デバイスのプロビジョニング - Apple

- Appleプロビジョニングの概要
- Apple の手動登録（登録プロファイル）
- Apple Automated Device Enrollment（ADE）
- Apple のアカウント主導の登録

Apple

Cerberus Enterprise iPhone iPad Mac Apple
 APNs

Apple Management
APNs

Apple **Apple Management** **APNs**

mobileconfig

URL mobileconfig
Apple

Automated Device Enrollment ADE

Apple Business **Apple Automated Device Enrollment ADE**

Managed Apple Account

Managed Apple Account iPhone iPad Mac User Enrollment Apple Business Device Enrollment **Apple**

User Enrollment iPhone iPad App Store Cerberus
Managed Apple Account
Managed Apple Account Apps and Books Apple Business

iPhone iPad Cerberus Enterprise

Cerberus **Cerberus Enterprise** **iOS** **iPadOS 18.4** iPhone iPad
User Enrollment
1
Apple Business **Apps & Books → App Store** Cerberus Enterprise
App Store
Apps and Books
Mac

ADE

Apple

の手動登録（登録プロファイル

）
Cerberus Enterprise は、 QR コード、登録 URL、または登録プロファイルファイルを使用した Apple デバイスの手動登録をサポートしています。

手動登録は、 Apple Management（APNs）が構成されている場合に利用できます。 APNs

のセットアップがまだ完了していない場合は、 Apple Management のセットアップ（ APNs）
を参照してください。

ユーザーは、デバイス設定で仕事用アカウントにサインインすることにより、プロファイルなしで

iPhone、 iPad、 Mac を登録することもできます。 Apple のアカウント主導の登録
を参照してください。

登録トークン
登録トークンには独自の登録 URL と QR
コードがあり、それを使用して登録するデバイスに次の設定を割り当てます。

ポリシー ：デバイスが登録されるとすぐに適用されます。
ユーザー
：デバイスに割り当てられます。トークンにユーザーがない場合、デバイスにはユーザーがありま
せん。
所有権
：会社所有または個人所有。設定されていない場合、監視対象デバイスは会社所有に、それ以外は
個人所有に設定されます。手動で登録した iPhone と iPad は監視対象ではありません。 Mac は監視対象であるため、会社所有に設定されます。
有効期限 ：この日を過ぎると登録 URL
は機能しなくなります。以前にダウンロードしたプロファイルは引き続きインストールできます。
許可される登録数
：トークンで登録できるデバイスの数。制限なしにする場合は空のままにします。

トークンを作成するには、ダッシュボードの 登録 セクションを開き、 Apple
の手動登録（登録プロファイル） タブを選択して 新しい登録トークン
をクリックします。名前と設定を指定して トークンを作成 をクリックします。トークンページには、登録 URL、QR コード、 登録プロファイルをダウンロード ボタンが表示されます。

トークンのテーブルには、各トークンの ステータス （有効、期限切れ、使用済み）、 有効期限
、許可された数に対する 登録数 、および 最終使用
（そのトークンで最後にデバイスが登録された日時）が表示されます。次に ポリシー 、ユーザー （ホバーするとメールが表示されます）、 所有権 、 作成日（ホバーするとトークンを作成したユーザーが表示されます）が続きます。新しいトークンが最初に表示さ
れ、任意の列で並べ替えられます。 最終使用
で並べ替えると、誰も使用していない有効なトークンを見つけられ、削除するとその登録 URL が機能しなくなります。トークンの保存後に削除されたポリシーまたはユーザーは、警告アイコン付きの
削除されたポリシー または 削除されたユーザー
として表示されます。トークンを編集して別のものを選択してください。

トークンへの変更は次回の登録に適用されます。すでに登録されているデバイスは、現在のポリシー
とユーザーを維持します。トークンが削除された場合、期限切れになった場合、または許可された登
録数に達した場合、その登録 URL は機能しなくなります。

トークンなしの登録
同じタブの トークンなしの登録 パネルには、組織の登録 URL があります。これを使用して登録されたデバイスにはポリシーもユーザーも設定されません。デバイスペー
ジから割り当ててください。

