eMudhra Certificate Remediation Guide for MacBook and iPhone

Prepared from Apple Support article HT149555 | 29 October 2026

1. Important — understand what Apple has already done

Apple states that, beginning 19 October 2026, its devices automatically block the 12 compromised eMudhra intermediate TLS certificates in Safari, Mail and apps that use Apple's networking and security frameworks. Apple also began blocking the emSign ECC Root CA - G3 on 23 October 2026. Most users do not need to take any action.

This guide covers only certificates that have been separately installed on a device or delivered through a configuration profile. It does not provide a GUI method to edit /etc/ssl/cert.pem. Apple's optional cleanup of that file on macOS is a Terminal/administrator task, not a Keychain GUI operation.

Do not delete Apple system roots or unrelated enterprise certificates. Removing a profile or certificate used for Wi-Fi, VPN, email, device authentication or other institutional services can interrupt access.

2. Which certificate names should be checked?

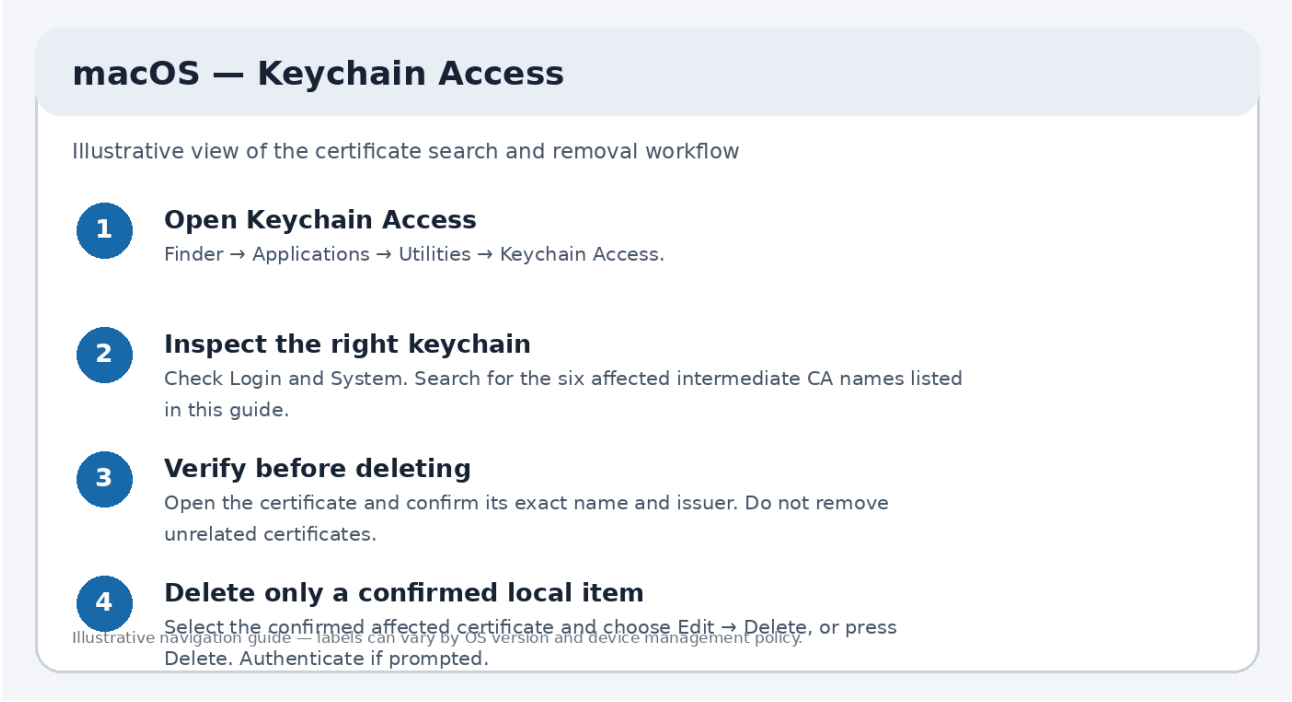
Apple identifies six affected TLS intermediate CA names. Each appears in two certificate chains (one chaining to emSign Root TLS CA - G3 and one cross-signed by Sectigo/AAA Certificate Services), making 12 certificates in total:

- EM EV TLS CA - G3B
- EM OV TLS CA - G3B
- EM DV TLS CA - G3B
- EM EV TLS CA - G3C
- EM OV TLS CA - G3C
- EM DV TLS CA - G3C

The two root CA names relevant to Apple's optional macOS cert.pem cleanup are emSign ECC Root CA - G3 and AAA Certificate Services. These are not the six intermediate CA names above. Do not remove either root from Keychain merely because its name appears here; follow your organisation's security/change process.

3. MacBook — inspect and remove a separately installed certificate

Use this procedure only when IT has confirmed that the affected certificate is present in a user-managed keychain. Menu wording may differ slightly between macOS versions.



