

# iOS9 Support Information

## Handling App Transport Security in iOS

The rollout of iOS 9 is expected to come this month and will introduce a new privacy feature called App Transport Security (ATS) to enforce best practices in secure connections between an app and its back end. This change will require your action if you are using current Phunware SDKs and building an app against the iOS 9 SDK.

Phunware's current SDK offerings communicate to our back-end using HTTP. Gating communication to our back-end is secured with authorization headers and all transmitted payloads are devoid of any kind of personally identifying information (PII). This means that applications compiled against the iOS 9 SDK will not be able to communicate to the Phunware back-end without adding the appropriate exceptions to your applications Info.plist file.

If you are unable to wait for Phunware HTTPS SDK updates we recommend you add the following exceptions to your Info.plist file. These exceptions will permit HTTP access to Phunware end-points only:

```
<key>NSAppTransportSecurity</key>
<dict>
  <key>NSAllowsArbitraryLoads</key>
  <false/>
  <key>NSExceptionDomains</key>
  <dict>
    <key>phunware.com</key>
    <dict>
      <key>NSIncludesSubdomains</key>
      <true/>
      <key>NSExceptionAllowsInsecureHTTPLoads</key>
      <true/>
    </dict>
    <key>digby.com</key>
    <dict>
      <key>NSIncludesSubdomains</key>
      <true/>
      <key>NSExceptionAllowsInsecureHTTPLoads</key>
      <true/>
    </dict>
  </dict>
</dict>
```

If you are integrating with our advertising SDK we recommend enabling arbitrary loads for all HTTP endpoints:

```
<key>NSAppTransportSecurity</key>
<dict>
  <key>NSAllowsArbitraryLoads</key>
  <true/>
</dict>
```

Phunware recommends doing the utmost to ensure the privacy and security of your users. As part of this commitment we will be updating all Phunware endpoints to support HTTPS.

If you have any questions regarding these changes, feel free to contact us.