Kronos WFR – Action required: TLS 1.2 Upgrade

Workforce Ready will disable the TLS 1.0 and TLS 1.1 encryption protocol for web-based applications, and switch to TLS 1.2 on **Friday, 7/20 at 12:01AM.** There will be a brief maintenance window during this time, and the system may not be accessible. Scroll down for more information or click the following link to view the full alert on the communities.

TLS 1.2 Upgrade Alert (POD 3 alert –see below)

What is TLS?

TLS is an acronym for "Transport Layer Security," which is the protocol that allows digital devices (such as computers and mobiles) to communicate over the internet securely without the transmission being vulnerable to an outside audience.

Why are we making this change?

This change is mandated by the Kronos Information Security team and it affects all product teams in Kronos. Multiple vulnerabilities were identified on TLS 1.0 and TLS 1.1, major defects being BEAST (CVE-2011-3389) - The Browser Exploit Against SSL/TLS attack affects SSL 3.0 and TLS 1.0, CRIME Compression Ratio Info-leak Made Easy, POODLE Padding Oracle On Downgraded Legacy Encryption, TLS/SSL Server Supports Weak Cipher Algorithms.

What does this mean for you?

1. You may want to check your browser versions to ensure you are compliant to TLS 1.2. Compliant browsers are as follows:

   a. Chrome – 30-32+
   b. Safari – 7+
   c. Firefox – 27-33+, ESR 31.0-31.2+
   d. Internet Explorer – 11+
   *Limited support for mobile platforms using the browsers listed above.
2. If you are connecting to our API (REST,SOAP), you will need to ensure that it allows for TLS 1.2 connections.
3. For InTouch 9000, the minimum firmware version needs to be at least V2.2.5.11. The firmware for InTouch 9100, V3 firmware does not need to be updated.
4. For Middleware, you have two options.
   a. The PC/Server hosting the Middleware it should be run with JAVA version 1.8.
   b. If you are using a version of Java less than 1.8, your Middleware installation must be at a minimum of v1.7v54.8.

How can you check if you are compatible?

Go To: https://www.ssllabs.com/ssltest/viewMyClient.html (Third-Party Service)

- If the user agent is green, you are compatible with TLS 1.2
- If not, update your browser to the latest version that supports TLS 1.2. If you are unsure of how to update your browser, please contact your IT Administrator on how to accomplish this.

By System Administrator
07/13/2018 12:25p

ACTION REQUIRED: TLS 1.2 UPGRADE - 7/20 –POD 3 Alert

Workforce Ready will disable the TLS 1.0 and TLS 1.1 encryption protocol for web-based applications, switch to TLS 1.2 on **Friday, 7/20 at 12:01AM EDT**. There will be a brief maintenance window during this time, and the system may not be accessible.

What is TLS?

TLS is an acronym for "Transport Layer Security," which is the protocol that allows digital devices (such as computers and mobiles) to communicate over the internet securely without the transmission being vulnerable to an outside audience.

Why are we making this change?

This change is mandated by the Kronos Information Security team and it affects all product teams in Kronos. Multiple vulnerabilities were identified on TLS 1.0 and TLS 1.1, major defects being BEAST (CVE-2011-3389) - The Browser Exploit Against SSL/TLS attack affects SSL 3.0 and TLS 1.0, CRIME Compression Ratio Info-leak Made Easy, POODLE Padding Oracle On Downgraded Legacy Encryption, TLS/SSL Server Supports Weak Cipher Algorithms.

What does this mean for you?

1. You may want to check your browser versions to ensure you are compliant to TLS 1.2. Compliant browsers are as follows:
    a. Chrome – 30-32+
    b. Safari – 7+
    c. Firefox – 27-33+, ESR 31.0-31.2+
    d. Internet Explorer – 11+

    *Limited support for mobile platforms using the browsers listed above.

2. If you are connecting to our API (REST,SOAP), you will need to ensure that it allows for TLS 1.2 connections.
3. For InTouch 9000, the minimum firmware version needs to be at least V2.2.5.11. The firmware for InTouch 9100, V3 firmware does not need to be updated.
4. For Middleware, you have two options.
    a. The PC/Server hosting the Middleware it should be run with JAVA version 1.8.
    b. If you are using a version of Java less than 1.8, your Middleware installation must be at a minimum of v1.7v54.8.

How can you check if you are compatible?

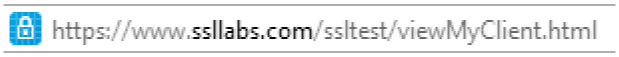
Go To: https://www.ssllabs.com/ssltest/viewMyClient.html **(Third-Party Service)**

- If the user agent is green, you are compatible with TLS 1.2
- If not, update your browser to the latest version that supports TLS 1.2. If you are unsure of how to update your browser, please contact your IT Administrator on how to accomplish this.

