Qualys. SSL Labs

Home Projects Qualys Free Trial Contact

You are here: Home > Projects > SSL Server Test > euw1-app-server.iot.i.tplinknbu.com > 54.170.21.120

# SSL Report: euw1-app-server.iot.i.tplinknbu.com (54.170.21.120)

**Assessed on:** Sun, 16 Jun 2024 16:43:28 UTC | Hide | Clear cache

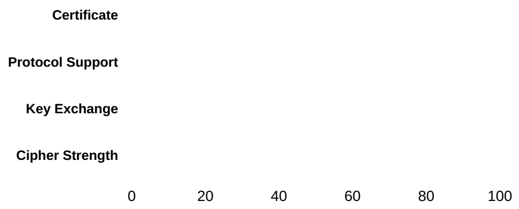
**Scan Another »**

## Summary

**Overall Rating**

# T

**If trust issues are ignored: B**



**Visit our documentation page for more information, configuration guides, and books. Known issues are documented here.**

**This server's certificate is not trusted, see below for details.**

**There is no support for secure renegotiation.** MORE INFO »

**This server supports TLS 1.0 and TLS 1.1. Grade capped to B.** MORE INFO »

## Certificate #1: RSA 2048 bits (SHA256withRSA)

### Server Key and Certificate #1

| | |
|---|---|
| **Subject** | *.tplinknbu.com<br>Fingerprint SHA256: e101dffa3878384ea73716dcec18be956d92c9183d75338dde9ec06ee26d0e96<br>Pin SHA256: czChulbLa+RN7mJdSNLup0uD+Kjvx5zUk3kqYpJ9AIU= |
| **Common names** | *.tplinknbu.com |
| **Alternative names** | *.tplinknbu.com *.i.tplinknbu.com *.iot.i.tplinknbu.com *.tapo-care.i.tplinknbu.com *.tapo-care-beta.i.tplinknbu.com *.dcipc.i.tplinknbu.com *.dcipc-beta.i.tplinknbu.com |
| **Serial Number** | 6400000129da0b0ba4ee9a570c000100000129 |
| **Valid from** | Wed, 24 Jan 2024 09:30:51 UTC |
| **Valid until** | Thu, 23 Jan 2025 09:30:51 UTC (expires in 7 months and 6 days) |
| **Key** | RSA 2048 bits (e 65537) |
| **Weak key (Debian)** | No |
| **Issuer** | TP-LINK CA P1 |
| **Signature algorithm** | SHA256withRSA |
| **Extended Validation** | No |
| **Certificate Transparency** | No |
| **OCSP Must Staple** | No |
| **Revocation information** | CRL<br>CRL: http://tpcrl.tp-link.com.cn/certdata/TP-LINK_CA_P1.crl |
| **Revocation status** | Unchecked (only trusted certificates can be checked) |
| **DNS CAA** | No (more info) |
| **Trusted** | No **NOT TRUSTED** (Why?)<br>**Mozilla Apple Android Java Windows** |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Certificates provided** | 3 (3094 bytes) |
| **Chain issues** | **Contains anchor** |

**#2**

| | |
|---|---|
| **Subject** | TP-LINK CA P1<br>Fingerprint SHA256: f3bf84760ea3d5b61b7fea1732d515b3bb3ac7bce149d9458265c3180a8c5740<br>Pin SHA256: FWN0bUK+G5UtW1TnZEs2o7RvMbuwcVO5Dv69SGU/xwQ= |
| **Valid until** | Thu, 19 Jan 2068 08:37:52 UTC (expires in 43 years and 7 months) |

### Additional Certificates (if supplied)

| | |
|---|---|
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | tp-link-CA |
| **Signature algorithm** | SHA256withRSA |

#### #3

| | |
|---|---|
| **Subject** | tp-link-CA Not in trust store<br>Fingerprint SHA256: 8b54f0364e840fb010d517324725f0d30245d35b45f9be4b6e50b84f03fdec19<br>Pin SHA256: esp3Rf3jZTN/NshwLAi/Yv76ZLtGJYHByPCPpCDc2Kg= |
| **Valid until** | Thu, 19 Jan 2068 08:37:52 UTC (expires in 43 years and 7 months) |
| **Key** | RSA 2048 bits (e 65537) |
| **Issuer** | tp-link-CA Self-signed |
| **Signature algorithm** | SHA256withRSA |

### Certification Paths ⊞

Click here to expand

## Configuration

### Protocols

| | |
|---|---|
| TLS 1.3 | No |
| TLS 1.2 | Yes |
| TLS 1.1 | Yes |
| TLS 1.0 | Yes |
| SSL 3 | No |
| SSL 2 | No |