Open Keychain Access

In Finder, choose Applications → Utilities → Keychain Access. You can also use Spotlight (Command-Space) and search for “Keychain Access”.

Search the keychains

Select Login first, then System if appropriate. Search each of the six exact intermediate CA names in Section 2. Do not modify System Roots.

Verify the certificate

Double-click a matching result. Confirm the exact certificate name and inspect its issuer/details. If the name or issuer does not match, stop and ask IT.

Delete a confirmed affected item

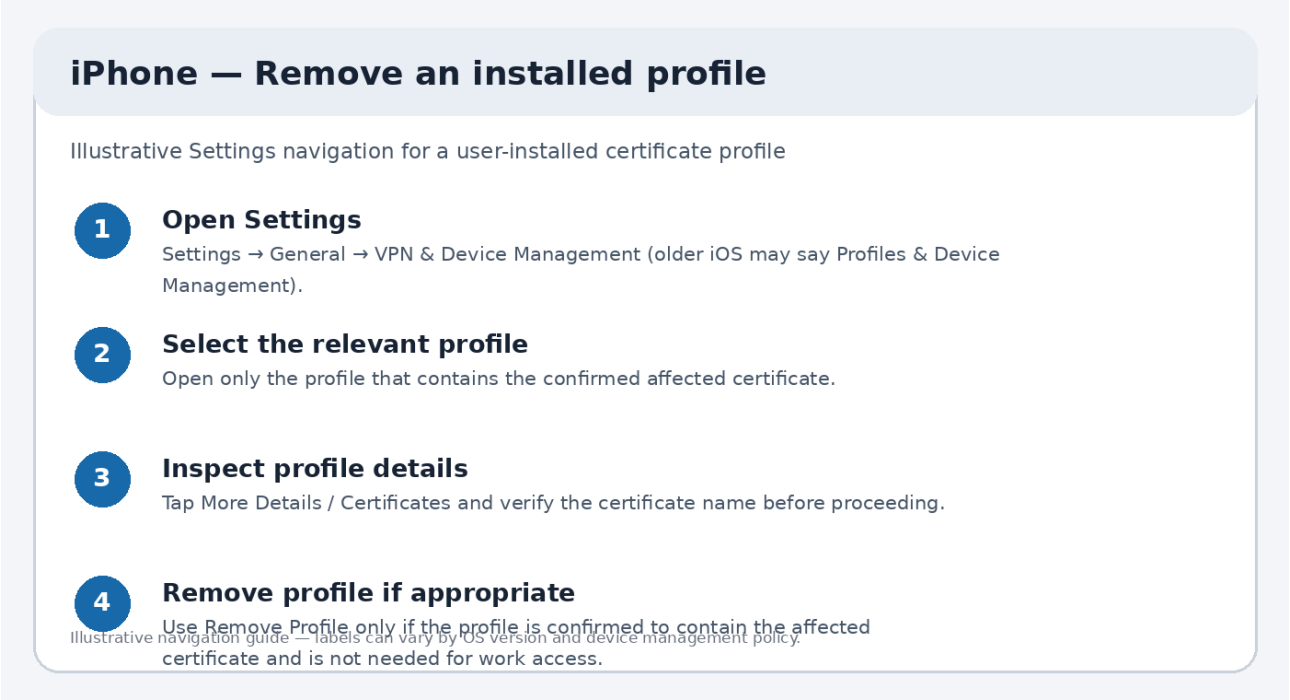
Select only the confirmed certificate and choose Edit → Delete (or press Delete). Approve the macOS authentication prompt if required.

Check dependent services

Reconnect and test Wi-Fi, VPN, email and any application that may rely on the certificate. If access fails, contact IT rather than deleting additional certificates.

4. iPhone — inspect and remove a separately installed certificate profile

The iPhone does not provide a general-purpose certificate manager equivalent to macOS Keychain Access. A user-installed certificate is commonly delivered inside a configuration profile. Removing the profile may remove several settings at once.



Open Device Management

Go to Settings → General → VPN & Device Management. Depending on iOS version, the screen may be labelled Profiles & Device Management.

Select the relevant profile

Review the listed management/configuration profiles. Open only the profile identified by IT as containing the affected certificate.

Inspect the details

Tap More Details or the certificate details section. Confirm the certificate name against Section 2. If the certificate is not visible or the profile is managed by your organisation, contact IT.