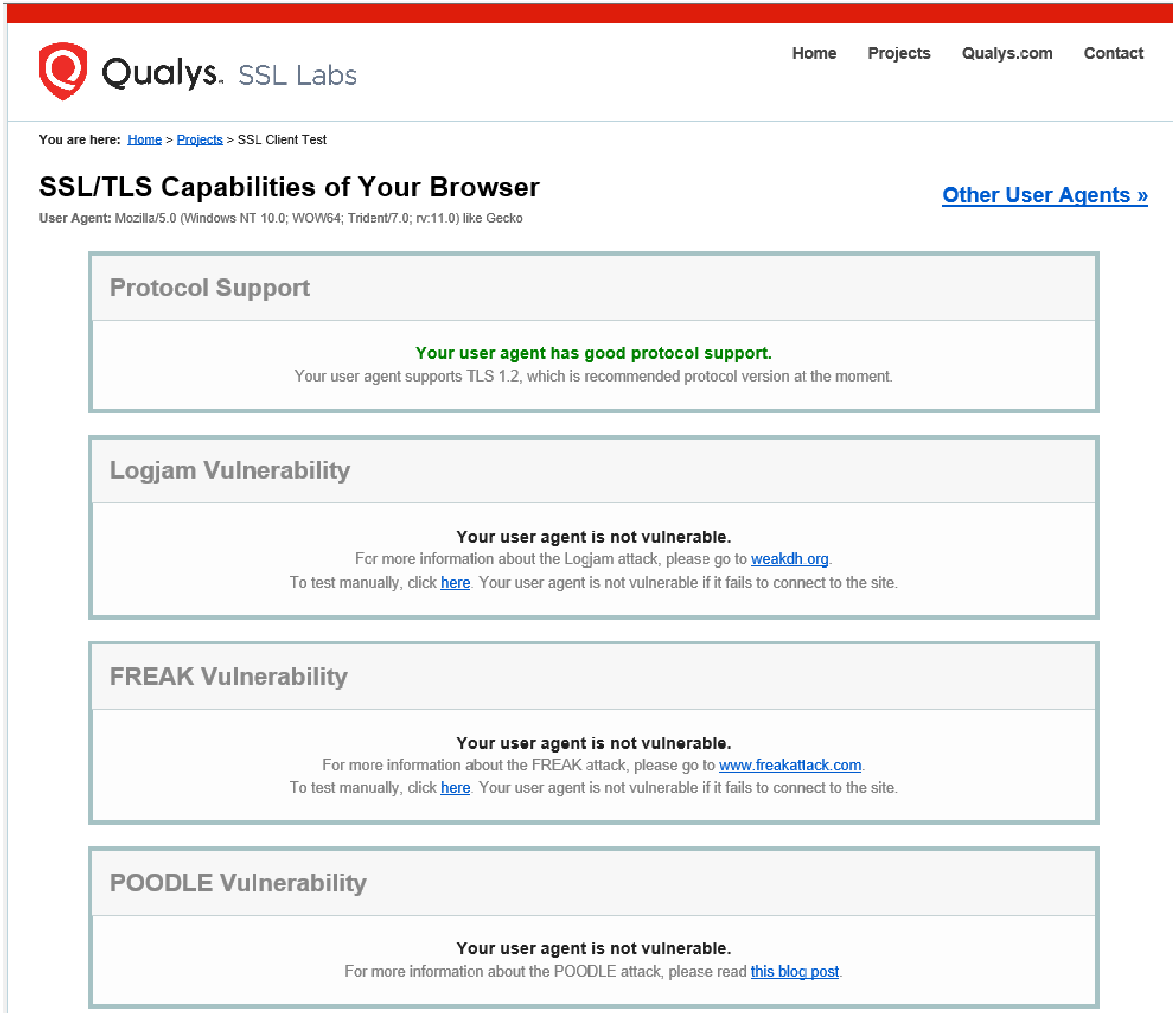
We will send reminders throughout this process, and if you have any questions, please submit a case.

If you are not part of the POD3 Alerts Group, please join today and make sure to update the notifications to "Every Post". Click on the following link: POD3 Alert Group to view/join the group. If you have any questions, please submit a case.

Browser Check:



https://www.ssllabs.com/ssltest/viewMyClient.html



You are here: Home > Projects > SSL Client Test

SSL/TLS Capabilities of Your Browser

Other User Agents »

User Agent: Mozilla/5.0 (Windows NT 10.0; WOW64; Trident/7.0; rv:11.0) like Gecko

Protocol Support

Your user agent has good protocol support.
Your user agent supports TLS 1.2, which is recommended protocol version at the moment.

