

HomeProjectsQualys.comContact

You are here: [Home](#) > [Projects](#) > [SSL Server Test](#) > [www.ualberta.ca](#) > 54.85.24.187

SSL Report: [www.ualberta.ca](#) (54.85.24.187)

Assessed on: Thu, 22 Feb 2018 22:08:25 UTC | [Hide](#) | [Clear cache](#)

[Scan Another »](#)

Summary

Overall Rating

A

Certificate

Protocol Support


Key Exchange

Cipher Strength

020406080100


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

Certificate #1: RSA 2048 bits (SHA256withRSA)



Server Key and Certificate #1

Subject	www.ualberta.ca Fingerprint SHA256: b2eedb1ba85ee9c141f839796a15a233246bc57574a30384e7a456b4650740f7 Pin SHA256: yib1aISqo24OPyae4nZAxVwCenwwa5DWi8QRVr7sZC8=
Common names	www.ualberta.ca
Alternative names	www.ualberta.ca uofa.ualberta.ca med.ualberta.ca pharm.ualberta.ca rehabilitation.ualberta.ca nativestudies.ualberta.ca business.ualberta.ca nursing.ualberta.ca publichealth.ualberta.ca law.ualberta.ca lawschool.ualberta.ca alumni.ualberta.ca athletics.ualberta.ca bears.ualberta.ca pandas.ualberta.ca newtrail.ualberta.ca cs.ualberta.ca csj.ualberta.ca ctl.ualberta.ca www.uofa.ualberta.ca www.med.ualberta.ca www.pharm.ualberta.ca www.rehabilitation.ualberta.ca www.nativestudies.ualberta.ca www.business.ualberta.ca www.nursing.ualberta.ca www.publichealth.ualberta.ca www.law.ualberta.ca www.lawschool.ualberta.ca www.alumni.ualberta.ca www.athletics.ualberta.ca www.bears.ualberta.ca www.pandas.ualberta.ca www.newtrail.ualberta.ca www.cs.ualberta.ca www.csj.ualberta.ca www.ctl.ualberta.ca ualberta.ca
Serial Number	283fa539d8296ef5289ea8d3
Valid from	Tue, 09 Jan 2018 15:46:01 UTC
Valid until	Thu, 19 Mar 2020 15:21:02 UTC (expires in 2 years)
Key	RSA 2048 bits (e 65537)
Weak key (Debian)	No
Issuer	GlobalSign Organization Validation CA - SHA256 - G2 AIA: http://secure.globalsign.com/cacert/gsorganizationvalsha2g2r1.crt
Signature algorithm	SHA256withRSA
Extended Validation	No
Certificate Transparency	Yes (certificate)
OCSP Must Staple	No
Revocation information	CRL, OCSP CRL: http://crl.globalsign.com/gs/gsorganizationvalsha2g2.crl OCSP: http://ocsp2.globalsign.com/gsorganizationvalsha2g2
Revocation status	Good (not revoked)
DNS CAA	No (more info)
Trusted	Yes Mozilla Apple Android Java Windows



Additional Certificates (if supplied)

Certificates provided	3 (4704 bytes)
-----------------------	----------------

https://www.ssllabs.com/ssltest/analyze.html?d=www.ualberta.ca&s=54.85.24.187

1/5

Additional Certificates (if supplied)

Chain issues		Incorrect order, Contains anchor
#2		
Subject	GlobalSign Root CA <span>In trust store</span> Fingerprint SHA256: ebd41040e4bb3ec742c9e381d31ef2a41a48b6685c96e7cef3c1df6cd4331c99 Pin SHA256: K87oWBWM9UZfyddvDfoxL+8lpNyoUB2ptGtn0fv6G2Q=	
Valid until	Fri, 28 Jan 2028 12:00:00 UTC (expires in 9 years and 11 months)	
Key	RSA 2048 bits (e 65537)	
Issuer	GlobalSign Root CA Self-signed	
Signature algorithm	SHA1withRSA Weak, but no impact on root certificate	
#3		
Subject	GlobalSign Organization Validation CA - SHA256 - G2 Fingerprint SHA256: 74ef335e5e18788307fb9d89cb704bec112abd23487dbff41c4ded5070f241d9 Pin SHA256: IQBnNBEiFuHj+8x6X8XLgh01V9lc5/V3IRQLNFFc7v4=	
Valid until	Tue, 20 Feb 2024 10:00:00 UTC (expires in 5 years and 11 months)	
Key	RSA 2048 bits (e 65537)	
Issuer	GlobalSign Root CA	
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

For TLS 1.3 tests, we currently support draft version 18.



