Gerätebereitstellung - Apple

- Überblick über die Apple-Bereitstellung
- Apple-Manualregistrierung (Registrierungsprofil)
- Apple Automated Device Enrollment (ADE)
- Kontogesteuerte Apple-Registrierung

Überblick über die Apple-Bereitstellung

Cerberus Enterprise unterstützt die Registrierung und Verwaltung von iPhones, iPads und Macs. Die Apple-Bereitstellung erfordert ein APNs-Zertifikat und kann mit verschiedenen Registrierungsmethoden durchgeführt werden.

Voraussetzung: Apple Management konfigurieren (APNs)

Bevor Sie ein Apple-Gerät registrieren, schließen Sie die **Apple Management-Einrichtung (APNs)** ab.

Registrierungsmethode auswählen

Manuelle Registrierung (Registrierungsprofil)

Diese Methode bietet eine Registrierungs-URL und eine Konfigurationsprofildatei (mobileconfig), die Sie auf dem Gerät installieren. Lesen Sie **Manuelle Apple-Registrierung**.

Automated Device Enrollment (ADE)

Diese Methode integriert sich in Apple Business, um die Registrierung unternehmenseigener Geräte zu automatisieren. Lesen Sie **Apple Automated Device Enrollment (ADE)**.

Kontogesteuerte Registrierung (mit einem Arbeitskonto anmelden)

Benutzer registrieren ihr iPhone, iPad oder ihren Mac, indem sie sich in den Geräteeinstellungen mit ihrem verwalteten Apple Account anmelden: User Enrollment für persönliche Geräte, Device Enrollment für Unternehmensgeräte, die nicht in Apple Business sind. Lesen Sie **Kontogesteuerte Apple-Registrierung**.

Auf persönlichen iPhones und iPads, die mit User Enrollment registriert wurden, werden die App-Store-Apps der Richtlinie mit einer Benutzerlizenz des verwalteten Apple Account installiert, die Cerberus selbst zuweist; der Benutzer wird gebeten, jede App zu installieren. Die verwalteten Apple Accounts und das Apps and Books-Token müssen zur selben Apple Business-Organisation gehören. Lesen Sie **Apps auf persönlichen Geräten**.

Cerberus Enterprise App auf iPhone und iPad

Nach der Registrierung installiert Cerberus seine **Cerberus Enterprise**-App auf iPhones und iPads mit **iOS oder iPadOS 18.4 oder neuer**, mit oder ohne Richtlinie. Die App teilt den Gerätestandort und empfängt Benachrichtigungen und Live-Ortungsanforderungen; auf persönlichen Geräten (User Enrollment) empfängt sie Nachrichten und teilt den Standort nur, wenn die Richtlinie **Standort und Geofences auf persönlichen Geräten** aktiviert und der Benutzer es zulässt. Sie erfordert einen einmaligen Schritt: Fügen Sie die kostenlose App Ihrer Apple Business-Mediathek hinzu (**Apps & Books** → **App Store**, suchen Sie nach „Cerberus Enterprise“, **Hinzufügen** für alle aktuellen und zukünftigen Organisationseinheiten). Überwachte Geräte installieren sie still; auf anderen Geräten wird der Benutzer gebeten, sie zu installieren. Wenn der Benutzer sie bereits aus dem App Store installiert hat, fordert das Gerät dazu auf, Ihrer Organisation die Verwaltung der App zu erlauben, und die App behält ihre Daten und Berechtigungen. Wenn der Benutzer ablehnt, verwenden Sie **Erneut versuchen** auf der Geräteseite. Der Benutzer kann die App nicht löschen, und sie bleibt installiert, wenn das Apps and Books-Token abläuft. Macs erhalten die App nicht.

> Sie können die manuelle Registrierung und ADE parallel verwenden, je nach Ihrem Gerätebestand und Einkaufsprozess.

Apple-Manualregistrierung (Registrierungsprofil)

Cerberus Enterprise unterstützt die manuelle Registrierung von Apple-Geräten über einen QR-Code, eine Registrierungs-URL oder eine Registrierungsprofildatei.

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

> Benutzer können ihr iPhone, iPad oder ihren Mac auch ohne Profil registrieren, indem sie sich in den Geräteeinstellungen mit ihrem Arbeitskonto anmelden. Lesen Sie **Kontogesteuerte Apple-Registrierung**.

