Kontogesteuerte Apple-Registrierung

Bei der kontogesteuerten Registrierung registrieren Benutzer ihr iPhone, iPad oder ihren Mac, indem sie sich in den Geräteeinstellungen mit ihrem Arbeitskonto (einem **Verwalteten Apple Account**, zum Beispiel *name@company.com*) anmelden. Kein Profil zum Herunterladen und kein QR-Code: Cerberus Enterprise findet den Benutzer, wendet die Richtlinie an und legt das Eigentum selbst fest.

Zwei Modi

- **Benutzerregistrierung** (private Geräte): Nur die Arbeits-Apps, Konten und Daten werden in einem separaten Bereich des Geräts verwaltet. Cerberus kann keine privaten Daten einsehen, das Gerät nicht löschen, nicht orten und die Seriennummer nicht lesen. Das Gerät wird als privat genutzt festgelegt. Erfordert iOS und iPadOS 15 oder macOS 14 oder höher.
- **Geräteregistrierung** (Unternehmensgeräte, die nicht in Apple Business sind): Das gesamte Gerät wird verwaltet, wie bei einer manuellen Registrierung. Ein so registrierter Mac ist überwacht; ein iPhone oder iPad nicht. Das Gerät wird als unternehmenseigen festgelegt. Erfordert iOS und iPadOS 17.1 oder macOS 14.1 oder höher.

> Sie wählen den Modus für iPhone und iPad und separat für Mac: zum Beispiel Benutzerregistrierung für private iPhones und Geräteregistrierung für Macs. Das Eigentum eines Geräts können Sie später auf der Geräteseite ändern.

> Die kontogesteuerte Registrierung ist verfügbar, wenn Apple Management (APNs) konfiguriert ist. Wenn Sie die APNs-Einrichtung noch nicht abgeschlossen haben, lesen Sie **Apple Management-Einrichtung (APNs)**.

Apple Business einrichten

Benutzer melden sich mit Verwalteten Apple Accounts an, die in Apple Business erstellt werden. Bevor Sie beginnen:

1. **Verifizieren Sie Ihre Domain** (zum Beispiel *company.com*) in Apple Business unter den Domains Ihrer Organisation.
2. **Erstellen Sie die Verwalteten Apple Accounts** Ihrer Benutzer oder verbinden Sie Apple Business mit Google Workspace oder Microsoft Entra ID: Dann ist das Konto jedes Benutzers seine geschäftliche E-Mail-Adresse, und er meldet sich mit deren Passwort an.
3. Prüfen Sie für die Benutzerregistrierung in den Zugriffsverwaltungseinstellungen, ob sich Verwaltete Apple Accounts auf **privaten Geräten** anmelden können: Wenn sie sich nur auf überwachten Geräten anmelden können, schlägt die Benutzerregistrierung fehl.
4. Nur für die unten beschriebene Option **Apple Business**: Öffnen Sie **Geräte** → **Verwaltungsdienste** → **Standardgerätezuweisung** (Bearbeiten) und wählen Sie den Geräteverwaltungsdienst Cerberus Enterprise für iPhone, iPad und Mac.

> Behalten Sie den Geräteverwaltungsdienst Cerberus Enterprise und sein Token in Apple Business, solange Geräte mit Verwalteten Apple Accounts registriert sind: Wenn Sie sie entfernen, funktionieren die Konten auf den Geräten möglicherweise nicht mehr.

Cerberus Enterprise einrichten

Öffnen Sie den Abschnitt **Registrierung** des Dashboards und wählen Sie die Registerkarte **Apple-Kontoanmeldung**. Eine Checkliste oben zeigt an, was noch fehlt. Nur Administratoren können die Einstellungen ändern.

