ZJTP20211110855

2021

Active Directory

Self-Service Password Management

TFA & Single Sign-on Solution

スタートアップガイド

ManageEngine

ADSelfService Plus

目次

ドキュメントの概要

本ドキュメントでは、ManageEngine ADSelfService Plus（以下、ADSelfService Plus）の機能と特徴、インストール手順について紹介します。ADSelfService Plus の概要と各機能の操作方法をわかりやすく解説し、製品導入者や運用者が製品を効率的に導入/運用できることを目的としています。このドキュメントでは、以下の内容について説明します。

- 主要機能
- インストール手順
- 製品準備の流れ
- 多様なサポート機能と利用方法
- 製品運用に必要となる一般設定

1. ADSelfService Plus の概要

ADSelfService Plus は、セルフサービスパスワード管理およびシングルサインオンソリューションを提供しております。このソリューションは、ドメインユーザーが自分自身でパスワードリセット、アカウントロック解除、個人情報（モバイル番号や写真など）の更新を実行するのに役立ちます。また Active Directory ベースのシングルサインオン（SSO）を介して、Microsoft 365、Salesforce、G Suite など SAML2.0 がサポートするすべてのエンタープライズアプリケーションへの安全なワンクリックアクセスも提供します。セキュリティを強化するために、すべてのリモートおよびローカルログインに対して 2 段階認証を提供することも可能です。これらの機能を利用することで IT 管理者の負担を減らすだけでなく、効率的かつセキュアな IT 運用を実現することが可能になります。

＜主な機能＞

- ユーザー自身によるパスワード管理/アカウントロック解除
- パスワード有効期限通知
- ユーザー自身による Active Directory 連絡先情報の更新
- シングルサインオン（SSO）
- Windows/MacOS エンドポイントの 2 段階認証
- パスワードポリシー強化

1-1 主な特長と利点

機能	特長と利点
パスワードセルフサービス	• 下記セルフサービス機能を提供 　○ パスワードのリセット 　○ アカウントのロック解除 　○ パスワード変更 • SMS/メールによる認証コード、セキュリティ質問、Google Authenticator 等のマルチファクタ認証による安全な ID 確認 • Web ブラウザーまたは Windows のログオン画面からパスワード変更/アカウントロックの解除が可能 • パスワードの変更を様々なプラットフォームやクラウドサービスと自動で同期可能
パスワード有効期限の通知	• パスワード有効期限の自動通知 • アカウント有効期限の自動通知 • 複数の通知を指定間隔でスケジュール
ユーザーによるディレクトリ更新	• ユーザー自身による Active Directory の連絡先、写真、プロフィールなどの情報の更新 • セルフサービスポータルの自由なカスタマイズによる表示項目やレイアウトの変更 • 組織情報を更新するためのカスタム属性の設定
シングルサインオン(SSO)	• 多くのクラウドアプリケーションにワンクリックでアクセス可能 • SAML2.0 対応であれば対象アプリケーションの追加も可能
エンドポイントの 2 段階認証	• 端末にログオンする際に通常のパスワード認証に加えて、別の認証を要求 • よりセキュアな端末運用が可能
パスワードポリシー強化	• 10 を超える強力なパスワードポリシーを組織に適用することでセキュリティ強化を実現 • OU またはグループベースでのパスワード強化

2. ADSelfService Plus のインストール

この項目では、ADSelfService Plus の運用開始に必要な動作環境の確認、インストールの手順やドメインの設定方法について説明します。

2-1 動作環境

ADSelfService Plus をご利用いただくためには、次の条件を満たすシステムが必要です。

以下の動作環境はビルド 6110 以上を対象にしています。

ハードウェア

CPU	2.13 GHz 以上 / マルチコア
メモリー	4GB 以上
ストレージ	10GB 以上

ソフトウェア

OS	Windows 8, 10, Windows Server 2012, 2012 R2, 2016, 2019（64bit）

※クライアント OS は評価目的のみで利用可能です。本番環境にはサーバーOS をご利用ください。

データベース	PostgreSQL（製品バンドル）, Microsoft SQL Server

Web クライアント

Web ブラウザー	Google Chrome, Firefox, Microsoft Edge 推奨解像度 1024 x 768 ピクセル以上

ポート要件などより詳しい動作環境につきましては以下をご参照ください。

https://www.manageengine.jp/products/ADSelfService_Plus/system-requirements.html

2-2 ADSelfService Plus のダウンロード

1. Web ブラウザーで次の URL を開き、ファイルをダウンロード

   https://www.manageengine.jp/products/ADSelfService_Plus/download.html

2-3 ADSelfService Plus のインストール

ADSelfService Plus は、ドメイン内のシステム要件を満たしたマシンであればインストールすることができます。
インストール方法は下記の通りです。

1. インストールするマシンのローカル管理者権限を持つユーザーで Windows にログオンします
2. ダウンロードが完了した「ManageEngine_ADSelfService_Plus.exe」ファイルをクリックします
3. インストール画面が表示されるので[次へ]をクリックします

