Understand SSL Certificate and Handshake Errors in Secure Access

Contents

Issue

HTTP traffic blocked due to certificate and TLS errors can now be viewed on the Dashboard Activity Search. This article provides a list of common error messages as well as a brief explanation for each of the errors.

Environment

- Cisco Secure Access — Secure Web Gateway SSL Inspection

Resolution

Upstream Certificate Expired

The website's certificate has passed its expiration date, so Cisco Secure Access does not trust it. This one is on the website owner to fix, so reach out to the site's webmaster and let them know.

Upstream Certificate Self-signed

The website is presenting a certificate it signed itself, rather than one issued by a trusted Certificate Authority. Because no independent authority is vouching for it, Cisco Secure Access has no way to confirm the certificate is genuine.

You often see self-signed certificates on resources meant for a small, internal audience — the admin portals on IT security appliances are a classic example. Just note that Cisco Secure Access cannot be set up to trust self-signed certificates.

Missing Intermediate Certificate

Cisco Secure Access could not gather all the intermediate certificates it needs, so it cannot build the complete chain of trust back to a root.

Here is why that matters: a website's certificate (the "leaf") is signed by an intermediate certificate, which can in turn be signed by another intermediate, and so on up to a trusted root. For this chain to check out, the website has to send its intermediate certificate(s) along with its own. When those are missing, validation breaks down — so let the site's webmaster know.

There is one exception: if the certificate includes the "Authority Information Access" (AIA) extension, Cisco Secure Access can try to fetch the missing intermediates on its own. Keep in mind this only works when both HTTPS Decryption and File Inspection are turned on.

Upstream Certificate Missing Subject Name

The certificate does not include a Subject name (a Distinguished Name) or a Subject Alternative Name, which means there is nothing that clearly identifies who the certificate belongs to. Without that, Cisco Secure Access cannot validate it. This is something the website owner needs to correct.

Upstream Certificate Missing Common Name

The certificate has no Common Name (CN) — the field that traditionally held the site's hostname and helped confirm the certificate actually belongs to the site you're visiting. These days, that check really depends on the Subject Alternative Name (SAN), and CN is considered a legacy field, but its absence can still trigger this error. Reach out to the webmaster to have it addressed.

Upstream Certificate Untrusted

Cisco Secure Access does not trust this certificate, usually because it does not recognize the Root CA that issued it.

Cisco Secure Access SWG keeps a built-in list of trusted Root Certificate Authorities, sourced from a reputable provider and kept up to date. If a site's certificate traces back to a CA that is not on that list, validation fails. If you are confident the Root CA is one that can be trusted, get in touch with technical support and we can take a look.

Hostname in Cert is Different from Expected

The address you requested does not match the name on the certificate — neither its Common Name (CN) nor any of its Subject Alternative Names (SAN). Since the certificate does not appear to belong to the site you are reaching, Cisco Secure Access does not trust it for this request. The webmaster needs to sort this out.

Upstream Certificate Revoked

The Certificate Authority that issued this certificate has since revoked it — in other words, it is no longer considered valid.

Cisco Secure Access confirms this using Online Certificate Status Protocol (OSCP), which checks in real time whether a certificate has been revoked. Let the site's webmaster know so they can replace it.

TLS Handshake Errors

Unsupported Upstream Cipher

The TLS handshake could not be completed because the website does not support any of the cipher suites Cisco Secure Access SWG uses. This tends to show up with older or outdated servers that only offer weaker ciphers. The fix is on the server side, so pass it along to the webmaster.

Upstream TLS Version Mismatch

The handshake failed because the website is not using a TLS version that Cisco Secure Access SWG supports. Right now, the Cisco Secure Access SWG proxy works with TLS 1.2 and TLS 1.3 — both for connections coming in from clients and for connections it makes out to destination servers.

Upstream DH key less than 1024 bits

The handshake could not complete because the website is using a Diffie-Hellman key that is too weak (under 1024 bits) for Cisco Secure Access to accept. This is a server-side limitation, so the webmaster needs to strengthen it.

Workarounds

It is possible to workaround these issues by making configuration changes in Cisco Secure Access.

This must only be done if you trust the authenticity of the server and certificate.

Workarounds can be applied using a "Selective Decryption List" entry to disable decryption or an "External Domains" entry to bypass the traffic from Cisco Secure Access entirely. Cisco Secure access does not perform certificate validation when decryption is disabled.

Be aware that in the majority of cases the browser still presents an error or warning when the traffic is bypassed from Cisco Secure Access - Web browsers perform similar certificate validation.

Cause

Cisco Secure Access SSL inspection proxy could not complete the TLS handshake — most commonly because the destination uses certificate pinning that rejects the CSA re-signed certificate.

• **Certificate pinning:** client hard-codes expected cert fingerprint

• **CSA CA not trusted on endpoint:** inspection CA cert not deployed to trusted root store

Related Content

- Cisco Technical Support & Downloads