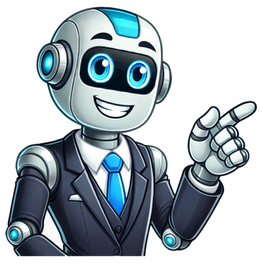
Click to verify



Business and Education / iPad in Business and Education I have iphone 14 pro max, on general - certificate trust setting only have trust store version and trust asset version, and do not have other option show up to manually to trust SSLI have problem to setting up my email on the iphone iPhone 12 Pro, iOS 15 Posted on Apr 13, 2023 9:52 PM Reply Page content loaded Apr 15, 2023 12:16 PM in response to garry_chan_3067 Hello garry_chan_3067,To help us get a better understanding of the issue, wed like to ask a few questions. Just to clarify, can you let us know more about the issue you're having when setting up your email? Are you being prompted to turn on trust for SSL/TLS after installing a profile that was sent to you via email, or something else? Are you receiving any specific errors? If so, what does the exact error say? If you want to trust manually installed certificate profiles, please be sure the process outlined in the link you came from is being used correctly, so we can make sure that's not part of the issue: Trust manually installed certificate profiles in iOS and iPadOSIf you manually install a profile that contains a certificate payload in iOS and iPadOS, that certificate isn't automatically trusted for SSL. Learn how to manually trust an installed certificate profile.This article is intended for system administrators for a school, business, or other organization.You must manually turn on trust for SSL/TLS when you install a profile that is sent to you via email or downloaded from a website.If you want to turn on SSL/TLS trust for that certificate, go to Settings > General > About > Certificate Trust Settings. Under "Enable full trust for root certificates," turn on trust for the certificate.Apple recommends deploying certificates via Apple Configurator or Mobile Device Management (MDM). Certificate payloads are automatically trusted for SSL when installed with Configurator, MDM, or as part of an MDM enrollment profile.Thanks! This thread has been closed by the system or the community team. You may vote for any posts you find helpful, or search the Community for additional answers. I can not able to trust certificate setting Page content loaded Oct 8, 2024 2:57 PM in response to Chesnutlodge Same issueTrust manually installed certificate profiles in iOS, iPadOS, and visionOS - Apple SupportBuddy, ,iOS 18.0.1!My question is shown in the figure below. It's always blank there. Its not shown any certificates in Certificate Trust Settings after I update to iOS 18.0.1 Sep 25, 2024 11:47 AM in response to Chesnutlodge Me too. Same cert works on iOS 16.7.10, iOS 17.6.1 and iPadOS 18.0But not on iOS 18.0 Also tried regenning a new test root on macOS Sonoma and installing using Configurator. No difference.Its broken - Ive reported it by Feedback - suggest you do the same? Strength in numbers as its a vital security flaw.[Edited by Moderator] Sep 26, 2024 5:51 AM in response to Chesnutlodge Kinda the same for me - bought an iPhone 16 and its not showing up in trust settings after installing it. On my iPad Air 4 it doesnt show though. As a sanity check I removed and reinstalled the profile on my iPad on iPadOS 18 and it worked. The same certificate continues to not show on my iPhone. I also tried another certificate that is known to work and it doesnt show on my iPhone either. Nov 18, 2024 4:34 AM in response to Chesnutlodge Resetting the iPhone to factory defaults worked for me.The option "Settings -> General -> About -> Certificate Trust Settings -> ENABLE FULL TRUST"is back again.Still waiting for a fix. Hopefully in 18.2 Sep 25, 2024 12:12 PM in response to Chesnutlodge Are you installing the certificates manually or via MDM? Sep 25, 2024 12:18 PM in response to celliott147 In my case, manually and via Configurator to unsupervised phones and iPads Was your iPhone working perfectly fine until you suddenly started receiving a 'certificate not trusted' prompt? For many people, this is a common experience, and they don't even recall downloading any certificates on their device. It's likely because the average person doesn't understand their purpose. So, here's what we'll do: Learn all about certificate profiles. Find ways to bypass the 'certificate not trusted' error on iPhone. And much more! Let's dive right in. What Is the Certificate Profile on iPhone? A certificate profile on an iPhone is like a digital ID card that helps your device securely connect to networks or services. Think of it as a special pass that your iPhone uses to prove it's allowed to access certain things, like corporate