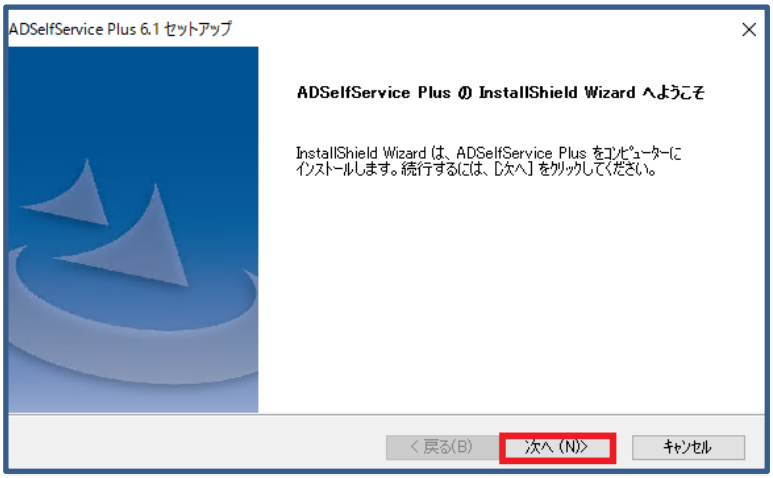


図 1 インストール画面

4. ライセンス条項を確認/承認後、[はい]をクリックします

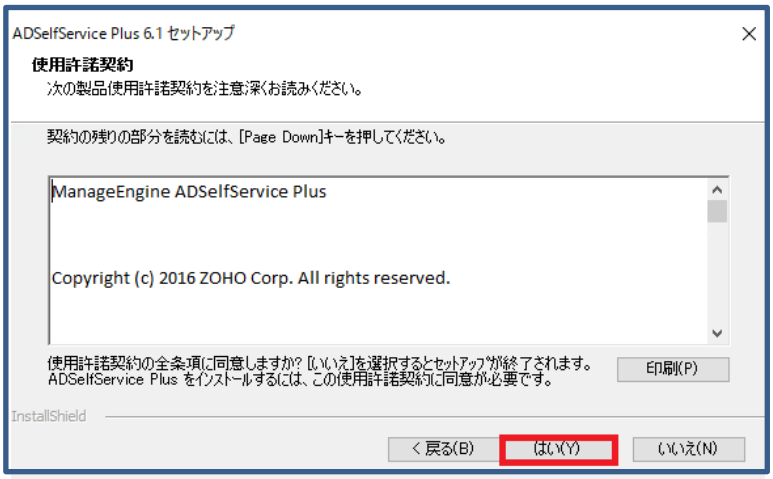


図 2 インストール画面

5. インストールディレクトリを選択します。デフォルトでは'C:¥ManageEngine¥ADSelfService Plus'です

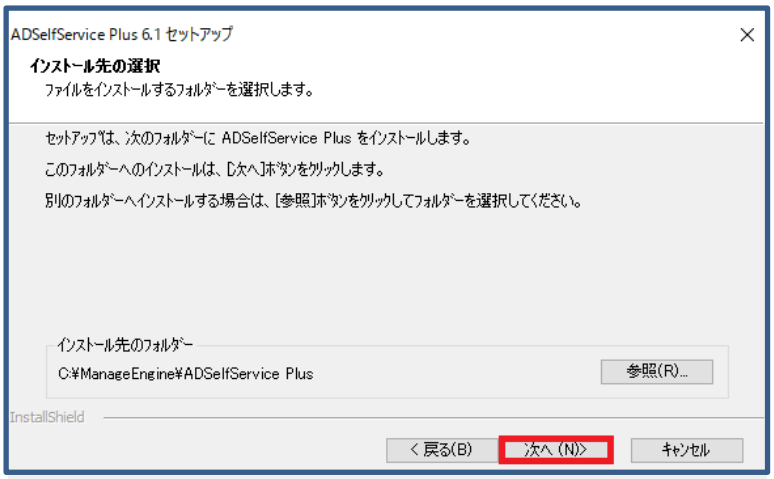


図 3 インストール画面

6. Web サーバーのポート番号を入力します。デフォルトでは **8888** です

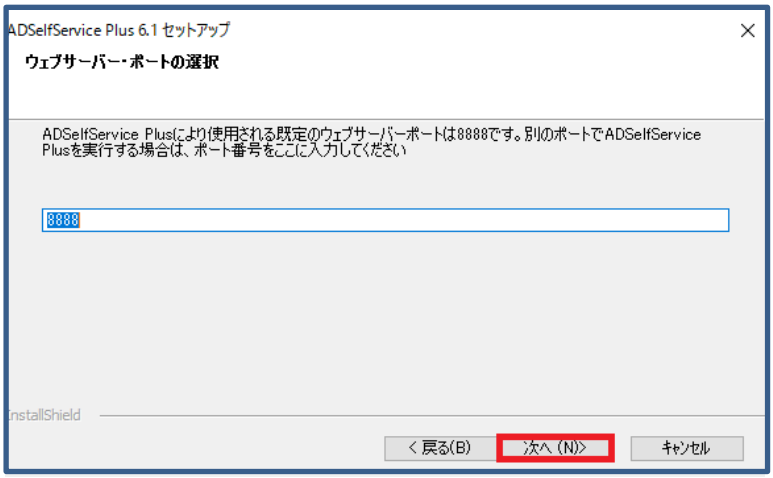


図 4 インストール画面

7. フォルダの設定ができます。変更がなければ、[次へ]をクリックします

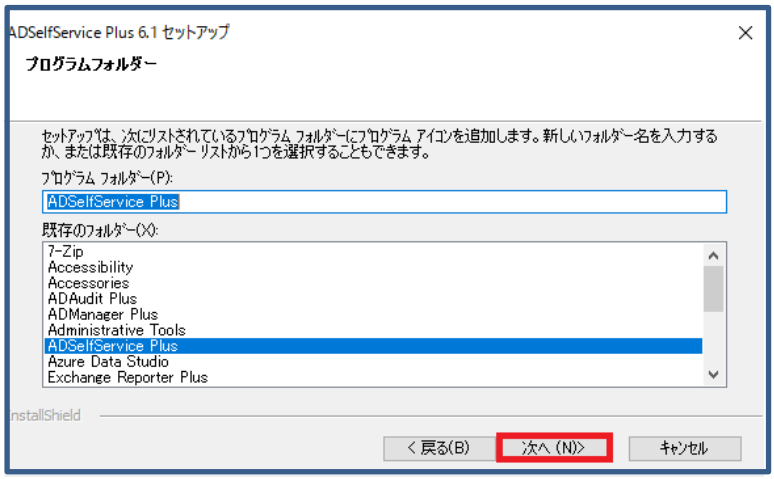


図 5 インストール画面

8. お客様情報を入力します。（任意）

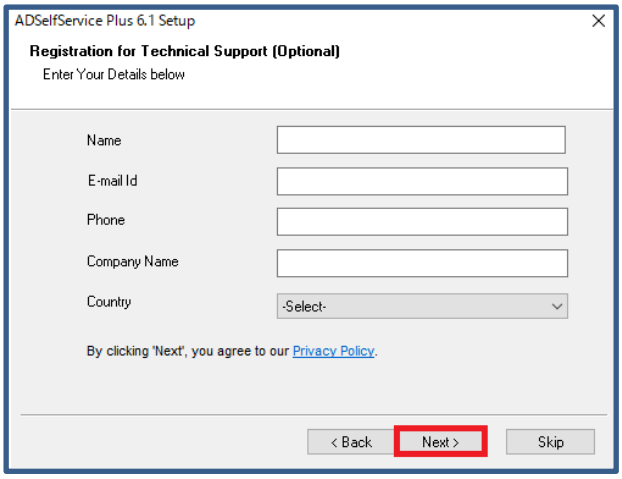


図 6 インストール画面

9. ADSelfService Plus をインストールするか選択を行います

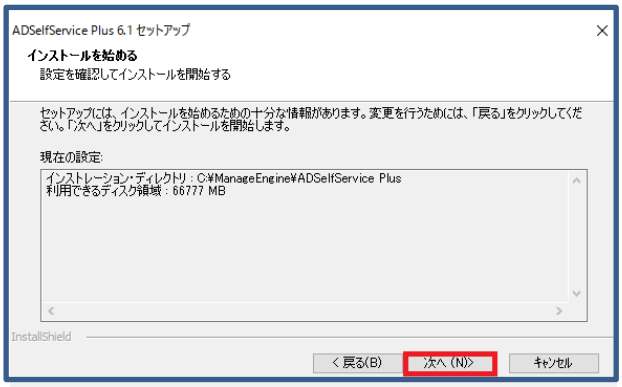


図 7 インストール画面

10. インストールの完了です。必要に応じてチェックボックスを選択し、[完了]をクリックします

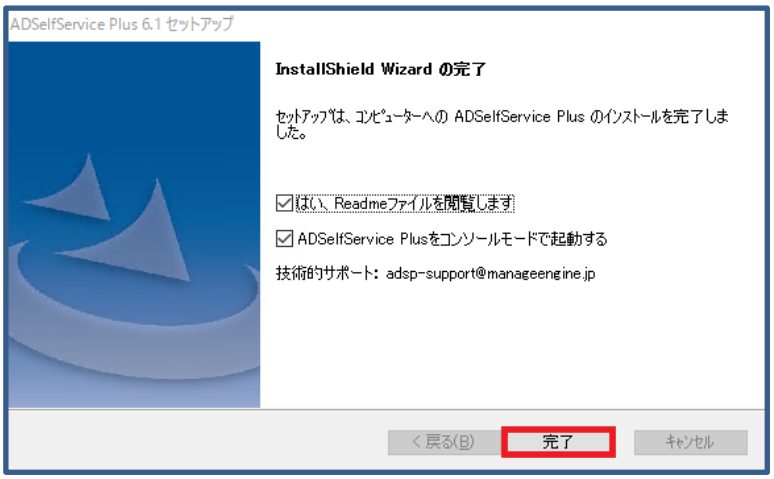


図 8 インストールウィザード

※各チェックボックスについて

[はい、Readme ファイルを閲覧します] -> リリースノート情報を記載したページ（英語版）が開きます。

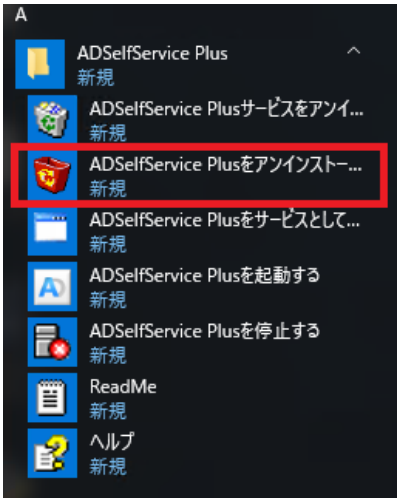
[ADSelfService Plus をコンソールモードで起動する] -> ADSelfService Plus がアプリケーション（コンソールモード）として起動されます。

※「アプリケーションとして起動」と「Windows サービスとして起動」の違いは、次章で説明します。

2-4 アンインストール

1. [コントロールパネル]→ [プログラムと機能]を開きます
2. ADSelfService Plus を選択し、[アンインストール]をクリックします
3. 画面の指示に従い、アンインストール作業を進めます

メモ：[スタート]メニュー → [ADSelfService Plus] → [ADSelfService Plus をアンインストールする]を選択してアンインストールすることもできます。



3. ADSelfService Plus の開始と停止