デバイスのポリシーとユーザーは登録方法によって異なります。登録トークンを使用した場合はトークンの
ポリシーとユーザー、 Automated Device Enrollment の場合は ADE
プロファイルのポリシー（デバイスページで割り当てられたユーザーは維持）、トークンなしの登録 URL、 QR コード、またはプロファイルの場合はポリシーもユーザーもなし（デバイスに ADE プロファイルがある場合でも）です。再登録したデバイスは、以前の登録のポリシーとユーザーを維持しま
せん。デバイスページに表示されるのは、新しい登録で割り当てられた場合のみです。 Return to Service で消去されたデバイスのみ、現在のポリシーとユーザーで再登録されます。

登録 URL とプロファイルを取得する
登録 セクションの Apple の手動登録（登録プロファイル） タブでトークンを開くか、
トークンなしの登録 を展開します。
登録 URLをコピーするか、メール送信アクションを使用します。

iPhone または iPad のカメラで、 Enrollment URL の横に表示される QR コード
をスキャンします。デバイス上で同じ Enrollment URL が開きます。 Mac では、 Enrollment URL
またはプロファイルファイルを使用します。
登録プロファイル （ mobileconfig ファイル）をダウンロードします。

iPhone または iPad を登録する方法
iOS/iPadOS 15.0 以降

まず、次のいずれかの方法を使用して、デバイスに登録プロファイルをダウンロードします：

方法 1：QRコード
デバイスで カメラ アプリを開き、登録 URLの横に表示される QR
コードにかざしてから、表示されるリンクをタップします。 Safariが登録 URL
を開き、構成プロファイルのダウンロードを許可するか確認するので、 許可 をタップします。

方法 2：登録 URL

登録 URLをユーザーに送信し（たとえばメール送信アクションを使用）、デバイスの Safari
で開いてから、構成プロファイルをダウンロードするために 許可 をタップします。

方法 3：登録プロファイルのファイル

登録プロファイルのファイル（ enroll.mobileconfig）をダウンロードし、たとえばメールの添付ファイルや
AirDropでデバイスに送信してから、デバイスで開きます。

次に、デバイスで登録を完了します：

1. デバイスで 設定 → ダウンロード済みのプロファイル → インストール
を開き、画面の指示に従います。
2. 登録後、 設定 → 一般 → VPN & デバイス管理 （または プロファイル & デバイス管理
）で状態を確認できます。

登録後、 iOSまたは iPadOS 18.4以降を搭載した iPhoneと iPadには Cerberus Enterprise アプリが配信されます。手動で登録された（監視されていない）デバイスでは、ユーザーにアプリの
インストールを求めるメッセージ、または App Store
からすでにインストールされている場合は組織による管理を許可するよう求めるメッセージが表示さ
れます。ユーザーが拒否した場合は、デバイスページの 再試行 を使用します。アプリは一度 Apple

Businessライブラリに追加されている必要があります（ アカウント設定 を参照）。

iPhone と iPad では、ダウンロードしたプロファイルが 8
分以内にインストールされない場合、デバイスによって削除されます。その場合は、もう一度ダウン
ロードしてください。

Mac を登録する方法

macOS 13.0+

QR コードは iPhone と iPad でのみ機能します。次のいずれかの方法で、 Mac
に登録プロファイルをダウンロードしてください:

方法 1: Enrollment URL

Enrollment URL をユーザーに送信し（例: メール送信アクションを使用）、 Mac の *Safari*
で開いてから、求められた場合はダウンロードを許可します。プロファイルが自動的に開かない場合は、ダ
ウンロードした *enroll.mobileconfig* ファイルを開きます。

方法 2: 登録プロファイルファイル

登録プロファイルファイル（ *enroll.mobileconfig*）をダウンロードし、メールの添付ファイルや AirDrop
などで Mac に送信してから、 Mac で開きます。

プロファイルを開いても、ダウンロード済みプロファイルに追加されるだけです。その後、 Mac
のメインユーザーとしてログインし、 Mac で登録を完了します:

1. システム設定 → 一般 → デバイス管理 （ macOS 13 および 14: プライバシーとセキュリティ → プロファイル ）を開きます。 ダウンロード済み セクションで 登録プロファイル をダブルクリックし、 登録 （または インストール ）をクリックして、指示に従います。求められた場合は、 Mac の管理者の名前とパスワードを入力します。
2. 登録後、 登録プロファイル が同じ場所に表示されます。 ターミナル で、 `profiles status -type enrollment` を実行すると、 *MDM enrollment: Yes (User Approved)* と表示されます。

手動で登録した Mac
は監視対象となり、プロファイルをインストールしたユーザーがデバイスページの **Mac** ユーザー
パネルに表示されます。 Mac には Cerberus Enterprise
アプリはインストールされません。プロファイルが ダウンロード済み

セクションにない場合は、もう一度ダウンロードしてください。

Cerberus Enterprise
ダッシュボードから取得した登録プロファイルのみをインストールしてください。

Apple Automated Device Enrollment（ADE）
Automated Device Enrollment（ADE）は Apple Business（旧 Apple Business Manager
）と連携し、会社所有の iPhone、iPad、 Mac
を初めて電源を入れたとき（または工場出荷状態にリセットした後）に自動的に登録します。

ADE を使用するには、先に Apple Management（APNs

）を構成する必要があります。必要な場合は、 Apple Management のセットアップ（ APNs）
を参照してください。

デバイスを自動登録する方法
1. Apple Business アカウントにデバイスを追加し、 Cerberus Enterprise
デバイス管理サービスに割り当てます。 Apple Business でDevices → Inventory
を開き、デバイスを選択して Assign Device Managementをクリックするか、 Devices → Management Services → Default Device Assignment

で新しいデバイスを自動的に割り当てます。 Manage device suppliersおよび Add devices using

Apple Configuratorを参照してください。
2. Apple Business アカウントに新しいデバイスを追加した後、 Cerberus Enterprise の デバイス
セクションから Apple Business から同期
アクションを使用して同期します。同期されたデバイスは、登録されて初めてライセンスを使用し
ます。
3. ダッシュボードで 登録 → Apple Automated Device Enrollment（ADE） → 新しい ADE プロファイル から ADE プロファイルを作成します。
4. デバイスの詳細ページで ADE プロファイル フィールドを使用して、デバイスに ADE
プロファイルを割り当てます。

登録後、 iOS または iPadOS 18.4 以降の iPhone と iPad には Cerberus Enterprise アプリがインストールされます。 ADE
で登録されたデバイスは監視対象であるため、ユーザーに確認せずにアプリがインストールされます
。セットアップはアプリのインストールを待ちません。アプリは一度 Apple Business
ライブラリに登録されている必要があります（ アカウント設定 を参照）。 Mac にはアプリはインストールされません。

ADE プロファイルの設定（概要）
ADE プロファイルは、デバイスの登録方法とセットアップアシスタントの動作を制御します。 Cerberus Enterprise では、 ADE
プロファイルに名前、オプションの初期ポリシー、登録オプション、スキップするセットアップアシスタン
トのペイン、サポート連絡先、信頼された証明書が含まれます。

プロファイル名

プロファイルの人間が読める名前（例： デフォルトの ADE プロファイル ）。

ポリシー
Automated Device Enrollment
（セットアップアシスタント）で登録するときにデバイスに適用されるポリシー。登録 URL または QR コードで登録されたプロファイルのデバイスには、代わりに登録トークンのポリシーが適用されます。トー
クンがない場合はポリシーは適用されません。ポリシーのみを変更した場合、プロファイルはそのまま維持
されます。

登録オプション

MDM を削除可能 ： MDM ペイロードをデバイスから削除できるかどうかを制御します。
ペアリングを許可 ：ペアリングを許可するかどうかを制御します（ Apple により iOS 13
で非推奨）。
セットアップの自動進行 ：セットアップアシスタントの画面を自動的に進めます（ macOS 11
以降の Mac と Apple TV）。
デバイスの構成完了を待機 ：セットアップアシスタントは、 ADE プロファイルのポリシーが適用されるまで待機するため、ユーザーはアプリと設定が適用された状
態で開始できます。その後、 Cerberus Enterprise は登録から最大 4
分後にデバイスの続行を許可します。
必須 ：セットアップ中にプロファイルの適用をスキップできないようにします。
マルチユーザー（ Shared iPad） ：デバイスを Shared iPad 用に構成します。
監視対象 ：デバイスの監視を要求します。

