Erweiterte Informationen zu Release 11.01.03.102

Inhaltsverzeichnis

1 Probleme bei IKEv2-basierten IPSec-Verbindungen (#4286 / CGS 389660)

Mit neueren Versionen von Apples Betriebssystemen iOS (aktuell 13.5.1) und macOS (aktuell 10.15.5) kommt es zu Abbrüchen von IKEv2-basierten IPSec-Verbindungen. Das Problem tritt nach dem zunächst erfolgreichen Aufbau einer IPSec-Verbindung von einem Apple Client zu einem bintec-elmeg-Gerät bei der Neuaushandlung des zur Datenverschlüsselung verwendeten Schlüssels, dem sog. „Rekeying“, auf.

Das Problem betrifft nur das Aufrechterhalten einer IPSec-Verbindung und tritt auch während aktiver Nutzung der Verbindung auf. Eine abgebrochene Verbindung kann jederzeit seitens des Clients neu aufgebaut werden. IKEv1-basierte Verbindungen sind nicht betroffen.

Release 10.2.8 Patch 1 behebt einen der zugrunde liegenden Fehler auf Seiten unserer Systemsoftware, kann aber leider die beschriebenen Probleme nicht völlig beheben, da derzeit keine ausreichenden technischen Informationen zu den von Apple vorgenommenen Änderungen vorliegen. Wir untersuchen den Sachverhalt weiterhin und werden ggf. neue Informationen oder Releases veröffentlichen.

Um eine stabilere Verbindung zu ermöglichen bzw. das Auftreten des Problems zu umgehen, können Sie die beiden folgenden Ansätze verfolgen.

1.1 Anpassung der Router-Konfiguration

Für iOS-Geräte erzielen Sie die besten Ergebnisse, wenn Sie im für den Peer verwendeten Phase-1-Profil die **DH-Gruppe** auf *5 (1536 Bit)* einstellen und im Phase-2-Profil die Option **PFS-Gruppe verwenden** deaktivieren.

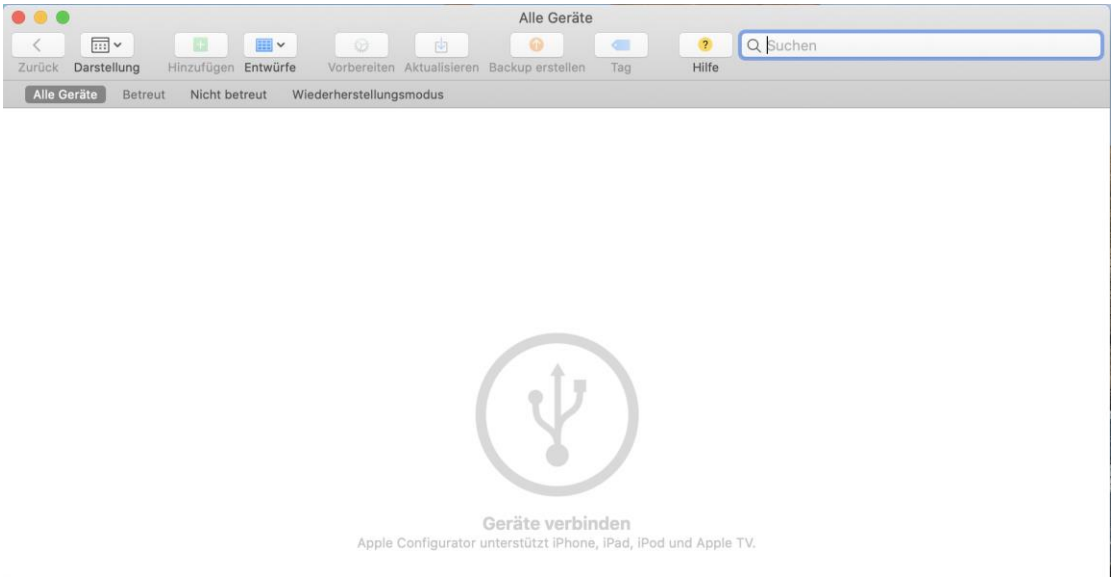
Hinweis:
Achten Sie in allen Fällen darauf, dem entsprechenden Peer die passenden Profile im Menü VPN > IPSec > IPSec-Peers > <Ihr Peer> > Erweiterte Einstellungen zuzuweisen.
Leider ist auch diese Einstellung nicht völlig zuverlässig und führt bei Geräten mit macOS nicht zum Erfolg.