Registrierungstoken

Ein Registrierungstoken hat seine eigene Registrierungs-URL und seinen eigenen QR-Code und weist den Geräten, die sich damit registrieren, diese Einstellungen zu:

- **Richtlinie**: wird auf das Gerät angewendet, sobald es sich registriert.
- **Benutzer**: wird dem Gerät zugewiesen. Ohne Benutzer im Token hat das Gerät keinen Benutzer.
- **Eigentum**: unternehmenseigen oder persönlich. Wenn es nicht festgelegt ist, werden überwachte Geräte als unternehmenseigen und die anderen als persönlich eingestuft. Manuell registrierte iPhones und iPads sind nicht überwacht; Macs sind es, daher werden sie als unternehmenseigen eingestuft.
- **Ablauf**: Nach diesem Tag funktioniert die Registrierungs-URL nicht mehr. Ein zuvor heruntergeladenes Profil kann weiterhin installiert werden.
- **Zulässige Registrierungen**: wie viele Geräte sich mit dem Token registrieren können. Lassen Sie das Feld leer, um kein Limit festzulegen.

Um ein Token zu erstellen, öffnen Sie im Dashboard den Abschnitt **Registrierung**, wählen Sie die Registerkarte **Apple-Manualregistrierung (Registrierungsprofil)** und klicken Sie auf **Neues Registrierungstoken**. Legen Sie den Namen und die Einstellungen fest und klicken Sie dann auf

Token erstellen: Die Tokenseite zeigt die Registrierungs-URL, den QR-Code und die Schaltfläche **Registrierungsprofil herunterladen**.

Die Tokentabelle zeigt für jedes Token seinen **Status** (Aktiv, Abgelaufen oder Aufgebraucht), den **Ablauf**, die **Registrierungen** im Verhältnis zu den erlaubten sowie **Zuletzt verwendet**, wann sich zuletzt ein Gerät damit registriert hat. Danach folgen die **Richtlinie**, der **Benutzer** (darauf zeigen, um die E-Mail-Adresse zu sehen), das **Eigentum** und das Datum **Erstellt** (darauf zeigen, um zu sehen, wer das Token erstellt hat). Die neuesten Tokens stehen zuerst, und Sie können nach jeder Spalte sortieren. Sortieren Sie nach **Zuletzt verwendet**, um aktive Tokens zu finden, die niemand mehr verwendet, und löschen Sie sie, damit ihre Registrierungs-URL nicht mehr funktioniert. Eine Richtlinie oder ein Benutzer, der nach dem Speichern des Tokens gelöscht wurde, wird als **Richtlinie gelöscht** oder **Benutzer gelöscht** mit einem Warnsymbol angezeigt: Bearbeiten Sie das Token, um ein anderes auszuwählen.

> Änderungen an einem Token gelten für die nächsten Registrierungen: Bereits registrierte Geräte behalten ihre Richtlinie und ihren Benutzer. Wenn ein Token gelöscht wird, abläuft oder seine zulässigen Registrierungen erreicht, funktioniert seine Registrierungs-URL nicht mehr.

Registrierung ohne Token

Das Panel **Registrierung ohne Token** derselben Registerkarte enthält die Registrierungs-URL Ihrer Organisation. Damit registrierte Geräte erhalten keine Richtlinie und keinen Benutzer: Weisen Sie diese auf der Geräteseite zu.

Die Richtlinie und der Benutzer eines Geräts hängen davon ab, wie es sich registriert: die Richtlinie und der Benutzer des Tokens bei einem Registrierungstoken; die Richtlinie des ADE-Profils bei Automated Device Enrollment, wobei der auf der Geräteseite zugewiesene Benutzer erhalten bleibt; keine Richtlinie und kein Benutzer bei der Registrierungs-URL, dem QR-Code oder dem Profil ohne Token (auch wenn das Gerät ein ADE-Profil hat). Ein Gerät, das sich erneut registriert, behält die Richtlinie und den Benutzer seiner vorherigen Registrierung nicht: Die Geräteseite zeigt sie nur an, wenn die neue Registrierung sie zuweist. Nur ein mit **Return to Service** gelöschtes Gerät registriert sich erneut mit seiner aktuellen Richtlinie und seinem aktuellen Benutzer.