email or a Wi-Fi network. When you set up your iPhone for work or join a specific network, you might need to install a certificate profile. This profile contains digital certificates, which are like electronic stamps of approval. They ensure that your iPhone is authorized to use certain features or connect to particular services. For example, if your job requires accessing secure company email, the IT department might give you a certificate profile to install on your iPhone. This profile ensures that your device is recognized and trusted, allowing you to securely receive and send work-related emails. Check If It Is a Corporate iPhone If your iPhone is supervised by your corporate, organization, enterprise, or school management, the initial step is to examine whether any profiles have been installed on your device by these entities. To do so, navigate to your iPhone settings and look for installed profiles. If you find any, it's crucial to reach out to the administrator of your organization. They can guide you through the process of removing and reinstalling the certificate on your iPhone. This action ensures that your device aligns seamlessly with the organizational settings and security protocols. Trust the Certificate Profile Manually When manually installing a profile with an embedded certificate payload in iOS and iPadOS, the certificate therein does not inherit automatic trust for SSL/TLS connections. To establish trust, particularly for profiles received via email or downloaded from a website, users are required to activate SSL/TLS trust manually. To enable SSL/TLS trust for a specific certificate: Step 1: Navigate to Settings > General > About > Certificate Trust Settings on your iOS or iPadOS device. Step 2: Within the settings, locate the option "Enable full trust for root certificates" and activate trust for the relevant certificate. This manual intervention ensures that the certificate is acknowledged and trusted for secure communications, mitigating potential security risks associated with untrusted certificates. Delete Spam Calendars on iPhone Another thing to keep in mind is that spam calendars and events on your iPhone can lead to certificate trust issues in the long run. It's always better to delete them and keep your phone clear than to take the risk. For iOS 14.6 or later: Open the Calendars app on your iPhone. Tap the unwanted calendar event. At the bottom of the screen, tap "Unsubscribe" to unsubscribe from this Calendar. Confirm by tapping "Unsubscribe." For earlier iOS versions: Open the Calendar app. At the bottom, tap "Calendars." Look for a calendar you don't recognize. Tap "More info" next to that calendar, then scroll down and tap "Delete Calendar." If the issue persists, follow these steps: Open the Settings app. Tap "Calendar" > "Accounts" (or "Passwords & Accounts" > "Accounts" for iOS 13). Tap "Subscribed Calendars." Identify the unfamiliar calendar, tap it, and then tap "Delete Account." Restart Your iPhone If the certificate on your iPhone is still causing issues, another thing to try is a simple restart. iPhones work similarly to Macs or Windows PCs under the surface, and just like those, a quick reboot can often fix things. Whether you're using the latest iPhone 15 Pro Max, the Touch ID iPhone SE (2022), or an older model like the 2013 iPhone 5s, the steps are the same: Step 1: Press and hold the right-side button along with either of the volume buttons until you see the "Slide to power off" control. If you're using an older iPhone like the first-gen iPhone SE (2016) or an iPhone 5s, that button will be on the top instead of the side. Step 2: Slide the slider from left to right. Step 3: Wait patiently for at least 30 seconds to ensure your device powers down completely. Step 4: Press and hold the right-side button until you see the Apple logo appear. Step 5: Your device will boot up and take you back to the lock screen after a few moments. Step 6: Depending on your iPhone model, either swipe up or press the front home button, enter your passcode, and voila, your device is good to go again. Update the iOS If you're still facing the issue of your iPhone not trusting a certain certificate, consider updating your iPhone to the latest iOS version. If you can navigate your way to the Settings app on your iPhone, the quickest and simplest way to update is by tapping on General > Software Update. If not, consider updating your iPhone to the latest iOS version via iTunes or Finder: Step 1: Connect your iPhone to your computer. Step 2: If you're using macOS Catalina 10.15 or higher, open Finder. For macOS Mojave 10.14 or