Serverseitige Verschlüsselung in Nextcloud aktivieren – Anleitung

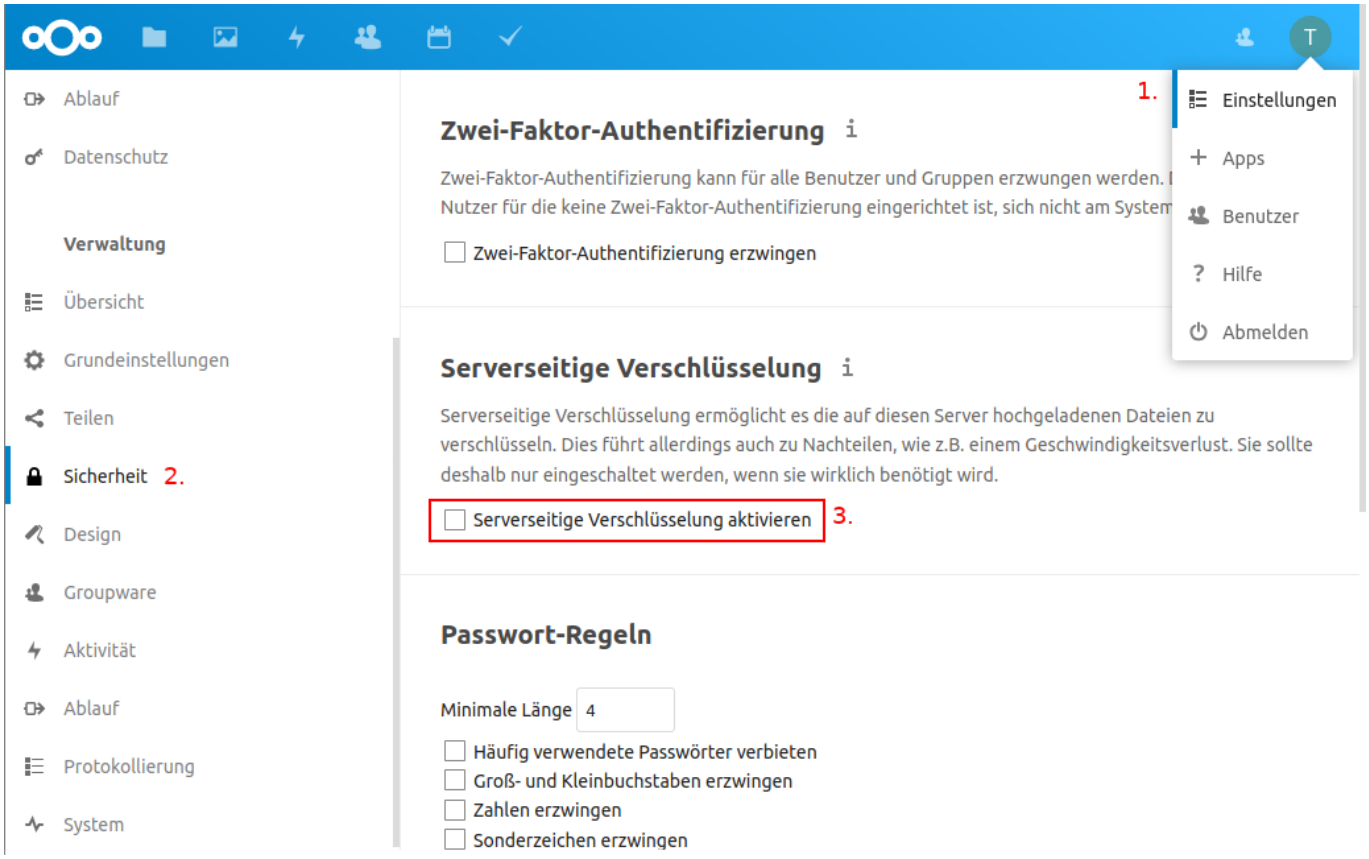
Geschrieben von: Sven

Veröffentlicht am: 24.04.2020, 10:42 Uhr

Die Aktivierung der serverseitigen Verschlüsselung in Nextcloud erhöht die Wahrscheinlichkeit, dass Ihre Dateien privat bleiben. Hierbei werden die Dateien auf dem Server verschlüsselt gespeichert, so dass Sie diese grundsätzlich nur noch über Ihre Nextcloud-Instanz lesen können. In dieser Anleitung erfahren Sie, wie Sie die serverseitige Verschlüsselung aktivieren können und einiges mehr.