ADSelfService Plus サーバーは「アプリケーションとして起動」と「Windows サービスとして起動」（推奨）の 2 通りの起動方法があります。それぞれの起動/停止方法について説明します。

3-1 アプリケーションとして起動

製品をアプリケーションとして起動する場合は、デスクトップの ADSelfService Plus アイコンをクリックすることで起動されます。加えて、次の手順でも起動が可能です。

1. *<ADSelfService Plus インストール先>*¥bin フォルダを開きます

図 9 エクスプローラーのウィンドウ

2. [run.bat] をダブルクリックして実行します

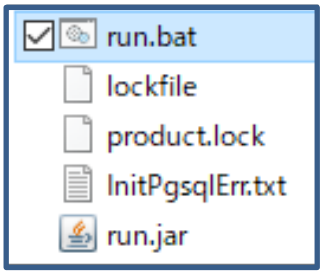
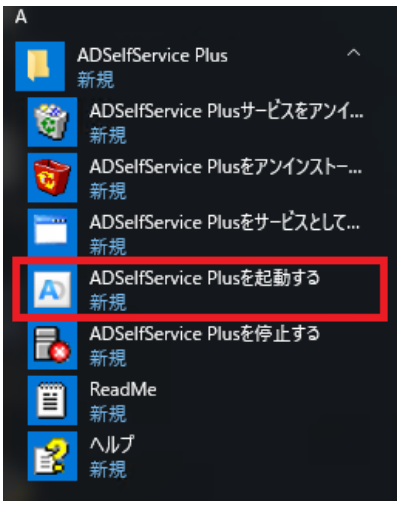


図 10 フォルダ内の run.bat を選択

メモ：スタートメニュー → ADSelfService Plus → [ADSelfService Plus を起動する]からも起動可能です。



3-2 Windows サービスとして起動

Windows サービスとして起動する方法は下記の通りです。

1. [スタート]メニュー → [ADSelfService Plus] → [ADSelfService Plus をサービスとしてインストール]をクリックし、ADSelfService Plus を Windows サービスとして登録します
2. [コントロールパネル] → [管理ツール] → [サービス]を開き[ManageEngine ADSelfService Plus] をダブルクリックします

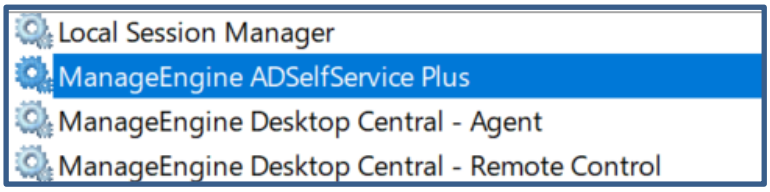


図 11 サービスのウィンドウ

3. スタートアップの種類から[自動]を選択し、[適用]をクリックします
4. サービスの状態の[開始]をクリックします

図 12 プロパティ画面

5. ManageEngine ADSelfService Plus サービスが起動します

メモ：上記手順により、今後は Windows の起動時に ADSelfService Plus サービスも自動的に起動します。

3-3 製品の停止（アプリケーションとして起動している場合）

1. *<ADSelfService Plus インストール先>*¥bin フォルダを開きます

図 13 エクスプローラーのウィンドウ

2. **shutdown.bat** をダブルクリックして実行します

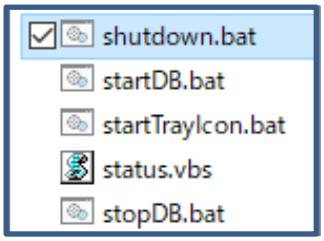
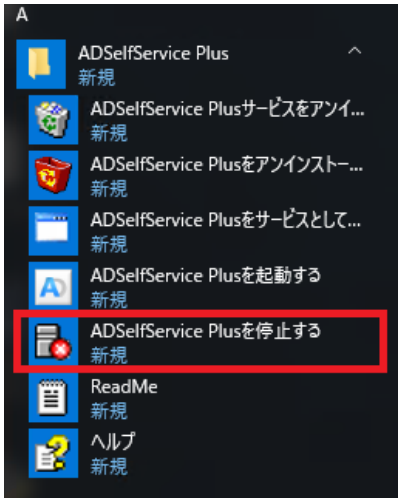


