

2024

Password Management

Privileged Account Management
& Remote Access Management
& Privileged Session Management



スタートアップガイド

ManageEngine
Password Manager Pro

2024 年発行

■著作権について

本ガイドの著作権は、ゾーホージャパン株式会社が所有しています。

■注意事項

本ガイドの内容は、改良のため、予告なく変更することがあります。

ゾーホージャパン株式会社は本ガイドに関しての一切の責任を負いかねます。当社はこのガイドを使用することにより引き起こされた偶発的もしくは間接的な損害についても責任を負いかねます。

■商標一覧

Oracle と Java は、Oracle Corporation 及びその子会社、関連会社の米国及びその他の国における登録商標です。文中の社名、商品名等は各社の商標または登録商標である場合があります。

Windows は、米国およびその他の国における米国 Microsoft Corp. の登録商標です。

ManageEngine は、ZOHO Corporation Pvt.Ltd 社の登録商標です。

なお、本ガイドでは、(R)、TM 表記を省略しています。

目次

1 はじめに.....	5
1 - 1 ManageEngine Password Manager Pro について.....	5
1 - 2 本ガイドについて	5
1 - 3 本書の目的と対象読者.....	5
1 - 4 Password Manager Pro の動作環境	6
ハードウェア（最小構成）	6
サイジング	6
ソフトウェア	6
Web クライアント.....	6
データベース.....	6
2 Password Manager Pro のインストール・アンインストール.....	7
2 - 1 Password Manager Pro のダウンロード.....	7
2 - 2 Password Manager Pro のインストール手順.....	7
Windows	7
Linux.....	10
2 - 3 アンインストール	11
Windows	11
Linux.....	12
3 Password Manager Pro の起動と停止.....	13
3 - 1 サーバーの起動	13
Windows	13
Linux.....	13
3 - 2 サービスの停止.....	14
Windows	14
Linux.....	14
4 Password Manager Pro の初回ログイン時の設定.....	15
4 - 1 Password Manager Pro へのアクセス.....	15
4 - 2 メールサーバー設定	17
4 - 2 ライセンスの適用.....	17
4 - 3 デフォルトの admin, guest のパスワード変更	18
4 - 4 PMP 暗号化鍵の保管.....	19
4 - 5 SSL/TLS 証明書のインポート	20
5 Password Manager Pro ユーザーの追加.....	21

5 - 1 手動で追加.....	21
5 - 2 API ユーザーを追加	22
5 - 3 ファイルからインポート	23
5 - 3 Active Directory / Azure AD / LDAP からインポート	24
5 - 4 ユーザーグループの作成.....	26
6 パスワードポリシーの設定	28
6 - 1 パスワードポリシーの定義項目	29
6 - 2 パスワードポリシーの設定手順	30
7 リソース・アカウントの追加	32
7 - 1 手動で追加.....	32
7 - 2 リソースのインポート.....	34
7 - 3 Keepass からのインポート.....	36
7 - 4 リソースディスカバリー (Windows)	36
7 - 5 リソースディスカバリー (Linux)	38
7 - 6 リソースディスカバリー (ネットワーク機器)	39
7 - 7 リソースディスカバリー (VMware)	41
8 アクセス制御設定	42
8 - 1 アクセス制御設定項目	42
8 - 2 リソース単位でのアクセス制御設定	45
8 - 3 アカウント単位でのアクセス制御設定	46
9 リソース/リソースグループの共有	49
9 - 1 リソースを共有	49
9 - 2 リソースグループを共有	51
9 - 3 アカウントを共有	53
10 申請・承認のワークフローの流れ	55
10 - 1 申請者からの申請	55
10 - 2 承認者への通知	57
10 - 3 承認者の承認/拒否	57
10 - 4 申請者への承認/拒否通知/チェックアウト	59

1 0 - 5 パスワードの借り出し	60
1 0 - 6 パスワードの返却	61
1 1 記録済みセッションの管理	63
1 1 - 1 セッションレコーディング設定	64
1 1 - 2 記録済みセッションの再生方法	65
1 2 各タブの機能概要	66
1 2 - 1 ダッシュボードタブ	66
1 2 - 2 リソースタブ	67
1 2 - 3 グループタブ	67
1 2 - 4 接続タブ	68
1 2 - 5 SSH 鍵タブ	69
1 2 - 6 証明書タブ	69
1 2 - 7 ユーザータブ	69
1 2 - 8 管理タブ	70
1 2 - 9 監査タブ	71
1 2 - 1 0 レポートタブ	72
1 2 - 1 1 パーソナルタブ	72
1 2 - 1 2 権限毎に表示可能なタブ	72
1 3 製品のお問い合わせ先	73

1 はじめに

1 - 1 ManageEngine Password Manager Pro について

ManageEngine Password Manager Pro（マネージエンジン パスワードマネージャー プロ）は、「必要な時だけ必要な人だけが使える特権 ID のパスワード」の申請/承認/貸出/返却のワークフロー自動化、オペレーター操作画面録画、パスワード定期変更等を圧倒的な低価格で手軽に実現するソフトウェアです。

Windows、Linux をはじめ、データベースやネットワーク機器、Web アカウント、クラウドアカウントなどの特権 ID のパスワード管理をエージェントレスで実施できます。^(注 1)

（注 1）：Linux サーバーにインストールした場合、Windows サーバーのパスワード変更にはエージェントが必要です。

1 - 2 本ガイドについて

本ガイドでは Password Manager Pro（PMP）のインストール方法から初期設定の内容について説明しています。

また本ガイドはビルド 12410 を基に作成しています。

1 - 3 本書の目的と対象読者

本書は、Password Manager Pro を購入された方やこれから評価版を試用される方が Password Manager Pro の概要を手早く理解し、ご利用を始めるまでの学習時間を短縮し、製品に慣れるための手がかりとなることを目的としています。

Password Manager Pro 製品のセットアップから実際にパスワード管理を開始するまでの流れ、Password Manager Pro の基礎的な利用方法についてステップバイステップでわかりやすく説明しています。

本書でカバーしている範囲は Password Manager Pro の基本的な操作方法です。Password Manager Pro には暗号化 HTML ファイルのエクスポート機能、IP アドレス制御機能、SSH コマンドセット機能、高可用性機能やリードオンリーサーバー機能など、本書では扱っていない数多くの機能が用意されています。

1 - 4 Password Manager Pro の動作環境

Password Manager Pro 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。 ^(注 1)

ハードウェア（最小構成）

CPU	メモリー	ストレージ
Dual Core/Core2Duo	4.0 GB 以上	10.0 GB 以上

サイジング

リソース数/ユーザー数	CPU	メモリー	ストレージ
小規模 1000 リソース/500 ユーザー以下	DualCore/Core2Duo	4.0 GB	10.0 GB 以上
中規模 5000 リソース/1000 ユーザー以下	Quad Core 以上	8.0 GB	20.0 GB 以上
大規模 5000 リソース/1000 ユーザー以上	Octa Core 以上	16.0 GB	30.0 GB 以上