### Cipher Suites

#### # TLS 1.2 (suites in server-preferred order) ⊟

| | |
|---|---|
| TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f) ECDH secp256r1 (eq. 3072 bits RSA) FS | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 (0xc027) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK** | 128 |
| TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030) ECDH secp256r1 (eq. 3072 bits RSA) FS | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384 (0xc028) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014) ECDH secp256r1 (eq. 3072 bits RSA) FS **WEAK** | 256 |
| TLS_RSA_WITH_AES_128_GCM_SHA256 (0x9c) **WEAK** | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c) **WEAK** | 128 |
| TLS_RSA_WITH_AES_128_CBC_SHA (0x2f) **WEAK** | 128 |
| TLS_RSA_WITH_AES_256_GCM_SHA384 (0x9d) **WEAK** | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d) **WEAK** | 256 |
| TLS_RSA_WITH_AES_256_CBC_SHA (0x35) **WEAK** | 256 |

#### # TLS 1.1 (suites in server-preferred order) ⊞

#### # TLS 1.0 (suites in server-preferred order) ⊞

### Handshake Simulation

| | | | |
|---|---|---|---|
| Android 2.3.7 No SNI [2] | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA No FS |
| Android 4.0.4 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.1.1 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.2.2 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.3 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA ECDH secp256r1 FS |
| Android 4.4.2 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 5.0.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 6.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 7.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 8.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |
| Android 8.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 ECDH secp256r1 FS |

## Handshake Simulation

| | | | | | |
|---|---|---|---|---|---|
| Android 9.0 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Baidu Jan 2015 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1 | FS |
| BingPreview Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Chrome 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Chrome 69 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Chrome 70 / Win 10 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Chrome 80 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 31.3.0 ESR / Win 7 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 47 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 49 / XP SP3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 62 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Firefox 73 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Googlebot Feb 2018 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| IE 7 / Vista | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1 | FS |
| IE 8 / XP No FS[1] No SNI[2] | Server sent fatal alert: handshake_failure | | | | |
| IE 8-10 / Win 7 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1 | FS |
| IE 11 / Win 7 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| IE 11 / Win 8.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| IE 10 / Win Phone 8.0 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1 | FS |
| IE 11 / Win Phone 8.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| IE 11 / Win Phone 8.1 Update R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| IE 11 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Edge 15 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Edge 16 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Edge 18 / Win 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Edge 13 / Win Phone 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Java 6u45 No SNI[2] | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA | No FS | |
| Java 7u25 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1 | FS |
| Java 8u161 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Java 11.0.3 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Java 12.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| OpenSSL 0.9.8y | RSA 2048 (SHA256) | TLS 1.0 | TLS_RSA_WITH_AES_128_CBC_SHA | No FS | |
| OpenSSL 1.0.1l R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| OpenSSL 1.0.2s R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| OpenSSL 1.1.0k R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| OpenSSL 1.1.1c R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Safari 5.1.9 / OS X 10.6.8 | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1 | FS |
| Safari 6 / iOS 6.0.1 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| Safari 6.0.4 / OS X 10.8.4 R | RSA 2048 (SHA256) | TLS 1.0 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA | ECDH secp256r1 | FS |
| Safari 7 / iOS 7.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| Safari 7 / OS X 10.9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| Safari 8 / iOS 8.4 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| Safari 8 / OS X 10.10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 | ECDH secp256r1 | FS |
| Safari 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Safari 9 / OS X 10.11 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Safari 10 / iOS 10 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Safari 10 / OS X 10.12 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Safari 12.1.2 / MacOS 10.14.6 Beta R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Safari 12.1.1 / iOS 12.3.1 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Apple ATS 9 / iOS 9 R | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| Yahoo Slurp Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |
| YandexBot Jan 2015 | RSA 2048 (SHA256) | TLS 1.2 | TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 | ECDH secp256r1 | FS |

### # Not simulated clients (Protocol mismatch)

| | |
|---|---|
| IE 6 / XP No FS[1] No SNI[2] | Protocol mismatch (not simulated) |

(1) Clients that do not support Forward Secrecy (FS) are excluded when determining support for it.

(2) No support for virtual SSL hosting (SNI). Connects to the default site if the server uses SNI.

(3) Only first connection attempt simulated. Browsers sometimes retry with a lower protocol version.

(R) Denotes a reference browser or client, with which we expect better effective security.

(All) We use defaults, but some platforms do not use their best protocols and features (e.g., Java 6 & 7, older IE).

