

# Abschaltung TLSv1 und TLSv1.1 – Softwareupdate notwendig



## Abschaltung am 09.06.2022 erfolgt

Seit dem 09.06.2022 ist zum Aufruf unserer Dienste mindestens TLSv1.2 erforderlich. Sollten Ihnen Fehler beim Aufruf von [www.divera247.com](http://www.divera247.com) angezeigt werden, melden Sie sich bei unserem Support über [support@divera247.com](mailto:support@divera247.com), wir helfen Ihnen gerne weiter!

Unseren Statistiken zufolge, betrifft die Abschaltung ca. 0,071% der Kunden, aber insbesondere teilweise selbstgeschriebene Skripte.

## Problem

Ich erhalte eine Fehlermeldung, dass ich mein Gerät updaten soll, da es eine unsichere Verschlüsselungsmethode verwendet.

### Geräte-Update notwendig!

Ihr Endgerät verwendet zur Verschlüsselung des Datenverkehrs TLSv1. Diese Version ist unsicher, bitte führen Sie ausstehende Softwareupdates aus. Ab Q2 2022 wird die Unterstützung von TLSv1 und TLSv1.1 auf unserer Seite abgeschaltet. Ohne ein Softwareupdate werden Sie DIVERA nicht mehr auf diesem Gerät nutzen können. Bei Fragen wenden Sie sich gerne an unseren Support!

## Wie erkenne ich, ob ich eine unsichere Verbindung aufbaue?

Wenn Ihnen der obige Hinweis „Geräte-Update notwendig“ im Browser direkt nach dem Login angezeigt wird, dann können Sie ohne eine Aktualisierung DIVERA ab Q2 2022 nicht mehr aufrufen.

Wenn der Hinweis nicht mehr angezeigt wird, haben Sie Ihr Gerät erfolgreich aktualisiert.

Alternativ können Sie auch auf <https://clienttest.ssllabs.com/sslttest/viewMyClient.html> prüfen, welche Verschlüsselungsstandards Ihr Gerät unterstützt.

## Warum schaltet DIVERA die Unterstützung für alte TLS Versionen ab?

Bei der Verwendung von DIVERA möchten wir unseren Nutzern stets den größtmöglichen Schutz bieten, und gleichzeitig eine größtmögliche Kompatibilität mit alten Geräten bieten. Daher orientieren wir uns an den Empfehlungen des [BSI, das eine Verwendung von TLS 1.0 und TLS 1.1 nicht empfiehlt](#). Um frühzeitig unsere Nutzer über die Abschaltung zu informieren, haben wir uns für einen markanten Hinweis während der Übergangsfrist entschieden.

## Lösung

Zur Verschlüsselung des Datenverkehrs im Internet, wird das Protokoll [SSL/TLS](#) verwendet. Diesen Verschlüsselungsstandard gibt es in mehreren Version, aktuell TLSv1 (1.0), TLSv1.1, TLSv1.2 und TLSv1.3. Für die Versionen 1.0 und 1.1 existieren bekannte Schwachstellen, wodurch nicht mehr garantiert werden kann, dass ihr Datenverkehr nicht abgefangen wird. Aus diesem Grund sollten Sie umgehend **ausstehende Updates Ihres Betriebssystems und Browsers durchführen**. Viele andere Websites haben ihre Unterstützung bereits abgeschaltet, nach aktueller Planung werden wir spätestens im **Q2 2022 keine Verbindungen über die unsicheren Protokolle TLSv1 und TLSv1.1 zulassen**.

## Kompatibilitätsliste

Diese Liste bietet eine Orientierung, ob für Ihr verwendetes Betriebssystem Updates zur Verfügung stehen, die die Unterstützung von TLSv1.2 oder höher ermöglichen. Eine Abschaltung von TLSv1.2 ist aktuell nicht geplant, da keine schwerwiegenden Sicherheitslücken bekannt sind. Sie erhalten aber einen groben Ausblick ob Ihr System auch mit dem neusten Verschlüsselungsstandard arbeitet.