ソフトウェア

サーバーOS	Windows Server 2016 / 2019 / 2022 Ubuntu 9.x 以降、CentOS 4.4 以降、Red Hat Linux 9.0、Red Hat Enterprise Linux 7.x,6.x,5.x
パスワード変更	Microsoft .NET Framework 4.5.2 以降 Visual Studio 2015 C ++ 再配布可能パッケージ（2015 以降であれば可） ^(注 2)

Web クライアント

Web ブラウザー	Mozilla Firefox、Microsoft Edge、Google Chrome 解像度 1280 x 800 ピクセル以上
-----------	---

データベース

データベース	PostgreSQL（製品バンドル）、 Microsoft SQL Server 2014 / 2016 / 2017 / 2019 (注 3)
--------	--

（注1）： 詳細なシステム要件、管理対象のリソースについては [Password Manager Pro 動作環境](#)をご覧ください。

（注 2）： パスワード変更を実行するため必要となるモジュールです。

（注 3）： Windows Server 2016 以降にインストールされていることが必要です。

2 Password Manager Pro のインストール・アンインストール

Password Manager Pro のインストーラー入手からインストールまでの流れを説明します。

2 - 1 Password Manager Pro のダウンロード

Web ブラウザーで次の URL を開き、ご利用の環境に適したインストーラーをダウンロードします。

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

2 - 2 Password Manager Pro のインストール手順

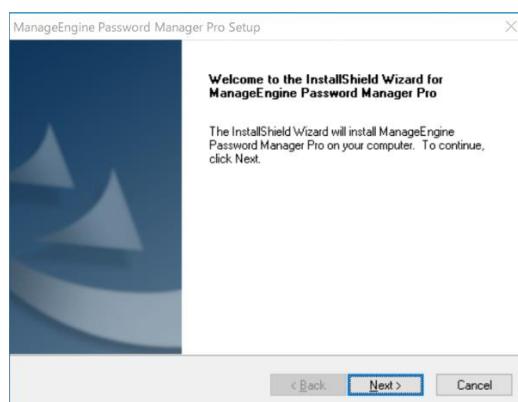
Windows

1. インストールするマシンのローカル管理者の権限を持つユーザーで Windows にログオンします。
2. ダウンロードしたインストーラーをダブルクリックして起動します。



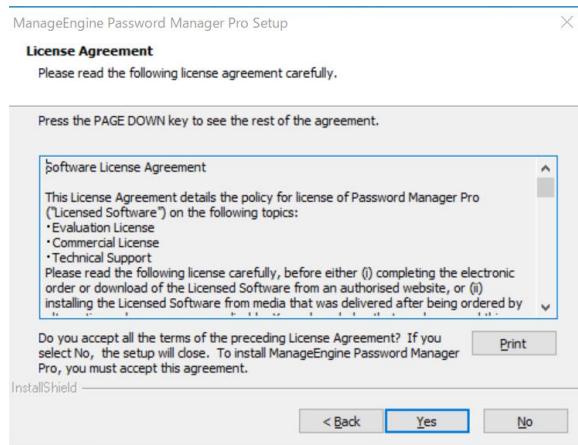
インストーラーの起動

3. インストール画面が表示されるので「Next」をクリックします。



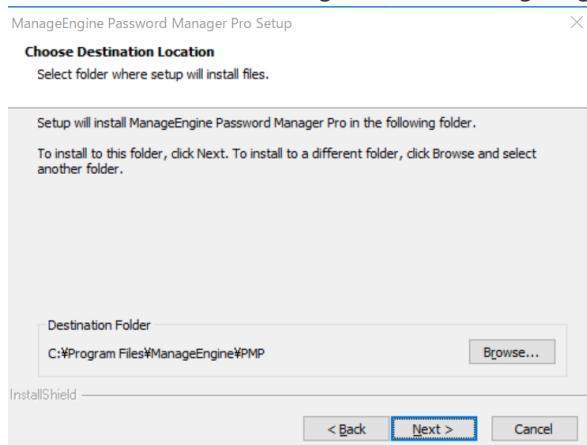
インストール画面

4. 使用許諾条項をお読みいただき、承諾後に「Yes」をクリックします。



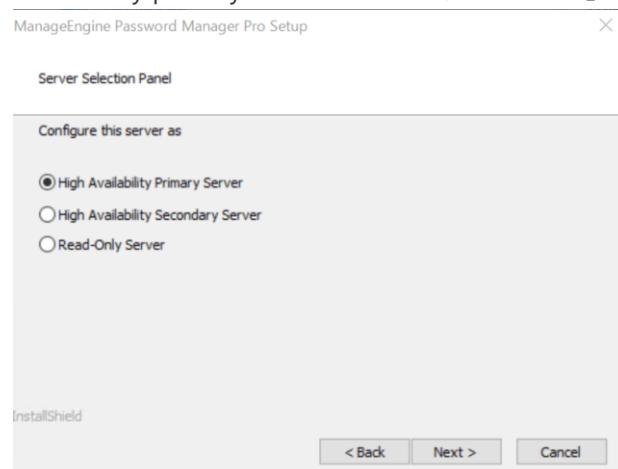
使用許諾条項

5. インストールフォルダーを選択します。デフォルトは 'C:\Program Files\ManageEngine\PMP' です。



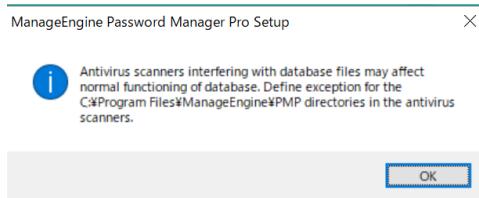
インストールフォルダーの選択

6. HA 構成（高可用性）を実装する場合にはプライマリーサーバー、セカンダリーサーバーをこちらで指定します。HA 構成未構成の場合は'High availability primary server'を選択した状態で「Next」をクリックします。