- **Registrierung durch Anmelden mit einem Arbeitskonto zulassen**: schaltet die kontogesteuerte Registrierung für die gesamte Organisation ein oder aus.
- **Domains**: die Domains der Konten Ihrer Benutzer (zum Beispiel *company.com*), bis zu 20. Nur Konten dieser Domains können sich registrieren, und erst nachdem die Domain verifiziert wurde (siehe unten).
- **iPhone und iPad** und **Mac**: Aus, Benutzerregistrierung oder Geräteregistrierung für jede Gerätefamilie.
- **Richtlinie** jedes Modus: wird auf die Geräte angewendet, sobald sie sich registrieren. Ohne Richtlinie werden die Geräte ohne Richtlinie registriert. Eine geänderte Richtlinie gilt für die nächsten Registrierungen.
- **Benutzer**: *Nur vorhandene Benutzer* (die E-Mail-Adresse eines Benutzers in Cerberus Enterprise muss mit dem auf dem Gerät eingegebenen Konto übereinstimmen) oder *Benutzer für Konten der Domains erstellen, die noch keinen haben*.

> Das auf dem Gerät eingegebene Konto wird mit dem Feld **Verwaltetes Apple Account** der Benutzer und dann mit ihrer E-Mail-Adresse abgeglichen. Der Code wird immer an die E-Mail-Adresse des Benutzers gesendet. Ein für einen Benutzer festgelegtes Verwaltetes Apple Account kann sich auch dann registrieren, wenn seine Domain in Cerberus nicht verifiziert ist, zum Beispiel ein Konto der reservierten Domain *org.appleid.com* von Apple Business. Bei

> der Service Discovery über Apple Business geben Benutzer immer ihr Verwaltetes Apple Account ein.

Domains verifizieren

Nachdem Sie die Einstellungen gespeichert haben, zeigt der Abschnitt **Domain-Verifizierung** für jede Domain einen TXT-Eintrag an. Fügen Sie ihn dem DNS der Domain hinzu und klicken Sie dann auf **Verifizieren**. DNS-Änderungen können einige Zeit dauern, bis sie sichtbar sind. Eine verifizierte Domain bleibt verifiziert: Sie können den Eintrag anschließend entfernen. Benutzer einer nicht verifizierten Domain können sich nicht registrieren.

Service Discovery: Wie Geräte Cerberus Enterprise finden

Wenn sich ein Benutzer anmeldet, fragt das Gerät die Domain des Kontos (zum Beispiel *https://company.com*), welcher Server sie verwaltet. Richten Sie mindestens eine dieser drei Optionen ein. Der Abschnitt **Service Discovery** der Registerkarte zeigt die Discovery-URL Ihrer Organisation und den genauen Text zum Kopieren für jede Option.

Option 1: Apple Business (empfohlen)

Klicken Sie auf **In Apple Business registrieren**: Cerberus Enterprise speichert seine Discovery-URL in Ihrer Apple Business-Organisation, und auf Ihren Domains muss nichts veröffentlicht werden. **In Apple Business prüfen** zeigt die URL, die Apple Business derzeit hat, und **Aus Apple Business entfernen** entfernt sie.

- Erfordert iOS und iPadOS 18.2 oder macOS 15.2 oder höher. Ältere Geräte benötigen Option 2 oder 3.
- Erfordert Apple Business, verbunden in Cerberus Enterprise (Service-Token für Automated Device Enrollment), sowie die oben beschriebene Standardgerätezuweisung.
- Das Gerät fragt Apple Business nur, wenn Ihre Domain nicht antwortet: Die Adresse *https://company.com/.well-known/com.apple.remotemanagement* darf nicht existieren (ein Fehler wie „nicht gefunden“). Wenn Ihre Website darauf mit einer Webseite antwortet, bleiben die Geräte dort stehen. Verwenden Sie **Konfiguration prüfen**, um zu sehen, was sie antwortet.

> Apple Business speichert eine Discovery-URL pro Organisation: Wenn Sie sie registrieren, werden alle Verwalteten Apple Accounts der Organisation an diese Cerberus Enterprise-

> Organisation geleitet. Registrieren Sie sie nicht aus zwei Cerberus Enterprise-Organisationen, die dieselbe Apple Business-Organisation verwenden.