Die serverseitige Verschlüsselung aktivieren

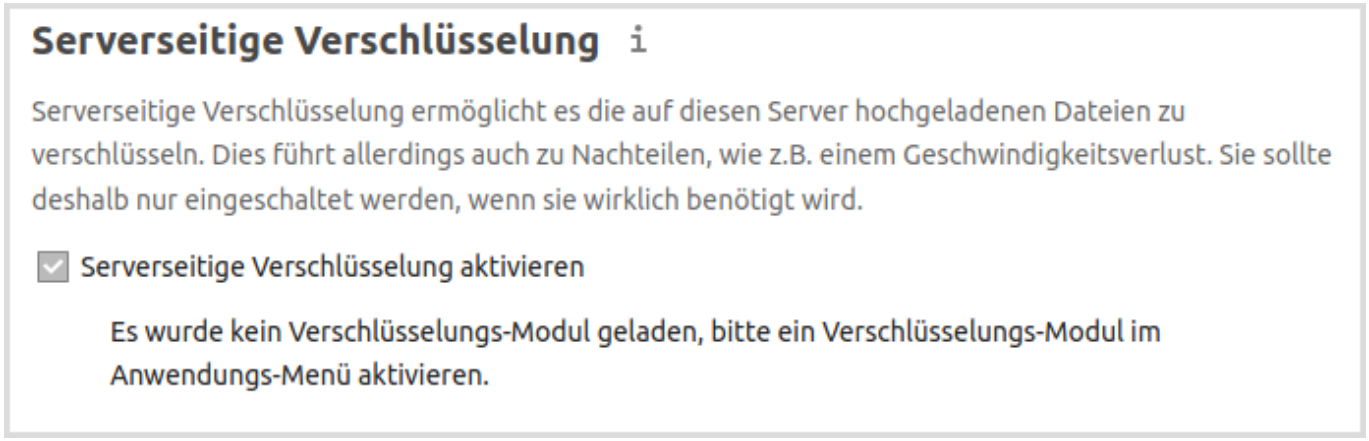
Um die Verschlüsselung zu aktivieren, begeben Sie sich als Administrator auf den Punkt „Einstellungen“ Ihres Benutzermenüs (1.). Wählen Sie als nächstes auf der linken Seite im Bereich „Verwaltung“ den Punkt „Sicherheit“ (2.) und setzen den Haken vor „Serverseitige Verschlüsselung aktivieren“ (3.).