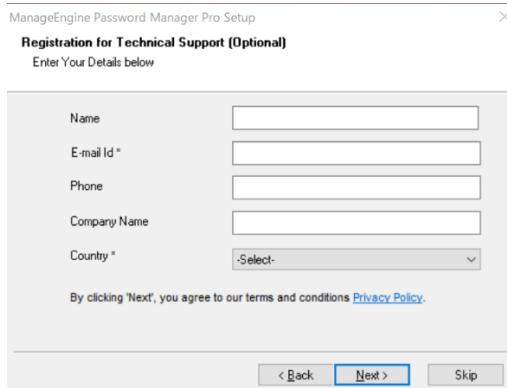
HA 構成の選択

7. インストールディレクトリをアンチウイルスソフトのスキャン対象から除外する設定を推奨するメッセージが表示されます。
「OK」をクリックして続行します。



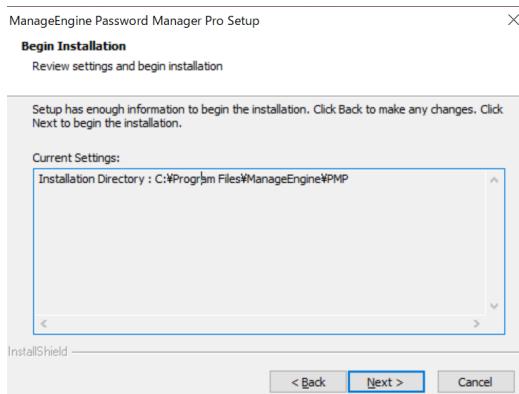
アンチウイルスソフトのスキャン対象からの除外

8. お客様情報を入力します。E-mail と Country は必須となります。それ以外の項目は任意です。



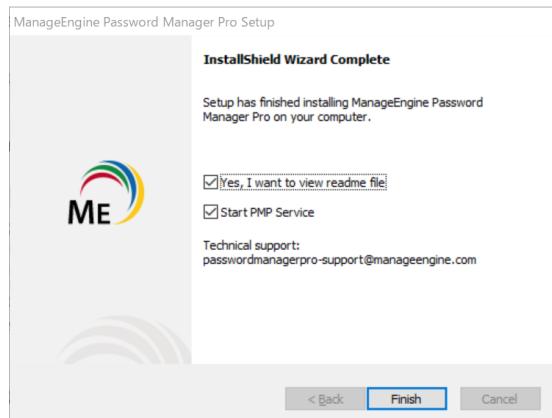
お客様情報の入力

9. Password Manager Pro をインストールするため、「Next」をクリックします。



内容の確認

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、「Finish」ボタンをクリックします。



インストール完了画面

Linux

1. ダウンロードしたインストーラーに実行権限を付与します。（インストールは root 権限以外のユーザーで行ってください。）

```
chmod 777 ManageEngine_PMP_64bit.bin
```

2. 次のコマンドを実行し、インストーラーを起動します。

```
./ManageEngine_PMP_64bit.bin -i console
```

3. Introduction をお読みいただいた上で、PRESS <ENTER> TO CONTINUE にて Enter を押下します。

```
PRESS <ENTER> TO CONTINUE:
```

4. License Agreement を適宜 PRESS <ENTER> TO CONTINUE にて Enter を押下しつつ読み進める。最後に以下のメッセージが表示されるため、「Y」を入力します。

```
DO YOU ACCEPT THE TERMS OF THIS LICENSE AGREEMENT? (Y?N): Y
```

5. Choose Installation Folder では PMP フォルダーのインストールディレクトリを決定します。デフォルトのパスで問題ない場合には Enter を押下し、変更する場合にはインストール先の絶対パスを指定します。

ENTER AN ABSOLUTE PATH, OR PRESS <ENTER> TO
ACCEPT THE DEFAULT:

6. Server Configuration では HA 構成時のサーバー種別を聞かれます。プライマリーサーバーの場合は 1 または Enter、セカンダリーサーバーの場合は 2 を入力してください。単体でのご利用の場合は 1 または Enter を入力してください。

ENTER THE NUMBER FOR YOUR CHOICE, OR PRESS
<ENTER> TO ACCEPT THE DEFAULT:: 1

7. Pre-Installation Summary ではインストールの確認がなされます。問題ない場合には Enter を押下してください。

PRESS <ENTER> TO CONTINUE:

8. Ready To Install ではインストールを実行します。Enter を押下してください。

PRESS <ENTER> TO INSTALL:

9. Installation Complete と表示されていればインストールは無事終了しています。Enter を押下してインストールを終了してください。

PRESS <ENTER> TO EXIT THE INSTALLER:

2 - 3 アンインストール

Windows

1. コントロールパネル → プログラムと機能 → プログラムのアンインストール を開きます。
2. ManageEngine Password Manager Pro を選択し、アンインストール をクリックします。

プログラムのアンインストールまたは変更

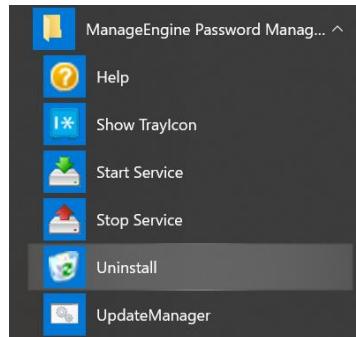
プログラムをアンインストールするには、一覧からプログラムを選択して [アンインストール]、[変更]、または [修復] をクリックします。

名前	発行元	インストール日	サイズ	バージョン
<input checked="" type="checkbox"/> ManageEngine Password Manager Pro	ZOHO Corp.	2020/06/19		1.00.000

Password Manager Pro のアンインストール

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 → ManageEngine Password Manager Pro Server → Uninstall からアンインストールすることもできます。Setup.exe が見つからないと表示される場合は、ダウンロードしたインストーラー ManageEngine_PMP_64bit.exe を指定します。



Password Manager Pro のアンインストール

Linux

1. <PMP>\$/bin へ移動します。
2. 次のコマンドを実行し、Password Manager Pro のサービスをアンインストールします。

```
sh pmp.sh remove
```

3. PMP フォルダーを手動で削除します。

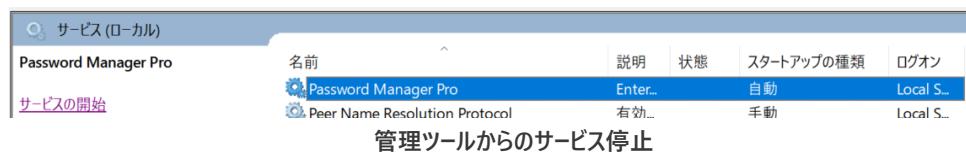
3 Password Manager Pro の起動と停止

Password Manager Pro の起動方法を説明します。

3 - 1 サーバーの起動

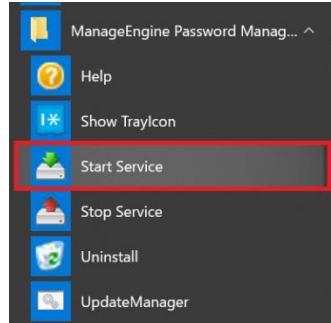
Windows

1. コントロールパネル → 管理ツール → サービスを開き、[Password Manager Pro]をクリックします。



2. [サービスの開始]をクリックします。

メモ：スタートメニュー → ManageEngine Password Manager Pro → Start Service からサービスを開始することもできます。



