


SSL Report: www.fsf.org

Home Projects Qualys.com Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.fsf.org](#)

SSL Report: www.fsf.org

Assessed on: Sat, 13 May 2017 17:17:18 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	208.118.235.174 www.fsf.org Ready	Sat, 13 May 2017 17:15:42 UTC Duration: 80.981 sec	A-
2	2001:4830:134:4:0:0:0:a www.fsf.org Unable to connect to the server	Sat, 13 May 2017 17:17:03 UTC Duration: 15.10 sec	.


Warning: Inconsistent server configuration

SSL Report v1.28.5

Copyright © 2009-2017 [Qualys, Inc.](#) All Rights Reserved. [Terms and Conditions](#)

Qualys is the leading provider of integrated [asset discovery](#), [network security](#), [threat protection](#), [compliance monitoring](#) and [web application security](#) solutions.

<http://www.fnmt.es/>

Home Projects Qualys.com Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.fnmt.es](#)

SSL Report: www.fnmt.es (193.104.0.100)

Assessed on: Sat, 13 May 2017 17:20:46 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

Assessment failed: Unable to connect to the server

Known Problems

There are some errors that we cannot fix properly in the current version. They will be addressed in the next generation version, which is currently being developed.

- No secure protocols supported** - if you get this message, but you know that the site supports SSL, wait until the cache expires on its own, then try again, making sure the hostname you enter uses the "www" prefix (e.g., "www.ssllabs.com", not just "ssllabs.com").
- no more data allowed for version 1 certificate** - the certificate is invalid; it is declared as version 1, but uses extensions, which were introduced in version 3. Browsers might ignore this problem, but our parser is strict and refuses to proceed. We'll try to find a different parser to avoid this problem.
- Failed to obtain certificate and Internal Error** - errors of this type will often be reported for servers that use connection rate limits or block connections in response to unusual traffic. Problems of this type are very difficult to diagnose. If you have access to the server being tested, before reporting a problem to us, please check that there is no rate limiting or IDS in place.
- NetScaler issues** - some NetScaler versions appear to reject SSL handshakes that do not include certain suites or handshakes that use a few suites. If the test is failing and there is a NetScaler load balancer in place, that's most likely the reason.
- Unexpected failure** - our tests are designed to fail when unusual results are observed. This usually happens when there are multiple TLS servers behind the same IP address. In such cases we can't provide accurate results, which is why we fail.

Common Error Messages

- Connect timed out** - server did not respond to our connection request, sometimes before we are dynamically blocked when our tests are detected
- No route to host** - unable to reach the server
- Unable to connect to server** - failed to connect to the server, it usually happens due to firewall restrictions
- Connection reset** - we got disconnected from the server
- Unrecognized SSL message, plaintext connection?** - the server responded with plain-text HTTP on HTTPS port
- Received fatal alert: handshake_failure** - this is either a faulty SSL server or some other server listening on port 443; if the SSL version of the web site works in your browser, please report this issue to us

<http://www.agpd.es>

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.agpd.es

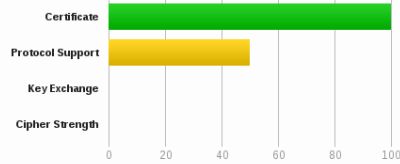
SSL Report: www.agpd.es (212.170.244.21)

Assessed on: Sat, 13 May 2017 17:27:09 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server supports insecure cipher suites (see below for details). Grade set to F.

This server supports insecure Diffie-Hellman (DH) key exchange parameters (Logjam). Grade set to F. [MORE INFO »](#)

This server supports 512-bit export suites and might be vulnerable to the FREAK attack. Grade set to F. [MORE INFO »](#)

This server is vulnerable to the POODLE attack. If possible, disable SSL 3 to mitigate. Grade capped to C. [MORE INFO »](#)

Intermediate certificate has an insecure signature. Upgrade to SHA2 as soon as possible to avoid browser warnings. [MORE INFO »](#)

The server supports only older protocols, but not the current best TLS 1.2. Grade capped to C. [MORE INFO »](#)

This server accepts RC4 cipher, but only with older protocols. Grade capped to B. [MORE INFO »](#)

<http://www.pp.es/>



[Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > www.pp.es

SSL Report: www.pp.es (217.116.18.213)

Assessed on: Sat, 13 May 2017 17:29:49 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Assessment failed: Unable to connect to the server

Known Problems


There are some errors that we cannot fix properly in the current version. They will be addressed in the next generation version, which is currently being developed.