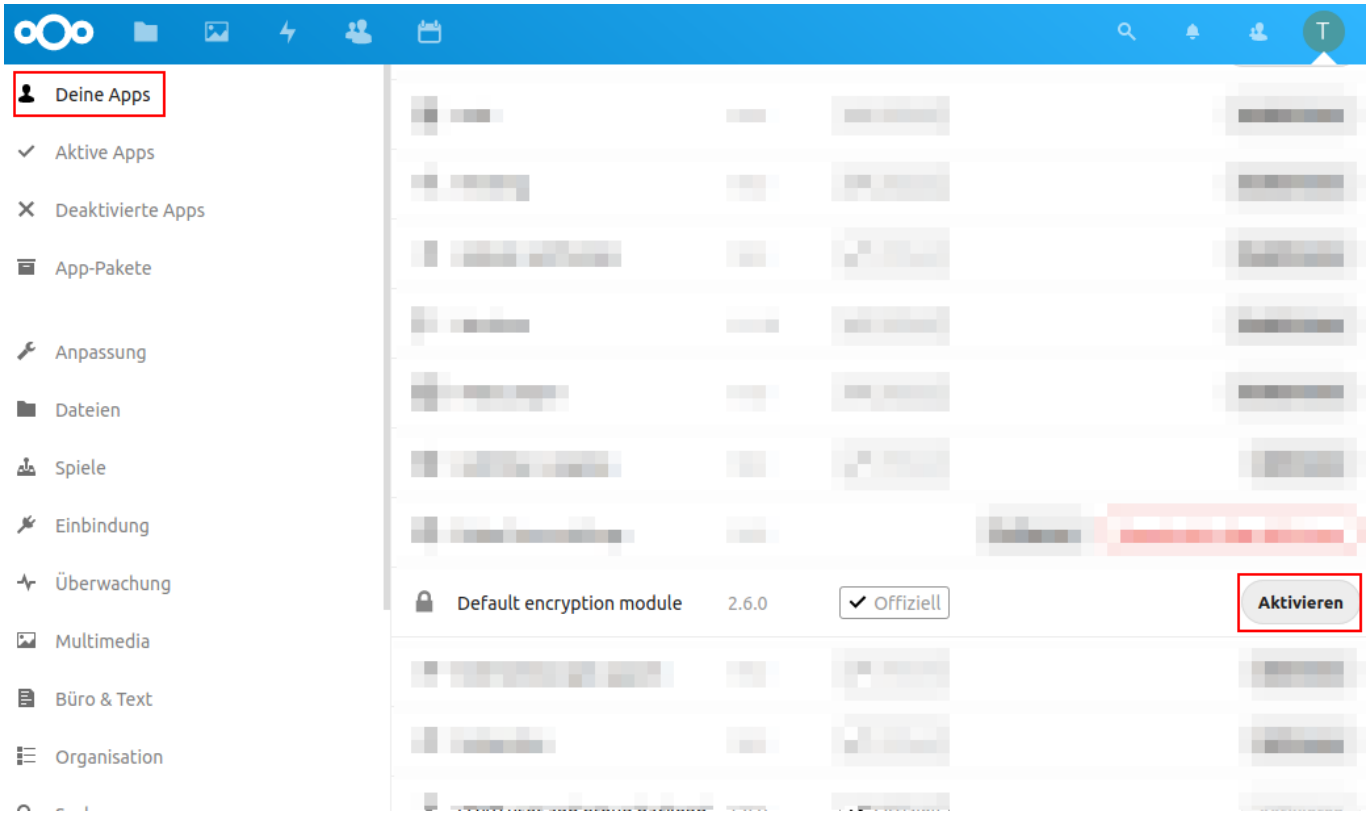
Nun werden Ihnen in einer gelben Box einige Hinweise aufgeführt. Mit einem Klick auf „Verschlüsselung aktivieren“ wird die Aktivierung bestätigt.

Standard-Verschlüsselungsmodul aktivieren

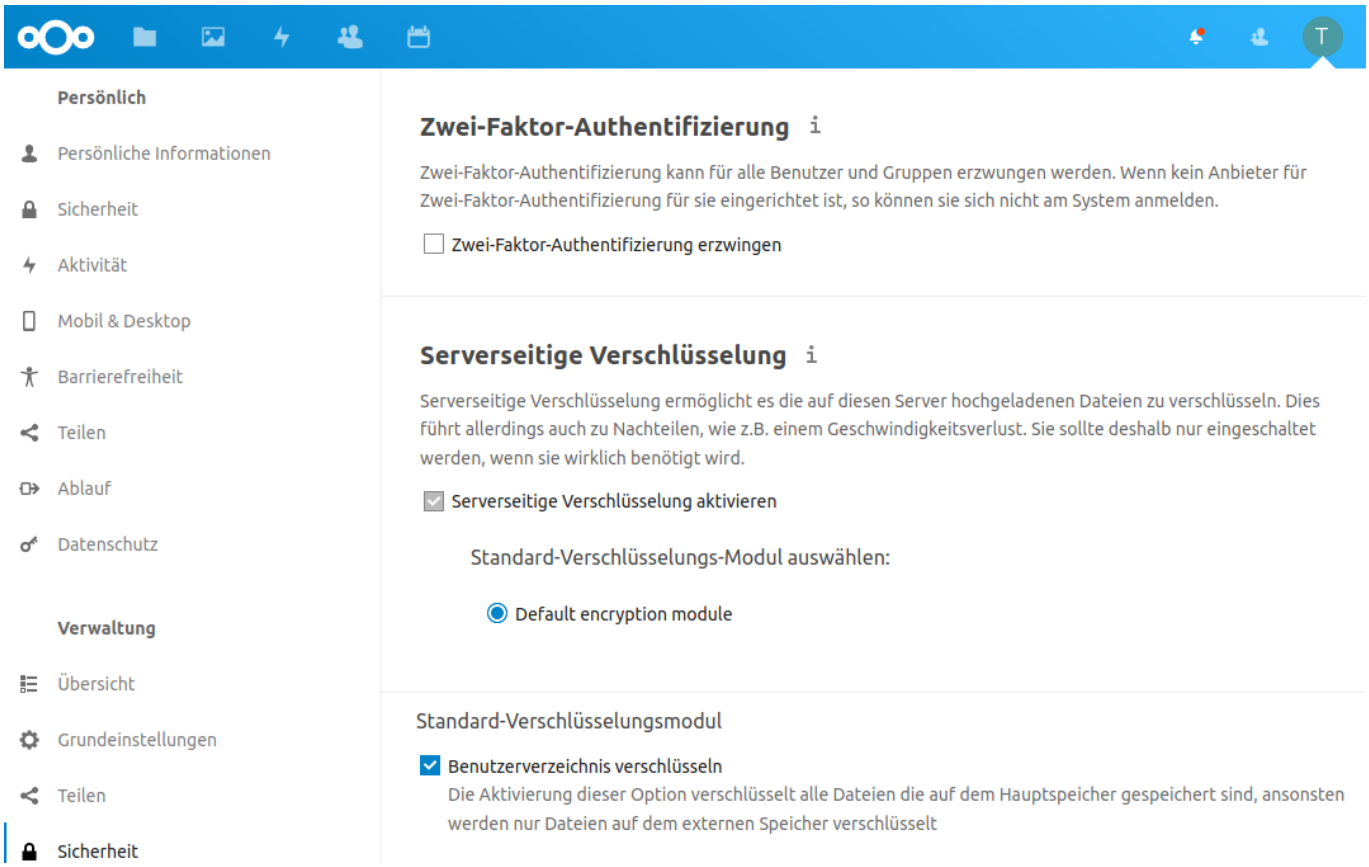
Noch funktioniert die Verschlüsselung allerdings nicht, da Sie erst noch ein Verschlüsselungsmodul laden bzw. aktivieren müssen.