earlier, or Windows, open iTunes. Step 3: If your iPhone is unlocked and recognized by the computer (using Face ID or Touch ID), select your iPhone in Finder or iTunes. Click on the "Update" button to download and install the latest iOS update. Step 4: If it's the first time connecting your iPhone to this computer, a prompt on your iPhone will ask you to "Trust" the computer. If your touchscreen is responsive, tap "Trust" to confirm, and then proceed with the update in the step above. These steps should help address the issue of an untrusted certificate on your iPhone. Contact Apple Consider reaching out to Apple Support if the error persists. Apple may be able to address the issue, even if it's related to hardware, without erasing your iPhone. However, keep in mind that there's no guarantee of a solution. If your iPhone has a significant hardware problem, Apple might replace it with a new unit. In such cases, you'll need to restore your data onto the new iPhone. It's important to note that Apple respects your privacy and security, so even their technicians can't bypass security measures to access your data. To Conclude Now that you've made it to the end of our guide, hopefully, your Certificate Not Trusted problem has taken care of itself. Remember, when it comes to personal vs company iPhones, the rules are a bit different. However, with our easy and quick solutions, you can get your phone working as good as new in no time. Just remember to reach out to Apple Support if you feel unsure about anything else; it's better to be safe than sorry. This article is intended for system administrators for a school, business, or other organization. You must manually turn on trust for SSL/TLS when you install a profile that is sent to you via email or downloaded from a website. If you want to turn on SSL/TLS trust for that certificate, go to Settings > General > About > Certificate Trust Settings. Under "Enable full trust for root certificates," turn on trust for the certificate.* Apple recommends deploying certificates via Apple Configurator or Mobile Device Management (MDM). Certificate payloads are automatically trusted for SSL when installed with Configurator, MDM, or as part of an MDM enrollment profile. *If Enable full trust for root certificates doesnt appear, you haven't installed any additional certificates. Tell us more about what's happening, and well suggest what you can do next.Get suggestions Published Date:March 26, 2025 Helpful? Thanks for your feedback. iPhones come with Trust Stores that contain trusted root certificates pre-installed on your device. However, there are several reasons why you will want to use custom certificates. Due to their low cost, custom certificates are usually the preferred option for development and testing environments. They are also often suitable for internal (intranet) servers as they can be deployed easily and quickly. Now, the question is, how do you make an iPhone trust a custom certificate? Provided the certificate has the CA Basic Constraint extension, Apple will allow you to trust the certificate manually. This article will explain the step-by-step process to fix trust certificate issues on the iPhone. Installing a self-signed or custom certificate is different for different versions of iOS devices. But for the sake of this guide, we will be using iOS 10.3 and later. Before now, to make an iPhone trust a custom certificate was easy since all you had to do was send the file to your iPhone, and it will automatically trust it. Now, thats no longer the case. Even after installing the certificate, your iPhone wouldnt trust it. The steps below explain how to make your iPhone trust a self-signed certificate. Export the certificate or profile to your iPhone by emailing the certificate to yourself, uploading it to a website, then downloading it with Safari, among others. When you get the certificate on your device, download it. If successful, you will get a prompt that a profile has been successfully downloaded, of which you can then click on the close button. To install the certificate, go to the Settings app on your iPhone, and on top of the settings menu, you will see the option Profile Downloaded below the Apple ID row. Tap on it to display the Install Profile menu. At the top-right corner of your screen, tap Install. If your iPhone has a passcode set, you will be prompted to enter it to proceed. Enter your password and tap Install again. Once installation is successful, tap on Done. After installing a self-signed certificate, it wouldnt be automatically verified. To enable trust for the certificate, open the