スタートメニューからのサービス開始

3. Password Manager Pro サービスが起動します。

メモ：今後は Windows の起動時に Password Manager Pro サービスも自動的に起動します。

Linux

以下のコマンドを実行し、サービスを起動させます。

```
/etc/rc.d/init.d/pmp-service start
```

3 - 2 サービスの停止

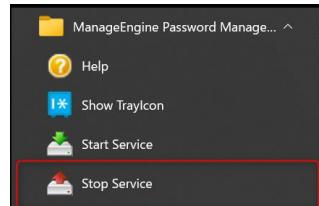
Windows

1. コントロールパネル → 管理ツール → サービスを開き、[Password Manager Pro]をクリックします。



2. [サービスの停止]をクリックします。

メモ：スタートメニュー → ManageEngine Password Manager Pro → Stop Service からサービスを停止することもできます。



スタートメニューからのサービス停止

Linux

以下のコマンドを実行し、サービスを停止させます。

```
/etc/rc.d/init.d/pmp-service stop
```

4 Password Manager Pro の初回ログイン時の設定

Password Manager Pro に初めてログインした後に必須となる設定について説明します。

メモ：管理者としてログインした後に「ダッシュボード」タブから必要となる作業が記載されています。



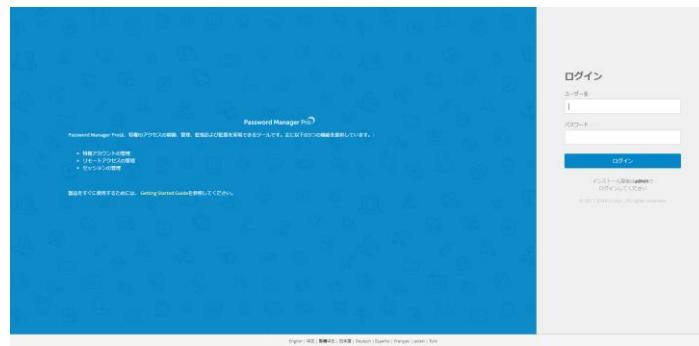
初期セットアップ項目

4-1 Password Manager Pro へのアクセス

- サービスを起動すると自動的に Web ブラウザーが起動し、ログイン画面が起動します。
- (Web ブラウザーが起動しない場合) Web ブラウザーを起動しアドレスバーに [https://\[サーバー名\]:\[ポート番号\]](https://[サーバー名]:[ポート番号]) を入力し、移動します。
例：<https://PMP-server:7272> (デフォルトのポート番号は 7272 です)

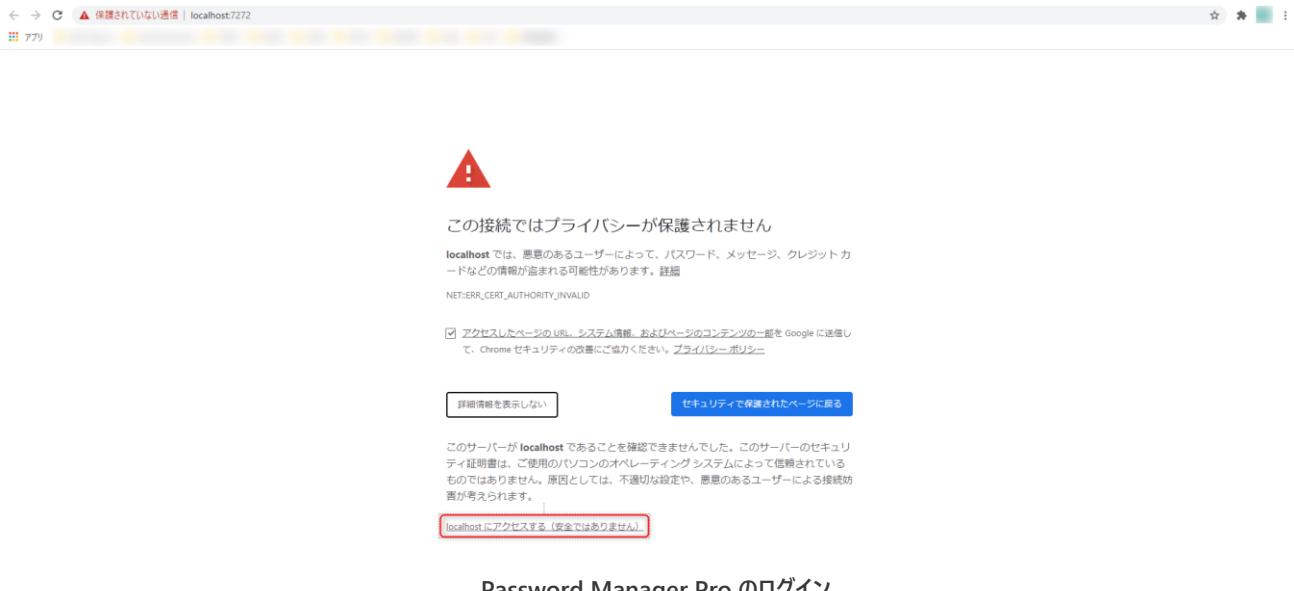
メモ：上記の方法でリモートマシン上の Password Manager Pro にアクセスできないときは、Password Manager Pro がインストールされているマシン上の Web ブラウザーから <https://localhost:7272> にアクセスできるかご確認ください。

- 管理者として Password Manager Pro にログインするには、初期ユーザー名・パスワードとして「admin」と入力して [ログイン]をクリックします。Google Chrome で開く場合には、[サーバー名]にアクセスする（安全ではありません）をクリックしてください。



ログイン画面

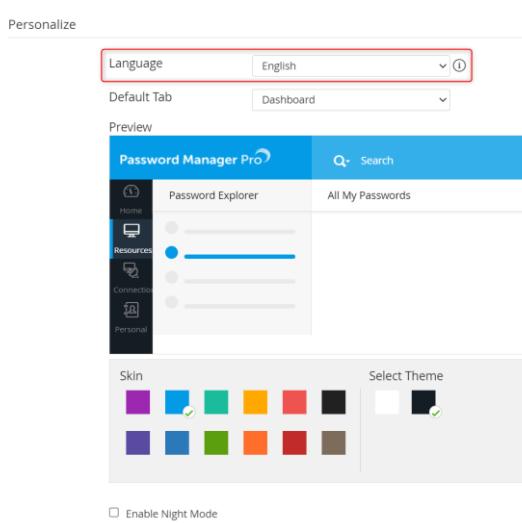
4. Password Manager Pro に対して証明書が未適用なためにブラウザーから警告が発生します。自己署名証明書を受け入れてコンソールにアクセスします。



Password Manager Pro のログイン

メモ：Password Manager Pro では HSTS が実装されており、https 接続を強制します。

メモ：インストール後の初回ログイン時、デフォルト言語は英語設定となっております。ログイン後、画面右上の人型パネル → Personalize タブ → Language から変更が可能です。