Logjam Vulnerability

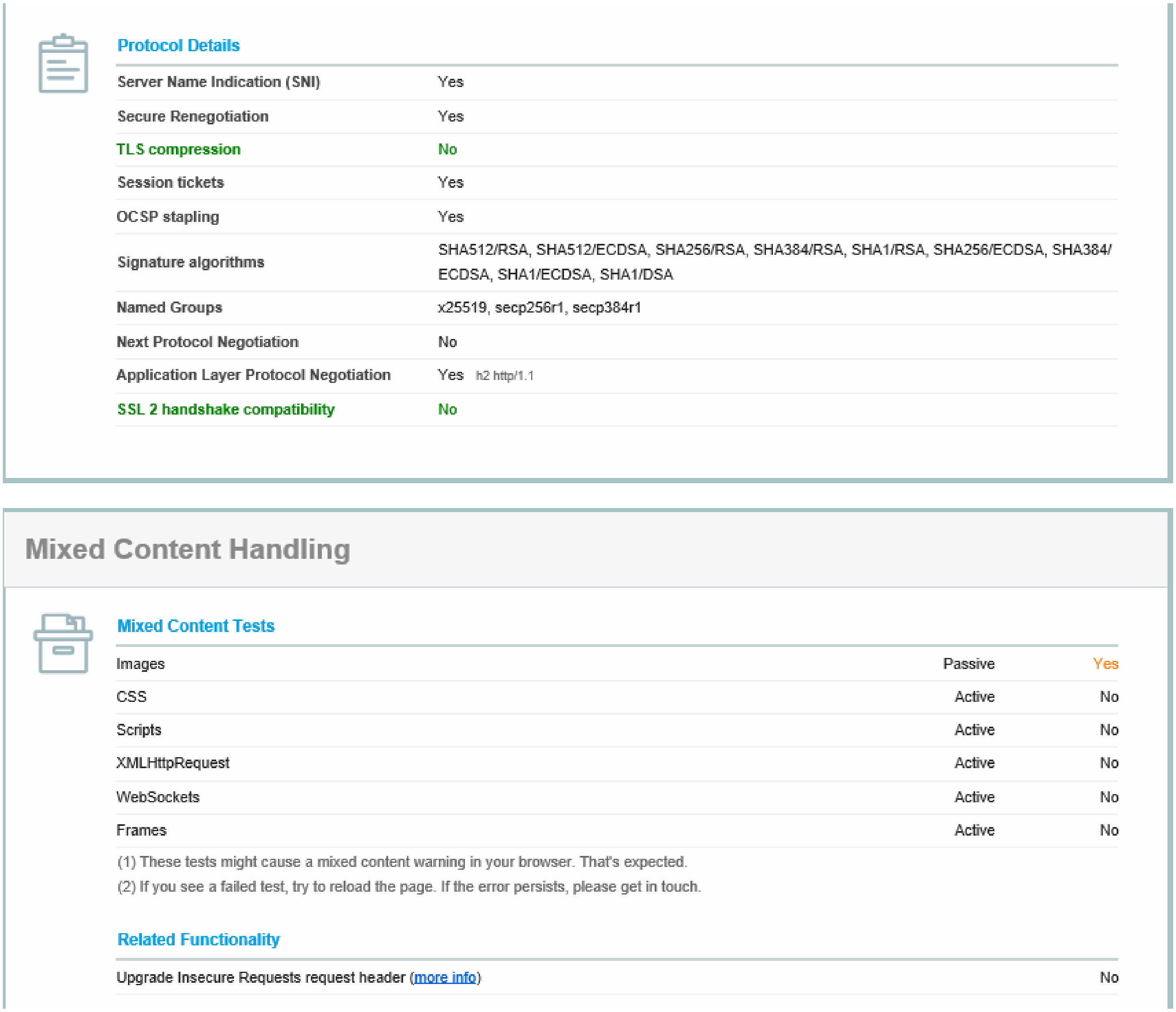
Your user agent is not vulnerable.
For more information about the Logjam attack, please go to weakdh.org.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

FREAK Vulnerability

Your user agent is not vulnerable.
For more information about the FREAK attack, please go to www.freakattack.com.
To test manually, click here. Your user agent is not vulnerable if it fails to connect to the site.

POODLE Vulnerability

Your user agent is not vulnerable.
For more information about the POODLE attack, please read this blog post.



Protocol Details

Server Name Indication (SNI)	Yes
Secure Renegotiation	Yes
TLS compression	No
Session tickets	Yes
OCSP stapling	Yes
Signature algorithms	SHA512/RSA, SHA512/ECDSA, SHA256/RSA, SHA384/RSA, SHA1/RSA, SHA256/ECDSA, SHA384/ECDSA, SHA1/ECDSA, SHA1/DSA
Named Groups	x25519, secp256r1, secp384r1
Next Protocol Negotiation	No
Application Layer Protocol Negotiation	Yes h2 http/1.1
SSL 2 handshake compatibility	No

Mixed Content Handling

Mixed Content Tests

Images	Passive	Yes
CSS	Active	No
Scripts	Active	No
XMLHttpRequest	Active	No
WebSockets	Active	No
Frames	Active	No

(1) These tests might cause a mixed content warning in your browser. That's expected.

(2) If you see a failed test, try to reload the page. If the error persists, please get in touch.

Related Functionality

Upgrade Insecure Requests request header (more info)	No