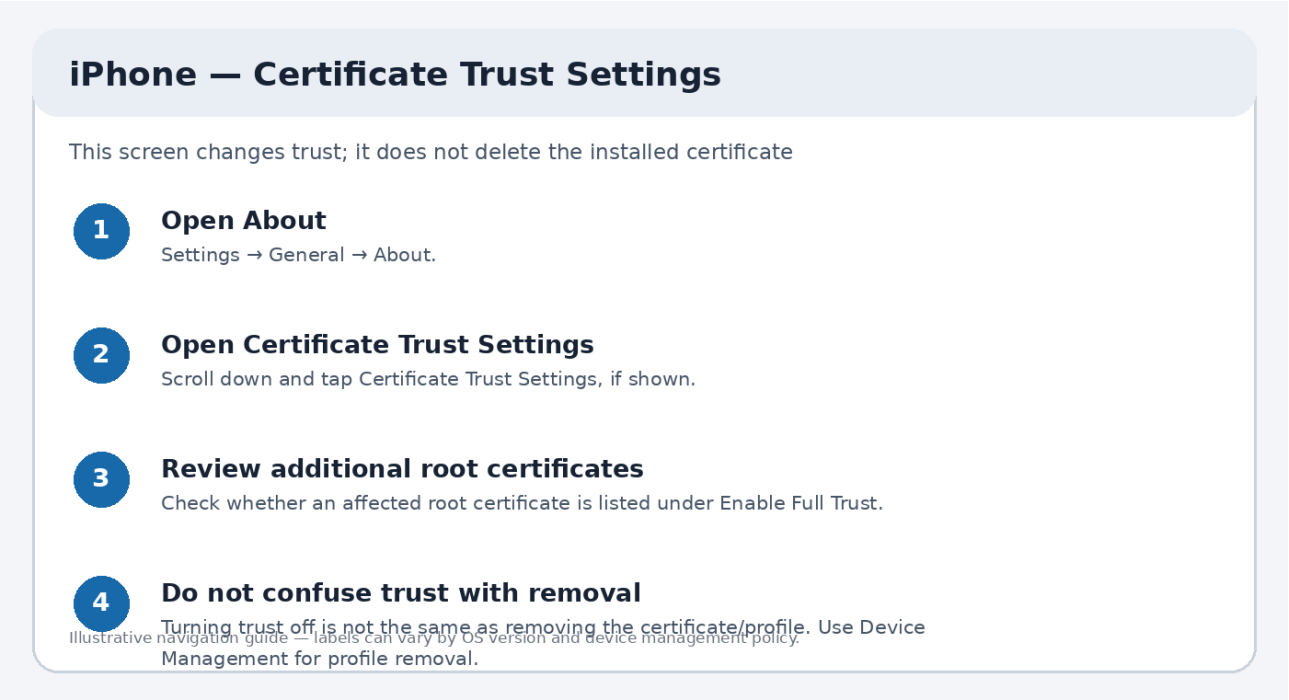
Remove only with authorisation

If the profile is user-installed and IT confirms it is safe to remove, select Remove Profile and authenticate. If the profile is organisation-managed or removal is unavailable, the administrator must remove/update it through the MDM service.

Test connectivity

Check institutional Wi-Fi, VPN, mail and work apps. Re-enrol or reinstall a replacement profile only when instructed by IT.

5. iPhone — Certificate Trust Settings (not a deletion screen)



Path: Settings → General → About → Certificate Trust Settings. This screen appears only when additional manually installed root certificates are present. Turning off full trust changes whether iOS trusts a root certificate for SSL/TLS; it does not remove the certificate or its configuration profile. For removal, use VPN & Device Management as described in Section 4.

6. What this GUI guide does not do

Apple's optional macOS procedure for removing emSign ECC Root CA - G3 and, optionally, AAA Certificate Services from /etc/ssl/cert.pem is performed in Terminal. Keychain Access does not edit this PEM file. This file is used by some command-line tools (for example curl and git), and Apple says most users do not need to edit it. Apple also says a future macOS software update will include the corresponding changes.

If NCU uses command-line tools that rely on /etc/ssl/cert.pem, the IT administrator should assess Apple's Terminal procedure separately, test it on a pilot Mac, preserve the backup, and plan verification/rollback. Do not ask end users to run privileged commands.

7. Suggested verification checklist

- Confirm macOS/iOS version and whether the device is organisation-managed.
- Confirm whether the affected certificate is actually installed as a user-managed item/profile.
- Record the exact certificate name and issuer before making a change.
- Confirm that the profile is not required for institutional Wi-Fi, VPN, email or device authentication.
- Remove only the confirmed affected certificate/profile with change approval.
- Verify Wi-Fi, VPN, email, browser access and relevant work applications after removal.
- Record device identifier, date, action taken and outcome in the helpdesk ticket.

8. Official Apple references

- **About the compromised eMudhra intermediate CAs (HT149555):** https://support.apple.com/en-us/149555
- **Distribute certificates to Apple devices — removal guidance:** https://support.apple.com/guide/deployment/distribute-certificates-depcdc9a6a3f/1/web/1.0
- **Trust manually installed certificate profiles in iOS/iPadOS:** https://support.apple.com/en-in/102390