



Android app showing blank page

Symptoms

The Android app shows a blank page, but the site works fine on iOS, desktop, and mobile browsers.

Cause

It is known that Android is more sensitive to SSL Certificates, and whilst it is OK to access the URL above in the browser, it may not be fine in the mobile app.

SSL Certificate needs to be in an A+ rating

Here is an example of a screenshot comparing a correct SSL configuration (Right) and an incorrect one (Left) through the SSL Diagnostic tool.

<https://digicert.com/help>

DigiCert, Inc. [US] | <https://www.digicert.com/help/>

digicert SSL PKI IoT Solutions About Support

SSL Certificate Checker

If you are having a problem with your SSL certificate installation, please enter the name of your server. Our installation diagnostics tool will help you locate the problem and verify your SSL Certificate installation.

Server Address: (Ex: www.digicert.com)

http://community.carit...

Check for common vulnerabilities

CHECK SERVER

- ✔ DNS resolves community.caritas.org to 35.186.201.26
- ✔ HTTP Server Header: Apache
- ✔ SSL certificate
 - Common Name = community.caritas.org
 - Subject Alternative Names = community.caritas.org
 - Issuer = DigiCert SHA2 Extended Validation Server CA
 - Serial Number = 0B4AB69F05D709DC9A897155E5906293
 - SHA1 Thumbprint = 548FC2B8984388C545C217054A8F9FD329038C3
 - Key Length = 2048
 - Signature algorithm = SHA256 + RSA (excellent)
 - Secure Renegotiation: Supported
- ✔ SSL Certificate has not been revoked
 - OCSP Staple: Not Enabled
 - OCSP Origin: Not Enabled
 - CRL Status: Not Enabled
- ✔ SSL Certificate expiration
 - The certificate expires October 9, 2019 (251 days from today)
- ✔ Certificate Name matches community.caritas.org



Subject: community.caritas.org
Valid from 01/Oct/2018 to 09/Oct/2019
Issuer: DigiCert SHA2 Extended Validation Server CA

✘ The server is not sending the required intermediate certificate.

In most cases, solving this problem in Apache is as simple as adding "SSLCertificateChainFile /path/to/DigiCertCA.crt" to your apache configuration file after/near your SSLCertificateFile line. If you manage this server, you can download the file from [this link](#) or from your customer account area. Follow the directions on our [certificate installation guide](#) to install the missing intermediate.

DigiCert, Inc. [US] | <https://www.digicert.com/help/>

digicert SSL PKI IoT Solutions About Support

SSL Certificate Checker

If you are having a problem with your SSL certificate installation, please enter the name of your server. Our installation diagnostics tool will help you locate the problem and verify your SSL Certificate installation.

Server Address: (Ex: www.digicert.com)

https://ivicad.myintranet

Check for common vulnerabilities

CHECK SERVER

- ✔ DNS resolves ivicad.myintranet.com to 104.196.110.143
- ✔ HTTP Server Header: Apache
- ✔ SSL certificate
 - Common Name = *.myintranet.com
 - Subject Alternative Names = *.myintranet.com, myintranet.com
 - Issuer = DigiCert SHA2 Secure Server CA
 - Serial Number = 0EB5FDE0D59580E2A7FA99FE876B98D0
 - SHA1 Thumbprint = 6F32671267CC0E366085F60F94B5B858F50248D
 - Key Length = 2048
 - Signature algorithm = SHA256 + RSA (excellent)
 - Secure Renegotiation: Supported
- ✔ SSL Certificate has not been revoked
 - OCSP Staple: Not Enabled
 - OCSP Origin: Good
 - CRL Status: Good
- ✔ SSL Certificate expiration
 - The certificate expires July 15, 2020 (531 days from today)
- ✔ Certificate Name matches ivicad.myintranet.com



Subject: *.myintranet.com
Valid from 11/Jul/2017 to 15/Jul/2020
Issuer: DigiCert SHA2 Secure Server CA



Subject: DigiCert SHA2 Secure Server CA
Valid from 08/Mar/2013 to 08/Mar/2023
Issuer: DigiCert Global Root CA

TLS Certificate Status must be validated/trusted

- ✔ DNS resolves [redacted] to [redacted]
- HTTP Server Header: Microsoft-IIS/10.0
- ⚠ The Certificate is not issued by DigiCert, GeoTrust, Thawte, or RapidSSL

Make sure the website you want to check is secured by a certificate from one of our product lines.

⚠ **TLS Certificate status cannot be validated**

- OCSP Staple: Not Enabled
- OCSP Origin: Not Enabled
- CRL Status: Not Enabled

- ✔ TLS Certificate expiration
 - The certificate expires August 5, 2026 (133 days from today)
- ✔ Certificate Name matches [redacted]



Subject: [redacted]
Valid from 07/Jul/2025 to 05/Aug/2026
Issuer: Sectigo Public Server Authentication CA DV R36



Subject: Sectigo Public Server Authentication CA DV R36
Valid from 22/Mar/2021 to 21/Mar/2036
Issuer: Sectigo Public Server Authentication Root R46

✘ TLS Certificate is not trusted

The certificate is not signed by a trusted authority (checking against Mozilla's root store). If you bought the certificate from a trusted authority, you probably just need to install one or more intermediate certificates. Contact your certificate provider for assistance doing this for your server platform.

Solution

Missing intermediate certificate

Install the missing chain certificate(s) on your web server to bridge the gap between your site certificate and the trusted root authority.

TLS Certificate Not Trusted

Ensure the certificate is valid, properly installed, and issued by a trusted authority.

Common solutions include updating your system date, installing missing intermediate certificates, renewing expired certificates, or ensuring the domain name matches the certificate.

How to fix

Server-Side Fixes (For Website Owners)

- **Install Intermediate Certificates:** Ensure the entire certificate chain (Root CA -> Intermediate CA -> Server Certificate) is installed on the server.
- **Verify Domain Match:** Confirm the domain name in the certificate exactly matches the URL, including www and non-www versions.
- **Renew Expired Certificate:** Check the expiration date and renew if necessary.
- **Use Trusted CAs:** Replace self-signed certificates with those from trusted authorities like Let's Encrypt, DigiCert, or Comodo.
- **Check Chain of Trust:** Use online tools like SSL Labs to test your site and identify missing links in the certificate chain

Last modified on 31 March 2026 by [Hannah Door](#)

Created on 24 March 2026 by [Michael Christian](#)