Um das Standard-Verschlüsselungsmodul aktivieren zu können, wählen Sie als erstes in Ihrem Benutzermenü oben rechts den Punkt „Apps“ aus. Als nächstes wechseln Sie in den Bereich „Ihre Apps“ bzw. „Deine Apps“ und suchen den Eintrag „Default encryption module“ und klicken auf den Button „Aktivieren“.



Wenn Sie nun wieder in die Sicherheitseinstellungen wechseln, sehen Sie, dass das Standard-Verschlüsselungsmodul ausgewählt und automatisch für alle Ihre Speicher aktiviert ist.



Alle Dateien, die Sie ab jetzt in Ihre Nextcloud hochladen, werden nun also

verschlüsselt abgelegt, belegen dabei aber auch mehr Speicherplatz. Auch die Dateien, die Sie über den Nextcloud-Client hochladen, werden verschlüsselt gespeichert. Als Nutzer Ihrer Cloud merkt man von der Änderung nichts, höchstens eine etwas verlangsamte Geschwindigkeit.

Die Verwendung der serverseitigen Verschlüsselung ist mittlerweile meist auch sinnvoll, wenn kein extern eingebundener Speicher verwendet wird, wie ursprünglich angedacht, denn die Schlüssel selbst werden neben den Dateien ebenfalls geschützt abgelegt. Es gibt aber leider dennoch Szenarien, wie ein Angreifer an die Daten herankommen kann. Beispielsweise könnte theoretisch während einer laufenden Nutzer-Session der entsprechende Schlüssel aus dem RAM des Servers ausgelesen werden, falls der Angreifer entsprechenden Zugriff auf den Server hat, wie Nextcloud selbst kommuniziert.

Nachträglich verschlüsseln

Wer Zugriff auf die Konsole und die entsprechenden Rechte hat, wie es beispielsweise bei einem vServer der Fall ist, kann mit dem folgenden Befehl die bis dato unverschlüsselten Dateien mit einem Schlag nachträglich verschlüsseln:

Verbinden Sie sich dazu per SSH mit Ihrem Server und wechseln in Ihr Nextcloud-Verzeichnis. Führen Sie darin den folgenden Befehl über das Terminal aus:

sudo -u www-data php occ encryption:encrypt-all

Hinweis: Während dieser Aktion wechselt Ihre Cloud automatisch in den Wartungsmodus.