図 14 フォルダ内の shutdown.bat を選択

メモ：スタートメニュー → ADSelfService Plus → [ADSelfService Plus を停止する]からも停止可能です。



3-4 製品の停止（Windows サービスとして起動している場合）

1. コントロールパネル → 管理ツール → サービス を開き[ManageEngine ADSelfService Plus]をダブルクリックします

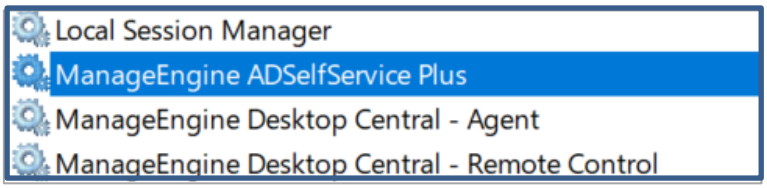


図 15 サービスのウィンドウ

2. サービスの状態の[停止]をクリックします

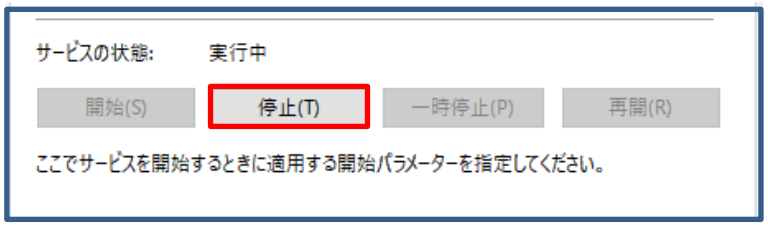


図 16 プロパティ画面

4. ADSelfService Plus の初期設定と構成

この章では、ADSelfService Plus 起動後の初期設定方法と管理者側とユーザー側それぞれのポータルについて説明します。

4-1 ADSelfService Plus へのアクセス

1. Web ブラウザーを起動します
2. アドレスバーに http://[*サーバー名/IP アドレス*]:[*ポート番号*] を入力し、移動します
   例：http://adssp-server:8888（デフォルトのポート番号は 8888 です）
3. 管理者として ADSelfService Plus にログインするには、初期ユーザー名として admin と入力し[ログイン]をクリックします。（ログイン先は「ADSelfService Plus の認証」のままにします）

図 17 ログイン画面（ユーザー名入力）

4. 初期パスワードとして admin と入力し、[ログイン]をクリックします。

図 18 ログイン画面（パスワード入力）

メモ：AWS Marketplace から ADSelfService Plus を購入した場合、管理者アカウントの初期パスワードは AWS の **インスタンス ID** となります。

メモ：上記の方法でリモートマシン上の ADSelfService Plus にアクセスできないときは、ADSelfService Plus がインストールされているマシン上のブラウザーから http://localhost:8888 にアクセス可能であるかご確認ください。

4-2 ドメイン設定

管理者ポータルの[ドメイン設定]の機能を利用することで、新しいドメインの追加や設定済みドメインの設定変更ができます。スタートアップ時には、検出可能なすべてのドメインが追加されますが、さらにドメインを追加する場合、またはドメインが自動的に検出されなかった場合は、この機能を使用して手動でドメインを追加します。

ドメインの追加（初期）

1. ADSelfService Plus にログインすると、次の画面が表示されます
2. ドメイン名を入力し、[検索]をクリックします

図 19 ドメインの詳細追加

3. 検出されたドメインコントローラーの中から選択し、[追加]をクリックします
   ※検出されない場合は、[ドメインコントローラー名]のテキストボックスに FQDN を入力して[追加]をクリックします

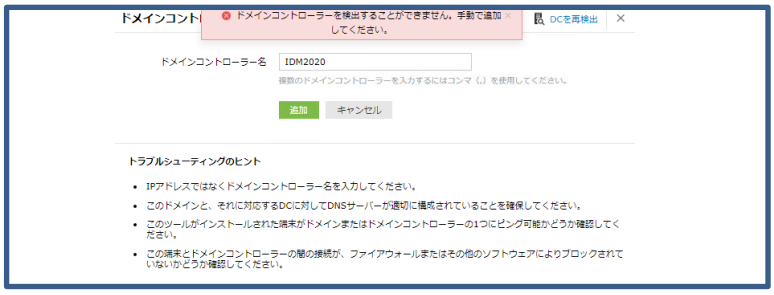


図 20 ドメインコントローラーの追加

4. [認証]にチェックを入れ、[ドメインユーザー名]および[パスワード]に Active Directory ドメイン管理者の資格を持ったユーザーの情報を入力します。すべてを入力後、[追加]をクリックします。

図 21 認証設定

ドメインの追加（運用時）

1. 管理者ポータル画面右上の[ドメイン設定]をクリックします

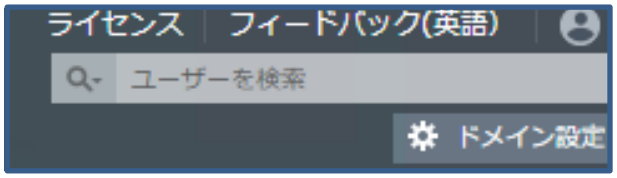


図 22 ドメイン設定

2. [新しくドメインを追加するにはここをクリックしてください]をクリックします
3. ポップアップ表示された[ドメインの詳細追加]の画面において、必要な情報を入力します
   ※入力方法は上記のドメインの追加（初期）をご覧ください

図 23 ドメインの詳細追加

4. [追加]をクリックして新しく設定したドメインを追加します

4-3 ADSelfService Plus の構成

ADSelfService Plus は IT 管理者が設定を行う管理者ポータル、および、ユーザーが製品を利用する際にログインするユーザーポータルの 2 種類ございます。本節では、それぞれが利用可能な機能について紹介します。

管理者ポータル

ADSelfService Plus の管理者ポータルでは、ドメインの設定、セルフサービスのポリシーの設定、製品のカスタマイズが可能です。管理機能/項目としては下記の通りです。

- レポート

  パスワード期限が近いユーザーなどを取得できる「ユーザーレポート」、製品使用状況などを把握できる「監査レポート」など管理者にとって必要な情報を簡単に可視化できます。
- セルフサービス

