iCreate Academy GENIUS

In iCreate Genius duiken we wat dieper in de Apple-materie. Met deze workshops leer je op een slimme manier nóg meer uit je Mac, iPhone en andere Apple-producten te halen.

# Stel goed in waar apps allemaal bij mogen

Tekst: Sven Lamers

Apps krijgen alleen toegang tot jouw gegevens als jij daar toestemming voor geeft. Maar wat betekent deze toegang in macOS, iOS en iPadOS precies en wat zijn de risico's?

Apps hebben altijd al toestemming moeten vragen om toegang te krijgen tot gevoelige informatie zoals je locatie. Maar veel andere gegevens bleven lange tijd onbeschermd. Apple heeft de controles inmiddels stap voor stap uitgebreid: tegenwoordig kun je tot in detail aangeven welke apps toegang mogen krijgen tot agenda's, contactpersonen, foto's, bluetooth, microfoon, camera, spraakherkenning of bepaalde mappen.

Deze autorisaties worden beheerd door het TCC-subsysteem – kort voor Transparency, Consent en Control. In macOS regelt het zelfs systeemgerelateerde zaken, zoals toegang tot automatiseringen of het systeemvolume. iOS en iPadOS maken het soms mogelijk om de toegang te nuanceren: zo maak je bijvoorbeeld alleen geselecteerde contacten of foto's toegankelijk, in plaats van het hele adresboek of de hele bibliotheek.

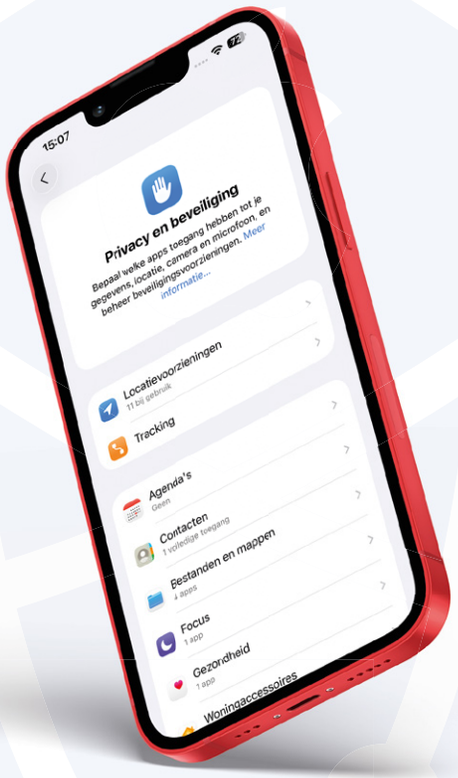
### Zo werkt TCC

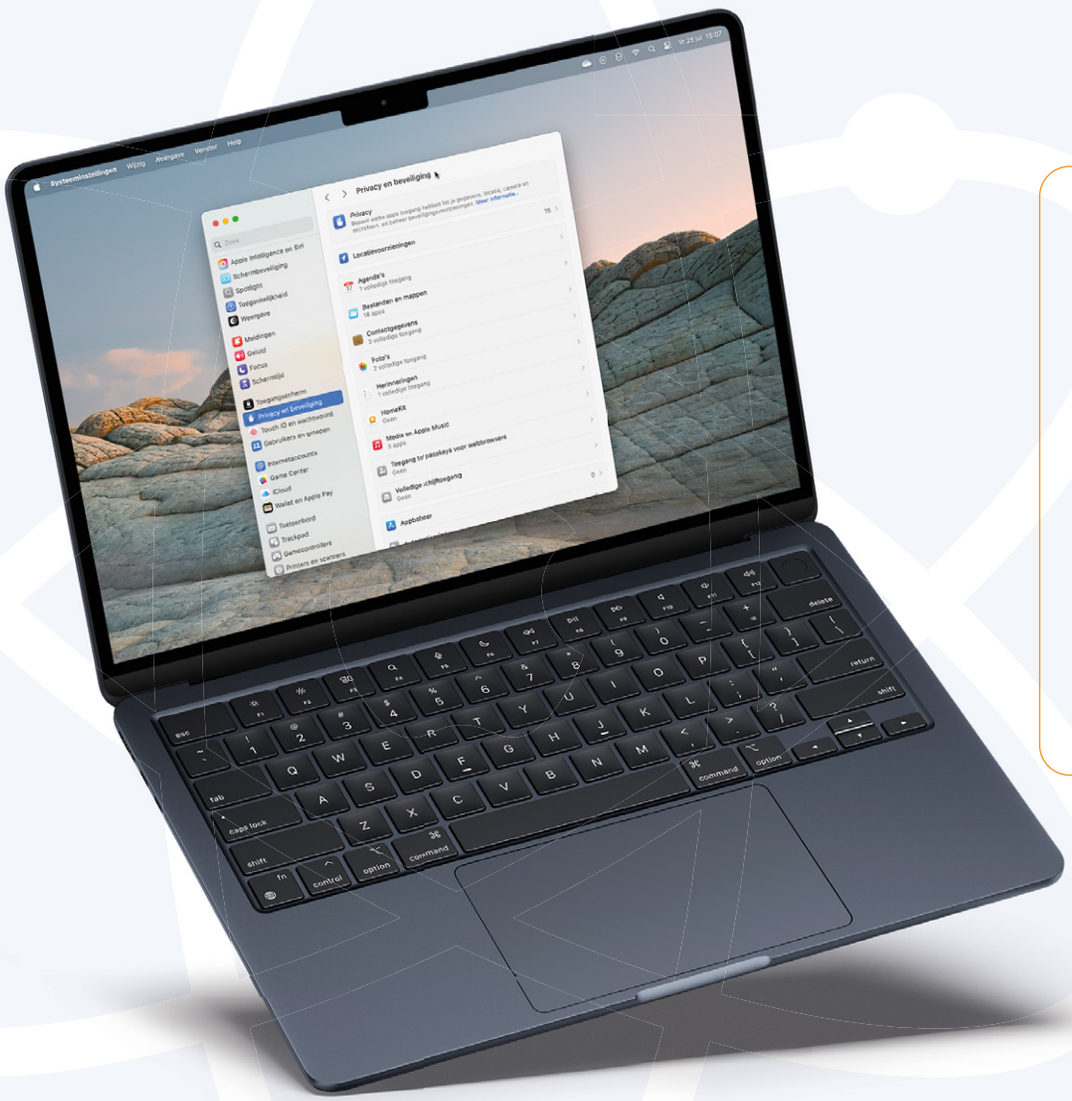
Als een app toegang wil krijgen tot 'beveiligde' zaken, wordt er een zogenaamde TCC Challenge gestart. Een systeemvenster vraagt of je de toegang wilt toestaan of weigeren. Je kunt je beslissing op elk moment wijzigen in de systeeminstelling 'Privacy en beveiliging'. Meestal verschijnt een app daar alleen als die daadwerkelijk om een beschermde bron vraagt. Op macOS kunnen programma's ook vooraf aan sommige categorieën worden toegevoegd met de plus-knop.

