STAR-MDM

Device Enrollment Program

初期設定手順

スターネット株式会社

第1.3版

目　次

Device Enrollment Programとは

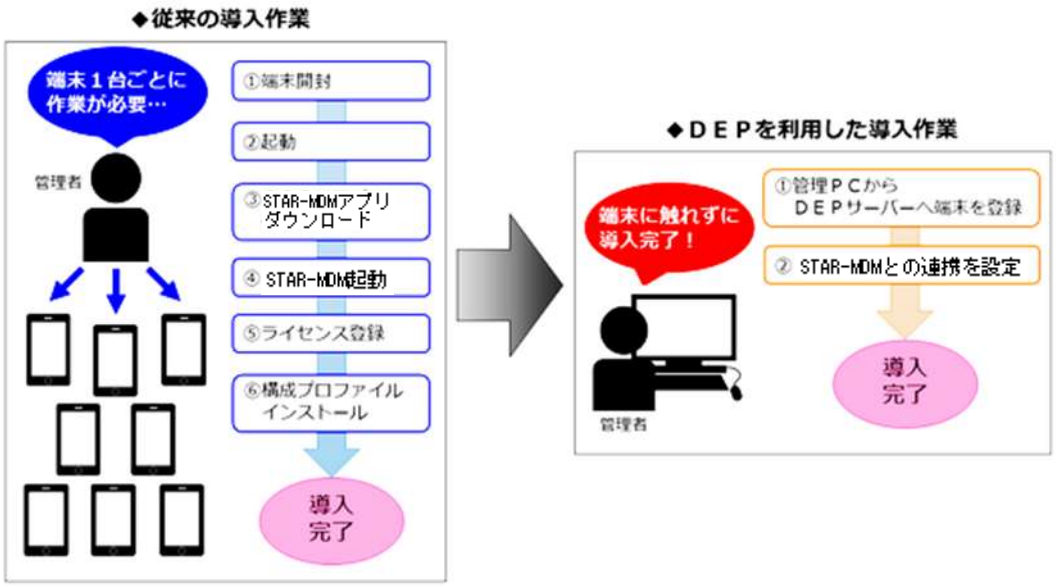
Device Enrollment Program（以下、DEP）は、Apple 社の提供する端末導入・設定の支援サービスです。STAR-MDM と DEP を併せて用いることで、従来必要とされていたキッティングの手間を大幅に削減し、STAR-MDM による制御をより強固なものにすることができます。

Apple 社の提供する“Apple Business Manager”専用 WEB ページ（以下、ABM）および STAR-MDM 管理画面で公開鍵・サーバトークンをダウンロード/アップロードし、STAR-MDM 管理画面から端末に反映したい設定を編集していただく必要があります。

*1 DEP を利用するには、Apple 社または指定の代理店から購入した、DEP 対応の iOS 端末が必要です。

Device Enrollment Programの利点

・キッティング作業を簡易に



DEP を利用することにより、STAR-MDM のキッティング（初期設定）作業を一括して行うことができます。
従来はユーザの端末 1 台 1 台に対してグループキー登録・ポリシー設定などの作業が必要であり、多数の端末をご利用の場合にはキッティング作業に時間がかかっていました。DEP を用いることで、管理者が一括して、リモートでキッティング作業を行うことが可能になります。
端末側ではアクティベート時に自動的 STAR-MDM が導入されるため、端末ユーザによる作業も必要ありません。購入した端末はそのまま端末ユーザに配布できます。

また、STAR-MDM 管理画面から行う DEP 設定により、端末初期設定時に必要とされる各種設定（パスコード、Apple ID、利用規約、Touch ID、Apple Pay、画面表示の拡大、Siri、診断）のうち、端末ユーザによる設定が不要だと判断される項目についてはスキップするよう設定することができます。スキップするよう設定すると、ユーザが端末を起動したとき、その項目に関する設定画面は表示されません。