Settings app again and navigate your way to the General. So on the profile menu, youd see the message Not Verified. Under General, tap on About and then tap on Certificate Trust Settings. Under Certificate Trust Settings, youd see the profile you just installed, and you can toggle it on to enable full trust for the profile. Enabling your iPhone to trust custom certificates is easy, but use it cautiously. Not all certificates are trustworthy. Giving trust permission to a profile you dont know could expose you to security issues. So, if you dont know much about the profile, it is better not to enable trust than to enable trust and be exposed to security breaches. What To Do When Your iPhone Cannot Verify Server Identity Restart Your iPhone. If you receive an alert saying that your iPhone cannot verify server identity, the first thing to do is restart your iPhone. Close The Mail App, Then Reopen It. Delete Your Email Account, Then Add The Email Account Again. Reset All Settings. Consequently, how do I trust a certificate on my iPhone?If you want to turn on SSL trust for that certificate, go to Settings > General > About > Certificate Trust Settings. Under "Enable full trust for root certificates," turn on trust for the certificate. Apple recommends deploying certificates via Apple Configurator or Mobile Device Management (MDM).Secondly, why does it keep saying verification failed? They try to connect to iTunes and Apple Store from their iPhone settings and instead see the error connecting Apple ID verification failed message. Readers often see this message after a restore or iOS update. Usually, it means that your device is not allowing you to connect to Apple's iCloud verification servers. Beside above, how do I verify my mail server on my iPhone? Go to the settings screen. From the iPhone, iPad, or iPod touch main screen, tap: Verify the Incoming Mail Server settings. Verify the Outgoing Mail Server settings. Verify the folder settings (optional). How do I trust certificates on iPhone iOS 13?If you want to turn on SSL trust for that certificate, go to Settings > General > About > Certificate Trust Settings. Under "Enable full trust for root certificates," turn on trust for the certificate. Apple recommends deploying certificates via Apple Configurator or Mobile Device Management (MDM). Importing an existing self- signed trusted root certificate no longer triggers option to trust cert in Settings / About / Certificate Trust Settings In iOS 18.Cert installed manually from internal website, as email attachment, and using profile in Configurator all produce same result.Same cert and processes work on iOS 16.7.10, iOS 17.6.1 and iPadOS 18.0But not on iOS 18.0 nor beta iOS 18.1 beta5 on iPhone 16Also tried regenning a new test root on macOS Sonoma and installing using Configurator. No difference.Its broken - Ive reported it by Feedback - its a vital security flaw.Anyone else see this or have a workaround? After upgrading to iOS 18.2 b4, I can finally see the missing certificates in the Certificate Trust SettingsYep. That gels with my expectations based on the resolution I see for the bug. Thanks for checking!After upgrading to iOS 18.2 b4, I can finally see the missing certificates in the Certificate Trust SettingsYeah, thats a different, but obviously related issue. And soI submitted FB15921702Thanks!Share and EnjoyQuinn The Eskimo! @ Developer Technical Support @ Applelet myEmail = "eskimo" + "1" + "@" + "apple.com" Got the same problem, which influence my usually work with whistle. I can't capture https package without trust the private certificate. Trust option is not appearing Certificate Trust Settings Yes,I also facing same issue . Tried different path but still unable to find the way. Currently , i m not able to test Apps for iOS 18.i m also waiting for this fix. Have the same issue on iOS 18 and iOS 18.1 Public beta. There some advices on the interned, but nothing works! It's really annoying and no workaround for now. I cant explain the behaviour youre seeing, but this continues to work for me. I have a personal CA that I use to issue certificates. I run this CA using Keychain Access > Certificate Assistant, using roughly the process described in Technote 2326 Creating Certificates for TLS Testing.I just installed this CAs root certificate on an iOS 18 device by:Downloading the .cer file in Safari.Importing the profile in Settings.Enabling the CA in Settings > About > Certificate Trust Settings.That is, roughly the process described in QA1948 HTTPS and Test Servers.I was then able to use Safari to access an HTTPS server whose certificate was issued