Wer den Befehl aufgrund fehlender Rechte nicht ausführen kann, kann sich aber dennoch über das Web-Interface weiterhelfen. Beispielsweise können Sie dort einen neuen Ordner anlegen und alle vorhandenen Dateien des Nutzers dahin verschieben (Verschieben-Funktion von Nextcloud), die Dateien bleiben dabei weiterhin unverschlüsselt. Wenn Sie von dort die Dateien aber wieder an den ursprünglichen Ort kopieren (Kopierfunktion von Nextcloud), sind auch diese Dateien verschlüsselt. Dann müssen Sie nur noch den neuen Ordner löschen, der ja noch die unverschlüsselten Dateien enthält. Vergessen Sie dabei aber nicht, den Papierkorb zu leeren. Alternativ möglich ist auch, die Dateien herunterzuladen, in der Cloud zu löschen und erneut in die Cloud hochzuladen.

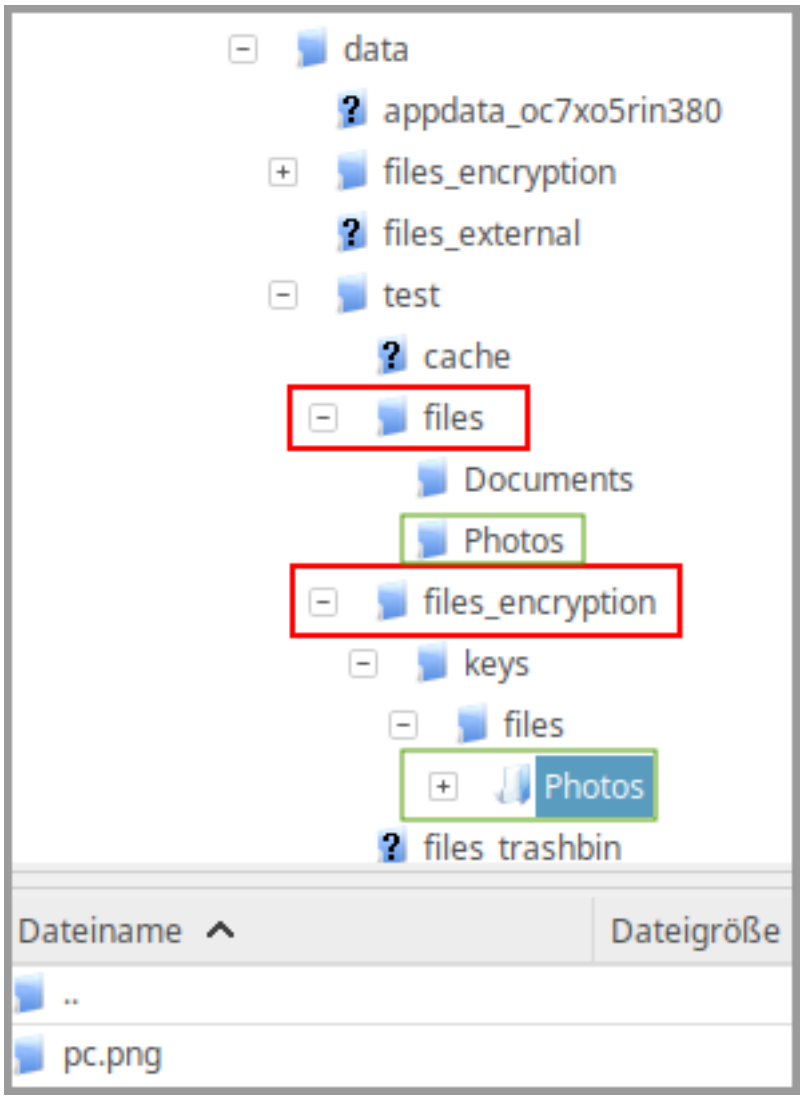
Wie kann ich erkennen, dass meine Dateien wirklich verschlüsselt sind?

Wenn Sie beispielsweise mit FTP auf Ihre Dateien zugreifen, werden diese zwar noch immer mit dem korrekten Dateinamen (bleibt unverschlüsselt) angezeigt. Sobald Sie eine verschlüsselte Datei herunterladen und öffnen möchten, werden Sie aber feststellen, dass Sie die Dateien nicht wie gewohnt öffnen können.

Zudem sind die verschlüsselten Dateien nun real etwa 35% größer als im Ursprung.