言語設定

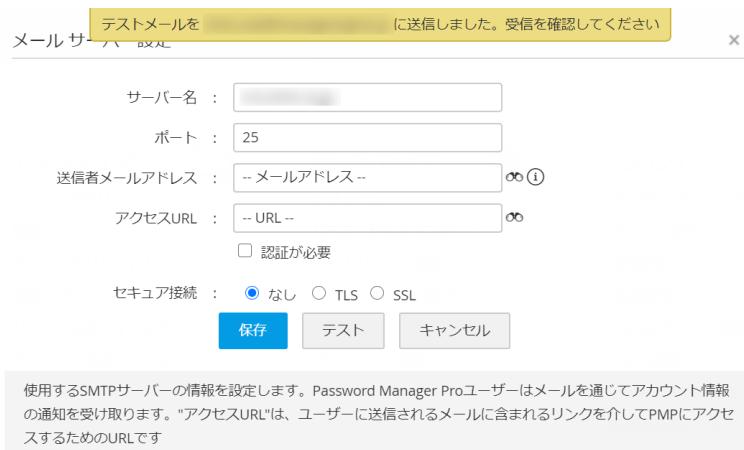
4 - 2 メールサーバー設定

1. 管理タブ → セットアップ欄 → メールサーバー設定 をクリックします。
2. サーバー名、ポート、送信者メールアドレスを指定します。必要に応じてアクセス URL、認証の有無、セキュア接続も指定します。



メールサーバー設定

3. 「テスト」をクリックし、テストメールが正しく送信されるか確認します。正しく送信された場合にはポップメッセージ「テストメールを×××@○○に送信しました。受信を確認してください」が表示されます。



テストメールの送信

4. 「保存」をクリックします。

4 - 2 ライセンスの適用

1. 管理者ユーザーで Password Manager Pro にログインします。
2. 画面右上の人型アイコンをクリックします。

3. 「ライセンス」をクリックします。

4. 受領しているライセンスファイルのパスを指定して「アップグレード」をクリックします。



ライセンス状況

5. ライセンスの適用に成功した旨のポップアップウィンドウが表示されていることを確認します。



ライセンス適用に成功

4 - 3 デフォルトの admin, guest のパスワード変更

Password Manager Pro ではセキュリティ上の理由からライセンス適用後にデフォルトユーザー (admin, guest) のパスワード変更を強制します。デフォルトのパスワードポリシーは Strong となります。



ログインパスワードの変更 (admin)



ログインパスワードの変更 (guest)

4 - 4 PMP 暗号化鍵の保管

Password Manager Pro はデータベース、その他機密情報に対して AES-256 による暗号化を施しています。その暗号化鍵 (pmp_key.key) は<PMP>¥conf フォルダーに保存されています。ただし、セキュリティ上の理由からライセンスの適用後、保管場所の設定を変更するように強制します。



PMP 暗号化鍵の保存先パスの変更

以下、pmp_key.key ファイルの保存先を変更する手順となります。

1. Password Manager Pro サーバーにログインします。

2. <PMP>¥conf 配下にある pmp_key.key ファイルを PMP フォルダー外に保存します。

メモ：PMP サーバーから PMP のサービスアカウントで pmp_key.key ファイルにアクセスできる状況であれば、外部サーバーでも保管可能です。ただし、サービス起動毎にデータベースのアクセスのために pmp_key.key ファイルを使用します。通信が取れない状況では PMP が起動できませんのでご注意ください。

メモ：保管場所のフォルダ名には日本語等の 2 バイト文字を含めないでください。

メモ：PMP インストールフォルダーと並列の場所に任意フォルダーを作成し、pmp_key.key ファイルを保管される場合は、該当のフォルダーに「PMP」（大文字小文字共に）から始まるフォルダ名を指定しないようにしてください。

3. UI 上で保存先パスを UNC 形式で変更の上、以下のチェックボックスをクリックします。

私は、PMP のマスター暗号化鍵を保護する必要と方法について理解しました

4. 「ファイルの場所を変更」をクリックします。

5. 「ホームに移動」をクリックします。

鍵ファイルの場所を設定しました

今後、PMPは以下のフォルダから鍵を読み取ります
C:\Program Files\ManageEngine
上記の場所にpmp_key.keyファイルを配置してください。

[ホームに移動](#)

pmp_key.key ファイルの保存先

4 - 5 SSL/TLS 証明書のインポート

CA 機関から取得された正式な SSL 証明書を本製品に組み込んで利用いただくことも可能です。

以下の手順にて UI 上でインポートできます。

1. 「管理」タブ → 「設定」欄 → サーバー設定へ移動します。

2. 鍵ストアの種別、ファイル名、パスワードを設定の上で保存をクリックします。

サーバー設定

サーバー設定 自動ログオン

独自のSSL証明書を使用する場合、ここからインストールを行います。また、既定のPMPサーバーポートを変更することもできます

鍵ストアの種別 :	JKS
鍵ストアのファイル名 :	<input type="text"/> 参照
鍵ストアのパスワード :	<input type="text"/>
サーバー ポート :	7272

[保存](#) [キャンセル](#)

設定変更後、PMPを再起動する必要があります。高可用性を設定している場合は、上記の変更をセカンダリ サーバーのWebインターフェースで保存してください

SSL 証明書、ポート番号の設定

5 Password Manager Pro ユーザーの追加

本章では Password Manager Pro ログインするユーザーの追加方法について解説します。

Password Manager Pro ユーザーを Password Manager Pro へ追加する方法は、以下の 4 種類があります。

- 手動で追加
- API ユーザーを追加
- ファイルからインポート
- Active Directory / Azure AD / LDAP からインポート

5 - 1 手動で追加

1. 「ユーザー」タブをクリックします。

2. 「ユーザー追加」から「手動で追加」をクリックします。



3. 「ユーザー追加」のウィンドウが表示された後に、名、姓、ユーザー名、電子メールをそれぞれ入力します。またパスワード生成方式、パスワードポリシーにて作成するユーザーのパスワードが準拠するポリシーを選択します。アクセスレベルから作成するユーザーの役割を選択します。その他の項目に関しても適宜入力します。

ユーザー追加

名 :

姓 :

ユーザー名 :

パスワードポリシー : Strong

電子メール :

アクセスレベル : パスワードユーザー

アクセス範囲 : 所有する/共有されたパスワード

部門 :

場所 :

モバイルアクセスを許可 : 有効化

ブックマーク機能アクセスを許可 : 有効化

ユーザー証明書 :

言語 : 日本語

保存 キャンセル

手動で追加

5-2 API ユーザーを追加

- 「ユーザー」タブをクリックします。
- 「ユーザー追加」から「API ユーザーを追加」をクリックします。



- 「API ユーザーの追加」のウィンドウが表示された後に、ユーザー名、ホスト名、フルネーム、電子メールをそれぞれ入力します。また、追加する API ユーザーの適切なアクセスレベルを選択します。その他の項目に関しても適宜入力します。REST API の横にある [有効化] ボタンをクリックして、REST API を有効にすると、API キーのテキストボックスが表示されます。ここで生成される API キーは、アクセス用の認証トークンです。このキーをコピーし、安全な場所に保管してください。このキーは GUI に一度だけ表示され、紛失した場合はこのウィンドウからキーを再生成する必要があります。