Wanneer je een beslissing hebt genomen, vraagt het systeem er niet opnieuw naar, maar verleent of weigert het voor altijd toegang. Hoe apps met geweigerde toegang omgaan, bepalen de ontwikkelaars. Sommige werken mogelijk helemaal niet meer, andere wel – maar met de nodige beperkingen.

Naast deze expliciete toestemmingen (dat heet 'consent') herkent macOS ook jouw impliciete intenties (een 'intent'). Als je bijvoorbeeld zelf vanuit een app een bestand opent of opslaat in beschermde mappen, dan wordt dit gezien als bewuste toestemming en krijg je geen melding om toestemming te geven. Wil een app voor altijd zelf toegang tot zo'n beveiligde map, dan is wel altijd expliciet toestemming nodig.

In deze Genius gaan we alle categorieën uit 'Privacy en beveiliging' langs waarin toegang kan worden verleend voor elke app. Naast mogelijke risico's geven we ook advies wanneer het zinvol is om toegang te verlenen. De secties zijn gegroepeerd per besturingssysteem. Voor macOS geven we ook de Engelse servicenaam voor het terminalprogramma 'tccutil', waarvan je gebruikmaakt om de machtigingen op de Mac opnieuw in te stellen (zie pagina 71).




### Algemene tips

- Vermijd dat je toegang tot alles geeft en sta alleen toe wat je echt nodig hebt.
- Je kunt toegang in eerste instantie weigeren en pas toestaan in de privacy-instellingen als de app niet werkt zoals verwacht.
- Controleer regelmatig welke apps toegang hebben tot gevoelige gegevens en trek onnodige autorisaties in.
- Geef de voorkeur aan Mac-apps uit de App Store. Apple controleert deze van tevoren. Zo weet je zeker dat apps geen rare dingen doen met je gegevens.

# macOS, iOS & iPadOS

### Beweging en conditie

Sport-apps mogen al je bewegingsgegevens van de iPhone of Apple Watch – zoals het aantal stappen, de gelopen afstand of de beklommen verdiepingen – alleen inzien na expliciete autorisatie. Voor Macs is dit nauwelijks relevant vanwege het ontbreken van sensoren.

#### Risico

Apple verwerkt weliswaar gegevens alleen lokaal en stuurt ze niet zomaar door, maar apps mogen dat wel als ze daarvoor jouw toestemming hebben. In combinatie met andere gegevens kan dit leiden tot gedetailleerde bewegings- of gezondheidsprofielen die gebruikt kunnen worden voor reclamedoeleinden.

#### Ons advies

Geef alleen toestemming voor toegang als er een duidelijk gezondheidsvoordeel is. Bijvoorbeeld voor apps voor training, revalidatie of documentatie. Controleer zo nodig het privacybeleid om te zien hoe apps met de gegevens omgaan.

#### Naam voor tccutil

Motion


### Bluetooth

Deze instelling bepaalt of apps je bluetooth mogen gebruiken. Bijvoorbeeld voor gegevensoverdracht, het detecteren van apparaten in de buurt of voor het koppelen van accessoires van derden zoals speakers, trackers en smartwatches. Op de Mac kunnen browsers ook om bluetooth-toegang vragen, bijvoorbeeld om via de iPhone met een wachtwoord in te loggen op websites.

#### Risico

Bluetooth kan worden gebruikt voor stille communicatie op de achtergrond. Bijvoorbeeld om de locatie te bepalen via zogeheten beacons of om bewegingspatronen in winkels te analyseren. Een gebrekkige bluetooth-integratie kan de deur openen voor aanvallen.