by that CA. Ive seen problems like this in the past and they usually involve one of two things:Folks trying to use a self-signed server certificate. Things go more smoothly if you create a CA, have it issue the server certificate, and then trust the CAs root certificate.The CA root certificate being weirdly formed, for example, the issue described here.Ive reported it by FeedbackWhat was your bug number?Share and EnjoyQuinn The Eskimo! @ Developer Technical Support @ Applelet myEmail = "eskimo" + "1" + "@" + "apple.com" I have generated my own SSL cert using openssl. The same cert worked on iOS 17. With iOS 18, I open the certificate in Safari and import it on the iPhone. I get "The authenticity of "mydomain.com" cannot be verified." To which I then click Install. But when I go to trust the cert, it does not show up.I use NextDNS and when I import their cert, it DOES show up to be trusted as a root CA.Something has changed to make this no longer work with self generated certs. In a school trust with 10000s of iPads . If iPad upgrades to iOS 18.0.0 MDM profile certs fail. If we disable the block on vpn we can install our jamf MDM profile with certs fine. We have 10+ year certs from Sophos xg firewall.Link seems to be - if we block vpn our jamf MDM profile breaks and so does certs.weird how this wasnt picked up in testing with jamf and apple for edu customers.a reset post upgrade to iOS 18.0.0 seems to fix it.hope this helps others @Dooleylastword - Why not use certificates from a real CA for production use? I encountered the same issue. I tried to investigate different scenarios with various colleagues. If a user upgrades directly from an iPhone running iOS 16 or earlier to iOS 18, or uses the migration feature to move to iOS 18, the certificate does not appear in the Certificate Trust Settings (Full Trust for Root Certificates) list. However, the same certificate can be successfully installed on an iOS 18 device that hasnt gone through migration or on a device that has upgraded from iOS 17 to iOS 18, where it appears normally in the Certificate Trust Settings list.We attempted many solutions and initially thought there might be an issue with our certificate. However, we then directly installed Apple's official Apple PKI webpage (and downloaded a certificate for testing. We found that devices with these issues also failed to display the certificate in the list for enabling it.Currently, the only workaround is to reset the entire phone and not use the migration feature or upgrade from iOS 16 or earlier to iOS 18. Only then will the certificate display correctly in the Full Trust list. I'm not sure if this bug will be fixed. Something has changed to make this no longer work with self generated certs.As I mentioned earlier, installing self-signed leaf certificates it definitely taking your off the beaten path and I recommend that you not do that. Instead, set up a test CA and have it issue your leaf.Why not use certificates from a real CA for production use?There are lots of good reasons why organisations want to use their own internal CA. A classic example of this is that you run an internal DNS using a well-known domain, like .internal, and most standard CAs wont issue certificates for such DNS names.Currently, the only workaround is to reset the entire phone and not use the migration feature or upgrade from iOS 16 or earlier to iOS 18.OK, thats a new wrinkle. Based on this and other threads its clear that folks are having significant problems here. If youre being affected by this, I strongly recommend that you file a bug describing the issue as you see it, what diagnostics you ran, and what they revealed. It would help if you included:A copy of the CA certificate that youre trying to use.A sysdiagnose log taken immediately after installing the certificate and seeing the problem in Settings.Please post your bug number here.Share and EnjoyQuinn The Eskimo! @ Developer Technical Support @ Applelet myEmail = "eskimo" + "1" + "@" + "apple.com" iosNumberOne said:Currently, the only workaround is to reset the entire phone and not >use the migration feature or upgrade from iOS 16 or earlier to iOS 18. >Only then will the certificate display correctly in the Full Trust list. I'm >not sure if this bug will be fixed.This isn't entirely accurate. It does not work when updating from iOS 17 to 18. Had this issue on an iPhone 15 Pro and an iPad Pro 11". The existing cert and process had been used as far back as iOS 16 and it worked fine.DTS Engineer said:As I mentioned earlier, installing self-signed leaf certificates it >definitely taking your off the beaten