1.2 Erweiterte Konfiguration des Apple Clients

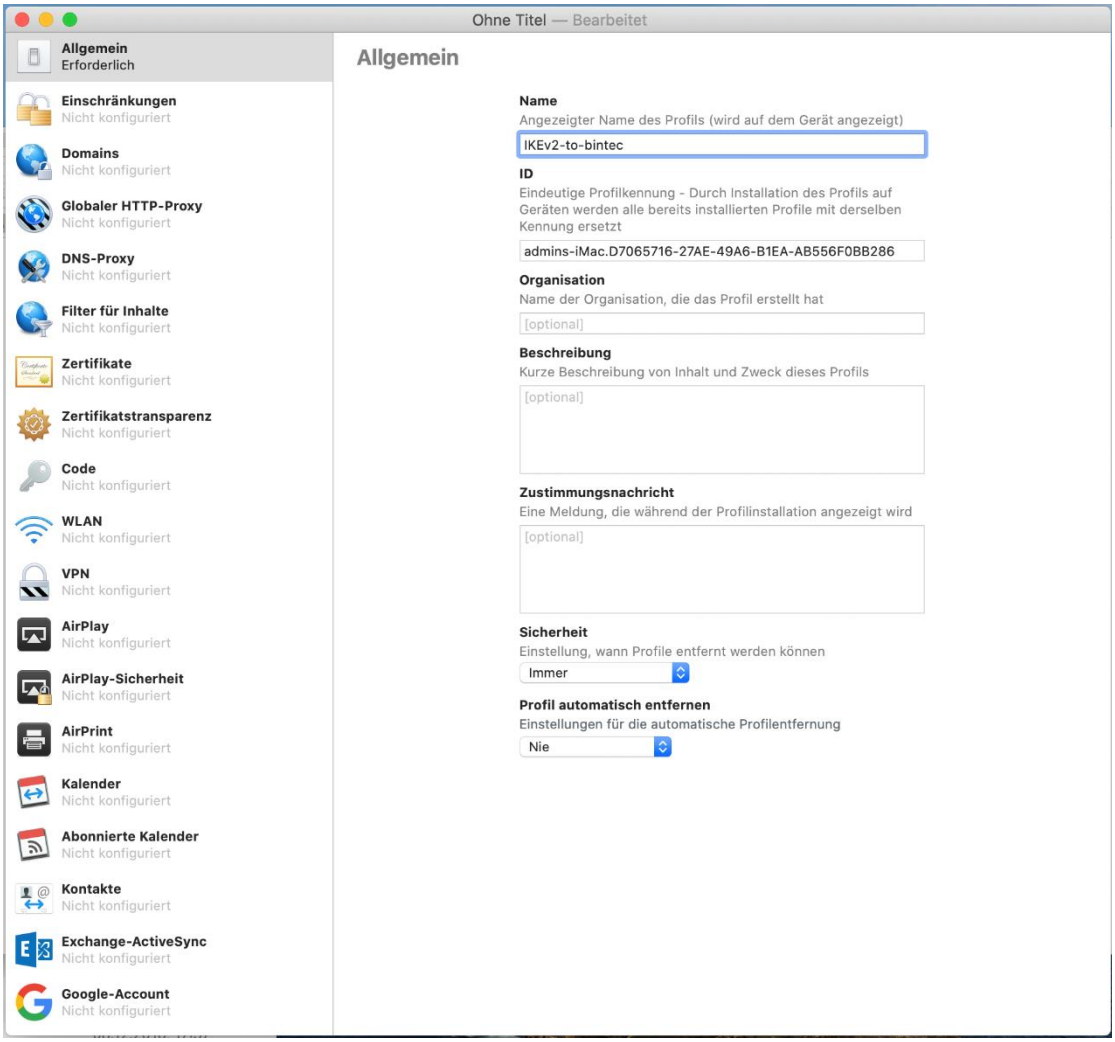
Mithilfe des **Apple Configurator 2** ist es möglich, die Konfiguration eines Apple IPSec Client so zu erstellen, dass das Rekeying erst nach langer Zeit erfolgt und daher während dieser Zeit nicht zu einem Abbruch der Verbindung führt. Diese angepasste Konfiguration können Sie direkt auf einem macOS-Gerät einsetzen, aber auch auf ein iOS-Gerät exportieren.