*1 端末ユーザによる初期設定スキップ項目について、詳細はこちらをご確認ください
関連情報☞「初期設定　スキップ項目」

STAR-MDM による制御をより強固なものに

DEP を利用することにより、端末ユーザによる構成プロファイルの削除を禁止し、STAR-MDM による制御が解除されることを防ぎます。

従来は、端末ユーザによる STAR-MDM 構成プロファイルの削除が可能でした。DEP を用いた場合、iOS によって提供される「監視モード」をリモートで有効に設定することで、端末の構成プロファイル管理画面に「削除」ボタン自体が表示させないように設定することが可能です。

*1 STAR-MDM 以外の構成プロファイルの削除は、通常通り可能です

*2 監視モードについて、詳細はこちらをご確認ください。関連情報☞「監視モード」

初期設定（事前の設定）

必要なもの

STAR-MDM で DEP 端末をご利用いただくには、以下のものが必要です。

- Apple ID/パスワード

  ・STAR-MDM 管理サーバに iOS 端末（iPhone/iPad）を登録して管理するには、Apple 社が提供する IP プッシュシステム APNs（Apple Push Notification）サービスの利用が**必須**となります。

  また、APNs（Apple Push Notification）サービスを利用するためには、
  「iOS プッシュ証明書」を取得し、ご利用の STAR-MDM 管理画面に登録を行う必要がございます。

  iOS プッシュ証明書の取得および登録の詳細な手順については、
  iOSプッシュ証明書新規登録・更新手順書をご確認ください。
  https://star-mdm.ne.jp/manualdl/manual.html

- DEP 登録

  ・Apple のページから登録してください（登録には端末販売代理店の情報が必要な場合はあります・Resseler ID など）

- DEP に対応した iOS 端末

  ・Apple 社もしくは指定の代理店からのみ購入可能です

- STAR-MDM アカウント契約

  ・STAR-MDM へのログイン情報等については、ご契約時に送付しているログイン情報をご参照ください

公開鍵のダウンロード

1. STAR-MDM 管理画面にアクセスし、その他＞DEP 設定を開いてください。

2. 公開鍵を DL してください
   [1. 公開鍵ファイル　SPPM_DEP_cert.pem をダウンロードしてください。]
   という記載の、SPPM_DEP_cert.pem をクリックすると公開鍵がダウンロードされます
3. [2. 1 でダウンロードした公開鍵ファイルを Apple Business Manager へアップロードしてください。] と案内にある通り、Apple 社の提供する HP “Apple Business Manager” (ABM)にアクセスしてください。

Apple Business Manager での操作

MDM サーバ名の設定・公開鍵のアップロード

ABM（https://business.apple.com/）にアクセスし、ABM 利用登録を行った Apple ID/パスワードでサインインしてください。

1. 左下のアカウント＞[環境設定]＞[MDM サーバの割り当て]＞[MDM サーバを追加]をクリックしてください。

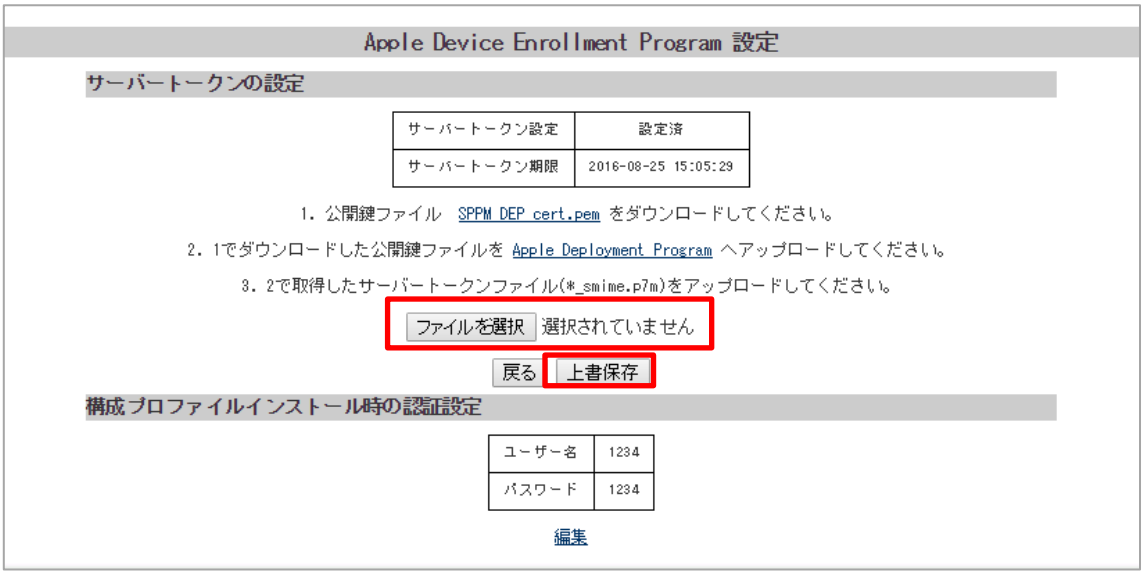
2. [MDM サーバ情報]に「STAR-MDM」等わかりやすい名称を入力してください。
3. [ファイルを選択]をクリックし、STAR-MDM 管理画面でダウンロードした公開鍵（“パブリックキー”と呼ばれます）をアップロードしてください。
4. アップロードが完了したら[保存]をクリックしてください。