セットアップアシスタント

部署 、サポート電話番号 、サポートメール （任意）：プロファイルとともに Apple
に送信されます。デバイスに表示されない場合があります。

スキップするペイン ：セットアップアシスタントは選択したペインを表示しません（例： Apple Account、Siri、スクリーンタイム）。各デバイスにはそのシステムのペインのみが表示されます（
FileVault や iCloud の書類とデスクトップなど、 Mac にのみ存在するものもあります）。
すべてスキップ とすべて表示 で、すべてのペインを選択または解除できます。
Apple TV：セットアップ自動進行を使用する Apple TV の言語と地域。
信頼された証明書 ：サーバーがデバイスで信頼されていない証明書（プライベート CA の証明書など）を使用している場合にのみ必要です。先に証明書ページで証明書をインポートして
ください。

ADE プロファイルの一覧

一覧には、各プロファイルの名前、ポリシー、デバイス、および Apple
がプロファイルに付与する識別子である Id
が表示されます。名前の後の鍵アイコンは、管理ユーザーが解除できない必須プロファイルを示します。
ポリシーなし または ポリシー削除済み
は、そのプロファイルで登録されたデバイスに初期ポリシーが適用されないことを警告します。

デバイス 列には、プロファイルの登録済みデバイスと、その横に待機中のデバイス（ Apple Business でプロファイルに割り当てられているが、まだ登録されていないデバイス）が表示されます。削除されたデ
バイスはカウントされません。

プロファイルの変更

Apple は ADE
プロファイルの変更を許可していません。プロファイルを変更すると（ポリシーのみの変更を除く）、
Cerberus Enterprise
は同じ名前で新しいプロファイルを定義し、古いプロファイルのデバイスに割り当てます。古いプロファイ
ルは、それを使用するデバイスがなくなると一覧に表示されなくなります。すでにセットアップアシスタン
トを完了したデバイスは、次回消去されたときに新しいプロファイルを使用します。

登録済みか待機中かを問わず、どのデバイスも使用していないプロファイルは、 ADE
プロファイルの一覧から削除できます。 Apple
はプロファイルの削除を許可していないため、そのプロファイルは使用されないまま Apple Business に残ります。

デバイスに ADE プロファイルが割り当てられると、自動登録の準備が整います。

Apple のアカウント主導の登録
アカウント主導の登録では、ユーザーはデバイス設定で仕事用アカウント（ Managed Apple Account 、例： name@company.com）でサインインして、 iPhone、iPad、Mac
を登録します。ダウンロードするプロファイルも QR コードも不要です。 Cerberus Enterprise がユーザーを検出し、ポリシーを適用し、所有権を自動的に設定します。

2つのモード
User Enrollment
（個人デバイス）：デバイス内の別エリアで、仕事用のアプリ、アカウント、データのみが管理さ
れます。 Cerberus
は個人データを表示したり、デバイスを消去したり、位置を特定したり、シリアル番号を読み取っ
たりすることはできません。デバイスは個人所有として設定されます。 iOS および iPadOS 15
以降、または macOS 14 以降が必要です。
Device Enrollment（Apple Business
に登録されていない会社のデバイス）：手動登録と同様に、デバイス全体が管理されます。この方
法で登録された Mac は監視対象になりますが、 iPhone または iPad
は監視対象になりません。デバイスは会社所有として設定されます。 iOS および iPadOS 17.1
以降、または macOS 14.1 以降が必要です。

iPhone および iPad と Mac では、別々にモードを選択します。たとえば、個人の iPhone には User Enrollment、 Mac には Device Enrollment
を選択できます。デバイスの所有権は、後からデバイスページで変更できます。