#### Ons advies

Bluetooth-toegang wordt alleen aanbevolen als een app het nodig heeft voor een duidelijk herkenbare functie, zoals bij audio-accessoires, gezondheidsapparaten of locatietrackers. Eenvoudige apps of games hebben over het algemeen geen toegang nodig.

#### Naam voor tccutil

BluetoothAlways


### Bestanden en mappen

Op iOS en iPadOS regelt dit of apps toegang krijgen tot door de gebruiker gedeelde inhoud in de Bestanden-app en of ze deze kunnen wijzigen. Op de Mac zijn bepaalde opslaglocaties speciaal beveiligd en kunnen ze afzonderlijk worden ontgrendeld – bijvoorbeeld 'Documenten', 'Downloads', 'Bureaublad', externe schijven of clouddiensten zoals iCloud Drive en Dropbox. Sinds macOS 10.15 geldt deze controle voor alle apps.

Apps hebben deze toegang nodig als ze vaak met bestanden werken waar ze van macOS, iOS of iPadOS niet standaard bij mogen – dat zijn bijvoorbeeld projectmappen of mediabibliotheken. Typische voorbeelden zijn bewerkingsprogramma's, muziek- en fotobeheerders, back-uptools of ontwikkelomgevingen. Bij het openen van je bestanden herkent het systeem de intentie van de gebruiker en staat het toegang toe, zelfs zonder expliciete deling. Overigens: als je volledige toegang tot de harde schijf geeft (zie pagina 69), dan is select delen van mappen niet langer mogelijk – de app in kwestie kan dan vrijwel altijd alle bestanden van de gebruiker bekijken.

#### Risico

Toegang stelt een programma in staat om automatisch de inhoud van mappen en bestanden te lezen en te wijzigen, ook op de achtergrond. Dit is noodzakelijk voor veel programma's, maar wordt gevaarlijk als iemand kwaadaardige bedoelingen heeft. Vooral als malware deze rechten krijgt, zijn je persoonlijke gegevens in gevaar.

#### Ons advies

Geef alleen toegang tot apps die duidelijk met bestanden werken, zoals Office-programma's,


ontwikkelaarstools, back-upsoftware of browsers (downloadmap). Voor andere apps kun je jouw bestanden beter rechtstreeks vanuit de app openen en geen volledige toegang geven.

**Namen voor tccutil**

Downloads: SystemPolicyDownloadsFolder
Externe volumes: SystemPolicyRemovableVolumes
iCloud Drive: FileProviderDomain
Netwerkvolumes: SystemPolicyNetworkVolumes
Documenten: SystemPolicyDocumentsFolder
Bureaublad: SystemPolicyDesktopFolder

## Herinneringen

Apps met deze autorisatie hebben toegang tot je taken in de app Herinneringen. Taken kunnen worden gemaakt, uitgelezen of gesynchroniseerd met andere diensten.

**Risico**

Je taken bevatten vaak persoonlijke inhoud, zoals vervaldatums, notities en gekoppelde locaties. Kwaadwillende apps zouden takenlijsten kunnen lezen, analyseren of doorgeven, bijvoorbeeld voor profilering of gedragsanalyse.

**Ons advies**

Autoriseer alleen vertrouwde agenda-apps, spraakassistenten of alternatieve taakplanners met een verbinding naar de Herinneringen-app.

**Naam voor tccutil**

Reminders

## Focus

Apps met toegangsrechten kunnen zien of een focusmodus zoals 'Niet storen' actief is, bijvoorbeeld om meldingen te onderdrukken of al jouw berichtenconversaties op stil te zetten.

**Risico**

Hoewel de focusstatus geen inhoud bevat, kan deze wel informatie geven over jouw bereikbaarheid. Kwaadwillende of (te) nieuwsgierige messaging-apps kunnen dit zoal misbruiken om je in de gaten te houden.

**Ons advies**

Sta alleen toegang toe als de app duidelijk laat zien waarvoor hij de focusmodus gebruikt. Welke focus je wilt delen, kun je aangeven via de systeeminstelling bij 'Focus>Focusstatus'.

**Naam voor tccutil**

FocusStatus

## Foto's

Je kunt kiezen of apps de volledige mediabibliotheek mogen zien of alleen een specifieke selectie van je foto's en video's. In iOS / iPadOS wordt deze nauwkeurigere instelling altijd gebruikt, op macOS vragen de meeste apps helaas meestal direct om volledige toegang.

**Risico**

Foto's bevatten vaak meer informatie dan je denkt, zoals locaties, data, cameragegevens of herkende personen. Kwaadwillende apps kunnen deze data en de beeldinhoud analyseren en ongemerkt doorsturen naar derden. Bijvoorbeeld om profielen aan te maken, je privéleven te onderzoeken of zelfs wachtwoorden te vinden in schermafbeeldingen.

**Ons advies**

Verleen alleen algemene toegang als een app duidelijk bedoeld is om foto's te beheren of als het handig is dat-ie bij al je foto's kan, zoals bij WhatsApp. Voor beeldbewerking van slechts bepaalde foto's kun je beter alleen toegang geven tot individuele media.

**Naam voor tccutil**

Photos

## Woningaccessoires

HomeKit-toegang omvat scènes, automatiseringen en apparaten zoals lampen, camera's, thermostaten en deursloten. Het grootste deel van de bediening vindt plaats in het lokale netwerk, zonder dat er externe servers bij betrokken zijn, en is ook versleuteld. Een Woninghub (Apple TV, HomePod) en een internetverbinding zijn alleen nodig als je je slimme woning op afstand wilt bedienen.