サーバトークンをダウンロード

[トークンをダウンロード]をクリックし、トークンをダウンロードしてください

※Apple Business Manager からトークンをダウンロードした場合、必ず管理サイトにトークンをアップロードしてください。このトークンを管理サイトにアップロードしなかった場合、一定時間経過後に、管理サイトは DEP サーバとの通信ができなくなります。

サーバトークンをアップロード



1. STAR-MDM 管理画面にアクセスし、[その他] > [DEP 設定]を開いてください
2. [ファイルを選択]から、ABM でダウンロード（保存）したサーバトークンをアップロードします
3. アップロードが完了したら、[上書き保存]をクリックしてください

※ サーバトークンの有効期間は 1 年間です。期間を過ぎる前に更新作業が必要です。
更新作業について、詳細はこちらをご確認ください > 「サーバトークンの更新」

端末へのDEP適用

①DEP 端末の更新

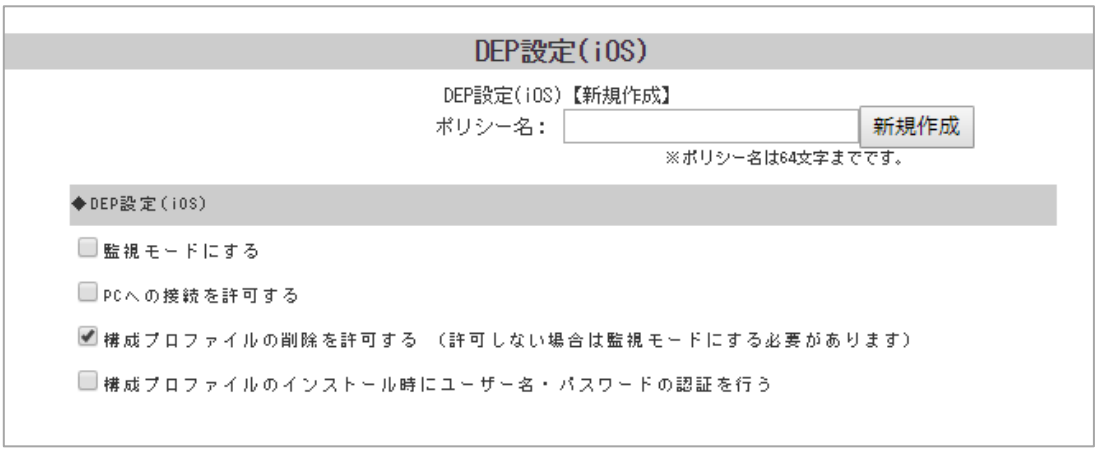
STAR-MDM 管理画面にアクセスし、必ず端末一覧画面の「DEP 端末更新」をクリックしてください。
DEP 登録した端末の「端末 ID」が自動的に登録されます。

②ポリシー作成

［ポリシー管理］ ＞ ［DEP 設定(iOS)］ ＞ ［新規作成]をクリックし、ポリシーを作成してください。

◆DEP 設定(iOS)