Gehen Sie zum Erstellen der Konfiguration wie folgt vor:

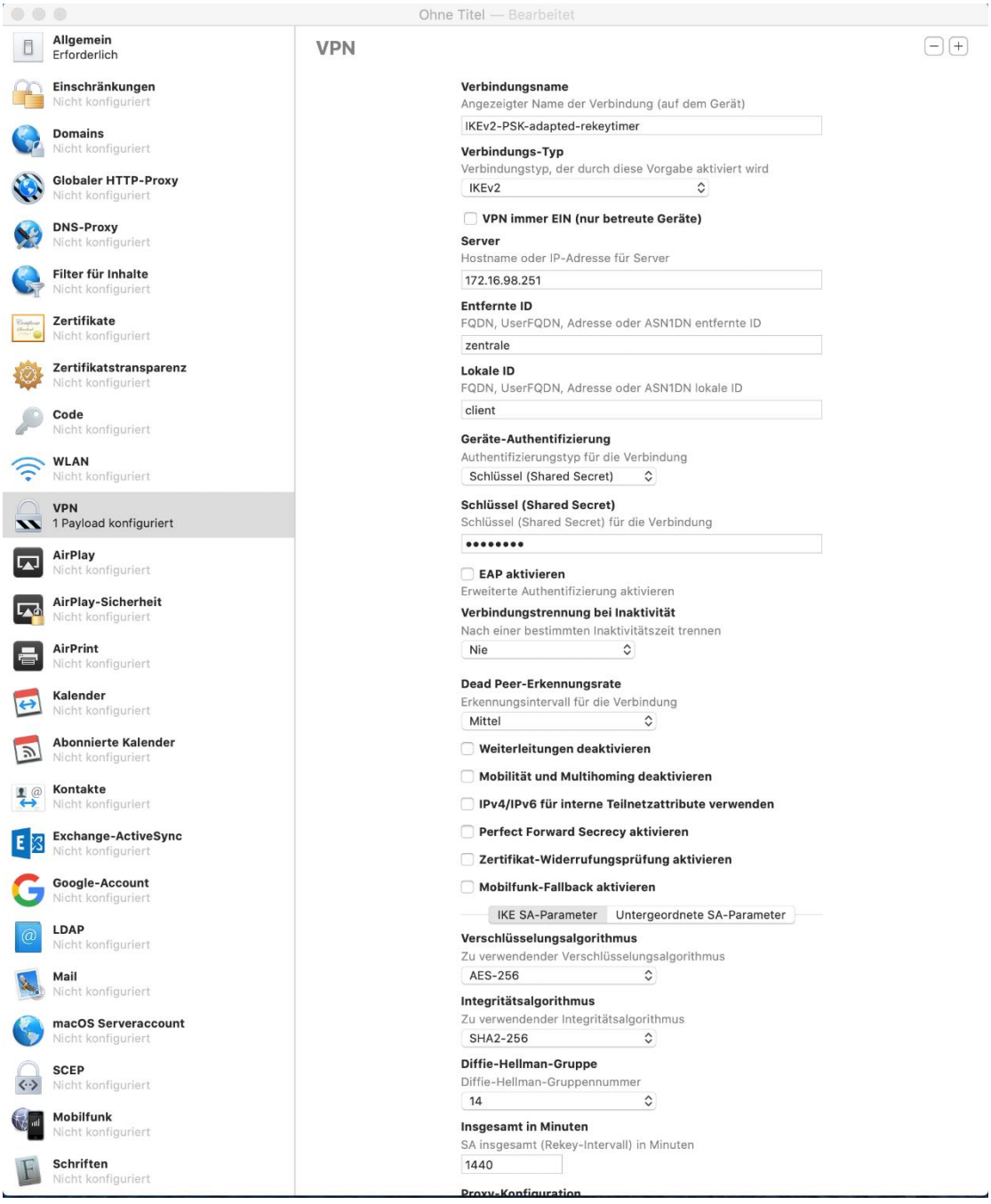
1. Installieren und öffnen Sie den **Apple Configurator 2**:



2. Drücken Sie **Command + n**, um ein neues Profil zu erstellen. In dem sich öffnenden Fenster, vergeben Sie im Abschnitt **Allgemein** einen Namen für das zu erstellende Profil, in unserem Beispiel *IKEv2-to-bintec*:



3. Nehmen Sie im Abschnitt VPN die folgenden Einstellungen vor:

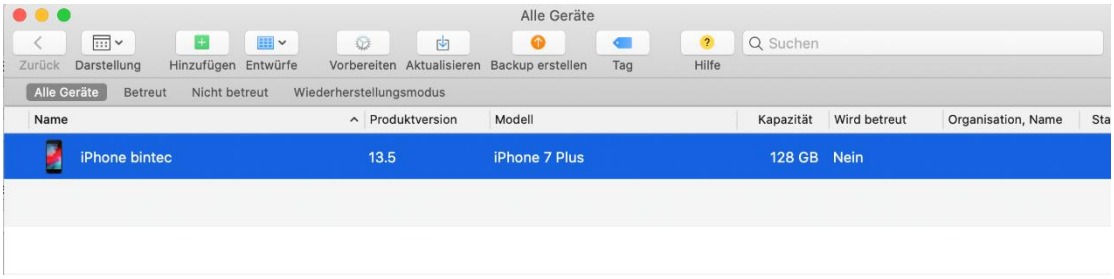


Passen Sie dabei die Einstellungen wie den **Server**, die **Lokale ID** und den **Schlüssel** an Ihre Erfordernisse – wie die Konfiguration des Peers auf Ihrem bintec-elmeg-Gerät – an. Achten Sie darauf, den Wert für die Option **Insgesamt in Minuten** entsprechend Ihrer Bedürfnisse ggf. hoch zu wählen. Dieser legt fest, wann ein Rekeying stattzufinden hat. In unserem Beispiel ist der Wert auf *1440* Minuten (24 Stunden) gesetzt.

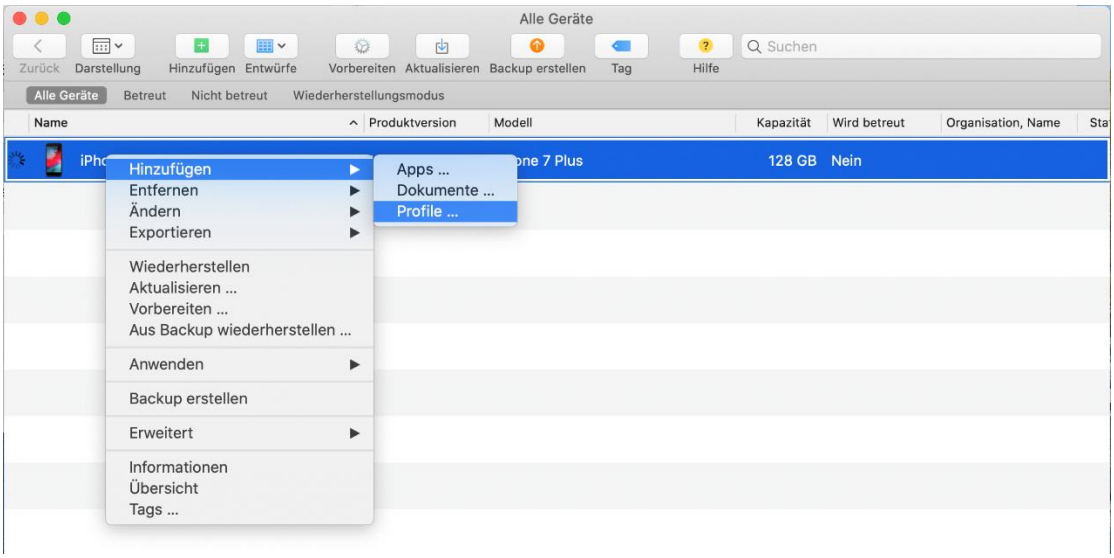
4. Mit der Tastenkombination Command + s können Sie das Profil z. B. im Ordner **Dokumente** speichern und anschließend mit einem Doppelklick auf dem macOS-Gerät aktivieren.