**Risico**

Smarthome-gegevens kunnen in de verkeerde handen veel onthullen over je dagelijkse routines, gewoontes en de beveiliging van je huis. HomeKit staat echter geen algemene toegang toe: je moet elke autorisatie specifiek toestaan. Beelden van HomeKit-camera's, kunnen apps zelfs helemaal niet bekijken. En een frauduleuze app kan niet zomaar je slimme deurslot op afstand openen. Hiervoor moet je iPhone ontgrendeld zijn en de app geopend.

**Ons advies**

Ondanks de bescherming van Apple: geef alleen toegang tot apps waarmee je bewust en actief je HomeKit-apparaten wilt bedienen. Sommige apps van fabrikanten van smarthome-apparaten vereisen deze toegang ook.

**Naam voor tccutil**

Willow

## Agenda

Geautoriseerde apps hebben toegang tot alle opgeslagen afspraken, ook van gekoppelde accounts zoals iCloud, Google of Exchange. Het is niet mogelijk om toegang tot individuele agenda's te beperken. Als een app dit ondersteunt, kun je ook toestaan dat alleen nieuwe items worden toegevoegd.

### Risico

Kalenders onthullen gevoelige informatie, zoals contacten en geplande afwezigheid. Kwaadwillende apps zouden deze gericht kunnen analyseren, bijvoorbeeld om neptelefoontjes met achtergrondinformatie voor te bereiden, bedrijfsprocessen te bespioneren of zelfs je afwezigheid te gebruiken voor inbraken.

### Ons advies

Volledige toegang wordt in dit geval alleen aanbevolen als je wilt dat een app actief je afspraken beheert. Denk aan alternatieve agenda's, zoals Fantastical of BusyCal. Stel bij twijfel liever in dat apps alleen nieuwe afspraken mogen toevoegen.

### Naam voor tccutil

Calendar

## Camera

Apps met cameratoegang kunnen foto's en video's maken, zoals camera-apps of documentscanners. Macs markeren de actieve camera met een groen lichtje bovenin, iOS en iPadOS via een groene stip in de balk bovenin.

### Risico

Naast het camerabeeld zelf, slaan veel apps ook metadata op zoals tijd, scherptediepte of locatie (indien toegestaan). Kwaadwillende apps kunnen zonder reden opnames maken of deze combineren met andere sensoren, bijvoorbeeld voor gezichtsherkenning. macOS en iOS geven dergelijke toegangen weer, maar het groene stipje valt niet altijd op. Het wordt ook kritiek als een app ongemerkt extra opnames maakt naast schijnbaar correcte functies.

### Ons advies

Geef alleen toestemming voor toegang als de camera een centraal onderdeel van de app is. Bijvoorbeeld bij apps voor videobellen, scanners of camera's. Weiger anders de toegang of verleen deze slechts tijdelijk.

### Naam voor tccutil

Camera

## Contacten

Als je apps toegang geeft tot het adresboek, kunnen ze alle opgeslagen contacten bekijken. Alleen in iOS en iPadOS kan de toegang worden beperkt tot individuele contacten of adreslijsten.

### Risico

Je contacten bevatten niet alleen jouw eigen persoonlijke gegevens, maar ook die van derden. Inclusief namen, telefoonnummers, notities, e-mailadressen en profielfoto's. Als apps de gegevens overzetten naar hun servers zonder toestemming van de betrokkenen, is dit technisch gezien in strijd met de Europese AVG-wetgeving. Kwaadwillende apps misbruiken dergelijke toestemmingen vaak voor identiteitsdiefstal.

### Ons advies

Verleen alleen toegang aan apps die actief met contactgegevens moeten werken, waaronder mailprogramma's of alternatieve beheer-apps voor contacten zoals Cardhop en BusyContacts. Gebruik indien mogelijk altijd 'Beperkte toegang' in 'Privacy en beveiliging>Contacten' in iOS en iPadOS om alleen toegang te verlenen tot je geselecteerde contactpersonen. Dat geldt vooral voor messengers op basis van telefoonnummers, zoals WhatsApp.

### Naam voor tccutil

AddressBook

## Media en Apple Music

Een app kan toegang krijgen tot je muziek- en videodata in jouw mediabibliotheek en tot je afspeellijsten en gebruiksinformatie van Apple Music, zoals recent afgespeelde nummers of aanbevelingen.

### Risico

Ook als de media zelf niet als gevoelige informatie wordt beschouwd, kunnen uit luistergewoontes conclusies worden getrokken over je voorkeuren, stemming of dagelijkse routines. In combinatie met andere gegevens is ook gebruik voor reclame of analytische doeleinden denkbaar.

### Ons advies

Weiger toegang, tenzij een toepassing interactie nodig heeft met de mediabibliotheek van je systeem – bijvoorbeeld als widget of alternatieve muziekspeler.

### Naam voor tccutil

MediaLibrary

## Lokaal netwerk

Als apps op het netwerk willen zoeken naar apparaten, zoals printers of diensten zoals mediaservers, dan hebben ze sinds macOS 15, iOS 14 en iPadOS 14 je uitdrukkelijke toestemming nodig. Die toestemming heeft alleen invloed op de detectie van apparaten in je netwerk. Gedeelde mappen van andere computers die je bijvoorbeeld in Finder opent, blijven toegankelijk – ook al geef je geen toestemming.