Option 2: Umleitung von Ihrer Website

Leiten Sie auf dem Webserver jeder Domain */.well-known/com.apple.remotemanagement* auf die Discovery-URL Ihrer Organisation um und **behalten Sie dabei die Abfragezeichenfolge bei** (sie enthält das vom Benutzer eingegebene Konto). Dies funktioniert mit jeder Betriebssystemversion, die die kontogesteuerte Registrierung unterstützt, und der Modus kann für iPhone und Mac unterschiedlich sein. Kopieren Sie den Text für Apache oder nginx aus der Registerkarte; er sieht wie folgt aus, mit dem Schlüssel Ihrer Organisation:

Apache (.htaccess oder virtueller Host):

```
RewriteEngine On
RewriteRule ^\.well-known/com\.apple\.remotemanagement$
https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/discovery [R=302,L,QSA]
```

nginx:

```
location = /.well-known/com.apple.remotemanagement {
    return 302 https://enterprise.cerberusapp.com/account-enroll/YOUR-
KEY/discovery$is_args$args;
}
```

Erstellen Sie auf anderen Webservern oder Diensten (IIS, Cloudflare, Hosting-Verwaltungsoberflächen) eine Umleitungsregel (302) vom selben Pfad auf die Discovery-URL mit der Option, die die Abfragezeichenfolge beibehält oder weiterleitet.

Option 3: Statische Datei auf Ihrer Website

Wenn Sie keine Umleitung hinzufügen können, veröffentlichen Sie eine Datei unter *https://company.com/.well-known/com.apple.remotemanagement* (ohne Dateierweiterung), die mit *Content-Type: application/json* bereitgestellt wird. Kopieren Sie ihren Inhalt aus der Registerkarte. Eine statische Datei kann den Modus nicht pro Gerät wählen: Sie verwendet denselben Modus für iPhone, iPad und Mac. Für die Benutzerregistrierung sieht sie wie folgt aus:

```
{"Servers":[{"Version":"mdm-byod","BaseURL":"https://enterprise.cerberusapp.com/account-
enroll/YOUR-KEY/byod"}]}
```

und für die Geräteregistrierung:

```
{"Servers":[{"Version":"mdm-adde","BaseURL":"https://enterprise.cerberusapp.com/account-enroll/YOUR-KEY/adde"}]}
```

> Der Modus der Datei muss außerdem dem in der Registerkarte für die Gerätefamilie festgelegten Modus entsprechen, andernfalls wird die Registrierung abgelehnt.

Konfiguration prüfen

Wählen Sie in **Konfiguration prüfen** eine Domain und ein Gerät (iPhone oder Mac) und klicken Sie auf **Prüfen**: Cerberus Enterprise fragt die Domain das, was ein Gerät fragen würde, und zeigt die Antwort, jede Umleitung und ein Ergebnis an. Wenn die Domain auf Cerberus Enterprise verweist, funktionieren Option 2 oder 3; eine Fehlerantwort (wie „nicht gefunden“) ist für Option 1 in Ordnung; eine Webseite oder eine Datei, die woandershin verweist, stoppt die Geräte. Die Prüfung warnt außerdem, wenn eine Umleitung die Abfragezeichenfolge verwirft oder die Datei nicht als *application/json* bereitgestellt wird.

Registrierungsschlüssel

Die Discovery- und Registrierungs-URLs enthalten einen Schlüssel Ihrer Organisation. Wenn die URLs versehentlich veröffentlicht wurden, klicken Sie auf **Schlüssel neu generieren**: Die alten URLs funktionieren sofort nicht mehr, aktualisieren Sie daher die Umleitungen und statischen Dateien auf Ihren Websites. Cerberus Enterprise registriert die neue URL selbst in Apple Business, wenn Option 1 verwendet wird.