アカウント主導の登録は、 Apple Management（APNs）が構成されている場合に利用できます。

APNs のセットアップがまだ完了していない場合は、 Apple Management のセットアップ（

APNs） を参照してください。

Apple Business をセットアップする
ユーザーは、 Apple Business で作成された Managed Apple Account
でサインインします。開始する前に：

1. Apple Business で、組織のドメインに ドメインを確認 （例： company.com）します。

2. **Managed Apple Account** Apple Business Google Workspace Microsoft Entra ID
3. User Enrollment Managed Apple Account User Enrollment
4. **Apple Business** **Devices → Management Services → Default Device Assignment** Edit iPhone iPad Mac Cerberus Enterprise

> Managed Apple Account Cerberus Enterprise Apple Business

Cerberus Enterprise

Apple

- *company.com* 20
- **iPhone** **iPad** **Mac** User Enrollment Device Enrollment
- Cerberus Enterprise

> **Managed Apple Account** Managed Apple Account Cerberus

で確認されていなくても登録できます。たとえば、 Apple Business の予約ドメイン org.appleid.com
のアカウントです。 Apple Business のサービス検出を使用する場合、ユーザーは常に Managed
Apple Account を入力します。

ドメインを確認する

設定を保存すると、 ドメインの確認 セクションに各ドメインの TXT
レコードが表示されます。それをドメインの DNS に追加し、 確認 をクリックします。 DNS
の変更が反映されるまでに時間がかかる場合があります。確認済みのドメインは確認済みのままです。後で
レコードを削除できます。確認されていないドメインのユーザーは登録できません。

サービス検出：デバイスが Cerberus

Enterprise を検出する方法
ユーザーがサインインすると、デバイスはアカウントのドメイン（例： https://company.com ）に、どのサーバーが管理しているかを問い合わせます。次の 3つのオプションのうち少なくとも 1
つを設定してください。タブの サービス検出 セクションには、組織の検出 URL
と、各オプションでコピーする正確なテキストが表示されます。

オプション 1：Apple Business（推奨）
Apple Business に登録 をクリックします。 Cerberus Enterprise は検出 URL を Apple Business
組織に保存し、ドメインに何も公開する必要はありません。 Apple Business で確認 をクリックすると、 Apple Business が現在保持している URL が表示され、 Apple Business から削除
をクリックすると削除されます。

iOS および iPadOS 18.2 以降、または macOS 15.2
以降が必要です。古いデバイスではオプション 2 または 3 が必要です。
Cerberus Enterprise で Apple Business が接続されていること（ Automated Device
Enrollment サービス トークン）、および上記のデフォルトのデバイス割り当てが必要です。
デバイスは、ドメインが応答しない場合にのみ Apple Business に問い合わせます。アドレス https://company.com/.well-known/com.apple.remotemanagement は存在してはなりません（「見つかりません」などのエラー）。 Web サイトが Web
ページで応答すると、デバイスはそこで停止します。 構成を確認
を使用して、応答内容を確認してください。

Apple Business は組織ごとに 1つの検出 URL を保持します。登録すると、組織のすべての Managed Apple Account がこの Cerberus Enterprise 組織に送信されます。同じ Apple Business

組織を使用する 2つの Cerberus Enterprise 組織から登録しないでください。

オプション 2：Web

サイトからのリダイレクト

各ドメインの Web サーバーで、 /.well-known/com.apple.remotemanagementを組織の検出 URL
にリダイレクトし、 クエリ文字列を保持
します（ユーザーが入力したアカウントが含まれています）。これは、アカウント主導の登録をサポートす
るすべての OS バージョンで機能し、 iPhone と Mac で異なるモードを使用できます。タブから Apache
または nginx 用のテキストをコピーしてください。組織のキーを含めると、次のようになります。

Apache（.htaccess または仮想ホスト）：

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/discoveryis_argsargs;
}

他の Web サーバーまたはサービス（ IIS、Cloudflare
、ホスティングコントロールパネルなど）では、同じパスから検出 URL へのリダイレクトルール（ 302 ）を、クエリ文字列を保持または転送するオプション付きで作成します。

