

→ [SSL Report: www.movistar.es \(81.47.192.13\)](#)

**QUALYS<sup>®</sup> SSL LABS** Home Projects Qualys.com Contact


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

### SSL Report: [www.movistar.es](#) (81.47.192.13)

Assessed on: Sat, 13 May 2017 14:27:15 UTC | [Hide](#) | [Clear cache](#) [Scan Another >>](#)

#### Summary

Overall Rating



Certificate: 100%  
Protocol Support: 100%  
Key Exchange: 90%  
Cipher Strength: 50%

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

This server is vulnerable to the POODLE TLS attack. Patching required. Grade set to F. [MORE INFO >](#)

This server uses RC4 with modern protocols. Grade capped to C.

The server does not support Forward Secrecy with the reference browsers. [MORE INFO >](#)

→ [SSL Report: www.telefonica.es](#)

**QUALYS<sup>®</sup> SSL LABS** Home Projects Qualys.com Contact

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

### SSL Report: [www.telefonica.es](#)

Assessed on: Sat, 13 May 2017 10:18:41 UTC | [Hide](#) | [Clear cache](#) [Scan Another >>](#)

	Server	Test time	Grade
1	<a href="#">2a02:9009:0:aa:aa01:0:0:0</a> www.ipv6.telefonica.com Ready	Sat, 13 May 2017 10:15:13 UTC Duration: 106.413 sec	B
2	<a href="#">212.170.36.79</a> Ready	Sat, 13 May 2017 10:16:59 UTC Duration: 101.971 sec	B

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.

→ [SSL Report: www.telefonica.es \(2a02:9009:0:aa:aa01:0:0:0\)](#)

**QUALYS<sup>®</sup> SSL LABS** [Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.telefonica.es](#) > 2a02:9009:0:aa:aa01:0:0:0

**SSL Report: [www.telefonica.es](#) (2a02:9009:0:aa:aa01:0:0:0)** [Scan Another »](#)

Assessed on: Sat, 13 May 2017 10:18:41 UTC | [Hide](#) | [Clear cache](#)

### Summary

Overall Rating

**B**

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

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

This site works only in browsers with SNI support.

→ [SSL Report: www.telefonica.es \(212.170.36.79\)](#)

**QUALYS<sup>®</sup> SSL LABS** [Home](#) [Projects](#) [Qualys.com](#) [Contact](#)

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.telefonica.es](#) > 212.170.36.79

**SSL Report: [www.telefonica.es](#) (212.170.36.79)** [Scan Another »](#)

Assessed on: Sat, 13 May 2017 10:18:41 UTC | [Hide](#) | [Clear cache](#)

### Summary

Overall Rating

**B**

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

The server does not support Forward Secrecy with the reference browsers. [MORE INFO »](#)

This site works only in browsers with SNI support.

## SSL Report: www.inditex.com (173.222.251.228)

**QUALYS<sup>®</sup> SSL LABS** [Home](#) [Projects](#) [Qualys.com](#) [Contact](#)


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

### SSL Report: www.inditex.com (173.222.251.228)

Assessed on: Sat, 13 May 2017 14:29:57 UTC | [Hide](#) | [Clear cache](#) [Scan Another >>](#)

#### Summary

Overall Rating





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](#).

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

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

 [Server Key and Certificate #1](#) 

## → SSL Report: cadilinea.com (5.135.40.3)

**QUALYS<sup>®</sup> SSL LABS** [Home](#) [Projects](#) [Qualys.com](#) [Contact](#)


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

### SSL Report: cadilinea.com (5.135.40.3)

Assessed on: Sat, 13 May 2017 14:34:27 UTC | [Hide](#) | [Clear cache](#) [Scan Another >>](#)

#### Summary

Overall Rating





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 site works only in browsers with SNI support.

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

 [Server Key and Certificate #1](#) 

# ==> Analisis Visual del Problema → movistar.es

Cipher Suites			
# TLS 1.2 (suites in server-preferred order)			
TLS_RSA_WITH_RC4_128_SHA (0x5)	<b>INSECURE</b>		128
TLS_RSA_WITH_AES_128_CBC_SHA (0x2f)			128
TLS_RSA_WITH_AES_256_CBC_SHA (0x35)			256
TLS_RSA_WITH_3DES_EDE_CBC_SHA (0xa)	<b>WEAK</b>		112
TLS_RSA_WITH_AES_128_CBC_SHA256 (0x3c)			128
TLS_RSA_WITH_AES_256_CBC_SHA256 (0x3d)			256
# TLS 1.0 (suites in server-preferred order)			
Handshake Simulation			
<a href="#">Android 2.3.7</a>	No SH1 <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Android 4.0.4</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Android 4.1.1</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Android 4.2.2</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Android 4.3</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Android 4.4.2</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Android 5.0.0</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Android 6.0</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Android 7.0</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Baidu Jan 2015</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">BingPreview Jan 2015</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Chrome 49 / XP SP3</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Chrome 51 / Win 7</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Firefox 31.3.0 ESP / Win 7</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>

<a href="#">Firefox 43 / XP SP3</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Firefox 49 / Win 7</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Googlebot Feb 2015</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">IE 6 / XP</a>	No FS <sup>1</sup> No SH1 <sup>2</sup>	Server sent fatal alert: handshake_failure	
<a href="#">IE 7 / Vista</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">IE 8 / XP</a>	No FS <sup>1</sup> No SH1 <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA <b>RC4</b>
<a href="#">IE 8-10 / Win 7</a>	R	RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">IE 11 / Win 7</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">IE 11 / Win 8.1</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">IE 10 / Win Phone 8.0</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">IE 11 / Win Phone 8.1</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">IE 11 / Win Phone 8.1 Update</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">IE 11 / Win 10</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Edge 13 / Win 10</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Edge 13 / Win Phone 10</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_AES_128_CBC_SHA No FS
<a href="#">Java 6u45</a>	No SH1 <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Java 7u25</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Java 8u31</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">OpenSSL 0.9.8y</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">OpenSSL 1.0.1j</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">OpenSSL 1.0.2e</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>		RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Safari 6 / IOS 6.0.1</a>		RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Safari 6.0.4 / OS X 10.8.4</a>	R	RSA 2048 (SHA256)	TLS 1.0 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Safari 7 / IOS 7.1</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Safari 7 / OS X 10.9</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Safari 8 / IOS 8.4</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>
<a href="#">Safari 8 / OS X 10.10</a>	R	RSA 2048 (SHA256)	TLS 1.2 TLS_RSA_WITH_RC4_128_SHA No FS <b>RC4</b>

etc, etc, ...