Wie Benutzer sich registrieren

1. iPhone und iPad: Öffnen Sie *Einstellungen → Allgemein → VPN & Geräteverwaltung → Bei Arbeits- oder Schulkonto anmelden*. Mac: *Systemeinstellungen → Allgemein → Geräteverwaltung → Anmelden* (unter macOS 14: *Datenschutz & Sicherheit → Profile → Anmelden*).
2. Geben Sie das Verwaltete Apple Account oder die geschäftliche E-Mail-Adresse des Benutzers in Cerberus ein (zum Beispiel *name@company.com*). Wenn das Verwaltete Apple Account des Benutzers von der eingegebenen Angabe abweicht, fordert das Gerät anschließend zur Anmeldung mit diesem Konto auf.
3. Eine Cerberus Enterprise-Seite wird geöffnet: Tippen Sie auf *Code senden* und geben Sie dann den per E-Mail erhaltenen 6-stelligen Code ein. Der Code läuft nach 10 Minuten ab; nach 5 falschen Codes muss der Benutzer die Seite schließen und sich erneut anmelden.

4. Melden Sie sich mit dem Passwort des Verwalteten Apple Accounts an (oder über die Anmeldeseite des Unternehmens, wenn Apple Business mit Google Workspace oder Microsoft Entra ID verbunden ist) und erlauben Sie dann die Geräteverwaltung.

> Konten, die sich nicht registrieren können (Domain nicht verifiziert, kein passender Benutzer, wenn Benutzer nicht automatisch erstellt werden, mehrere Benutzer mit derselben E-Mail-Adresse), sehen die Meldung „Dieses Konto ist nicht für die Registrierung eingerichtet. Wenden Sie sich an Ihren IT-Administrator.“ Die Ereignisse werden in den Systemprotokollen des Dashboards angezeigt.

Nach der Registrierung

- Die Geräteseite zeigt das zur Registrierung verwendete **Verwaltete Apple Account** und den Registrierungstyp (Benutzerregistrierung oder kontogesteuerte Geräteregistrierung). In der Geräteliste zeigen Geräte mit Benutzerregistrierung „Benutzerregistrierung“ an.
- Auf Geräten mit Benutzerregistrierung werden die Befehle und Richtlinieneinstellungen, die Apple nicht zulässt (Löschen, Standort, Verloren-Modus, Betriebssystemupdates, viele Einschränkungen), nicht angeboten oder nicht gesendet. App Store-Apps der Richtlinie verwenden eine Benutzerlizenz anstelle einer Gerätelizenz (siehe **Apps auf privaten Geräten** unten).
- Auf Geräten mit Benutzerregistrierung erscheinen Webclips auf dem Home-Bildschirm, werden aber nicht unter *Einstellungen → Allgemein → VPN & Geräteverwaltung* aufgeführt.
- Das MDM-Zertifikat dieser Geräte wird nicht automatisch erneuert, und **Return to Service** ist nicht verfügbar: Bitten Sie den Benutzer, das Gerät erneut zu registrieren, bevor das MDM-Zertifikat abläuft (ein Jahr nach der Registrierung, siehe Geräteseite).
- Um die Verwaltung zu beenden, meldet sich der Benutzer an derselben Stelle in den Einstellungen vom Arbeitskonto ab, oder Sie heben die Geräteregistrierung in Cerberus Enterprise auf. Bei der Benutzerregistrierung werden nur die Arbeits-Apps, Konten und Daten entfernt; private Daten bleiben erhalten. Ein Gerät, das sich erneut registriert, erscheint als neues Gerät.

> Direkt nach der Registrierung können einige Profile der Richtlinie (Zertifikate, Wi-Fi-Netzwerke, Webclips) mit einem unbekannten Fehler als fehlgeschlagen gemeldet werden, und das Gerät kann eine Zeit lang als **Nicht konform** angezeigt werden. Das Gerät versucht sie von selbst erneut, und sie werden nach einer Weile ohne erforderliche Aktion installiert. Speichern Sie die Richtlinie deshalb nicht erneut und registrieren Sie das Gerät nicht erneut.

Apps auf privaten Geräten

Mit der Benutzerregistrierung registrierte iPhones und iPads haben keine Seriennummer, daher können Apps and Books ihnen keine Gerätelizenz zuweisen. Cerberus Enterprise weist den App Store-Apps ihrer Richtlinie stattdessen eine **Benutzerlizenz** zu: Die Lizenz geht an das auf dem Gerät angemeldete Verwaltete Apple Account. An der Richtlinie ändert sich nichts: Dieselbe Richtlinie dient Unternehmens- und privaten Geräten, und Cerberus wählt den Lizenztyp für jedes Gerät.