オプション 3：Web サイト上の静的ファイル
リダイレクトを追加できない場合は、 https://company.com/.well-
known/com.apple.remotemanagement（ファイル拡張子なし）にファイルを公開し、 Content-Type: application/json
で配信します。その内容はタブからコピーしてください。静的ファイルではデバイスごとにモードを選択で
きません。 iPhone、iPad、 Mac で同じモードを使用します。 User Enrollment
の場合は次のようになります。

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

Device Enrollment の場合は次のとおりです。

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

> ファイルのモードは、タブでデバイスファミリーに設定されたモードと同じである必要があります。
> そうでない場合、登録は拒否されます。

構成を確認

構成を確認 で、ドメインとデバイス（ iPhone または Mac）を選択し、 確認 をクリックします。 Cerberus Enterprise は、デバイスが問い合わせる内容をドメインに問い合わせ、応答、各リダイレクト、判定を表示します。ドメインが Cerberus Enterprise を指している場合は、オプション 2 または 3 が機能します。エラー応答（「見つかりません」など）はオプション 1 で問題ありません。 Web ページまたは別の場所を指すファイルは、デバイスを停止させます。また、リダイレクトがクエリ文字列を削除した場合や、ファイルが *application/json*として配信されていない場合にも警告が表示されます。

登録キー

検出 URL と登録 URL には、組織のキーが含まれています。 URL が誤って公開された場合は、 キーを再生成 をクリックしてください。古い URL はすぐに機能しなくなるため、 Web サイトのリダイレクトと静的ファイルを更新してください。オプション 1 を使用している場合、 Cerberus Enterprise は新しい URL を自動的に Apple Business に登録します。

ユーザーが登録する方法

1. iPhone と iPad: 設定 → 一般 → *VPN* とデバイス管理 → 職場または学校のアカウントでサインイン 。Mac: システム設定 → 一般 → デバイス管理 → サインイン （ macOS 14: プライバシーとセキュリティ → プロファイル → サインイン ）。
2. Managed Apple Account、または Cerberus のユーザーの仕事用メールアドレス（例: *name@company.com*）を入力します。ユーザーの Managed Apple Account が入力したものと異なる場合、デバイスはそのアカウントでのサインインを求めます。
3. Cerberus Enterprise のページが開きます。 コードを送信 をタップし、メールで受け取った 6 桁のコードを入力します。コードは 10分後に期限切れになります。 5 回間違えると、ユーザーはページを閉じて再度サインインする必要があります。
4. Managed Apple Account のパスワード（または Apple Business が Google Workspace や Microsoft Entra ID に接続されている場合は会社のサインインページ）でサインインし、デバイス管理を許可します。

>

登録できないアカウント（ドメインが確認されていない、ユーザーが自動作成されない設定で一致す
るユーザーがいない、同じメールアドレスのユーザーが複数いる）には、「このアカウントは登録用
に設定されていません。 IT
管理者に問い合わせてください」と表示されます。イベントはダッシュボードのシステムログに記録
されます。

登録後
デバイスページには、登録に使用した Managed Apple Accountと登録タイプ（ User
Enrollment またはアカウント主導の Device Enrollment
）が表示されます。デバイスリストでは、 User Enrollment デバイスに「 User Enrollment
」と表示されます。
User Enrollment デバイスでは、 Apple
が許可しないコマンドやポリシー設定（消去、位置情報、紛失モード、 OS
アップデート、多くの制限）は提供されず、送信されません。ポリシーの App Store
アプリは、デバイスライセンスではなくユーザーライセンスを使用します（下記の
個人デバイス上のアプリ を参照）。
User Enrollment デバイスでは、 Web クリップはホーム画面に表示されますが、 設定 → 一般 →
VPNとデバイス管理 には表示されません。
これらのデバイスの MDM 証明書は自動的に更新されず、 Return to Service
は利用できません。 MDM 証明書が期限切れになる前（登録から 1
年後。デバイスページを参照）に、ユーザーにデバイスの再登録を依頼してください。
管理を離れるには、ユーザーが設定の同じ場所で仕事用アカウントからサインアウトするか、
Cerberus Enterprise からデバイスを登録解除します。 User Enrollment では仕事用のアプリ、アカウント、データのみが削除され、個人データは残ります。再登録したデ
バイスは新しいデバイスとして表示されます。