path and I recommend that you >not do that. Instead, set up a test CA and have it issue your leaf.While this did work, generating my own CA and then using a cert generated from that, this was not a requirement with prior iOS versions. It needs to be spelled out in the upgrade notes if this is now a requirement. Previously, I would remove and reinstall the cert (without CA) for the last two years if it needed to be regenerated. This no longer works and is an extra step to have your own CA. We've had 4 devices out of 1,160 that have exhibited signs of this problem. A couple of things that we've noticed;All 4 devices where on some iOS version older then 17.xThey all would have had a profile blocking VPNOn the last one, we tried installing a profile containing the certs and the profile would install but the cert never was available to trust.On the last one, the MDM profile was showing as unverified but the device had just checked in with the MDM a day or so before and in the MDM the expiration date looked fine.So far it's been 3 iPhones and 1 iPad that were affectedWith our devices being almost 100% remote, I've not been able to get a sysdiagnose log.We have found that the only way to recover is by doing an Erase All Contents and Settings. It needs to be spelled out in the upgrade notes if this is now a requirement.Thats not what I said. Quoting myself here:it [takes] your off the beaten path and I recommend that you not do that.My point is that the having a custom CA that issues certificates for internal servers is a well-trodden path thats exercised a lot. Speaking personally, Im pretty sure that works because I use this technique for my own server!Thats not claiming that this is now a requirement, or that installing a leaf certificate is unsupported.Regardless, the issue being reported on this thread is that, in situations we dont yet understand, the custom CA path isnt working. To move forward with that issue, we need some bug reports. Chivalry0499, Thanks for sharing that info.With our devices being almost 100% remote, I've not been able to get a sysdiagnose log.Oh, tricky.One option that might work for you is to ask a user to file their own bug report. They can do that using the Feedback Assistant app, even on stock versions of iOS. The app is hidden, but you can start it by opening an applefeedback: URL, for example, applefeedback://start.Share and EnjoyQuinn The Eskimo! @ Developer Technical Support @ Applelet myEmail = "eskimo" + "1" + "@" + "apple.com" @DTS Engineer Hi Quinn. Just wondering if you had a chance to review my bug report and whether the problem is now recognised as a bug. The device in question had been upgraded from iOS 16 so I guess its some interaction with the restore process. The device had previously had the related cert installed and working.Any further info you require? @DTS EngineerHi QuinnI had some time today to do some more testing to help narrow down the problem. It does appear to be related to restoring a backup from a previous iOS version (in my case iOS 16.7.10.I did two strands of tests, one to confirm the correct behaviour in a iOS 18 environment, and second restoring various backups created from the original phone after removing both the cert and trust and from the non-working iOS 18 systemfirst resetting the phone, seeing if the cert was handled correctly (it was) and then trying a fresh backup and restore to see it was something fundamental in the restore process. This worked exactly as desired. I was surprised to see that the restore process preserved both the configuration profile and its trust so there is obviously some code in the restore process that attempts to restore that aspect which is failing on a non-iOS 18 backup and introducing some sort of corruption into the certificate store?second, I removed the cert from the old iOS 16.8 iPhone completely (turned off trust and removed configuration profile). There are no (other) certificates on the phone. I created a new fresh backup and restoring that to the new iPhone 16 got me back to where I started. The cert loaded OK but fails to appear in "Certificate Trust Settings"**So the bug potentially appears to be in the processing of iOS 18's restore from backup where the backup is from iOS 16 (and given other users feedback) or iOS 17. **Resetting the phone = "Erase All Contents and Settings"Loading the cert = Installing the relevant configuration profile created by opening the CER file in Files.Hope this helps

Certificate trust settings. Certificate iphone not trusted. Iphone trust certificate. Ios certificate not trusted. Certificate trust settings iphone.