DEP を利用し STAR-MDM に登録された端末に下記項目が適用されます。



・監視モードにする

DEP 端末の監視モードを有効にできます。
STAR-MDM の構成プロファイルの削除を禁止する場合、監視モードを有効にする必要があります。
※監視モードを解除する方法
端末を初期化し、「監視モードにする」のチェックを外した DEP 設定ポリシーを端末に設定・反映してキッティングを開始してください。
※iOS13 以降では「監視モードにする」にチェックがない場合でも、監視モードが有効になります。

・PC への接続を許可する
端末の iTunes への接続を制限できます。

・構成プロファイルの削除を許可する（許可しない場合は監視モードにする必要があります）
STAR-MDM の構成プロファイルの削除を禁止することができます。
禁止にするには[監視モード]を有効にする必要があります。
※構成プロファイルの削除を禁止した状態で該当端末のライセンスキーをリセットした場合は、STAR-MDM の再登録に端末初期化が必須となるためご注意ください。

・構成プロファイルのインストール時にユーザー名・パスワードの認証を行う
構成プロファイルのインストール時に、管理画面で設定したユーザー名とパスワードが必要となります。

〈ユーザー名・パスワード設定方法〉

1. STAR-MDM 管理画面の ［その他］ ＞ ［DEP 設定(iOS)］ ＞ ［編集］ をクリックします。

2. ユーザー名・パスワードを入力し「上書保存」をクリックします。

3. 設定されたユーザー名・パスワードは ［その他］ ＞ ［DEP 設定(iOS)］ 画面に表示されます。

◆初期設定 スキップ項目

端末初期設定時にスキップする項目を選択できます。

チェックを付けた項目はアクティベート時に設定画面が表示されません。

<設定項目>

パスコード	位置情報サービス	復元
Apple ID	利用規約	Touch ID
Apple Pay	画面表示の拡大	Siri
診断	データとプライバシー	iPhone を常に最新の状態にする
iMessage と FaceTime	スクリーンタイム	外観モード
ようこそ	新機能の概要	復元完了
Android から移行	True Tone ディスプレイ	ホームボタンの触覚
モバイル通信を設定		

