboarding Apps are in Deep Sleep

SecureW2's JoinNow app ensures the device is authenticated through EAP-TLS in order to access Wi-Fi. Our support team has been made aware of the Deep Sleep mode removing the app's use case. When JoinNow is placed on the deep sleep list, Samsung devices will not be able to connect to their Secure SSID and EAP-TLS configurations will be removed.



6:27 72%

< Background usage limits

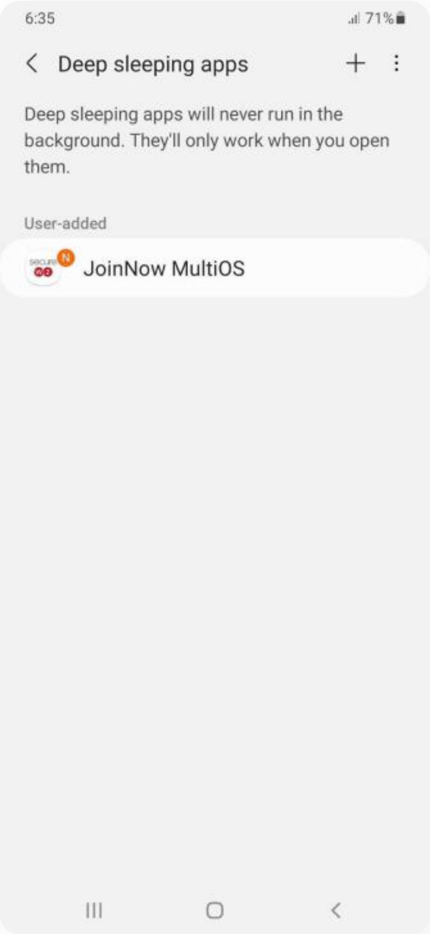
Limit battery usage for apps that you don't use often.

Put unused apps to sleep

Sleeping apps 0

Deep sleeping apps 0

Never sleeping apps 0



6:35 71%

< Deep sleeping apps

Deep sleeping apps will never run in the background. They'll only work when you open them.

User-added

JoinNow MultiOS

What Devices Are Affected?

The problem began with the Samsung One UI 3.1 update, which rolled out the same time as Android 11. Our support team was first made aware of the issue in Samsung S20 devices, but it can affect any Samsung device that supports One UI (Galaxy S, A, M, & Notes series and Android 9 & 10).

How to re-connect Android Device to Secure Wi-Fi

Our dev team will work on a solution to ensure the SecureW2 app will not be accidentally placed in deep sleep mode. For now, admins should instruct users to place the SecureW2 app under the “Never Sleeping Apps”.

If the SecureW2 app is on the deep sleep list, follow this quick guide.

1. Manually remove the JoinNow app from deep sleep.
2. Add the JoinNow app to the “Never Sleeping Apps” list.
3. Open the JoinNow app and re-enroll the end user for a certificate to connect to your Secure SSID.
    a. When removed the app does not push back the same Wi-Fi configuration, so re-enrollment is necessary.

FAQ

Is The Server Certificate Mandate Active For Android 10?

It's possible to continue to use Android 10 devices that don't require server certificate validation, however it is best practice to update your device.

What is Onboarding Software?

Onboarding users is much simpler when using onboarding software because it eliminates the need for manual configuration from the end user. Admins don't need to waste time creating documentation and dealing with support tickets when users have trouble with said documentation.

Onboarding is traditionally set up with an open SSID that directs users towards onboarding software so they can self-service their devices for secure WPA2-Enterprise network connectivity. Conceptually, it's not a difficult thing to set up. However in our experience with customers, configuring and troubleshooting the Walled Garden can be particularly time consuming.

A solution for this is an advanced onboarding service from a third-party, where the heavy lifting is handled mostly by their engineers. Key differences are the onboarding SSID needs to be authenticated against a RADIUS server, and the Walled Garden setup is much less complex.

Setting up and configuring a RADIUS server is an area where the Advanced Onboarding configuration can be more complex, unless you use a service that already comes with a RADIUS server.

Why did Google Take Away The "Do Not Validate" Option?

In short, the option allowed users to bypass server certificate validation which Google rightly decided poses too great a security risk to warrant.

Is Server Certificate Validation Necessary?

Absolutely! If you want your network to perform the highest level of security, enabling server certificate validation ensures that your users and devices connect to the approved RADIUS server before exchanging information. Server certificate validation goes in line with the Zero Trust philosophy.

How can I tell which Version I have?

The steps for checking your version vary depending on your device. Below are general instructions that should work for most Android devices.

1. Open your device's settings.
2. Look for an option that says About Device, About Phone, or something similar.
3. Find your Android version on the list of specifications.