- **No secure protocols supported** - if you get this message, but you know that the site supports SSL, wait until the cache expires on its own, then try again, making sure the hostname you enter uses the "www" prefix (e.g., "www.ssllabs.com", not just "ssllabs.com").
- **no more data allowed for version 1 certificate** - the certificate is invalid, it is declared as version 1, but uses extensions, which were introduced in version 3. Browsers might ignore this problem, but our parser is strict and refuses to proceed. We'll try to find a different parser to avoid this problem.
- **Failed to obtain certificate and Internal Error** - errors of this type will often be reported for servers that use connection rate limits or block connections in response to unusual traffic. Problems of this type are very difficult to diagnose. If you have access to the server being tested, before reporting a problem to us, please check that there is no rate limiting or IDS in place.
- **NetScaler issues** - some NetScaler versions appear to reject SSL handshakes that do not include certain suites or handshakes that use a few suites. If the test is failing and there is a NetScaler load balancer in place, that's most likely the reason.
- **Unexpected failure** - our tests are designed to fail when unusual results are observed. This usually happens when there are multiple TLS servers behind the same IP address. In such cases we can't provide accurate results, which is why we fail.

Common Error Messages

- **Connect timed out** - server did not respond to our connection request, sometimes before we are dynamically blocked when our tests are detected
- **No route to host** - unable to reach the server
- **Unable to connect to server** - failed to connect to the server, it usually happens due to firewall restrictions
- **Connection reset** - we got disconnected from the server
- **Unrecognized SSL message, plaintext connection?** - the server responded with plain-text HTTP on HTTPS port
- **Received fatal alert: handshake_failure** - this is either a faulty SSL server or some other server listening on port 443; if the SSL version of the web site works in your browser, please report this issue to us

<http://www.psoe.es/>

Home Projects Qualys.com Contact

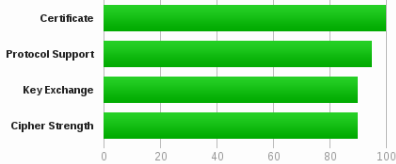

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.psoe.es](#)

SSL Report: [www.psoe.es](#) (199.83.134.231)

Assessed on: Sat, 13 May 2017 17:36:32 UTC | [Hide](#) | [Clear cache](#) [Scan Another »](#)

Summary

Overall Rating



Category	Score
Certificate	100
Protocol Support	95
Key Exchange	90
Cipher Strength	90


Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

This server is vulnerable to the DROWN attack. Grade set to F. [MORE INFO >](#)

This site works only in browsers with SNI support.

Certificate #1: RSA 4096 bits (SHA256withRSA)

<https://www.nasa.gov/>

Home Projects Qualys.com Contact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.nasa.gov](#)

SSL Report: [www.nasa.gov](#)

Please wait... ⌂

	Server	Test time	Grade
1	208.111.179.103 https-208-111-179-103.sea.llnwd.net In progress - 71% complete	Sat, 13 May 2017 17:40:55 UTC -	-
2	2607:f4e8:130:a000:0:0:0:e https-2607-f4e8-130-a000-e.sea.ipv6.llnwd.net Pending	- -	-

SSL Report v1.28.5

Copyright © 2009-2017 [Qualys, Inc.](#) All Rights Reserved. [Terms and Conditions](#)

Qualys is the leading provider of integrated [asset discovery](#), [network security](#), [threat protection](#), [compliance monitoring](#) and [web application security](#) solutions.

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.nasa.gov](#) > 208.111.179.103

SSL Report: [www.nasa.gov](#) (208.111.179.103)

Summary

Overall Rating



Visit our [documentation page](#) for more information, configuration guides, and books. Known issues are documented [here](#).

HTTP Strict Transport Security (HSTS) with long duration deployed on this server. [MORE INFO >](#)

Certificate #1: RSA 2048 bits (SHA256withRSA)



[Server Key and Certificate #1](#)

[www.nasa.gov](#)

www.microsoft.com

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.microsoft.com](#)

SSL Report: [www.microsoft.com](#)

Assessed on: Sat, 13 May 2017 17:50:16 UTC | [Hide](#) | [Clear cache](#)

[Scan Another >>](#)

	Server	Test time	Grade
1	2600:1406:1a:390:0:0:0:747 Ready	Sat, 13 May 2017 17:47:38 UTC Duration: 51.391 sec	A+
2	23.213.138.195 a23-213-138-195.deploy.static.akamaitechnologies.com Ready	Sat, 13 May 2017 17:48:29 UTC Duration: 55.981 sec	A+
3	2600:1406:1a:3a3:0:0:0:747 Ready	Sat, 13 May 2017 17:49:25 UTC Duration: 51.101 sec	A+

SSL Report v1.28.5

Copyright © 2009-2017 [Qualys, Inc.](#) All Rights Reserved.

Qualys is the leading provider of integrated [asset discovery](#), [network security](#), [threat protection](#), [compliance monitoring](#) and [web application security](#) solutions.

[Terms and Conditions](#)