※ [Apple Pay]は iOS10.1 から表示される設定項目です。

※[モバイル通信を設定]は、iOS12 以上かつ eSIM 対応端末の場合に表示される設定項目です。

※ iOS8.x までは[Apple Pay]のチェックを外した場合、[パスコード][Touch ID]がスキップ不可となります。

※ iOS8.x までは端末初回キッティング時以外では、[位置情報サービス][復元]がスキップされない場合があります。

※iOS16 以降、初期設定時に AppleID にサインインした場合、[利用規約]はスキップ不可となります。

ポリシー適用

[DEP 端末更新]で表示された該当端末 ID に DEP 設定(iOS)ポリシーを適用します。

※このとき DEP 設定(iOS)ポリシー以外のポリシーを保存しても、端末登録後にリセットされます。

<端末 ID 毎にポリシーを適用する場合>

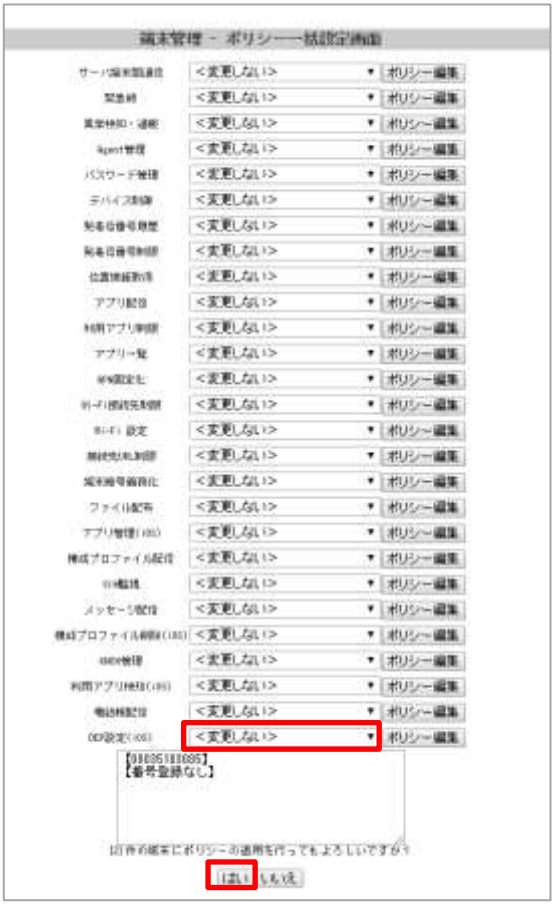
1. 端末一覧画面で、該当端末 ID の[編集]をクリックします。

2. DEP 設定(iOS)のプルダウンリストから適用したいポリシーを選択します
3. [上書保存]をクリックします

※この設定は DEP 端末登録用の事前設定のため、その他ポリシーは適用できません。

<複数の端末 ID に同一のポリシーを適用する場合>

1. 端末一覧画面で、該当端末 ID の[選択]にチェックを付けます
2. [ポリシー適用]をクリックします



3. DEP 設定(iOS)のプルダウンリストから適用したいポリシーを選択します
4. [はい]をクリックします

端末キッティング

これまでの各設定が完了している状態で DEP 端末のキッティング時（アクティベート時）に、
DEP 設定(iOS)ポリシーで設定した内容が反映されます。
※端末によってはアクティベートに SIM が必要になる場合があります。

初期設定の最後に構成プロファイルのインストールを行います。
インストールが完了すると STAR-MDM の管理画面に該当端末が登録されます。

SPPM Agent をインストール

「App Store」を起動してください。

「SPPM」もしくは「SPPM Agent」を
キーワードで検索してください。

③ SPPM Agent を**ダウンロード・インストール**してください

④ インストール完了後、**「開く」**
ボタンをタップすることで
SPPM Agent が開きます

⑤連絡先へのアクセス許可を求められます。「OK」をタップしてください。

⑥ 位置情報の利用許可を求められます。「**許可**」をタップしてください。

⑦プッシュ通知の利用許可を求められます。「**許可**」をタップしてください。

⑧ **グループキー、端末のシリアル番号**を入力し、「**登録**」をタップしてください。

※シリアル番号のコピー方法は
次ページをご参照ください

⑨ STAR-MDM 管理サーバへの登録の確認画面が表示されます。「OK」をタップしてくださ

⑩「端末登録が完了しました」
と表示されましたら、「OK」
をタップしてください。

⑪「SPPM Agent」を起動して、
管理サーバ URL が表示される事を確認します。
（管理画面でメッセージ機能が対応している事を
確認してください。）

【端末シリアル番号のコピー方法】

※iOS バージョンにより、画面の表示が異なる場合があります

① 端末設定の『一般』をタップ

② 『情報』をタップ

③ 『シリアル番号』の項目を長押して
表示される『コピー』をタップし、
手順⑧の画面で貼付けを実行

端末の登録完了

STAR-MDM 管理サーバと通信が行われ、端末に基本ポリシーが適用され、「STAR-MDM」の構成プロファイルがインストールされ、STAR-MDM 管理画面の「端末一覧」にて端末が登録されていること、**SPPM Agent を起動して**サーバ URL が表示されることを確認してください。