Registrierungs-URL und Profil abrufen

- Öffnen Sie das Token auf der Registerkarte **Apple-Manualregistrierung (Registrierungsprofil)** des Abschnitts **Registrierung**, oder erweitern Sie **Registrierung ohne Token**.
- Kopieren Sie die **Registrierungs-URL**, oder verwenden Sie die Aktion zum Senden per E-Mail.
- Scannen Sie den neben der Registrierungs-URL angezeigten **QR-Code** mit der Kamera eines iPhone oder iPad: Er öffnet dieselbe Registrierungs-URL auf dem Gerät. Verwenden Sie auf einem Mac die Registrierungs-URL oder die Profildatei.
- Laden Sie das **Registrierungsprofil** herunter (mobileconfig-Datei).

iPhone oder iPad registrieren

iOS/iPadOS 15.0+

Laden Sie zunächst das Registrierungsprofil auf dem Gerät mit einer der folgenden Methoden herunter:

Methode 1: QR-Code

Öffnen Sie die *Kamera*-App auf dem Gerät und richten Sie sie auf den QR-Code, der neben der Registrierungs-URL angezeigt wird, und tippen Sie dann auf den angezeigten Link. Safari öffnet die Registrierungs-URL und fragt, ob das Herunterladen eines Konfigurationsprofils erlaubt werden soll: Tippen Sie auf *Erlauben*.

Methode 2: Registrierungs-URL

Senden Sie die Registrierungs-URL an den Benutzer (zum Beispiel mit der Aktion „Per E-Mail senden“) und öffnen Sie sie in *Safari* auf dem Gerät, und tippen Sie dann auf *Erlauben*, um das Konfigurationsprofil herunterzuladen.

Methode 3: Registrierungsprofildatei

Laden Sie die Registrierungsprofildatei (*enroll.mobileconfig*) herunter und senden Sie sie an das Gerät, zum Beispiel als E-Mail-Anhang oder mit AirDrop, und öffnen Sie sie dann auf dem Gerät.

Schließen Sie dann die Registrierung auf dem Gerät ab:

1. Öffnen Sie auf dem Gerät *Einstellungen* → *Profil geladen* → *Installieren* und folgen Sie anschließend den Anweisungen.

2. Nach der Registrierung können Sie den Status unter *Einstellungen → Allgemein → VPN & Geräteverwaltung* (oder *Profile & Geräteverwaltung*) prüfen.

> Nach der Registrierung erhalten iPhones und iPads mit iOS oder iPadOS 18.4 oder neuer die App **Cerberus Enterprise**. Auf einem manuell registrierten (nicht überwachten) Gerät wird der Benutzer gebeten, sie zu installieren oder Ihre Organisation verwalten zu lassen, wenn sie bereits aus dem App Store installiert wurde. Wenn der Benutzer ablehnt, verwenden Sie **Erneut versuchen** auf der Geräteseite. Die App muss einmal in Ihrer Apple Business-Bibliothek vorhanden sein (siehe **Kontoeinstellungen**).

> Auf iPhone und iPad wird ein heruntergeladenes Profil, das nicht innerhalb von 8 Minuten installiert wird, vom Gerät entfernt. Laden Sie es in diesem Fall erneut herunter.

So registrieren Sie einen Mac

macOS 13.0+

Der QR-Code funktioniert nur auf iPhone und iPad. Laden Sie das Registrierungsprofil mit einer der folgenden Methoden auf den Mac herunter:

Methode 1: Registrierungs-URL

Senden Sie die Registrierungs-URL an den Benutzer (zum Beispiel mit der Aktion Per E-Mail senden) und öffnen Sie sie in *Safari* auf dem Mac und erlauben Sie den Download, wenn Sie gefragt werden. Wenn sich das Profil nicht von selbst öffnet, öffnen Sie die heruntergeladene Datei *enroll.mobileconfig*.

Methode 2: Registrierungsprofildatei

Laden Sie die Registrierungsprofildatei (*enroll.mobileconfig*) herunter und senden Sie sie an den Mac, zum Beispiel als E-Mail-Anhang oder mit AirDrop; öffnen Sie sie dann auf dem Mac.