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		128
TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)	ECDH secp256r1 (eq. 3072 bits RSA) FS		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		256
TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)	ECDH secp256r1 (eq. 3072 bits RSA) FS		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



## Handshake Simulation

<a href="#">Android 2.3.7</a> <sup>No SNI</sup> <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
<a href="#">Android 4.0.4</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">Android 4.1.1</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">Android 4.2.2</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">Android 4.3</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">Android 4.4.2</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Android 5.0.0</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Android 6.0</a>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; http/1.1</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Android 7.0</a>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Baidu Jan 2015</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">BingPreview Jan 2015</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Chrome 49 / XP SP3</a>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Chrome 57 / Win 7</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Firefox 31.3.0 ESR / Win 7</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Firefox 47 / Win 7</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Firefox 49 / XP SP3</a>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Firefox 53 / Win 7</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Googlebot Feb 2015</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">IE 7 / Vista</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">IE 8 / XP</a> <sup>No FS</sup> <sup>1</sup> <sup>No SNI</sup> <sup>2</sup>	Server sent fatal alert: handshake_failure			
<a href="#">IE 8-10 / Win 7</a> <b>R</b>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">IE 11 / Win 7</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">IE 11 / Win 8.1</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; http/1.1</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">IE 10 / Win Phone 8.0</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">IE 11 / Win Phone 8.1</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; http/1.1</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">IE 11 / Win Phone 8.1 Update</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; http/1.1</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">IE 11 / Win 10</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Edge 13 / Win 10</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Edge 13 / Win Phone 10</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Java 6u45</a> <sup>No SNI</sup> <sup>2</sup>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
<a href="#">Java 7u25</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">Java 8u31</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">OpenSSL 0.9.8y</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_RSA_WITH_AES_128_CBC_SHA	No FS
<a href="#">OpenSSL 1.0.1l</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">OpenSSL 1.0.2e</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 5.1.9 / OS X 10.6.8</a>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 6 / iOS 6.0.1</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 6.0.4 / OS X 10.8.4</a> <b>R</b>	RSA 2048 (SHA256)	TLS 1.0	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 7 / iOS 7.1</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 7 / OS X 10.9</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 8 / iOS 8.4</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 8 / OS X 10.10</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 9 / iOS 9</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 9 / OS X 10.11</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 10 / iOS 10</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Safari 10 / OS X 10.12</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Apple ATS 9 / iOS 9</a> <b>R</b>	RSA 2048 (SHA256)	<b>TLS 1.2 &gt; h2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">Yahoo Slurp Jan 2015</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>
<a href="#">YandexBot Jan 2015</a>	RSA 2048 (SHA256)	<b>TLS 1.2</b>	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256	ECDH secp256r1 <b>FS</b>

## # Not simulated clients (Protocol mismatch)

[IE 6 / XP](#) <sup>No FS</sup> <sup>1</sup> <sup>No SNI</sup> <sup>2</sup> 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.

Handshake Simulation

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



Protocol Details

DROWN	No, server keys and hostname not seen elsewhere with SSLv2 (1) For a better understanding of this test, please read <a href="#">this longer explanation</a> (2) Key usage data kindly provided by the <a href="#">Censys</a> network search engine; original DROWN website <a href="#">here</a> (3) Censys data is only indicative of possible key and certificate reuse; possibly out-of-date and not complete	
Secure Renegotiation	Supported	
Secure Client-Initiated Renegotiation	No	
Insecure Client-Initiated Renegotiation	No	
BEAST attack	Not mitigated server-side ( <a href="#">more info</a> ) TLS 1.0: 0xc013	
POODLE (SSLv3)	No, SSL 3 not supported ( <a href="#">more info</a> )	
POODLE (TLS)	No ( <a href="#">more info</a> )	
Downgrade attack prevention	Yes, TLS_FALLBACK_SCSV supported ( <a href="#">more info</a> )	
SSL/TLS compression	No	
RC4	No	
Heartbeat (extension)	No	
Heartbleed (vulnerability)	No ( <a href="#">more info</a> )	
Ticketbleed (vulnerability)	No ( <a href="#">more info</a> )	
OpenSSL CCS vuln. (CVE-2014-0224)	No ( <a href="#">more info</a> )	
OpenSSL Padding Oracle vuln. (CVE-2016-2107)	No ( <a href="#">more info</a> )	
ROBOT (vulnerability)	No ( <a href="#">more info</a> )	
Forward Secrecy	With modern browsers ( <a href="#">more info</a> )	
ALPN	Yes h2 http/1.1	
NPN	Yes h2 http/1.1	
Session resumption (caching)	Yes	
Session resumption (tickets)	Yes	
OCSP stapling	No	
Strict Transport Security (HSTS)	No	
HSTS Preloading	Not in: Chrome Edge Firefox IE	
Public Key Pinning (HPKP)	No ( <a href="#">more info</a> )	
Public Key Pinning Report-Only	No	
Public Key Pinning (Static)	No ( <a href="#">more info</a> )	
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, secp521r1, brainpoolP512r1, brainpoolP384r1, secp384r1, brainpoolP256r1, secp256k1, sect571r1, sect571k1, sect409k1, sect409r1, sect283k1, sect283r1 (server preferred order)	
SSL 2 handshake compatibility	Yes	



HTTP Requests



1 https://www.ualberta.ca/ (HTTP/1.1 500 Internal Server Error)



Miscellaneous

Test date	Thu, 22 Feb 2018 22:04:27 UTC
Test duration	120.440 seconds
HTTP status code	500
HTTP server signature	-
Server hostname	ec2-54-85-24-187.compute-1.amazonaws.com

SSL Report v1.30.8

Copyright © 2009-2018 [Qualys, Inc.](#) All Rights Reserved.

[Terms and Conditions](#)

Qualys is the leading provider of integrated [infrastructure security](#), [cloud infrastructure security](#), [endpoint security](#), [devsecops](#), [compliance](#) and [web app security](#) solutions.