※SPPM Agent を起動しないと、JailBrake 検知、メッセージ配信、位置情報取得、電話帳配信機能が利用できません。

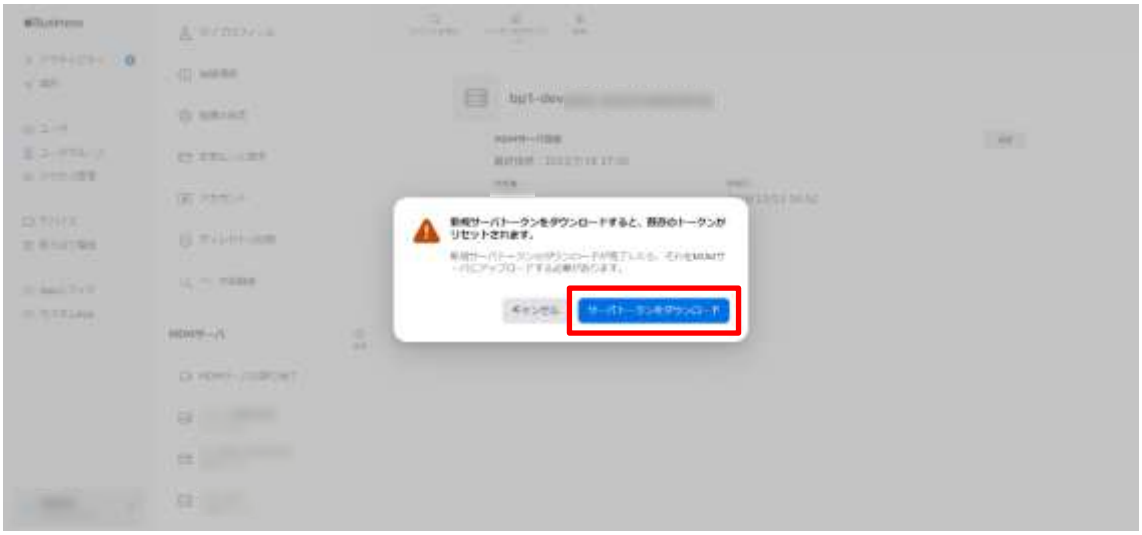
※icloud・iTunes バックアップデータから SPPM Agent をインストールすると正常に登録できない場合があります。その場合は一度アンインストール後に app store から再インストールをしてください。

サーバトークンの更新（Apple Business Managerでの操作）

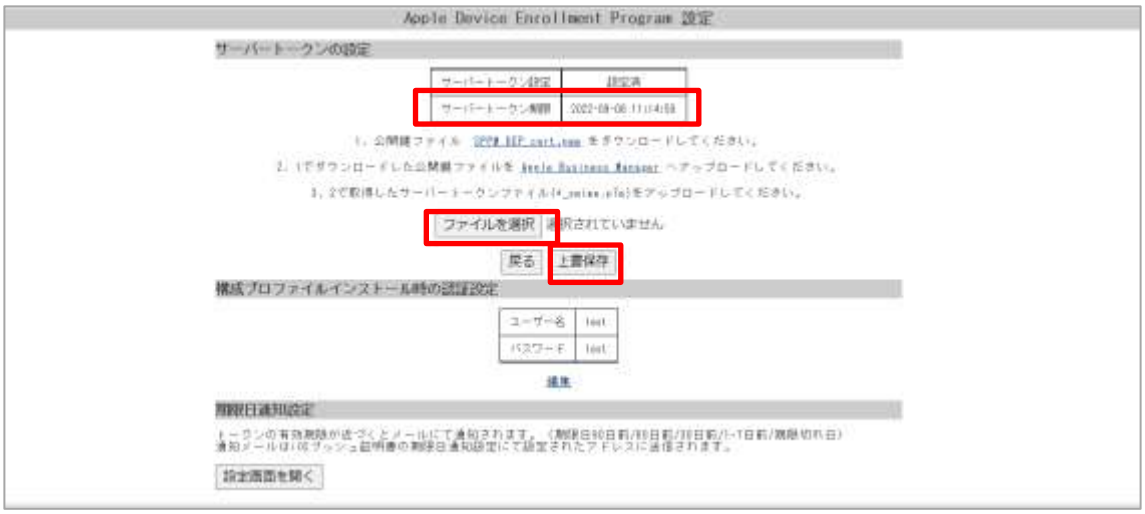
1. ABM にサインインし、ユーザーアカウント＞［環境設定］の順にクリックします。

2. 該当する MDM サーバをクリックします。

3. [トークンをダウンロード]をクリックします



4. [サーバトークンをダウンロード]をクリックし、サーバトークンをパソコンに保存してください



5. STAR-MDM 管理画面にアクセスし、その他 ＞ DEP 設定 を開いてください
6. [ファイルを選択]から新しく保存したサーバトークンを選択してください
7. サーバトークンをアップロードしたら、[上書き保存]をクリックします
8. ページ上部の表示、サーバトークンの新しい有効期限が表示されます