APIユーザーの追加 ⑨

① 現在お使いのライセンスでは、あと 99 名の管理者ユーザーを追加できます。購入

ユーザー名 :	<input type="text"/>	①
ホスト名 :	<input type="text"/>	①
フルネーム :	<input type="text"/>	①
電子メール :	<input type="text"/>	メールサーバー設定
アクセス レベル :	<input type="button" value="REST API"/>	
アクセス範囲 :	<input checked="" type="radio"/> 所有する/共有されたパスワード <input type="radio"/> システム上のすべてのパスワード (こちらを選択するとユーザーはスーパー管理者になります)	
SSH CLUアクセス用の公開鍵 :	<input type="text"/>	参照 ①
XML-RPC APIアクセス用のSSL証明書 :	<input type="text"/>	参照 ①
REST API :	<input checked="" type="radio"/> 有効化 <input type="radio"/> 無効化 <input type="button" value="認証トークンを生成"/> 認証トークン <input type="button" value="生成"/>	
認証トークンの妥当性 :	<input checked="" type="radio"/> 無期限 <input type="radio"/> 使用期限 <input type="text"/>	
部門 :	<input type="text"/>	
場所 :	<input type="text"/>	
このユーザーは、他のユーザーが所有するリソースを追加/編集する: <input type="checkbox"/> ことが許可されています		
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>		

API ユーザーの追加

5-3 ファイルからインポート

ファイル（CSV/TXT/TSV/XLS/XLSX ファイル）から一括でインポートする機能もあります。

4. 「ユーザー」タブをクリックします。

5. 「ユーザー追加」から「ファイルからのインポート」をクリックします。

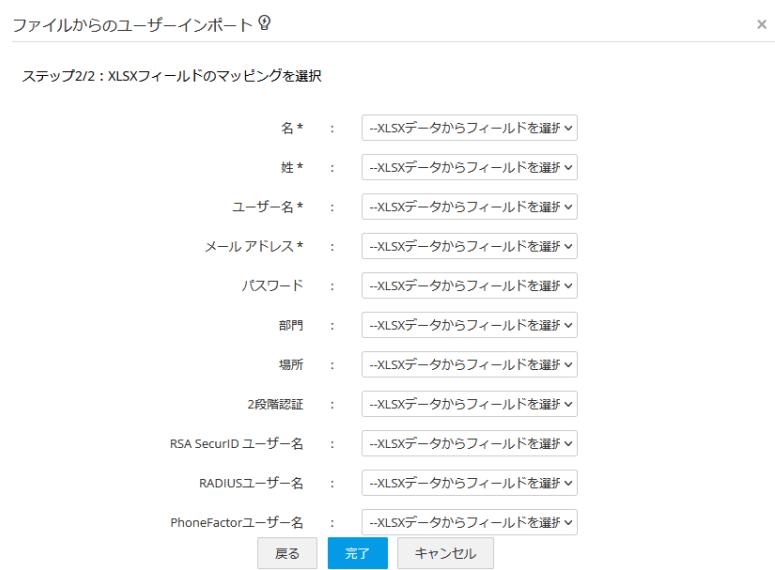


6. ファイルフォーマットを指定し、「参照」からファイルを指定します。



ファイルからのインポート

7. 「ファイルからのユーザーインポート」にて各フィールドと対応する列をそれぞれ指定します。



各フィールド

- 「完了」をクリックします。

メモ：名、姓、ユーザー名に日本語等の2バイト文字は使用できません。英数字をご利用ください。

5 - 3 Active Directory / Azure AD / LDAP からインポート

Active Directory や Azure AD、LDAP 等のディレクトリサービスと連携する機能もあります。本項では Active Directory を利用したユーザーのインポート機能について解説します。

- 「ユーザー」タブをクリックします。



ユーザーの追加画面

- 「ユーザー追加」から「Active Directory からインポート」をクリックします。
- 新規ドメインを「追加」し、プライマリドメインコントローラーの FQDN と管理者権限を有するアカウント情報を入力します。

メモ：ドメインのユーザーオブジェクトに対する参照権限を持っているアカウントを指定する必要があります。

- インポートするユーザー、グループ、OU を指定することも可能です。同期間隔を設定し、「列挙」をクリックしてください。

Active Directoryからインポート

ドメイン名を選択: 新規ドメイン

プライマリドメインコントローラー:

セカンダリドメインコントローラー:

接続モード: SSLなし SSL

資格情報を入力: 手動でユーザー名とパスワードを指定 Password Manager Proに保管されているアカウントを使用

ユーザー名: administrator

パスワード:

インポートするユーザー:

インポートするユーザーグループ:

インポートする組織単位(OU):

[メモ: 複数の名前はカンマ","で区切ります]

同期間隔: 00 日 00 時間 00 分

列举 **保存** **キャンセル**

Active Directory からインポート

5. グループまたは OU を指定して「インポート」をクリックします。

Active Directoryからインポート

グループ 組織単位

グループ: Administrators Users

インポート **キャンセル**

メモ: Active Directoryからインポートするユーザーグループを選択します。PMPユーザーグループの名前は、間連付けられたADドメイン名+ユーザーグループ名で作成されます

グループ/OU 選択画面

6. Active Directory インポート概要からユーザーがインポートされたことを確認します。



インポート結果

5 - 4 ユーザーグループの作成

ユーザーをグループ化することで管理を体系化できます。また Active Directory/Azure AD/LDAP からインポートした OU、グループはユーザーグループからまとめて確認できます。以下ユーザーグループを手動で作成する手順を紹介します。

1. 「ユーザー」タブをクリックします。
2. ユーザーグループをクリックします。

グループ名	説明	ユーザーの関連付け	アクション	レポート
PMP_admins		●	●	
ME-DEVELOP\Domain Users	Users from ME-DEVELOP\Domain U...	●	●	
ME-DEVELOP\Users	Users from ME-DEVELOP\Users of ...	●	●	
ME-DEVELOP\Final Group 1	ユーザー from ME-DEVELOP\Final Gr...	●	●	
ME-DEVELOP\Sub Group 1	ユーザー from ME-DEVELOP\Sub Gr...	●	●	

ユーザーグループ画面

3. 「グループ追加」をクリックします。
4. グループ名と説明を記載して、「保存して続行」をクリックします。

ユーザ グループ追加

x

グループ名:

PMP_auditors

説明:

保存して続行

キャンセル

この手順ではユーザーグループを作成します。グループにユーザーを追加するには、別途  アイコンをクリックして操作を行う必要があります

ユーザーグループ追加

5. グループに追加したいユーザーを選択し、「グループへ追加」をクリックします。

メモ：ユーザーグループではユーザーをまとめて管理できます。「ユーザー」タブ→「ユーザーグループ」→ユーザーグループのアクションアイコン→ユーザー設定にてグループに対して許可されているアクションを確認できます。デフォルトでは以下の設定項目にチェックがついています。