### Desktopbetriebssysteme

Microsoft Windows

### Smartphone-Betriebssysteme

iOS

### Sonstige

.Net Framework

Framework	TLSv1.2	TLSv1.3
-----------	---------	---------

Betriebssystem	TLSv1.2	TLSv1.3
Windows XP	✘ <sup>1</sup>	✘
Windows Server 2008	⚠	✘
Windows Vista	⚠	✘
Windows 7	✔	✘
Windows 8	⚠ <sup>2</sup>	✘
Windows 8.1	✔	✘
Windows 10	✔	⚠
Windows 11	✔	✔

#### Apple Mac OS

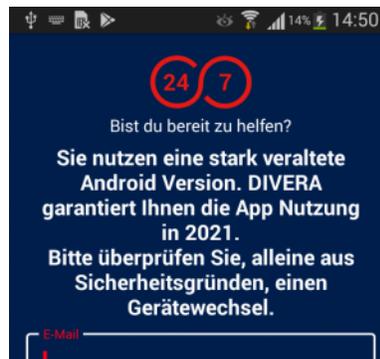
Betriebssystem	TLSv1.2	TLSv1.3
Mac OS X 10.8 und älter	✘	✘
Mac OS X 10.9	✔	✘
macOS 10.15+	✔	✔
ab macOS 11	✔	✔

Betriebssystem	TLSv1.2	TLSv1.3
iOS 9	⚠	✘
iOS 9.3	✔	✘
iOS 10	✔	✘
iOS 11	✔	✘
iOS 12.2	✔	⚠
ab iOS 13	✔	✔

#### Android

Betriebssystem	TLSv1.2	TLSv1.3
Android 3 und älter	✘	✘
Android 4.0	⚠	✘
Android 4.1+ (geräteabhängig)	✔	✘
Android 5-9	✔	✘
ab Android 10	✔	✔

*Hinweis: die Unterstützung für Geräte älter als Android 5 haben wir 2021 auslaufen lassen. Den betroffenen Nutzern wird ein entsprechender Hinweis im Login/Logout-Bildschirm seit März 2021 angezeigt. Die Nutzung der DIVERA 24/7 Webapp sollte, bei aktuellem Browser, nicht betroffen sein.*



*Ab Android App Version 2.2.51 können Sie versuchen, gültige SSL Zertifikate auf dem Gerät zu installieren, in dem Sie im Loginschirm ganz unten auf "Probleme mit SSL? hier klicken" klicken.*



4.7.	⚠	✘
4.7.1	✔	✘
ab 4.8	✔	✔

Quelle: *Bewährte Methoden für Transport Layer Security (TLS) mit .NET Framework | Microsoft Docs*

#### DIVERA Software & unterstützte Drittanbieter

Framework	TLSv1.2	TLSv1.3
Alarmmanager	✔	✘
Alarmgeber	⚠ Zum Update 0.80	✘
Bosmon Push (getestet mit v1.5.9)	✔	✘
Bosmon Netzwerkeignis	BosMon Workaround TLS	BosMon Workaround TLS
TETRAcontrol (ab v4.1)	✔	✘
rescueTABLET	⚠ Herstellerrangabe	✘

✘ = keine Unterstützung

⚠ = Aktuellste Updates müssen installiert sein, oder Einstellungen getroffen werden

✔ = Unterstützung standardmäßig aktiv

Quellen: <https://docs.microsoft.com/de-de/archive/blogs/kaushal/support-for-ssl-tls-protocols-on-windows>  
<https://support.globalsign.com/ssl/general-ssl/tls-protocol-compatibility#Note%205>

## **1 Windows XP**

Der Support und Sicherheitsupdates für Windows XP wurden von Microsoft bereits 2009 eingestellt. Weitere Informationen wie Sie Ihr System auf Windows 10 aktualisieren, finden Sie hier: <https://support.microsoft.com/de-de/windows/der-support-für-windows-xp-wurde-eingestellt-47b944b8-f4d3-82f2-9acc-21c79ee6ef5e>

Falls es für Sie unmöglich ist auf Windows 7/10 zu aktualisieren, können Sie eine aktuelle [Firefox](#) Version installieren, um TLSv1.2 Support zu erhalten. Die letzte unterstützte Version für Windows XP ist [Firefox ESR 52.9.0](#) . Hier geht es zum Download: <https://www.mozilla.org/en-US/firefox/52.9.0/releasenotes/>

## **Windows 7**

Der Support für Windows 7 wurde 2015 von Microsoft eingestellt. TLSv1.2 steht zwar zur Verfügung, wir empfehlen trotzdem ein Update auf Windows 10, um sicherzustellen, dass Sie die neusten Sicherheitsupdates erhalten haben, und auch die neuste Version TLSv1.3 unterstützen.

## **2 Windows 8**

Der Support und Sicherheitsupdates für Windows 8 wurden 2016 von Microsoft eingestellt. Bitte aktualisieren Sie Ihr System auf mindestens Windows 8.1 (Support eingestellt 2018), besser Windows 10 (Support bis 2025), um auch künftig Sicherheitsupdates zu erhalten.

## **Verwandte Artikel**

- [Abschaltung TLSv1 und TLSv1.1 – Softwareupdate notwendig](#)