### Handshake Simulation

**(All) Certificate trust is not checked in handshake simulation, we only perform TLS handshake.**

### Protocol Details

| | |
|---|---|
| **Secure Renegotiation** | **Not supported ACTION NEEDED** (more info) |
| **Secure Client-Initiated Renegotiation** | Yes |
| **Insecure Client-Initiated Renegotiation** | No |
| **BEAST attack** | Not mitigated server-side (more info) TLS 1.0: `0xc013` |
| **POODLE (SSLv3)** | No, SSL 3 not supported (more info) |
| **POODLE (TLS)** | No (more info) |
| **Zombie POODLE** | No (more info) TLS 1.2 : `0xc027` |
| **GOLDENDOODLE** | No (more info) TLS 1.2 : `0xc027` |
| **OpenSSL 0-Length** | No (more info) TLS 1.2 : `0xc027` |
| **Sleeping POODLE** | No (more info) TLS 1.2 : `0xc027` |
| **Downgrade attack prevention** | No, TLS_FALLBACK_SCSV not supported (more info) |
| **SSL/TLS compression** | No |
| **RC4** | No |
| **Heartbeat (extension)** | No |
| **Heartbleed (vulnerability)** | No (more info) |
| **Ticketbleed (vulnerability)** | No (more info) |
| **OpenSSL CCS vuln. (CVE-2014-0224)** | No (more info) |
| **OpenSSL Padding Oracle vuln. (CVE-2016-2107)** | No (more info) |
| **ROBOT (vulnerability)** | No (more info) |
| **Forward Secrecy** | With modern browsers (more info) |
| **ALPN** | No |
| **NPN** | No |
| **Session resumption (caching)** | **No (IDs assigned but not accepted)** |
| **Session resumption (tickets)** | No |
| **OCSP stapling** | No |
| **Strict Transport Security (HSTS)** | No |
| **HSTS Preloading** | **Not in: Chrome Edge Firefox IE** |
| **Public Key Pinning (HPKP)** | No (more info) |
| **Public Key Pinning Report-Only** | No |
| **Public Key Pinning (Static)** | No (more info) |
| **Long handshake intolerance** | No |
| **TLS extension intolerance** | No |
| **TLS version intolerance** | No |
| **Incorrect SNI alerts** | No |
| **Uses common DH primes** | No, DHE suites not supported |
| **DH public server param (Ys) reuse** | No, DHE suites not supported |
| **ECDH public server param reuse** | No |
| **Supported Named Groups** | secp256r1 |
| **SSL 2 handshake compatibility** | Yes |

### HTTP Requests

➕

1 **https://euw1-app-server.iot.i.tplinknbu.com/** (HTTP/1.1 404 Not Found)

### Miscellaneous

| | |
|---|---|
| **Test date** | Sun, 16 Jun 2024 16:35:41 UTC |
| **Test duration** | 121.525 seconds |
| **HTTP status code** | 404 |
| **HTTP server signature** | istio-envoy |
| **Server hostname** | ec2-54-170-21-120.eu-west-1.compute.amazonaws.com |

## Why is my certificate not trusted?

There are many reasons why a certificate may not be trusted. The exact problem is indicated on the report card in bright red. The problems fall into three categories:

1. Invalid certificate
2. Invalid configuration
3. Unknown Certificate Authority

**1. Invalid certificate**

A certificate is invalid if:

- It is used before its activation date
- It is used after its expiry date
- Certificate hostnames don't match the site hostname
- It has been revoked
- It has insecure signature
- It has been blacklisted

**2. Invalid configuration**

In some cases, the certificate chain does not contain all the necessary certificates to connect the web server certificate to one of the root certificates in our trust store. Less commonly, one of the certificates in the chain (other than the web server certificate) will have expired, and that invalidates the entire chain.

**3. Unknown Certificate Authority**

In order for trust to be established, we must have the root certificate of the signing Certificate Authority in our trust store. SSL Labs does not maintain its own trust store; instead we use the store maintained by Mozilla.

If we mark a web site as not trusted, that means that the average web user's browser will not trust it either. For certain special groups of users, such web sites can still be secure. For example, if you can securely verify that a self-signed web site is operated by a person you trust, then you can trust that self-signed web site too. Or, if you work for an organisation that manages its own trust, and you have their own root certificate already embedded in your browser. Such special cases do not work for the general public, however, and this is what we indicate on our report card.

**4. Interoperability issues**

In some rare cases trust cannot be established because of interoperability issues between our code and the code or configuration running on the server. We manually review such cases, but if you encounter such an issue please feel free to contact us. Such problems are very difficult to troubleshoot and you may be able to provide us with information that might help us determine the root cause.

SSL Report v2.3.0