

## Neue SSL-fähige Versionen und Verschlüsselungsstärke in Parallels Remote Application Server v14

- Parallels Remote Application Server 19.1
- Parallels Remote Application Server 18.2
- Parallels Remote Application Server 18.3
- Parallels Remote Application Server 18.0
- Parallels Remote Application Server 19.0
- Parallels Remote Application Server 18.1

### Informationen

In Version 14 von Parallels Remote Application Server wurde die Möglichkeit eingeführt, spezifische SSL-Versionen durchzusetzen und zu verwenden sowie eine benutzerdefinierte Konfiguration der Verschlüsselungsstärke vorzunehmen.

In diesem Artikel wird erläutert, wie Sie die Verschlüsselungsstärke konfigurieren, wenn eine Gateway-SSL- oder eine direkte SSL-Verbindung von einem Remote Application Server Client mit einem Secure Client Gateway hergestellt wird.

Die Konfiguration ist in den Secure Client Gateway-Eigenschaften verfügbar und befindet sich in der Registerkarte ?SSL/TLS?:

In Version 14 werden die folgenden SSL-Versionen akzeptiert:

- Nur TLS v1.2 (stark)
- TLS v1.1 - TLS v1.2
- TLS v1 - TLS v1.2
- SSL v3 - TLS v1.2
- SSL v2 - TLS v1.2 (schwach)

Mit diesen Optionen kann ein Administrator die bevorzugte Version auswählen und Sicherheitslücken in älteren SSL-Versionen vermeiden.

Außerdem kann die Verschlüsselungsstärke konfiguriert werden. Alle verfügbaren Optionen basieren auf OpenSSL-Standards, die [hier](#) dokumentiert sind.

Gemäß der OpenSSL-Dokumentation sind die folgenden Optionen für die Verschlüsselungsstärke in 2X RemoteApplicationServer verfügbar:

- **Niedrig:** Niedrige Verschlüsselungssammlungen (derzeit diejenigen, die 64- oder 56-Bit-Verschlüsselungsalgorithmen verwenden, aber andere Verschlüsselungssammlungen ausschließen)
- **Mittel:** Mittlere Verschlüsselungssammlungen (derzeit einige, die 128-Bit-Verschlüsselung verwenden)
- **Hoch:** Hohe Verschlüsselungssammlungen (derzeit solche mit längeren Schlüsseln als 128 Bit und einige Verschlüsselungssammlungen mit 128-Bit-Schlüsseln)

Darüber hinaus können Sie eine benutzerdefinierte Verschlüsselungszeichenfolge eingeben. Sie können die aktuelle Verschlüsselungsstärke im Bereich **Informationen** > Registerkarte **Siteinformationen** prüfen:

Eine Verschlüsselungszeichenfolge kann erstellt werden, indem Sie verschiedene Verschlüsselungsparameter aus der [hier](#) verfügbaren Liste verknüpfen.

Für die folgende Verschlüsselung beispielsweise: !SSLv2:ALL:!DH:!ADH:!EDH:!MD5:!EXPORT:@SPEED sind die folgenden Parameter definiert:

!SSLv2: SSL-Version 2 nicht verwenden ALL: Alle SSL-Verschlüsselungen im Standard-SSL-Stack verwenden !DH: DH-Verschlüsselungen nicht verwenden !ADH: ADH-Verschlüsselungen nicht verwenden !EDH: EDH-Verschlüsselungen nicht verwenden !MD5: MD5-Verschlüsselungen nicht verwenden !EXPORT: Keine EXPORT-Verschlüsselungen (schwach) verwenden @SPEED: Verschlüsselungsreihenfolge nach Geschwindigkeit festlegen

Die gesamte Dokumentation zu Verschlüsselungen und deren möglichen Konfigurationen ist hier verfügbar:

<https://www.openssl.org/docs/apps/ciphers.html>

Ab Version 14.1 sind die vordefinierten Verschlüsselungen auch in den Secure Client Gateway-Eigenschaften sichtbar.

**#- INTERNAL (content below this line is not visible in published article) -**

---

© 2024 Parallels International GmbH. All rights reserved. Parallels, the Parallels logo and Parallels Desktop are registered trademarks of Parallels International GmbH. All other product and company names and logos are the trademarks or registered trademarks of their respective owners.