

Frequently Asked Questions  
Concur Mobile app

# iOS App Transport Security (ATS) Enforcement

At SAP Concur, our goal is to provide a seamless user experience for our clients. We prepared this FAQ to help affected customers understand an upcoming change that Apple has announced. App Transport Security (ATS), introduced in Apple's iOS 9 and OS X v10.11, improves user security and privacy by requiring apps to use secure network connections over HTTPS (as opposed to HTTP). Some SAP Concur clients who are Single Sign-On (SSO)-enabled redirect to HTTP pages and not HTTPS.

**SAP Concur is enforcing this requirement beginning with the late November 2018 mobile release.** Once enforcement of ATS goes into effect, users of these customers will receive an error when attempting to use our SAP Concur mobile app. Apple could choose to enforce ATS sooner than SAP Concur's enforcement. Exceptions cannot be accommodated.

**All customers who are SSO-enabled on the Concur mobile app should confirm with their IT department and/or third parties that all of the SSO connections and redirects are compliant using the diagnostic tools (appendix) and information below.**

## What is happening?

Apple has announced they will update their App Transport Security (ATS) requiring apps including the Concur mobile app to use HTTPS. This affects a number of SSO-enabled SAP Concur customers who redirect to HTTP to log into Concur. All SSO-enabled mobile customers should confirm that their connections are compliant. With the late November 2018 mobile release, users of these customers will receive an error and not be able to log into Concur mobile.

## Who is asking to make this change?

At WWDC 2016, Apple announced that apps submitted to their App Store would be required to support ATS at the end of the year (2016). However, to give customers additional time to prepare, this deadline has been extended (date TBD). SAP Concur is being proactive and requiring clients to transition before late November 2018.

## Who is affected?

Concur mobile app users on iOS devices at SSO-enabled clients who use HTTP vs HTTPS. SAP Concur sent direct emails to customers who are known to be impacted, and communicated via the monthly release notes. All SSO clients are encouraged to review the configuration of their Mobile SSO URL and make sure HTTP is not used. This includes third-party connections and internal URLs.



## What products are affected?

Only the Concur mobile application on iOS devices is affected, and only at SSO-enabled customers who use HTTP at any point during the SSO process.

## What actions do I or my organization need to take?

Immediately begin a conversation with your IT department so that they can migrate all your Single Sign-On (SSO) services and communications to HTTPS using TLSv1.2. Review the Appendix below for troubleshooting assistance.

1. Check your server meets ATS requirements listed below
2. If your servers are compliant and you are using a third-party Identity Provider (idP) you will need to contact them to update security settings on your SSO server to support TLS v1.2 and Forward Secrecy

To be ATS compliant:

- Server must support at least Transport Layer Security (TLS) 1.2
- Connection ciphers must provide forward secrecy
- Certificates must be signed with either an RSA key with a length of at least 2048 bits or an ECC key with a size of at least 256 bits

*You must work with your IT team and any third parties to make changes! SAP Concur is not able to make changes on your behalf.*

## How might this affect my users?

If SSO customers and vendors do not move to using HTTPS, then they will not be able to log into the Concur mobile app or use vendors' services. When Concur mobile navigates to a vendor that does not use HTTPS, then the user will see a blank page. If a Concur mobile customer does not move to using HTTPS, Concur mobile screens will be blank and unusable upon login.

## What is HTTP & HTTPS?

Hyper Text Transfer Protocol Secure (HTTPS) is the secure version of HTTP, the protocol over which data is sent between your browser and the website that you are connected to. The 'S' at the end of HTTPS stands for 'Secure'. It means all communications between your browser and the website are encrypted. HTTPS is often used to protect highly confidential online transactions like online banking and online shopping order forms.

## What other applications are requiring/recommending this change?

All iOS mobile applications will need to fulfill Apple's requirements.

## If there are any issues who do I contact?

Customers should contact Customer Support for further reference, or their account team. Submit a Support Case where for "Topic: Expense" and "Case Type: Mobile – Expense".