<期限日通知設定について>

「設定画面を開く」をクリックすると iOS プッシュ証明書登録の期限日通知設定に遷移します。
期限日通知設定の設定方法については、「STAR-MDM 管理者マニュアル iOS 版」の「 iOS プッシュ証明書登録」＞【期限日通知設定】を参照ください。
https://star-mdm.ne.jp/manualdl/manual.html

Q&A

Q. DEP 設定ポリシーはどの端末でも利用できますか？

A. DEP を利用するには、Apple 社または指定の代理店から、所定の方法で DEP 対応の iOS 端末を購入する必要があります。

Q. ハードリセットによる DEP 再キッティングの動作

A. ハードリセット時に”DEP 設定ポリシー”が、該当の端末に適用されているかで動作が変わります。

■DEP 設定ポリシー有り

1.″DEP 設定ポリシー″設定済み
2.ハードリセット指示発令
→初期化後、DEP 端末としてキッティング。
Agent インストール時は[DEP 対応端末の方はこちら]を選択する。
※通常の DEP 端末キッティングと同様の方法でキッティングして下さい。

■DEP 設定ポリシー無し

1.″DEP 設定ポリシー″未設定
2.ハードリセット指示発令
→初期化後、通常端末になる。
3.″DEP 設定ポリシー″を設定する
4.端末初期化
→初期化後、DEP 端末としてキッティング。
Agent インストール時は[DEP 対応端末の方はこちら]を選択する。
※通常の DEP 端末キッティングと同様の方法でキッティングして下さい。

Q. DEP 端末が登録されたライセンスキーを誤ってリセットしてしまった場合、STAR-MDM に再登録できますか？

A. 再登録できます。
構成プロファイルの削除を許可しているか禁止しているかで、方法が異なります。
構成プロファイルが削除禁止されている場合は端末初期化が必要になるためご注意下さい。

■DEP 設定が構成プロファイル削除を許可している場合

1.管理画面の[DEP 端末更新]をクリック
※再登録前に[DEP 端末更新]をクリックしなかった場合、通常端末として登録され、DEP 設定ポリシーを利用できなくなります。
2.ユーザにてアプリ削除・構成プロファイル削除を実施
3.AppStore から SPPM Agent をインストール
4.SPPM Agent を起動
5.[DEP 非対応端末の方はこちら]を選択し、構成プロファイルをインストール
⇒DEP 端末として登録されます。
※[DEP 対応端末の方はこちら]を選択しないようご注意下さい。

■DEP 設定が構成プロファイル削除を禁止している場合

※STAR-MDM への再登録には端末初期化が必須になります。

※初期化前に DEP 設定の準備をすることで初期化後に DEP によるキッティングが可能です。

1.管理画面の[DEP 端末更新]をクリック

※再登録前に[DEP 端末更新]をクリックしなかった場合、通常端末として登録され、
DEP 設定ポリシーを利用できなくなります。

2.端末設定から端末初期化を行う

⇒DEP によるキッティングが行われ、構成プロファイルインストール後に DEP 端末として
登録されます。

Q. [構成プロファイルのインストール時にユーザー名・パスワードの認証を行う]
設定の利用シーンは？

A. DEP 端末に[構成プロファイルのインストール時にユーザー名・パスワードの認証を行う]設定を有効にしたポリシーが適用されていることで、端末紛失時に第三者によって端末が初期化されてもユーザー名・パスワードが認証されない限り端末を利用できない状態にできます。

Q. 構成プロファイルの削除を禁止している場合、
STAR-MDM 以外の構成プロファイルを削除できますか？

A. 構成プロファイル削除(iOS)ポリシーを利用し、削除することができます。

Q.DEP 設定ポリシーを変更しポリシー即時適用を行っても、
端末状態シグナルが黄色のままですが正常に適用されていますか？

A.DEP 設定ポリシーは端末情報編集画面で「上書保存」をした時点で設定が完了し、次回端末アクティベート時に適用される仕様となります。
そのため、シグナルが黄色の状態でも正常に適用されています。
端末状態シグナルを緑色に更新したい場合は、他ポリシーを更新・適用をすることで緑色に更新できます。