ユーザー設定

x

- 自動ログオン設定済みのパスワードをユーザーが取得を許可 ①
- パスワードのプレーンテキスト表示を無効にしている場合に、ブラウザ拡張機能を介して、URLで設定されたリソースへの自動ログオンを許可する。 ①
- パスワード取得時、ユーザーに理由の入力を強制
- 個人用パスワードの管理を許可する
- 個人用パスワードのエクスポートを許可する
- グループメンバーに条件ベースのリソースグループを'共有管理'することを許可する ①
- パスワード取得時、ユーザーにチケットIDの入力を強制する
- チケットIDが無い場合にパスワード取得を許可
- ユーザーがモバイルのオフラインアクセス用にパスワードをキャッシュすることを許可
- ユーザーに指紋認証によるモバイルアプリログインを許可
- リモートシステムやアプリケーションへの自動ログインをユーザーに許可する
- ブラウザ拡張機能を使用して、Webサイトへの自動入力操作を許可。
- ユーザーにブラウザ拡張を利用したWebサイトに自動ログオンおよびユーザー名とパスワードの自動入力を許可
- ブラウザ拡張機能経由でアカウントの追加を無効

保存

キャンセル

ユーザーグループ追加

6 パスワードポリシーの設定

組織にて独自のパスワードポリシーを設定できます。Password Manager Pro ではデフォルトで以下 4 つのパスワードポリシーを用意しています。

Low

...厳格な制約がほとんどないパスワード

Medium

...厳格な制約の少ないパスワード

Strong

...厳格な制約が伴うパスワード

Offline Password File

...オフラインパスワードアクセスポリシー

メモ：デフォルトのパスワードポリシーは編集することができません。

メモ：デフォルトでは Strong が規定として設定されています。つまり Strong にパスワードポリシーに準拠した形でパスワード

を変更します。他のパスワードポリシーを規定とする場合には「既定に設定」のチェックマークをクリックして切り替えます。



パスワードポリシー画面

6 - 1 パスワードポリシーの定義項目

項目名	解説
ポリシー名	定義するポリシー名を一意の名前で設定します
説明	ポリシーの内容を設定します
最小値	パスワードの最小文字数を設定します（最小数 4）
最大値	パスワードの最大文字数を設定します（最大数 255）
大文字と小文字の混在を強制	パスワードに大文字と小文字を混在させるかどうかを設定します
大文字と小文字の数	パスワードに設定する大文字と小文字の数をそれぞれ設定します
数値を強制	パスワードに数字の設定を強制するか設定します
最小数	パスワードに設定する数字の数を設定します
特殊文字を強制	特殊文字を混在させるかどうかを設定します ※特殊文字としてカウントされる文字は以下となります。 !#\$%&'(~{+*}<>?-^¥@[;,.]/ ※パスワード自動生成機能によってサポートしている文字は以下となります。 @\$-%&*()=^<>!#
最小数	特殊文字の数を設定します
文字は許可されていません。	パスワードとして許可しない文字を入力します。 ※<>（レスザン グレーターザン）は設定できません。
パスワードは辞書に載っている単語が含まれるべきではありません	パスワードに辞書単語を使用しないよう設定します。 例：apple、ranger
パスワードは明らかな書き換えが含まれるべきではありません	@pple (apple) ,0rangep (orange) 等の他の文字で置換された辞書単語を使用しないように設定します。
アルファベットからの開始を強制します	パスワードの最初の文字をアルファベットで指定するよう設定します

パスワードはログイン名と一致すべきではありません	アカウント名が含まれるパスワードの設定を許可しないよう設定します。
パスワードはログイン名のつづり換えであるべきではありません	パスワードにログイン名のつづり替えの設定を許可しないよう設定します。
パスワードは繰り返される部分文字列を含むべきではありません	aa や bb 等、同じ文字を繰り返すパスワードを許可しないよう設定します。
パスワードはパスワード長のシーケンスが含まれるべきではありません	3～10 の値に準じた連続する文字で構成されるパスワードの使用を制限するよう設定します。 ※こちらを有効化することで、⑬～⑯の項目詳細を設定可能です。
アルファベット順	abcd、hgfe 等のアルファベット正順や逆順を使用することを許可しないよう設定します。
キーボード配列順	qwerty、zcvbn 等のキーボード上、隣接配列されたアルファベットを使用することを許可しないよう設定します。 ※キーボード配列の種類は QWERTY/AZERTY/DVORAK/COLMAK から選択可能です。
数字順	1234、9876 等の連続する数字の正順や逆順を使用することを許可しないよう設定します。
連番	aaa、!!!、222 等の連続して繰り返される文字のシーケンスを使用することを許可しないよう設定します。
パスワードは直近のパスワードと同じであるべきではありません	直近、1～10 つ前のパスワードと同じパスワードを使用することを許可しないよう設定します。
パスワードは直近のパスワードと類似すべきではありません	直近、1～10 つ前のパスワードと類似するパスワードを使用することを許可しないよう設定します。 例）過去パスワードで test@123 を使用した場合、rest@123 や test@12 等が使用できなくなります。
○日 後パスワードを有効期限切れとなります。	パスワードの有効期限を設定します。

6 - 2 パスワードポリシーの設定手順

- 「管理」タブをクリックします。
- 「リソース設定」→「パスワードポリシー」をクリックします。

3. 「ポリシーを追加」をクリックします。

パスワードポリシー			
ポリシーを追加		ポリシーを削除	
<input type="button" value="検索"/>			Showing 1 - 4 of 4 ◀◀ 1 ▶▶ 25 50 75 100
ポリシー名	ポリシーの説明	既定に設定	編集
Low	厳格な制約がほとんどないパスワード	<input checked="" type="radio"/>	<input type="button" value="編集"/>
Medium	厳格な制約の少ないパスワード	<input checked="" type="radio"/>	<input type="button" value="編集"/>
Offline Password File	オフライン パスワード アクセスの...	<input checked="" type="radio"/>	<input type="button" value="編集"/>
Strong	厳格な制約が伴うパスワード	<input checked="" type="radio"/>	<input type="button" value="編集"/>

パスワードポリシー画面

4. 「パスワードのポリシーを追加」にて組織のパスワードポリシーに準拠する形で設定します。

ポリシー名 :

説明 :

既存のテンプレートを使用します。 :

範囲 & 文字セット

最小値	<input type="text"/>	<input type="checkbox"/> 数値を強制
最大値	<input type="text"/>	<input type="checkbox"/> 最小数 : <input type="text"/>
<input type="checkbox"/> 大文字と小文字の混在を強制	<input type="checkbox"/> 特殊文字を強制	
大文字の最小数	<input type="text"/>	<input type="checkbox"/> 最小数 : <input type="text"/>
小文字の最小数	<input type="text"/>	文字は許可されています : <input type="text"/>