Das Öffnen des Profils fügt es nur den heruntergeladenen Profilen hinzu. Schließen Sie dann die Registrierung auf dem Mac ab, angemeldet als dessen Hauptbenutzer:

1. Öffnen Sie *Systemeinstellungen → Allgemein → Geräteverwaltung* (unter macOS 13 und 14: *Datenschutz & Sicherheit → Profile*). Doppelklicken Sie im Bereich *Geladen* auf *Registrierungsprofil*, klicken Sie auf *Registrieren* (oder *Installieren*) und folgen Sie den Anweisungen. Geben Sie bei Aufforderung den Namen und das Passwort eines

Administrators des Mac ein.
2. Nach der Registrierung wird *Registrierungsprofil* an derselben Stelle aufgeführt. Im *Terminal* zeigt `profiles status -type enrollment` *MDM enrollment: Yes (User Approved)* an.

> Manuell registrierte Macs sind überwacht, und der Benutzer, der das Profil installiert, wird im Bereich **Mac-Benutzer** der Geräteseite angezeigt. Macs erhalten die Cerberus Enterprise-App nicht. Wenn das Profil nicht mehr im Bereich *Geladen* vorhanden ist, laden Sie es erneut herunter.

> Installieren Sie nur Registrierungsprofile, die Sie aus Ihrem Cerberus Enterprise Dashboard bezogen haben.

Apple Automated Device Enrollment (ADE)

Automated Device Enrollment (ADE) lässt sich in Apple Business (früher Apple Business Manager) integrieren, um unternehmenseigene iPhones, iPads und Macs automatisch zu registrieren, wenn sie zum ersten Mal eingeschaltet werden (oder nach einem Zurücksetzen auf die Werkseinstellungen).

> ADE setzt voraus, dass Apple Management (APNs) zuerst konfiguriert wird. Lesen Sie bei Bedarf **Apple Management-Einrichtung (APNs)**.

Geräte automatisch registrieren

1. Fügen Sie Ihrem Apple Business-Konto Geräte hinzu und weisen Sie sie dem Geräteverwaltungsdienst Cerberus Enterprise zu: Öffnen Sie in Apple Business **Geräte** → **Inventar**, wählen Sie die Geräte aus und klicken Sie auf **Geräteverwaltung zuweisen**, oder weisen Sie neue Geräte automatisch über **Geräte** → **Verwaltungsdienste** → **Standardgerätezuweisung** zu. Siehe Geräteanbieter verwalten und Geräte mit Apple Configurator hinzufügen.
2. Nachdem Sie neue Geräte zu Ihrem Apple Business-Konto hinzugefügt haben, synchronisieren Sie sie in Cerberus Enterprise im Abschnitt **Geräte** mit der Aktion **Von Apple Business synchronisieren**. Synchronisierte Geräte verbrauchen erst eine Lizenz, wenn sie sich registrieren.
3. Erstellen Sie im Dashboard ein ADE-Profil über **Registrierung** → **Apple Automated Device Enrollment (ADE)** → **Neues ADE-Profil**.
4. Weisen Sie einem Gerät auf der Gerätedetailseite über das Feld **ADE-Profil** ein ADE-Profil zu.

> Nach der Registrierung erhalten iPhones und iPads mit iOS oder iPadOS 18.4 oder höher die App **Cerberus Enterprise**. Mit ADE registrierte Geräte sind überwacht, daher wird die App ohne Nachfrage beim Benutzer installiert; die Einrichtung wartet nicht darauf. Die App muss einmal in Ihrer Apple Business-Mediathek vorhanden sein (siehe **Kontoeinstellungen**). Macs erhalten die App nicht.

Einstellungen für ADE-Profile (Übersicht)

Ein ADE-Profil steuert, wie das Gerät registriert wird und wie sich der Setup-Assistent verhält. In Cerberus Enterprise umfasst ein ADE-Profil einen Namen, eine optionale anfängliche Richtlinie, Registrierungsoptionen, die zu überspringenden Bereiche des Setup-Assistenten, Supportkontakte und vertrauenswürdige Zertifikate.

Profilname

Ein lesbarer Name für das Profil (zum Beispiel *Standard-ADE-Profil*).