### Risico

De samenstelling van je netwerk is vrij uniek en aan de hand daarvan kunnen bedrijven een profiel van je aanmaken, je volgen en gerichte reclame sturen. Daarnaast kunnen kwaadaardige apps de toegang gebruiken om te zoeken naar mogelijk kwetsbare apparaten in het thuis- of bedrijfsnetwerk, bijvoorbeeld om deze aan te vallen.

### Ons advies

Sta alleen toegang toe voor de apps die daadwerkelijk afhankelijk zijn van apparaten in hetzelfde netwerk, zoals diagnostische tools, smarthome-gereedschappen of streaming-apps. Programma's zoals spelletjes, tekstverwerkers of Office-apps hebben deze toegang niet nodig.

### Naam voor tccutil

Geen

## Microfoon

Apps met deze toestemming mogen geluid opnemen via de interne of externe microfoon. macOS geeft actief gebruik aan via een oranje stip naast het Bedieningspaneel-icoon, in iOS en iPadOS vind je die in de statusbalk.

### Risico

Als kwaadaardige apps toegang hebben tot de microfoon, kunnen ze ongemerkt gesprekken of andere audio opnemen. Als de waarschuwing van het systeem over het hoofd wordt gezien, kan dit problematisch zijn, zeker met gevoelige informatie in een professionele context.

### Ons advies

Je moet geen toegang verlenen zonder een duidelijk herkenbare verbinding met audio, zoals voor spraakchats, muziekopnames of dicteren. Tijdelijk delen kan alleen op een nogal omslachtige manier via de instellingen.

### Naam voor tccutil

Microphone


## Locatievoorzieningen

Hier geef je aan of apps, websites en systeemservices de huidige locatie mogen bepalen, bijvoorbeeld via bluetooth, gps of wifi. Locatievoorzieningen geven informatie over je woonplaats, werkplek en verblijfplaats en zijn daarom van centraal belang voor privacy, vooral op de iPhone. Tegelijkertijd geeft Apple je hier nog veel uitgebreidere instellingsmogelijkheden. In het volgende nummer wijden we hier nog een aparte workshop aan.

### Naam voor tccutil

Location

## Spraakherkenning

Sinds iOS 13 en macOS 10.15 is expliciete toestemming vereist als apps spraakopnames willen omzetten naar tekst via het besturingssysteem. Veel talen worden lokaal verwerkt, maar Apple benadrukt dat audiogegevens eventueel ook anoniem op hun servers worden verwerkt.

### Risico

Apps van derden met twijfelachtige of verborgen bedoelingen kunnen mogelijk inhoud lezen, opslaan en analyseren. Ze hebben microfoontoegang nodig voor een permanent live transcript van gesprekken in de buurt. Die toegang herken je dan aan de oranjegekleurde systeemindicator.

### Ons advies

Geef alleen toegang als spraakherkenning een centrale functie is, bijvoorbeeld voor dicteerhulpmiddelen, transcriptiediensten of toegankelijkheidstools.

### Naam voor tccutil

SpeechRecognition

## Toegang tot passkeys voor webbrowsers

Sinds iOS 17 en macOS 14 Sonoma hebben browsers van derden ook toegang tot passkeys die in de (iCloud-)sleutelhanger zijn bewaard. Passkeys zullen op den duur traditionele wachtwoorden vervangen en werken alleen op het oorspronkelijk geregistreerde of geautoriseerde Apple-apparaat.

### Risico

Passkeys bieden een effectieve bescherming tegen phishing: ze werken alleen met de oorspronkelijk geregistreerde website of dienst, dus niet op een nagemaakte kopie. Ze zijn toegankelijk via de eigen interfaces van het besturingssysteem – de app krijgt geen directe toegang tot de sleutel, en die verlaat het apparaat ook nooit. Het enige probleem zou een gemanipuleerde browser zijn die websites verandert of gebruikersinteracties bespioneert. De kans daarop is miniem.

### Ons advies

Gebruik alleen betrouwbare browsers die goed worden onderhouden. Installeer extensies alleen via officiële kanalen en zorg dat je ze up-to-date houdt.

### Naam voor tccutil

WebBrowserPublicKeyCredential

## Accessoires

Sinds macOS 13 wordt er altijd aan je gevraagd of nieuw aangesloten usb- en Thunderbolt-apparaten geactiveerd mogen worden, maar alleen op Macs met Apple Silicon. Dit beschermt tegen aanvallen met gemanipuleerde usb-apparaten die zich bijvoorbeeld voordoen als toetsenbord of netwerkinterface. De autorisatie geldt voor het hele systeem en kan in verschillende stappen worden geconfigureerd, ergens tussen 'Vraag altijd' en 'Sta altijd toe'

In iOS 18 en iPadOS 18 geeft deze instelling een lijst van apps die toegang mogen hebben tot accessoires die zijn ingesteld via de zogeheten AccessorySetupKit. Dit menuutje zie je ook als je bijvoorbeeld een HomeKit-apparaat toevoegt of je AirPods koppelt. Het maakt het koppelen veel makkelijker en werkt met bluetooth, wifi en vele andere standaarden. Bluetooth-apparaten kun je overigens nog steeds apart beheren in 'Bluetooth'.