  セルフサービスでは下記の設定が可能です。
  - ポリシー設定（参照：5-1 セルフサービスの設定）
  - パスワード期限の通知（参照：6. パスワード/アカウント有効期限の通知）
  - パスワードポリシーの強化（参照：7. パスワードポリシーの強化）
  - パスワード同期/シングルサインオン（参照：8. シングルサインオン/パスワード同期について）
  - ディレクトリーセルフサービス（参照：9. ディレクトリーセルフサービス）
- 管理ツール

  管理者による一括登録（参照：手順 3：クイック登録）や GINA/CP（参照：Windows ログオン画面（GINA））の管理などが可能です。
- セキュリティセンター（参照：10. セキュリティセンター）

  セキュリティ質問の回答強度やパスワード強度設定等の各種セキュリティ関連の設定を行えます。
- カスタマイズ（参照：11-1 カスタマイズ）

  製品へのログオン設定（管理者ポータルへの接続 IP アドレス制限など）、製品の言語や表示画面の変更などを行えます。
- システムユーティリティ（参照：11-2 システムユーティリティ）

  製品のダッシュボード更新間隔の設定、バンドルインストールされた PostgreSQL のバックアップスケジュールなどの設定が行えます。
- 製品設定（参照：11-3 製品設定）

  ポート番号の変更、メールサーバー/プロキシサーバーの設定など製品運用に関連する設定を行えます。
- ライセンス管理（参照：11-4 使用されていないユーザーの制限）

  ライセンス消費を抑制できる機能である制限ユーザーの管理を行えます。

ユーザーポータル

管理者による設定後、ユーザー（利用者）はユーザーポータルにログインすることができるようになり、自身のプロフィール情報やパスワードを変更することができます。

- プロフィール

  Active Directory の属性情報（メールアドレス/携帯電話など）をユーザー自身が更新できます。
- パスワードの変更

  ユーザー自身のパスワードを、有効期限が切れる前に変更することができます。
- 登録

  ユーザーはそれぞれ ADSelfService Plus にユーザー登録を行い、パスワードのリセットやアカウントのロック解除の際に使用する本人確認の情報（セキュリティ質問など）を設定します。
- グループ

  Active Directory のグループを自分自身で管理できるようになります。グループをメーリングリストとして活用している場合などに有効です。
- アプリケーション

  クラウドサービスや SAML2.0 ベースのアプリケーションにログイン情報を入力することなくシームレスに移動できます。
- ユーザー検索

  ユーザー検索ボックスを使用し、他のユーザーの情報を検索することができます。

5. セルフサービス

この章では、管理者によるセルフサービスの設定の流れ、ユーザーによるパスワードのリセット/アカウントのロック解除の手順を説明します。

5-1 セルフサービスの設定

手順 1：セルフサービスポリシーの設定

1. 管理者として ADSelfService Plus にログインします
2. [設定]タブ → [セルフサービス] → [ポリシー設定]をクリックします
3. [ポリシーの追加]をクリックします
4. ポリシー名を入力します
5. 要件に合わせて必要なポリシーを選択します

図 24 ポリシー設定

6. [OU/グループの選択]をクリックし、ポリシーを適用するドメイン/OU/グループを指定します
7. [ポリシーを保存]をクリックします

ポリシーの作成後にポリシー編集画面を開き[詳細設定]をクリックしますと、セキュリティ強化ならびにセルフサービスアクションをカスタマイズするための様々な設定ができます。

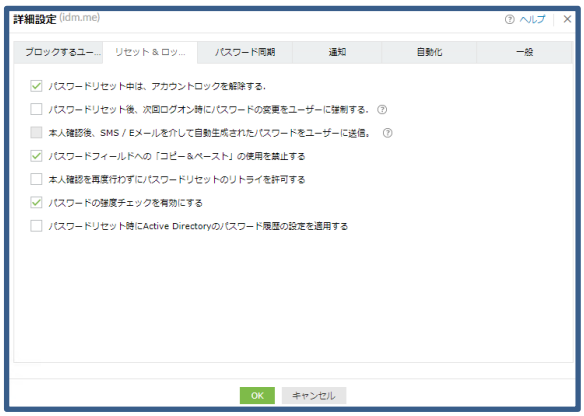


図 25 詳細設定

手順 2：本人確認の設定

1. [設定]タブ → [セルフサービス] → [マルチファクター認証]をクリックします

2. ポリシーを選択し、[設定]において各認証方法の設定をします

図 26 マルチファクター認証

3. [リセット/ロック解除用の MFA]タブでは、リセット/ロック解除時またはログイン時に利用する二段階認証（TFA）などを設定可能です

図 27 リセット/ロック解除用の MFA

4. [エンドポイント用 MFA]タブでは、エンドポイントおよび VPN 接続時の二段階認証などを設定可能です

図 27 エンドポイント用 MFA

メモ：

・[セキュリティ質問＆回答]：質問の設定、回答の設定、質問を編集（質問の追加/修正/削除、回答必須項目の設定）が可能です。

・[メール認証]/[SMS 認証]：送信されるメッセージの編集が可能です。

・[詳細設定]：セキュリティ質問/回答、認証コードの詳細設定を行えます。

メモ：メール認証/SMS 認証を使用する場合には、[管理]タブ → [製品設定] → [メール/SMS 設定]内の[メール設定]/[SMS 設定]に正しい情報が入力されていることをご確認ください。

手順 3：クイック登録（任意）

ユーザーがセルフサービス機能を使用するためには、ユーザー自身が事前に ADSelfService Plus でユーザー登録をしておく必要があります。クイック登録では、ユーザー登録をエンドユーザーに促すことができます。

具体的には、以下のような設定が可能です。

・管理者がユーザーに対して ADSelfService Plus への登録依頼メール通知を行う

・CSV ファイルなどを利用して一括登録すること　など

<操作手順>

[設定]タブ → [管理ツール] → [クイック登録]をクリックし、ユーザーを ADSelfService Plus に登録する方法を以下から選択します:

- **強制登録**：ログオンスクリプトを使用して、自動的に検出された非登録ユーザーがドメインにログオンした際に ADSelfService Plus への登録を強制したり、登録を促すメッセージを表示したりできます
- **登録依頼メール**：ADSelfService Plus への登録を促す通知メールをユーザーへ送信します
- **自動登録**：CSV ファイルからセキュリティ質問と回答などをインポートし、ユーザーが介入することなく、ユーザー情報を登録します
- **データベースから登録**：外部データベースよりユーザー情報を取得し、ユーザー登録を行えます

メモ：「外部データベースから登録情報をインポート」機能は登録のみのプロセスです。そのため DB からユーザーが削除された場合でも、製品上での登録は削除されません。

