SABRE SSL to TLS MIGRATION

SECURITY COMPLIANCE STANDARDS

TLS MANDATE

The Payment Card Industry ("PCI") council, as well as Visa and Mastercard, have issued a mandate that all Merchants and Service Providers configure their systems to use the TLS 1.2 standard for secure connections between systems. This means systems must disable SSL and earlier versions of TLS as they will no longer be compliant and will not be allowed to connect.

WHO IS IMPACTED?

All Sabre customers and partners accessing any Sabre network or solution must upgrade /configure systems for use of TLS 1.2. This is a security requirement regardless if the data being accessed is PCI related or not. As this is an industry-wide initiative, your IT organizations should already be determining what actions are required to comply, including applications and systems beyond those connecting to Sabre.

UPGRADE REQUIREMENTS

There are three primary methods for communicating with Sabre systems:

- ✓ **Connecting to Sabre via a Web Browser (i.e., Agency eServices, ClientBase Online)**
- ✓ **Connecting to Sabre via Sabre APIs (i.e., SOAP APIs, ReST APIs, but not JCSAPI/CCSAPI) or**

  *Supplier customers with systems connected to **Sabre's Supplier Side Gateway (SSG)** should also ensure they are using the correct security protocols.*
- ✓ **Utilizing Sabre's Software as a Service applications (i.e., Sabre Red Workspace, Qik)**

BACKGROUND

INDUSTRY MANDATE REFERENCES

- **PCI Council:**
  https://www.pcisecuritystandards.org/pdfs/15_02_12_PCI_SSC_Bulletin_on_DSS_revisions_SSL_update.pdf

- **Visa:**
  http://usa.visa.com/download/merchants/alert_SSL3Poodle_102914.pdf

- **United States Computer Emergency Readiness Team:**
  https://www.us-cert.gov/ncas/alerts/TA14-290A

CONFIRM TLS COMPLIANCE - SRW

Sabre Red Workspace

Sabre Red Workspace version 2.13.2, which was released in July 2015, is compatible with TLS 1.2. Customers should ensure that all installations are using this version to comply with this mandate.

The release and deployment process will be the same as all previous Sabre Red Workspace versions and documented in the relevant release notes and installation guides.

Customers can confirm what version they are running from within Sabre Red Workspace from the top menu bar, selecting “Help” and then “About Sabre Red Workspace”.

Sabre Red Workspace has published minimum specifications regarding the operating system and web browser versions are relevant to this mandate, as they must also be using the correct security settings. More specifically, Sabre Red Workspace must be installed on the following to function correctly:

- Microsoft Windows 7 – 32 and 64 bit
- Microsoft Windows 8 – 32 and 64 bit (Does not include Windows 8 RT)
- Mac OS 10.6 and greater
- Basic support for Terminal Services environment: Microsoft Windows Server 2003 and 2008, Citrix

All other operating system versions (i.e., Windows Vista, Windows XP) are either not supported by the vendor, by Sabre, or are not able to communicate via TLS 1.2.

Additionally, Sabre Red Workspace leverages the native Internet Explorer version installed on the customer’s workstation for some graphical content. See the “Sabre products accessed via Web browsers” section below for more detail on ensuring the correct browser versions and settings are used.

UPGRADE/CONFIGURATION - BROWSERS

Sabre products accessed via Web browsers

Customers must ensure they are using correct browser with appropriate configurations.

Internet Explorer

Supported Versions: Internet Explorer 8 and 9 (on Windows 7 or Server 2008 v R2 only), Internet Explorer 10 (on Windows 8 and Server 2012 only) and Internet Explorer 11.

To enable TLS 1.2 in Internet Explorer:

Go to Tools in the top menu bar of the IE browser
Go to Internet Options -> Advanced Tab ->Under security, Check Use TLS 1.2

Google Chrome

Supported Versions: Google Chrome 30 to 42. Versions below 30 do not support TLS 1.2.

How to enable TLS 1.2 in Google Chrome:

Go to Chrome settings or type chrome://settings/ in the Chrome browser.
Click on show Advanced setting
Under Network section, click on Change proxy settings.
Go to Advanced tab, under security section enable TLS 1.2

UPGRADE/CONFIGURATION - BROWSERS

Firefox

Supported Versions: Firefox 24 to 39 . Versions 24 to 26 are disabled by default. Versions below 24 do not support TLS 1.2.

How to enable TLS 1.2 in Firefox

Go to Tools in the top menu bar of the Firefox browser
Go to Options -> Advanced Tab ->Encryption -> Check Use TLS 1.2

NOTE: If you don't see the encryption tab, follow steps mentioned below to enable TLS 1.2:
Type in about:config in the address bar and move past the warning.
In the search, type tls
Set the security.tls.version.max=3

Set the security.tls.version.min=3

UPGRADE/CONFIGURATION - APIs

Sabre APIs (SOAP and ReST APIs)

No new versions of Sabre APIs are required to comply with this mandate, but developers should review their configurations to ensure all systems are using the correct protocols. To comply with this mandate, Sabre will disable the ability to connect to Sabre APIs using encryption protocol SSLv3.0, and all versions of Transport Layer Security (TLS) prior to version 1.2. In addition, certain Ciphers using keys with less than 128 bits will no longer be supported for secure communication.

The table below identifies the recommended Encryption protocols and Ciphers that should be utilized. Once the changes are implemented, any communication that cannot negotiate to TLS v1.2 or is using an unsupported Cipher will be rejected.

Unsupported Encryption Protocols	Supported Encryption Protocols
Secure Sockets Layer (SSL) versions 1.0, 2.0,and 3.0 Transport Layer Security (TLS) versions 1.0 and 1.1	TLSv1.2 and higher
Unsupported Ciphers	**Supported Cipher**
MD5, RC4, DES, EXPORT, aNULL and eNULL	Strong ciphers with key lengths >= 128 bits must be used

The following URLs can be used to test connection with your client application:

https://sws-tls.cert.sabre.com/ (SOAP APIs)
https://api-tls.cert.sabre.com/ (ReST APIs)

NOTE: JCSAPI, and CCSAPI customers do not need to take action on their applications, as the changes required to comply with this mandate are at the network level, not the application level.

CONFIRM TLS COMPLIANCE - QIK

Sabre Qik Developer

Sabre will release Qik 7.1 to all customers in August 2015 to provide a version that is compatible with TLS 1.2. All current Qik customers will be provided with this new release for free, to be downloaded from eServices. All customers that use Qik to develop their own applications will need to re-compile and provision a new version of the runtime and application to each workstation. Customers should use the standard, documented process for compiling, testing, and deploying the new versions of the application. Sabre will be sun-setting all previous versions of Qik as of January 1, 2016 and will no longer provide support for them.

There will be an announcement when Qik 7.1 is available for download.