登録直後、ポリシーの一部のプロファイル (証明書、 Wi-Fi ネットワーク、 Web クリップ)
が不明なエラーで失敗として報告され、デバイスがしばらく コンプライアンス違反
と表示されることがあります。デバイスは自動的に再試行し、しばらくすると何も操作しなくてもイ
ンストールされます。このため、ポリシーを再度保存したり、デバイスを再登録したりしないでくだ
さい。

個人デバイス上のアプリ
User Enrollment で登録された iPhone および iPad にはシリアル番号がないため、 Apps and Books
はデバイスライセンスを付与できません。 Cerberus Enterprise は、ポリシーの App Store
アプリに代わりに ユーザーライセンス を付与します。ライセンスは、デバイスでサインインしている
Managed Apple Account
に付与されます。ポリシーに変更はありません。同じポリシーが会社のデバイスと個人のデバイスに使用さ

れ、 Cerberus がデバイスごとにライセンスの種類を選択します。

自動 ：最初の登録時に、 Cerberus は Managed Apple Account を Apps and Books
に登録し、ポリシーの各 App Store アプリのライセンスを Apple
に要求します。無料アプリにもライセンスが必要です。 Apple
は無料アプリに無制限のライセンスを付与します。有料アプリは Managed Apple Account ごとに
1つのライセンスを使用し、そのアカウントのすべての個人デバイスで共有されます。
同じ組織 ： Managed Apple Account と Cerberus Enterprise の Apps and Books
トークンは同じ Apple Business
組織に属している必要があり、アプリはトークンの場所のライブラリに存在する必要があります。
ライセンス優先 ：アプリは、 Apple
がライセンスを確認した後にのみデバイスに送信されます。通常は数分以内です。それまでは、デ
バイスの アプリケーション パネルに ユーザーライセンスを待機しています
と理由が表示されます。
インストール プロンプト : 個人デバイスは監督されないため、 iOS
は各アプリをインストールする前にユーザーに確認します。これには、 Cerberus がこれらのデバイスにもインストールする Cerberus Enterpriseアプリが含まれます (
インストール または キャンセル)。Apple Account
へのサインインは不要です。ユーザーがキャンセルした場合、アプリには
ユーザーによるインストールの承認を待機中 と表示されます。デバイス ページで 再要求を使用して、プロンプトを再度表示してください。 必須
としてインストールされたアプリは、ユーザーが削除できません。
登録前にインストールされたアプリ ：Apple は、 User Enrollment で登録されたデバイスにユーザーが個人的にインストールしたアプリを組織が引き継ぐことを許可していません。登録前にユーザーに自分のコピーを削除してもらうか、削除してからデバイスペー
ジで 再リクエスト を使用してください。その後、組織が管理対象のコピーをインストールします。
管理を離れる場合 ：デバイスの登録が解除されると、 iOS
は管理対象アプリとそのデータを削除します。ライセンスは、同じ Managed Apple Account
の他の登録済みデバイスがそれを必要としなくなったときに解放されます。たとえば、アプリがポ
リシーから削除された場合や、最後のデバイスが登録解除された場合です。不要になったライセン
スは、毎日のチェックで 1日以内に解放されます。

Apple
がライセンスを割り当てられない場合（たとえば、有料アプリに残りのライセンスがない場合）、ア
プリには Apple のメッセージとともに ユーザーライセンスに失敗しました が表示されます。 Apple Business でライセンスを追加してから、デバイスページで 再リクエスト を使用してください。
Cerberus も毎日のチェックで自動的に再試行します。アプリリストの上の行には、 Managed Apple Account とその Apps and Books
ユーザーのステータスが表示されます。同じステータスはユーザーのページにも表示されます。

ユーザーライセンスは iPhone と iPad でのみ使用されます。 User Enrollment で登録された Mac
では、ポリシーの App Store アプリはインストールされません。 Books と個人用 Apple Account
はサポートされていません。