Um den Vorteil des verlängerten Rekeying-Intervalls auch auf einem iOS-Gerät nutzen zu können, können Sie das erstellte Profil exportieren. Gehen Sie dazu folgendermaßen vor:

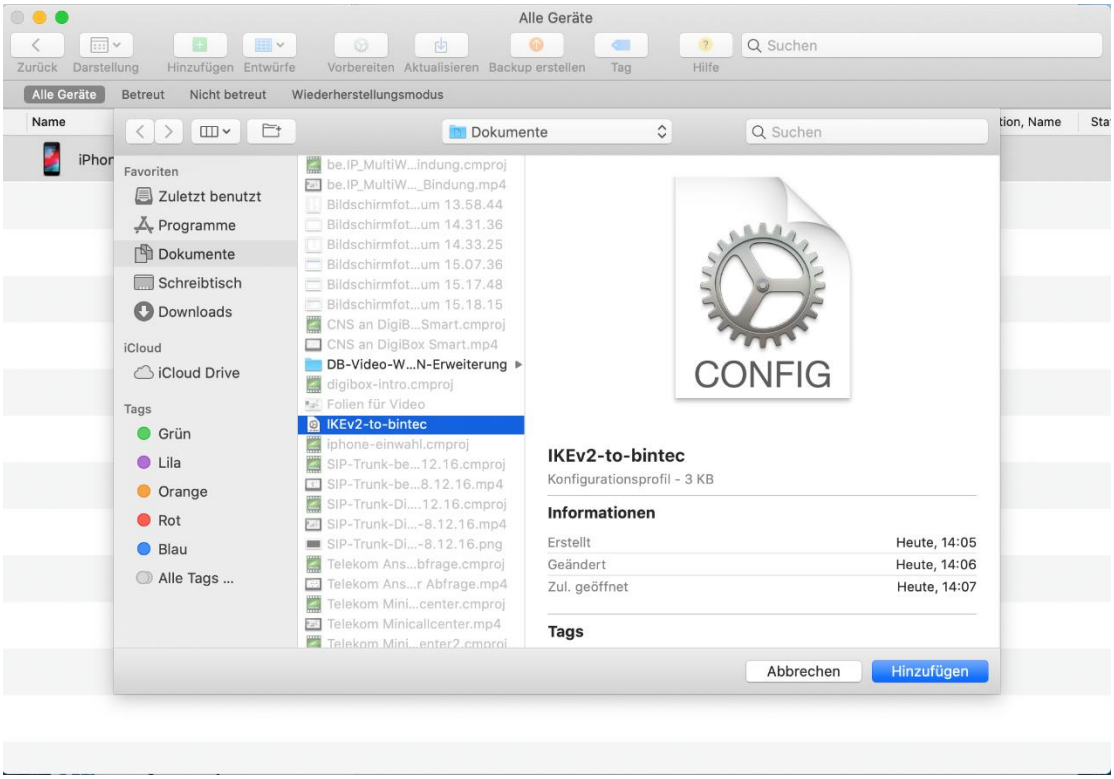
1. Verbinden Sie das iOS-Gerät mit dem macOS-Gerät, auf dem das Profil gespeichert ist. Bestätigen Sie den Geräte-Code.



2. Wechseln Sie mit einem rechten Mausklick (CTRL-Klick) in das Menü **Hinzufügen > Profile**:



3. Übertragen Sie das zuvor erstellte Profil *IKEv2-to-bintec* auf das iOS-Gerät. Folgen Sie den Anweisungen auf dem Bildschirm:



4. Im Anschluss können Sie das importierte Profil zum Aufbau einer IPSec-Verbindung nutzen.