### Risico

Op een Mac kunnen gemanipuleerde accessoires, mits ze zijn geautoriseerd, gegevens uitlezen of kwaadaardige code toevoegen. Onder iOS zorgt de nieuwe accessoirecategorie voor aanzienlijk meer transparantie en controle dan de algemene 'Bluetooth'-instelling.

### Ons advies

Selecteer onder macOS ten minste 'Vraag voor nieuwe accessoires'. 'Vraag altijd' is nog veiliger, maar behoorlijk onhandig. Als je het verzoek afwijst, voorzie je bedraad aangesloten apparaten overigens nog wel van stroom.

### Naam voor tccutil

Geen

# Alleen in macOS

### Appbeheer

macOS regelt hier welke programma's andere software mogen installeren, verwijderen of bijwerken, zoals pakketbeheerders, admin- of update-tools en hulpprogramma's voor installaties met uitgebreide systeemtoegang.

**Risico**

Malware met deze toegang kan in het geheim programma's laden, verwijderen of manipuleren. En zo bijvoorbeeld hardnekkige backdoors opzetten of beschermende functies van het besturingssysteem omzeilen.

**Ons advies**

Alleen betrouwbare tools, waaronder MacUpdater of Setapp, en installatieprogramma's van bekende bedrijven mogen deze toegang krijgen.

**Naam voor tccutil**

SystemPolicyAppBundles

### Scherm- en systeemaudio-opname

Deze toegang stelt apps in staat om de scherminhoud op te nemen, inclusief muisbewegingen, vensterinhoud en systeemgeluiden. Typische toepassingen zijn apps voor schermafbeeldingen, software voor videobellen en programma's voor beheer op afstand. Sommige apps (vaak kleine hulpprogramma's) gebruiken Schermopname ook als omweg voor compleet andere functies, net zoals dat bij Toegankelijkheid het geval is.

**Risico**

Programma's met kwaadaardige bedoelingen kunnen een breed scala aan gevoelige inhoud opnemen, waaronder e-mails, chatgeschiedenis, vertrouwelijke documenten, presentaties of financiële gegevens, maar ook gesprekken en videoconferenties. Hulpmiddelen voor beheer op afstand met permanente toegang zijn bijzonder gevaarlijk. Deze kunnen ongemerkt worden misbruikt voor afluisteren.

**Ons advies**

Geef alleen toegang tot programma's met een duidelijk doel, bijvoorbeeld de apps Zoom, Loom of CleanShot. Geef bij software voor onderhoud op afstand (Remote Desktop, TeamViewer) de voorkeur aan tijdelijke toegang in plaats van permanente toegang.

**Naam voor tccutil**

ScreenRecording

### Automatisering

Populaire tools zoals Keyboard Maestro, BetterTouchTool, Alfred of Raycast breiden de functies van macOS uit door andere programma's aan te sturen via Apple Events, vergelijkbaar met AppleScript, Automator of sneltoetsen. Ze kunnen worden gebruikt om vensters te sluiten, inhoud te kopiëren of om complexe processen in meerdere programma's te automatiseren.

**Risico**

Malware kan deze toegang gebruiken om externe processen op afstand te besturen, inhoud te lezen of ongemerkt opdrachten uit te voeren, bijvoorbeeld om gevoelige gegevens uit te lezen. Hoewel macOS vraagt om autorisatie voor elke nieuwe app, geeft het blind bevestigen hiervan uitgebreide controle aan de malware.

**Ons advies**

Geef alleen toegang tot automatisering als je de app vertrouwt en begrijpt waarom hij andere processen op afstand wil besturen. Als je echt twijfelt, stuur dan vooral even een mail naar redactie@icreatemagazine.nl of neem direct contact op met de ontwikkelaar.

**Naam voor tccutil**

AppleEvents

### Toegankelijkheid

Programma's met toegang tot de toegankelijkheidsfuncties kunnen macOS actief besturen. Bijvoorbeeld muisacties nabootsen, toetsaanslagen activeren of beeldscherminhoud onderzoeken. Deze interface werd oorspronkelijk gebruikt voor toegankelijkheid, maar inmiddels ook door gewone tools zoals Keyboard Maestro, TeamViewer of AnyDesk en vensterbeheerders zoals Rectangle en Moom.

**Risico**

Als malware misbruik maakt van deze uitgebreide toegang, dan kan het ongemerkt vertrouwelijke inhoud zoals teksten en documenten lezen of wijzigen. In combinatie met schermopname of automatisering is theoretisch bijna volledige controle over het systeem mogelijk.

**Ons advies**

Geef alleen toegang als het essentieel is voor een app, bijvoorbeeld voor automatisering, toegang op afstand of vensterbeheer. Gerenommeerde ontwikkelaars geven meestal een duidelijke uitleg waarom toegang nodig is.

**Naam voor tccutil**

Accessibility

### Invoer vastleggen

Een geautoriseerde app mag toetsaanslagen binnen het hele systeem vastleggen. Toegestaan gebruik is er voor tekstvervangers, sneltoetsbeheerders of automatiseringstools zoals Keyboard Maestro, TextExpander, BetterTouchTool of Alfred.

**Risico**

Gemanipuleerde software kan deze toegang gebruiken om alle invoer te lezen (keylogging). Inclusief geschreven berichten, creditcardgegevens en in het ergste geval wachtwoorden. Hoewel macOS de opname van speciaal gemarkeerde wachtwoordvelden blokkeert, implementeren niet alle apps deze bescherming correct.