- **Automatisch**: Bei der ersten Registrierung registriert Cerberus das Verwaltete Apple Account bei Apps and Books und fordert dann bei Apple eine Lizenz für jede App Store-App der Richtlinie an. Kostenlose Apps benötigen ebenfalls eine Lizenz; Apple stellt dafür unbegrenzte Lizenzen bereit. Eine kostenpflichtige App verwendet eine Lizenz pro Verwaltetem Apple Account, die von allen privaten Geräten dieses Kontos gemeinsam genutzt wird.
- **Gleiche Organisation**: Die Verwalteten Apple Accounts und das Apps and Books-Token von Cerberus Enterprise müssen zur selben Apple Business-Organisation gehören, und die Apps müssen in der Mediathek des Token-Standorts enthalten sein.
- **Lizenz zuerst**: Eine App wird erst an das Gerät gesendet, nachdem Apple ihre Lizenz bestätigt hat, normalerweise innerhalb weniger Minuten. Bis dahin zeigt das Panel **Anwendungen** des Geräts sie als **Warten auf Benutzerlizenz** mit der Begründung an.
- **Installationsaufforderung**: private Geräte sind nie überwacht, daher fragt iOS den Benutzer vor der Installation jeder App, einschließlich der **Cerberus Enterprise**-App, die Cerberus auch auf diesen Geräten installiert (**Installieren** oder **Abbrechen**); eine Anmeldung mit einem Apple Account ist nicht erforderlich. Wenn der Benutzer abbricht, zeigt die App **Warten auf die Genehmigung der Installation durch den Benutzer**: Verwenden Sie **Erneut anfordern** auf der Geräteseite, um die Aufforderung erneut anzuzeigen. Apps, die als **Erforderlich** installiert werden, können vom Benutzer nicht gelöscht werden.
- **Vor der Registrierung installierte Apps**: Apple erlaubt der Organisation nicht, eine App zu übernehmen, die der Benutzer persönlich auf einem mit Benutzerregistrierung registrierten Gerät installiert hat. Bitten Sie den Benutzer, seine eigene Kopie vor der Registrierung zu löschen, oder löschen Sie sie und verwenden Sie dann **Erneut anfordern** auf der Geräteseite: Die Organisation installiert dann die verwaltete Kopie.
- **Verwaltung beenden**: Wenn die Registrierung des Geräts aufgehoben wird, entfernt iOS die verwalteten Apps und ihre Daten. Eine Lizenz wird freigegeben, wenn kein anderes registriertes Gerät desselben Verwalteten Apple Accounts sie benötigt, zum Beispiel wenn die App die Richtlinie verlässt oder das letzte Gerät abgemeldet wird; Lizenzen, die niemand mehr benötigt, werden durch die tägliche Prüfung innerhalb eines Tages freigegeben.

> Wenn Apple keine Lizenz zuweisen kann, zum Beispiel weil für eine kostenpflichtige App keine Lizenz mehr verfügbar ist, zeigt die App **Benutzerlizenz fehlgeschlagen** mit Apples Meldung an. Fügen Sie in Apple Business Lizenzen hinzu und verwenden Sie dann **Erneut anfordern** auf der Geräteseite; Cerberus versucht es auch bei der täglichen Prüfung erneut. Die Zeile über der App-Liste zeigt das Verwaltete Apple Account und den Status seines Apps and Books-Benutzers; derselbe Status ist auf der Seite des Benutzers zu sehen.

>

> Benutzerlizenzen werden nur auf iPhones und iPads verwendet: Auf Macs, die mit User Enrollment registriert sind, werden die App-Store-Apps der Richtlinie nicht installiert. Bücher und persönliche Apple Accounts werden nicht unterstützt.

Revision #7
Created 2026-11-10 15:14:30 UTC by Admin
Updated 2026-11-12 09:54:15 UTC by Admin