

SAP SuccessFactors Mobile Learning Impact Bulletin

HTTPS Required for Content in iOS

This document is published on November 22, 2016.

There are new Apple iOS requirements that impact customers using SAP SuccessFactors Mobile Learning. This notice is Apple iOS specific and **not** unique to SAP SuccessFactors Mobile Learning. Any company transmitting data over the network is affected. This notice applies to all iOS versions.

IMPORTANT:

*On **January 1, 2017** these new requirements will take effect. In order to ensure that access to offline Mobile Learning content is not interrupted, these changes must be made by the **January 1, 2017** deadline. Any company transmitting data over the network is affected and must take action.*

NEW REQUIREMENTS TO TRANSMIT DATA OVER THE NETWORK

App Transport Security (ATS)

On Apple platforms, a networking security feature called App Transport Security (ATS) is available to apps. It improves privacy and data integrity. This helps instill user trust that the app does not accidentally leak transmitted data to malicious parties. Apple will require that all iOS apps, including the SAP SuccessFactors Mobile App, use ATS and secure HTTP protocol (HTTPS) to transmit data over the network by **January 1, 2017**.

Secure HTTP

Customers using learning content in the SAP SuccessFactors Mobile App must ensure that network calls happen over HTTPS connections by **January 1, 2017**. Content servers must be upgraded to ensure compatibility and allow content to continue to work properly. If you are an iContent customer, then the server is already upgraded for you.

TECHNICAL REQUIREMENTS

Requirements for Connecting Using ATS

With ATS fully enabled, any content server (both third party and internal content servers hosted by the customer) should satisfy the following security requirements:

- The X.509 digital server certificate must meet *at least one* of the following trust requirements:
 - Issued by a certificate authority (CA) whose root certificate is incorporated into the operating system
 - Issued by a trusted root CA and installed by the user or a system administrator
- The negotiated Transport Layer Security (TLS) version must be TLS 1.2. Attempts to connect without TLS/SSL protection, or with an older version of TLS/SSL, are denied by default.

- The connection must use either the AES-128 or AES-256 symmetric cipher. The negotiated TLS connection cipher suite must support perfect forward secrecy (PFS) through Elliptic Curve Diffie-Hellman Ephemeral (ECDHE) key exchange, and *must be one of the following*:
 - TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_ECDSA_WITH_AES_256_CBC_SHA
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA256
 - TLS_ECDHE_ECDSA_WITH_AES_128_CBC_SHA
 - TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256
 - TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA384
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA256
 - TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA
- The leaf server certificate must be signed with one of the following types of keys:
 - Rivest-Shamir-Adleman (RSA) key with a length of at least 2048 bits
 - Elliptic-Curve Cryptography (ECC) key with a size of at least 256 bits

Also, the leaf server certificate hashing algorithm must be Secure Hash Algorithm 2 (SHA-2) with a digest length, sometimes called a “fingerprint” of at least 256 (i.e., SHA-256 or greater).

The security requirements listed in this section are current as of this document’s publication date, with stricter requirements possible in the future. Changes to these requirements will not break app binary compatibility.

Important Disclaimers and Legal Information

Coding Samples

Any software coding and/or code lines / strings ("Code") included in this documentation are only examples and are not intended to be used in a productive system environment. The Code is only intended to better explain and visualize the syntax and phrasing rules of certain coding. SAP does not warrant the correctness and completeness of the Code given herein, and SAP shall not be liable for errors or damages caused by the usage of the Code, unless damages were caused by SAP intentionally or by SAP's gross negligence.

Accessibility

The information contained in the SAP documentation represents SAP's current view of accessibility criteria as of the date of publication; it is in no way intended to be a binding guideline on how to ensure accessibility of software products. SAP in particular disclaims any liability in relation to this document. This disclaimer, however, does not apply in cases of willful misconduct or gross negligence of SAP. Furthermore, this document does not result in any direct or indirect contractual obligations of SAP.

Gender-Neutral Language

As far as possible, SAP documentation is gender neutral. Depending on the context, the reader is addressed directly with "you", or a gender-neutral noun (such as "sales person" or "working days") is used. If when referring to members of both sexes, however, the third-person singular cannot be avoided or a gender-neutral noun does not exist, SAP reserves the right to use the masculine form of the noun and pronoun. This is to ensure that the documentation remains comprehensible.

Internet Hyperlinks

The SAP documentation may contain hyperlinks to the Internet. These hyperlinks are intended to serve as a hint about where to find related information. SAP does not warrant the availability and correctness of this related information or the ability of this information to serve a particular purpose. SAP shall not be liable for any damages caused by the use of related information unless damages have been caused by SAP's gross negligence or willful misconduct. All links are categorized for transparency (see: <http://help.sap.com/disclaimer>).