**Ons advies**

Verleen deze toegang uiterst voorzichtig en alleen voor al je vereiste functies. Bijvoorbeeld voor sneltoetsen die overal moeten werken of voor tekstvervanging.

**Naam voor tccutil**

ListenEvent

### Ontwikkeltools

Xcode en andere ontwikkelgereedschappen in Terminal hebben deze toegang nodig om bepaalde software uit te voeren die niet door Apple goedgekeurd is. Of in andere woorden: die niet voldoet aan de beveiligingseisen van macOS. Dit is vooral nodig bij het testen van je eigen programma's.

**Risico**

Malware kan deze toegang gebruiken om niet-ondertekende programma's uit te voeren en zo specifieke beveiligingsfuncties zoals Gatekeeper te omzeilen. Vooral gemanipuleerde scripts of ontwikkelaarstools met verborgen kwaadaardige code zijn verraderlijk.

**Ons advies**

Geef deze toegang alleen als je actief software ontwikkelt of een officieel ontwikkelprogramma gebruikt. Wees vooral voorzichtig met code van externe bronnen, zoals GitHub: controleer de herkomst en functionaliteit altijd zorgvuldig. Apps buiten de ontwikkelcontext, zoals kantoorsuites, games of browsers, hebben deze autorisatie écht niet nodig.

**Naam voor tccutil**

DeveloperTool

### Volledige schijftoegang

Back-upprogramma's zoals Carbon Copy Cloner, antivirus-apps (zoals Malwarebytes) en sommige systeemtools hebben volledige toegang tot de harde schijf nodig om beschermde delen van de Mac te kunnen lezen en bewerken. Hieronder vallen ook mails, berichten, Safari-gegevens, agenda's, contactpersonen en delen van de Bibliotheek-map die niet kunnen worden gedeeld in de categorie 'Bestanden en mappen'. Logisch: als je toegang tot de volledige schijf geeft, zijn alle instellingen van 'Bestanden en mappen' (zie pagina 64) niet meer geldig.

**Risico**

Volledige schijftoegang is een van de meest vergaande autorisaties in macOS. Malware met deze toegang is in staat om gevoelige informatie te stelen, belangrijke bestanden te verwijderen, te versleutelen (ransomware) of je systeem op andere manieren binnen te dringen. Het is bovendien gemakkelijk om per ongeluk volledige toegang te geven zonder dat je het doorhebt.

**Ons advies**

Wees extreem voorzichtig met volledige toegang tot de schijf. Verleen deze alleen aan programma's die het aantoonbaar nodig hebben voor de centrale functies, zoals back-ups van de hele Mac, malwarescans of systeemanalyses. Als alledaagse programma's zoals browsers, kantoorprogramma's of spelletjes zonder duidelijke reden om deze toegang vragen, moet je ze meteen verwijderen.

**Naam voor tccutil**

SystemPolicyAllFiles

### Remote Desktop

Deze categorie is met macOS Sequoia geïntroduceerd en vult de bestaande categorieën 'Schermopname' en 'Toegankelijkheid' aan met een specifieke toegang voor beheer op afstand. Programma's voor remote desktop, zoals TeamViewer, hebben deze extra toegang nodig om via het netwerk toegang te krijgen tot schermen en systeemaudio en om de muis en het toetsenbord op afstand te bedienen.

**Risico**

Als malware toegang krijgt tot deze interface, kan het je Mac volledig op afstand besturen en beeld, geluid en andere invoer opnemen. Aanvallers kunnen zo toegang krijgen tot vertrouwelijke informatie, malware installeren, systeeminstellingen wijzigen of in jouw naam acties uitvoeren. In het ergste geval kunnen ze het systeem volledig overnemen.

**Ons advies**

Activeer Remote Desktop alleen als je externe toegang nodig hebt. Bijvoorbeeld voor vertrouwde IT-ondersteuning of voor toegang tot je eigen apparaten. Wees heel alert bij ongevraagde e-mails of telefoontjes waarin vermeend ondersteunend personeel je vraagt om zulke apps te installeren. Dit is een veelvoorkomende truc om toegang te krijgen tot je systeem.

**Naam voor tccutil**

RemoteDesktop

# Alleen in iOS en iPadOS

### Kritieke berichten

Apps met toegang kunnen berichten versturen naar opgegeven telefoonnummers via de Critical Messaging API. Apple staat deze functie alleen toe in uitzonderlijke, duidelijk gedefinieerde gevallen, zoals veiligheids- of gezondheidswaarschuwingen, Check-in-berichten of andere kritieke scenario's. Voor gebruik is expliciete toestemming van Apple nodig. Tot nu toe zijn er (volgens ons) nog geen apps die deze interface daadwerkelijk gebruiken.

**Risico**

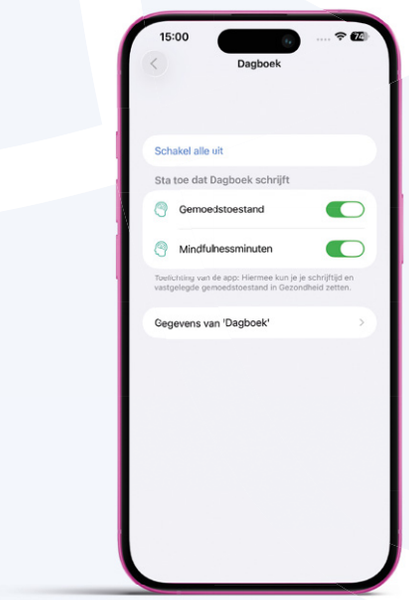
Een app kan ongemerkt op de achtergrond tekstberichten versturen, zelfs als je apparaat is vergrendeld.