<ユーザー登録解除方法>

2 通りの方法がございます。いずれかの方法をご参照ください。

1. [レポート]タブ → [登録ユーザーのレポート]をクリックします。

2-A. 解除したいユーザーを選択し、[登録解除]をクリックします。

2-B. [一括で登録解除]より CSV を利用して一括解除します。

5-2 セルフサービスの利用（パスワードのリセット/アカウントのロック解除）

ユーザーは ADSelfService Plus のログイン画面、または Windows ログオン画面からパスワードのリセット/アカウントのロック解除リンクをクリックすることにより、自身のパスワードのリセット/アカウントのロック解除を行えます。

Web ブラウザー

LAN、あるいはインターネットから ADSelfService Plus の Web ポータルのログイン画面にアクセスし、
パスワードリセット用またはアカウントロック解除用のリンクを使用します。

<アクセスの手順>

1. Web ブラウザーを開きます
2. http://[ホスト名/IP アドレス]:[ポート番号] をアドレスバーに入力して、移動します
   例：http://adssp-server:8888（デフォルトのポート番号は 8888 です）
3. [パスワードを忘れた場合]または[アカウントがロックされた場合]をクリックし、ユーザー名を入力します
4. 本人確認を実施します
5. 新しいパスワードを設定します(パスワードリセットします)

図 28 ログイン画面

Windows ログオン画面（GINA）

Windows ログオン画面からパスワードのリセット/アカウントのロック解除へアクセスするためには、ADSelfService Plus のエージェント（クライアントソフトウェア）との連携が必須です。インストールされたエージェントは Microsoft GINA/Credential Provider を拡張し、ユーザーが使用している端末の Windows ログオン画面上にパスワードのリセット用/アカウントのロック解除用リンクを表示します。

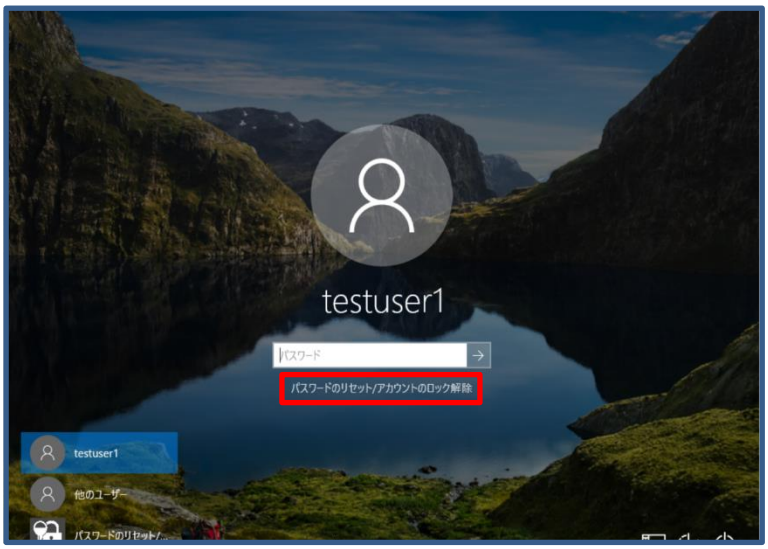


図 29 パスワードのリセット用/アカウントのロック解除リンク

<インストール手順>

1. [設定]タブ → [管理ツール] → [GINA/Mac/Linux (Ctrl+Alt+Del)] → [GINA/Mac/Linux のインストール]を選択します

※新規インストールするマシンは、[ドメインの選択]に指定されたドメインに属している必要がございます

2. [新規インストール]タブにて、対象の端末を選択します
3. 最後に[インストール]をクリックします

<アンインストール>

1. [設定]タブ → [管理ツール] → [GINA/Mac/Linux (Ctrl+Alt+Del)] → [GINA/Mac/Linux のインストール] を選択します
2. [インストールされたコンピューター]タブ → アンインストール対象のマシンを選択します
3. [アンインストール]をクリックします

<カスタマイズ>

ログオン画面に表示するテキストおよびアイコンのカスタマイズが可能です。

- アイコン（画像ファイル）

<スケジューラー>

以下のスケジューラーを設定することにより、インストール手順を自動化できます。

・GINA/Mac/Linux のインストール：GINA を自動的にインストールするスケジューラー

・GINA/Mac/Linux のカスタマイズ：GINA を自動的にカスタマイズするスケジューラー

メモ：セルフサービス操作によるパスワードやアカウントステータスの変更は、即時に Active Directory に反映されます。複数のドメインコントローラーが存在し、特定のドメインコントローラーに対して最初に反映したい場合は、[管理]タブ → [システムユーティリティ] → [サイトごとのドメインコントローラー]を設定します。※本設定での OU は、コンピューターが所属する OU ではなく、ユーザーが所属する OU です。

メモ：管理者の設定によっては、ユーザーが事前に本人認証情報を登録する必要がある場合がございます。

<指紋認証、プッシュ通知認証などを利用する場合>

モバイルアプリのインストール/設定が必要です。

<セキュリティ質問を利用する場合>

質問項目の選択と回答を登録する必要があります。

質問項目の編集は、管理者ポータルの[マルチファクター認証]から設定可能です。

6. パスワード/アカウント有効期限の通知

パスワード/アカウントの有効期限が近いユーザーに対して、自動的に通知を送信する設定ができます。

本機能を利用することで、ユーザーに対して、パスワード/アカウントの有効満了前に、パスワード/アカウント変更などを促すことができます。これにより、業務への影響を最小限にとどめることが可能です。

<操作手順>

1. [設定]タブ → [セルフサービス] → [パスワードの期限切れに関する通知]をクリックします
2. [新規通知の追加]をクリックします
3. 通知対象となるドメイン/OU/グループに加えて、必要な項目（通知タイプや通知頻度など）をすべて設定します
4. [保存]をクリックします

図 30　パスワード期限の通知

メモ：パスワード/アカウントの有効期限切れが迫っていることをユーザーに複数回通知する場合は、指定した頻度で通知を送ることができます。通知タイミングを指定するには、「通知頻度」の項目で[特定の日]を選択します。

メモ：パスワード期限切れのユーザーに対して通知を行う場合は、[詳細設定]より設定できます。

7. パスワードポリシーの強化

本章では、パスワードポリシーの強化機能について紹介します。本機能を利用することで脆弱なパスワードをドメインから排除し、よりセキュアなパスワード管理を実現できます。

<操作手順>

1. [設定]タブ → [セルフサービス] → [パスワードポリシーの強化] → [パスワードポリシーの強度を上げる]を選択します
2. 要件にあったオプションを選択し、[保存]をクリックします