Richtlinie

Die Richtlinie, die auf die Geräte angewendet wird, wenn sie sich mit Automated Device Enrollment registrieren (Setup-Assistent). Geräte des Profils, die sich über die Registrierungs-URL oder den QR-Code registrieren, erhalten stattdessen die Richtlinie ihres Registrierungstokens oder ohne Token keine Richtlinie. Wenn Sie nur die Richtlinie ändern, bleibt das Profil unverändert.

Registrierungsoptionen

- **MDM entfernbar**: steuert, ob die MDM-Nutzlast vom Gerät entfernt werden kann.
- **Kopplung zulassen**: steuert, ob die Kopplung erlaubt ist (von Apple in iOS 13 veraltet).
- **Setup automatisch fortsetzen**: führt den Setup-Assistenten automatisch durch seine Bildschirme (Mac mit macOS 11 oder neuer und Apple TV).
- **Auf Gerätekonfiguration warten**: Der Setup-Assistent wartet, bis die Richtlinie des ADE-Profils angewendet wurde, damit Benutzer mit den zugehörigen Apps und Einstellungen beginnen. Cerberus Enterprise lässt das Gerät dann spätestens 4 Minuten nach der Registrierung fortfahren.
- **Erforderlich**: verhindert das Überspringen der Profilanwendung während der Einrichtung.
- **Mehrere Benutzer (Shared iPad)**: konfiguriert das Gerät für Shared iPad.
- **Überwacht**: fordert die Überwachung für das Gerät an.

Setup-Assistent

- **Abteilung**, **Support-Telefon** und **Support-E-Mail** (optional): werden mit dem Profil an Apple gesendet. Das Gerät zeigt sie möglicherweise nicht an.

- **Zu überspringende Bereiche**: Der Setup-Assistent zeigt die ausgewählten Bereiche nicht an (zum Beispiel Apple Account, Siri oder Bildschirmzeit). Jedes Gerät zeigt nur die Bereiche seines Systems (einige, wie FileVault oder iCloud-Dokumente und Schreibtisch, gibt es nur auf Macs); **Alle überspringen** und **Alle anzeigen** wählen alle aus bzw. heben die Auswahl auf.
- **Apple TV**: Sprache und Region für Apple TV mit automatischer Setup-Fortsetzung.
- **Vertrauenswürdige Zertifikate**: nur erforderlich, wenn der Server ein Zertifikat verwendet, dem die Geräte nicht vertrauen, zum Beispiel von einer privaten CA. Importieren Sie das Zertifikat zuerst auf der Seite Zertifikate.

Liste der ADE-Profile

Die Liste zeigt den Namen jedes Profils, seine Richtlinie, seine Geräte und seine ID, die Kennung, die Apple dem Profil gibt. Ein Schloss nach dem Namen kennzeichnet ein obligatorisches Profil, dessen Verwaltung Benutzer nicht entfernen können. **Keine Richtlinie** oder **Richtlinie gelöscht** weist darauf hin, dass mit dem Profil registrierte Geräte keine anfängliche Richtlinie erhalten.

Die Spalte **Geräte** zählt die registrierten Geräte des Profils und daneben die wartenden Geräte: in Apple Business dem Profil zugewiesen, aber noch nicht registriert. Entfernte Geräte werden nicht gezählt.

Ändern eines Profils

Apple erlaubt das Ändern eines ADE-Profils nicht. Wenn Sie eines ändern (außer nur die Richtlinie), definiert Cerberus Enterprise ein neues Profil mit demselben Namen und weist es den Geräten des alten Profils zu; das alte Profil wird nicht mehr aufgeführt, sobald es kein Gerät mehr verwendet. Geräte, die den Setup-Assistenten bereits abgeschlossen haben, verwenden das neue Profil beim nächsten Löschen.

Ein Profil, das kein Gerät verwendet – weder ein registriertes noch ein wartendes –, kann aus der Liste der ADE-Profile gelöscht werden. Apple erlaubt das Löschen eines Profils nicht, daher verbleibt es ungenutzt in Apple Business.

> Nachdem einem Gerät ein ADE-Profil zugewiesen wurde, kann es automatisch registriert werden.

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.