## APPENDIX:

The below methods can help you troubleshoot within your network:

**Method 1:** for URLs that are publicly accessible (<https://apptransport.info/>)

- Pass your domain in as a parameter this can take anywhere from 2 to 5 min to process (e.g. <https://apptransport.info/craigslist.com>) you'll get the following information:
  1. Whether or not your server is ATS compliant
  2. How to fix your server if necessary
  3. How to add ATS exceptions if necessary
  4. The results from SSL Labs

craigslist.com  
is ATS Compliant

### Test Results

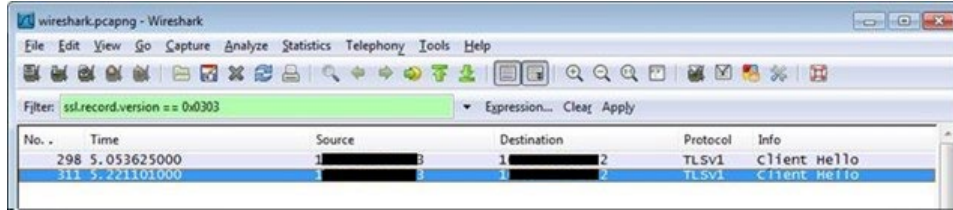
Test	Compliant	Value(s)
cipher	true	TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 TLS_DHE_RSA_WITH_AES_128_GCM_SHA256 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256 TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_256_CBC_SHA TLS_RSA_WITH_AES_256_GCM_SHA384 TLS_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_256_CBC_SHA TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 TLS_DHE_RSA_WITH_AES_256_GCM_SHA384 TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA TLS_DHE_RSA_WITH_AES_128_CBC_SHA256 TLS_DHE_RSA_WITH_AES_256_CBC_SHA256 TLS_RSA_WITH_AES_128_GCM_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA256 TLS_RSA_WITH_AES_128_CBC_SHA TLS_RSA_WITH_3DES_EDE_CBC_SHA
protocol	true	TLSv1.0 TLSv1.2 TLSv1.1
trust	true	trusted
sigAlg	true	SHA256withRSA
keyAlg	true	RSA
keySize	true	2048

Built by **Vectorform**

Using **Vapor** and **SSL Labs**

**Method 2:** for URLs that are not publicly accessible

- Use **Wireshark** to monitor the communication to the URL. You can use a Wireshark filter to display only TLSv1.2 packets with the following:  
`ssl.record.version == 0x0303`
- You will see packets that use the TLSv1.2 protocol if the server has been configured for TLS version 1.2. If you only see a Client Hello packet when monitoring requests coming into the URL, then TLSv1.2 was not negotiated between the mobile device and the URL.



## Additional technical documentation

Here are some additional documentation from Apple that provide a summary of ATS (and general TLS) changes in the new OS releases:

Topic	Summary
NSAllowsArbitraryLoadsInWebContent (recognized from iOS10)	ATS dictionary; still allow to load content in web view (WKWebView, UIWebView, WebView)
<b>[new since WWDC]</b> NSAllowsLocalNetworking	Allows to opt out of ATS for local networking  To learn more, see the <i>NSAppTransportSecurity</i> section of the <a href="#">Information Property List Key Reference</a>
<b>[new since WDC]</b> NSAllowsArbitraryLoadsForMedia	Allows to opt out of ATS for media resources  To learn more, see the <i>NSAppTransportSecurity</i> section of the <a href="#">Information Property List Key Reference</a>
NSRequiresCertificateTransparency	Allows to opt in to <a href="#">Certificate Transparency</a> checking
Cypher suites employing RC4	Disabled by default
SSLv3 protocol	Disabled by default at the Security Transport layer
Cypher suite employing SHA-1 or 3DES	Supported (recommended to transition away from use)
<b>[new since WWDC]</b> NSURLConnection	Honours ATS minimum TLS version  Previously NSURLConnection ignored the minimum TLS version prescribed by ATS (r. <a href="#">23167645</a> ). This bug has been fixed.  If using NSURLConnection for networking, run the app on the latest released OS to ensure that the app still works as expected.
<a href="#">WWDC presentation</a>	Provides general background  For details see the <i>App Store Review for ATS</i> section of the <a href="#">ATS documentation</a>
<a href="#">News and Updates</a>	Provides any future changes to ATS policy; includes an RSS feed

---

<p><b>[new since WWDC]</b> Apple Developer News indicates the ATS deadline has been extended into 2017</p>	<p><a href="#">Supporting App Transport Security</a> for details.</p>
--	---

Copyright/Trademark