**Ons advies**

Geef deze toegang alleen als het echt absoluut noodzakelijk is, bijvoorbeeld in een professionele context. Anders moet je het altijd gedeactiveerd laten.

### Gezondheid

Hier bepaal je welke apps toegang tot gezondheids- en fitnessgegevens hebben, zoals stappen, hartslag, slaapduur, fietsgeschiedenis, voedingsinformatie of je geestelijke gezondheid. Deze toegang kan afzonderlijk worden geconfigureerd voor elke app en elk van de meer dan 170 gegevenscategorieën, zelfs met verschil in lees- en schrijfrechten. Veel applicaties hebben slechts gedeeltelijke toegang nodig, bijvoorbeeld om trainingsgegevens op te slaan of calorieverbruik uit te lezen.




**Risico**

Gezondheidsgegevens behoren tot de meest gevoelige informatie op je iPhone. Als deze gegevens uitgebreid worden gedeeld, dan kunnen er gedetailleerde conclusies worden getrokken over je fysieke en mentale toestand. Apple beschermt deze informatie met lokale toegangscontroles, transparante toegangsmeldingen en versleuteling via iCloud. Frauduleuze apps kunnen echter proberen om toegang te krijgen tot gevoelige gezondheidsgegevens via vermeend onschuldige functies.

**Ons advies**

Apps met deze toegang moeten een duidelijk verband hebben met gezondheid en een logisch gebruik. Bijvoorbeeld voor het analyseren van trainings-, slaap- of voedingsgegevens. Zelfs als een app om algemene toegang vraagt, geef je alleen maar toegang tot de voor jou relevante gegevenscategorieën.

### Interacties in de buurt

Systeemfuncties zoals AirDrop of 'Zoek mijn' maken gebruik van bluetooth, ultra-wideband (UWB) en andere draadloze technologieën om te communiceren met apparaten in de buurt. Apps van derden kunnen nu soortgelijke functies bieden, maar dat vereist expliciete toestemming van de gebruiker.

**Risico**

De onderliggende draadloze technologieën maken zeer nauwkeurige detectie en lokalisatie van apparaten in de buurt mogelijk. Ondanks beschermingsmechanismen zoals app-reviews en wisselende MAC-adressen (dat zijn eigenlijk unieke adressen van álle apparaten met netwerktoegang), kunnen apps proberen om bewegingsprofielen aan te maken. Bijvoorbeeld om mensen te volgen of te achterhalen wie wanneer iemand heeft ontmoet.

**Ons advies**

Sta toegang alleen toe als een app daadwerkelijk moet communiceren met apparaten of mensen in je omgeving. Bijvoorbeeld voor AirDrop-achtige overdrachten of koppelingsfuncties. Er is meestal geen legitieme reden om deze interface te gebruiken voor toepassingen zoals muziek afspelen, messenger of agenda.

### Tracking

Sommige aanbieders willen graag het gedrag van gebruikers in apps en websites analyseren, mogelijk om gepersonaliseerde advertenties weer te geven. Technisch gezien gebeurt dit vaak via de zogeheten reclame-ID (IDFA). Sinds iOS 14.5 vereist het systeem je uitdrukkelijke toestemming.

**Risico**

Uitgebreide tracking stelt aanbieders in staat om je interesses, gewoonten en gedrag nauwkeurig te analyseren. Vaak zonder dat je het weet.

**Ons advies**

Er is geen reden om deze tracking toe te staan. Schakel daarom de optie 'Sta trackingverzoeken van apps toe' uit. Dit zal de functionaliteit van apps niet beperken.

# Zo herstel je de toegangsinstellingen naar fabrieksinstellingen

Nu ken je alle categorieën waar apps toegang tot kunnen hebben. Wil je alles opnieuw en goed instellen? Dat doe je zo.


### iOS en iPadOS

Als je veel apps hebt geïnstalleerd en niet moeizaam app voor app wilt controleren welke toegang actief is, kun je ook alles in één klap opnieuw instellen. Zo begin je helemaal opnieuw en beslis je welke toegangsrechten echt nodig zijn de volgende keer dat je een app gebruikt.

Ga naar 'Instellingen>Algemeen', kies 'Zet over of stel iPhone opnieuw in' en tik vervolgens op 'Stel opnieuw in'. Selecteer 'Herstel locatie en privacy' in het menu dat verschijnt. Bevestig het proces met je code.

### macOS

In macOS werkt het resetten alleen via Terminal. Hiermee kun je echter niet alleen alles resetten, maar ook een specifiek aspect zoals de toegang tot de microfoon. Start Terminal, bijvoorbeeld vanuit Spotlight. Typ het volgende commando om alle privacy-instellingen te resetten:

```
tccutil reset all
```

Als je bijvoorbeeld alleen de toegang tot de map Downloads opnieuw wilt instellen, vervang dan 'all' door de gewenste servicenaam. Je vindt deze in de secties over de verschillende categorieën.

```
tccutil reset ScreenRecording
```