Wenn Sie Ihre Dateien nun einmal per FTP und einmal über Ihre Nextcloud auflisten lassen, sind die verschlüsselten Dateien über FTP größer als über das Interface Ihrer Cloud, denn darin sehen Sie die Dateien im entschlüsselten Zustand. Die Dateigröße einer nicht verschlüsselten Datei ist dagegen in beiden Fällen identisch. Wenn Sie die Dateigrößen zwischen Cloud-Interface und FTP vergleichen möchten, sollten Sie ggf. in Ihrem FTP-Programm das Dateigrößenformat von dezimal (KB) auf binär (KiB) stellen, damit die Größenangaben bei identischer Dateigröße nicht abweichen.

Für jede verschlüsselte Datei wird parallel ein Verzeichnis mit dem entsprechenden Schlüsselteil in dem Ordner „files_encryption“ abgelegt. In dem Screenshot wird ein Ausschnitt von Filezilla gezeigt, hier sehen Sie den entsprechenden Ordner für die Datei „pc.png“, die verschlüsselt in dem Ordner „Photos“ abgelegt wurde.



Die Dateien bleiben selbst auf dem Server verschlüsselt, wenn Sie diese mit Anderen teilen oder gar öffentlich freigeben.

Verschlüsselung wieder deaktivieren

Im Backend Ihrer Nextcloud können Sie die Verschlüsselung nicht wieder deaktivieren, dies ist Normalerweise auch eher nicht sinnvoll. Wenn Sie sich aber

doch dazu entschließen möchten, können Sie mit dem nachfolgenden Befehl über das Terminal die serverseitige Verschlüsselung wieder deaktivieren:

sudo -u www-data php occ encryption:disable

Hinweis: Zur Sicherheit sollte für diese Aktion der Wartungsmodus aktiviert und am Ende wieder deaktiviert werden, falls in der Zwischenzeit Nutzer auf die Cloud zugreifen könnten!

Alle ab dem Zeitpunkt hochgeladenen Dateien werden dann nicht mehr verschlüsselt. Bereits verschlüsselte Dateien bleiben aber verschlüsselt und um diese weiterhin lesen zu können müssen Sie das Verschlüsselungsmodul aktiviert lassen.

Dateien wieder entschlüsseln und unverschlüsselt speichern

Wenn Sie die Dateien wieder entschlüsseln möchten, beispielsweise um Speicherplatz auf dem Server zurückzugewinnen, können Sie dies mit dem folgenden Befehl tun:

sudo -u www-data php occ encryption:decrypt-all

Hinweis: Auch während dieser Aktion versetzt sich die Cloud automatisch in den Wartungsmodus. Bedenken Sie auch, dass dieser Prozess im Verhältnis sehr lange dauern kann.

Wenn Sie den obigen Befehl ausführen, wird neben der Entschlüsselung der Daten auch die Verschlüsselung deaktiviert. Falls Sie die Verschlüsselung bereits im Vorfeld deaktiviert haben sollten, müssen Sie diese erst wieder aktivieren, sonst wird die Entschlüsselung der Dateien leider nicht durchgeführt.

Sollten Sie nur die Dateien von einem einzelnen Nutzer entschlüsseln wollen, hängen Sie den Benutzernamen an den Befehl an, wie nachfolgend zu sehen:

sudo -u www-data php occ encryption:decrypt-all nutzername

In diesem Fall wird die Verschlüsselung nicht deaktiviert, sondern nur die Dateien des angegebenen Nutzers entschlüsselt und in diesem Zustand auf dem Server abgelegt.

Notiz: Auch nach der Entschlüsselung verbleiben Schlüssel im Ordner „files_encryption“.

Weitere Informationen zur serverseitigen Verschlüsselung

Weitere Informationen zum Thema finden Sie in der offiziellen Dokumentation zur serverseitigen Verschlüsselung. Leider ist die Dokumentation bereits etwas älter,

denn der Text bezieht sich noch auf Nextcloud 9, aktuell ist Version 18 und die 19 steht in den Startlöchern. Offensichtlich stimmen auch manche Aussagen nicht mehr, beispielsweise soll es Probleme mit verschlüsselten Dateien bei Passwortänderungen von Benutzer-Accounts geben. Diesbezüglich konnte ich in meinen Tests in den neueren Versionen aber keine Einschränkungen feststellen. Es scheint sich hier also ordentlich etwas getan zu haben.

Eindeutige ID: #1089
Verfasser: Hans-Wolfgang Hunsaenger
Letzte Änderung: 2020-06-24 16:46