<パスワードポリシーの強化オプション>

- パスワードの最小文字数
- パスワードの最大文字数
- 含まなければならない特殊文字の数
- 含めなければならない数字の数
- 含めなければならない大文字の数
- 含めなければならない小文字の数
- パスワードの先頭を指定の文字（大文字、小文字、特殊文字、数字）にする
- パスワードの最後に数字を使用することを禁止する
- 少なくとも 1 つ Unicode の文字を含まなければならない
- 回文をパスワードとして使用するのを禁止する
- 同じ文字を n 回以上繰り返し使用することを禁止する
- ユーザー名に含まれる、連続した n 文字の使用を禁止する
- 古いパスワードから連続した n 文字の使用を禁止する
- 単語リストにある文字の使用を禁止する
- 指定した文字の組み合わせを禁止する
- 指定した回数の過去のパスワードの使用を制限する
- 以下の最短パスワード長を満たす場合、パスワードの複雑さの条件を無効にする

メモ：[単語リストにある文字の使用を禁止する]オプションでは、既存の単語リストへの追加または任意の単語リストを上書き指定することも可能です。

メモ：[指定した回数の過去のパスワードの使用を制限する]オプションを有効化した場合は、ユーザーのパスワードが ADSelfService Plus のデータベースに SHA-512 アルゴリズムを使用して格納されます。

メモ：GPO および ADSelfService Plus のパスワードポリシーを同じレベルにする必要があります。
（例　パスワードの最小文字数）

8. シングルサインオンについて

本章では、シングルサインオンの設定方法を Cybozu Office の設定を例として解説します。シングルサインオン同期には両製品での設定が必要になります。

<ADSelfService Plus 側>

1. [設定]タブ → [セルフサービス] → [パスワードシンクロナイザ]をクリックします
2. シングルサインオンを設定するサービスを選択します
3. モジュール/ドメイン名/ SP 識別子 （独自ドメイン）/表示名などを入力し保存をクリックします

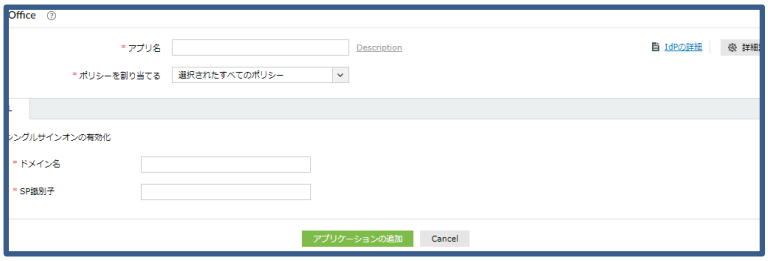


図 31 シングルサインオン

<Cybozu Office 側>

シングルサインオンするユーザー名は ADSelfService Plus 内のユーザー名とサービス側のユーザー名を紐付ける必要があります。

1. Cybozu Office に管理者権限でログインします
   ・左側に並んでいる[cybozu.com 共通管理]ボタンをクリックします
   ・左にあるシステム管理＞セキュリティ＞ログインをクリックします
   ・「ログインのセキュリティ設定」画面の下部に「SAML 認証」の項目があるので[SAML 認証を有効にする]にチェックを入れます
2. ADSelfService Plus、パスワード同期/シングルサインオンの Cybozu 設定画面の右上にある [SSO 証明書をダウンロード]をクリックします

3. 「SSO/SAML 詳細」中の項目を次の項目に入力します

・「Identity Provider の SSO エンドポイント URL（HTTP-Redirect）」に「ログイン URL」の項目を入力し、「cybozu.com からのログアウト後に遷移する URL」に「ログアウト URL」の項目を入力します

図 32 SSO/SAML 詳細入力画面

4. [SSO 証明書をダウンロード]をクリックし、SSO 証明書をダウンロードします

・Cybozu 画面の「Identity Provider が署名に使用する公開鍵の証明書」の「参照」をクリックし先ほどダウンロードした証明書をアップロードします

5. 保存をクリックします

※こちらからログインする時は ADSelfService Plus を経由するため Cybozu Office を必ず起動してください。

9. ディレクトリーセルフサービス

本章では、ユーザーがポータル上で利用できるセルフアップデート/ユーザー検索/グループ追加の設定方法を紹介します。

<セルフアップデート操作手順>

1. [設定]タブ → [セルフサービス] → [ポリシー設定]を選択します
2. ポリシーの編集アイコン（鉛筆マーク）をクリックし、編集画面で[セルフアップデート]にチェックを入れます。
3. [セルフアップデートのレイアウト]をクリックし、ドロップダウンメニューから任意のレイアウトを選択します
4. [ポリシーを保存]をクリックします

図 33 セルフアップデート

<セルフアップデートのレイアウト変更手順>

セルフアップデートのレイアウトのカスタマイズや、ユーザーに許可する指定が可能です。

1. [設定]タブ → [セルフサービス] → [ディレクトリーセルフサービス] → [セルフアップデートのレイアウト]を選択します
2. [新規レイアウトの作成]をクリックする、または、リストにあるレイアウトの編集アイコン（鉛筆マーク）をクリックします
3. レイアウトをカスタマイズするには、各属性をドラッグ＆ドロップします

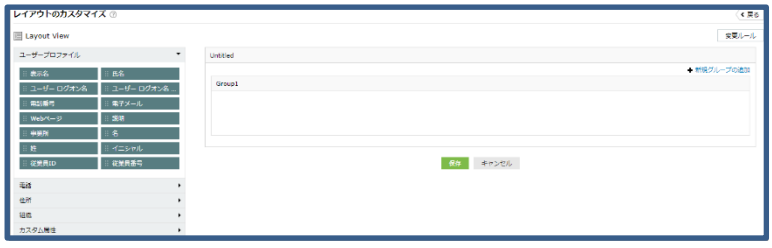


図 34 レイアウトのカスタマイズ

メモ：属性の編集アイコンからフィールドのフォーマットや必須項目などの設定を行うことが可能です。

メモ：デフォルトの属性とは別に、独自のカスタム属性を作成できます。「属性のリスト」の右側にある
ドロップダウンメニューから「カスタム属性」を選択し、必要な情報を入力します。

<ユーザー検索の有効化>

1. [設定]タブ → [セルフサービス] → [ディレクトリーセルフサービス] → [従業員の検索]を選択します
2. [ユーザー検索を有効にする]にチェックを入れ、ドメインを選択します
3. オブジェクトの種類（ユーザー、連絡先、グループ）ごとにユーザーが表示できる属性を選択します

<組織情報の有効化>

1. [設定]タブ → [セルフサービス] → [ディレクトリーセルフサービス] → [従業員の検索]を選択します
2. [詳細説明]をクリックします
3. [組織情報の表示を有効にする]にチェックを入れ、[保存]をクリックします。

図 35 組織情報の表示例

10. セキュリティセンター

すべてのアプリケーションにとってセキュリティ管理は重要ですが、なかでもユーザーのパスワードに関するセキュリティの確保は特に重要です。ADSelfService Plus は、組織の内外からの攻撃に対応するための強固なセキュリティ構成基準を用意しています。ADSelfService Plus のさまざまなセキュリティ機能は、セキュリティセンターに集約され、アクセス性と管理の容易さを確保しています。セキュリティセンターの各機能にアクセスするには、[設定]タブ→[セキュリティセンター]を選択します。セキュリティセンターでは、セキュリティに関する以下の設定が可能です:

- パスワードの強化
- セキュリティ質問＆回答の強度
- ハッキング対策システム

11. ADSelfService Plus の一般設定

本章では製品全体にかかわる設定をご紹介します。

11-1 カスタマイズ

ADSelfService Plus をカスタマイズし、組織の環境に合わせた設定や表示に変更することができます。

<操作手順>

1. [管理]タブ → [カスタマイズ]を選択します

ログオン設定

下記のような製品にログオンする際のカスタマイズ設定が可能です。

- 管理者画面への IP アドレス制限
- キャプチャ（文字認識）の設定
- ログイン画面上のドメインリスト設定
- 製品への SSO 設定

表示設定

下記の製品画面の表示カスタマイズが可能です:

- ロゴ
- テーマカラー
- フォントの種類
- フォントサイズ
- ブラウザータイトル
- ブラウザータイトルの画像
- パスワードポリシーメッセージ

メモ：パスワードポリシーは、パスワードのリセット/アカウントのロック解除を行うページに表示されるテキストです。
ユーザーに対して、より強力なパスワード設定を強制することができます。
ユーザーは、表示されているすべてのパスワードポリシーを満たすパスワードのみ、設定可能です。

パーソナライズ

ADSelfService Plus のデフォルト管理者のパスワード変更、言語設定、日付形式などを変更することができます。

ADSelfService Plus は 21 ヶ国語に対応しており、パーソナライズページから言語を変更することができます。

1. [管理]タブ　→　[カスタマイズ]　→　[パーソナライズ]を選択します

2.ドロップダウンメニューから、使用する言語を選択します

※「ブラウザーデフォルト」を選択しますと、使用しているブラウザーの言語設定に合わせた言語が表示されます

11-2 システムユーティリティ

ダッシュボードの更新設定

Active Directory と ADSelfService Plus の同期、ダッシュボードの更新間隔を設定可能です。

スケジュールバックアップ

バンドルしている PostgreSQL データベースのバックアップを自動的に実行するためのスケジュールを設定可能です。

ドメインコントローラー設定

セルフサービスで更新するドメインコントローラーを選択可能です。

※本設定での OU は、コンピューターが所属する OU ではなく、ユーザーが所属する OU です。

11-3 製品設定

接続

ポートの設定、セッション有効期限などを設定可能です。

メモ：[アクセス URL]は、ユーザーが製品に簡単にアクセスできるようにする URL です。

マシン名をユーザーに公開したくない場合などにも利用できます。

また設定された URL は、GINA/CP ログオンエージェントのアクセス URL、

メール通知機能におけるメール本文内のアクセス URL として使用されます。

サーバー設定

メールサーバー、SMS プロバイダー、プロキシの設定が可能です。

11-4 使用されていないユーザーの制限

Active Directory の有効期限切れユーザー、無効化されたユーザー、削除されたユーザーなど、ADSelfService Plus を利用しなくなったユーザーのアクセスを制限し、ライセンスの消費を抑制することができます。

<操作手順>

1. [管理]タブ → [ライセンス管理] → [制限ユーザー]を選択します
2. ドメインを選択後[OU の追加]をクリックします
3. 手動で制限ユーザーを設定する、または自動で制限するスケジュールを作成することができます

11-5 スーパー管理者とオペレーター

他のユーザーをオペレーターとして設定することにより、製品の管理タスクの一部またはすべてを委任できます。
ユーザーをオペレーターとして追加する方法は以下の通りです。

1. [設定]タブ → [管理ツール] → [オペレーター]を選択します
2. [オペレーターの新規追加]をクリックします
3. [ドメインの選択]にて、ドメインを選択します
4. [オペレーターの選択]より割り当てるユーザーを選択します
5. [役割の選択]にて、割り当てる役割を選択します

オペレーターの種類は次の 2 種類があります。

- スーパー管理者（Super Admin）: ADSelfService Plus のほぼすべての管理操作が可能です
- オペレーター（Operator）: 監査およびレポートの設定が可能です

> メモ：スーパー管理者（Super Admin）でもドメインの追加はできません。
> ドメインの追加を行う場合は、デフォルトの admin アカウントを使用してください。

12. モバイルアプリ

ADSelfService Plus は iOS、Android、Blackberry 対応のモバイルアプリケーションを提供しています。

このアプリケーションでは、次の機能を利用できます。

- パスワードのリセット
- アカウントロックの解除
- パスワードの変更
- 本人確認（プッシュ通知/指紋認証/QR コード認証/TOTP 認証）
- 登録

図 36 モバイルアプリ画面

付録

関連ドキュメント

次のリストは、ADSelfService Plus の使用を支援するドキュメントと資料の一覧（英語）です。

ドキュメント名	説明
管理者ガイド	ADSelfService Plus のヘルプドキュメント
ユーザーガイド	エンドユーザー向けのヘルプドキュメント
ナレッジベース	ADSelfService Plus に関するよくあるご質問や、トラブルシューティング、製品仕様などを公開しています。
クライアントソフトウェアのインストール（GPO / Web ポータル）	ユーザーのワークステーションへの ADSelfService Plus エージェント（クライアントソフトウェア）の導入方法（英語ドキュメント）
ADSelfService Plus をインターネットで安全に利用するためのガイド	ADSelfService Plus を以下の環境で利用する場合の構築手順を記載したガイドです。 ・DMZ に構築する場合 ・リバースプロキシを利用する場合
ADSelfService Plus を利用するために必要な Active Directory の権限について	ADSelfService Plus のサービスごとに必要な Active Directory 権限および手動での権限の付与方法のガイドです。
セキュリティ関連	セキュリティ関連のホワイトペーパーの資料を提供しています。
その他のドキュメント	リリースノートなど各種ドキュメントのリンクを提供しています。

製品のお問い合わせ先

ADSelfService Plus に関するご質問、ご購入の相談は下記までお問い合わせください。

製品提供元

ゾーホージャパン株式会社

神奈川県横浜市西区みなとみらい 3-6-1 みなとみらいセンタービル 13 階

Tel: 045-319-4612（ManageEngine 営業担当）

E-mail: jp-mesales@zohocorp.com

Web: https://www.manageengine.jp/