語法

<input type="checkbox"/> パスワードは辞書に載っている単語が含まれるべきではありません	<input type="checkbox"/> パスワードはログイン名と一致すべきではありません
辞書を選択する: <input type="button" value="Common Words"/> <input type="button" value="管理"/>	<input type="checkbox"/> パスワードはログイン名のつづり換えであるべきではありません①
<input type="checkbox"/> パスワードは明らかに書き換えが含まれるべきではありません①	<input type="checkbox"/> パスワードは繰り返される部分文字列を含むべきではありません
<input type="checkbox"/> アルファベットからの開始を強制します	

シーケンス

<input type="checkbox"/> パスワードはパスワード長のシーケンスが含まれるべきではありません。	<input type="button" value="3"/>
<input type="checkbox"/> アルファベット順 ①	<input type="checkbox"/> 数字順 ①
<input type="checkbox"/> キーボード配列順 ①	<input type="checkbox"/> 連番 ①

パスワード類似性

<input type="checkbox"/> パスワードは直近のパスワードと同じであるべきではありません	<input type="button" value="1"/> パスワード
<input type="checkbox"/> パスワードは直近のパスワードと類似すべきではありません	<input type="button" value="1"/> パスワード ①

パスワード有効期限

<input type="checkbox"/> 後パスワードを有効期限切れとなります。	<input type="text"/> 日
--	------------------------

パスワードポリシー設定画面

5. 「保存」をクリックします。

7 リソース・アカウントの追加

本章では Password Manager Pro が管理するリソース・アカウントの追加方法について解説します。

リソース・アカウントを Password Manager Pro へ追加する方法は、以下の 3 種類があります。

- 手動で追加
- ファイルからインポート
- KeePass からインポート
- リソースディスカバリー (Windows/Linux/ネットワーク機器/VMware)

7 - 1 手動で追加

1. 「リソース」タブをクリックします。
2. 「リソース追加」をクリックします。



3. 各項目を入力して、[保存して続行]をクリックします。表示名は[リソース名]に、ホスト名/IP アドレスは、[FQDN/IP アドレス]に設定します。また、[リソース種別]、[パスワードポリシー]も最低限設定が必要です。

リソース追加 ⑨

リソース名 :

FQDN / IPアドレス : ①

リソース種別 : Windows

グループ名 : Default Group

説明 :

ドメイン名 :

部門 :

リソースURL : ②

場所 :

パスワードポリシー : Strong

ローカルアカウント使用によるRDP接続を制限 : ①

自動ログオン用のVNCポート : 5900

自動ログオン用のRDPポート : 3389

手動で追加 (リソース)

- アカウント (リソース上の特権 ID) を追加します。複数のアカウントを追加可能です。[ユーザー アカウント]、[パスワード]、[パスワード確認]は必須項目です。
- [追加]をクリックすると、設定内容が下の一覧に移動します。設定後、[保存]をクリックします。

アカウントを追加 ⑨

リソース名 : test

ユーザー アカウント :

パスワード : ②

パスワード確認 :

パスワードポリシー : Strong

メモ :

パスワードリセット : ①

RDPセッション記録 : ①

サービスアカウントのパスワードリセット : ①

ユーザー アカウント	サービス アカウント/アプリケーションプール アカウント	編集	削除
------------	------------------------------	----	----

⚠️ アカウントが追加されていません

手動で追加（アカウント）

7 - 2 リソースのインポート

1. ファイル（CSV/TXT/TSV/XLS/XLSX ファイル）から一括でインポートする機能もあります。
2. 「リソース」タブをクリックします。
3. 「リソース」追加をクリックします。



リソース追加

4. 「リソースのインポート」をクリックします。
5. ファイルフォーマットを指定し、「参照」からファイルを指定します。



ファイルからのリソースインポート

6. リソースの各フィールドとファイルの列を対応させます。

ファイルからのリソースインポート 

×

ステップ2/2 : XLSXフィールドのマッピングを選択 

リソース属性のマップ

リソース名 *	:	--XLSXデータからフィールドを選択▼
FQDN	:	--XLSXデータからフィールドを選択▼
説明	:	--XLSXデータからフィールドを選択▼
部門	:	--XLSXデータからフィールドを選択▼
場所	:	--XLSXデータからフィールドを選択▼
リソース種別	:	--XLSXデータからフィールドを選択▼
リソースURL	:	--XLSXデータからフィールドを選択▼

アカウント属性のマップ

ユーザー アカウント *	:	--XLSXデータからフィールドを選択▼
パスワード *	:	--XLSXデータからフィールドを選択▼
メモ	:	--XLSXデータからフィールドを選択▼
識別名	:	--XLSXデータからフィールドを選択▼

既に存在するリソースのインポートを試みると、Password Manager Proの既定の設定では、それをインポートしません。新規エントリを上書きするには以下のオプションを選択します

既存のリソースを上書き :

フィールドのマッピング

メモ : 既に存在するリソースはインポートされません。既に存在するリソース情報を上書きする場合には「既存のリソースを上書き : 」のチェックボックスにチェックを入れてください。

7 - 3 Keepass からのインポート

1. 「リソース」タブをクリックします。

2. 「リソース」追加をクリックします。



3. 「Keepass からインポート」をクリックします。

4. 表示されるポップアップフォームで、必要な KeePass データベースファイルを選択し、マスターpasswordを入力します。



5. 「今すぐインポート」をクリックします。

メモ：既に存在するリソースはインポートされません。既に存在するリソース情報を上書きする場合には「既存のリソースを上書き」 : のチェックボックスにチェックを入れてください。

7 - 4 リソースディスカバリー (Windows)

1. 「リソース」タブをクリックします。

2. 「リソースディスカバリー」をクリックします。

3. 「Windows」タブからドメイン名、プライマリドメインコントローラーを指定した上で、その資格情報を入力し、「列挙」をクリックしてください。

リソースディスカバリーの設定画面（Windows）

メモ：インポートするリソース、グループ/OU を直接指定することもできます。

4. インポート対象のグループ/OU を選択して、「インポート」をクリックします。

グループ/OU の選択

5. インポートが成功したことを確認します。

ディスカバリー結果

7 - 5 リソースディスカバリー (Linux)

1. 「リソース」タブをクリックします。
2. 「リソースディスカバリー」をクリックします。
3. 「Linux」タブをクリックします。
4. IP アドレスの範囲、接続モード、プロファイル、タイムアウトを指定して、「列挙」をクリックします。



リソースディスカバリーの設定画面 (Linux)

5. プロファイルが未作成の場合は、「プロファイル追加」をクリックし、リソース取得に必要な認証情報を追加します。



プロファイルの追加

6. 「ディスカバリーの確認」のポップアップ画面が表示されます。通知先を指定した上で、「続行」をクリックします。



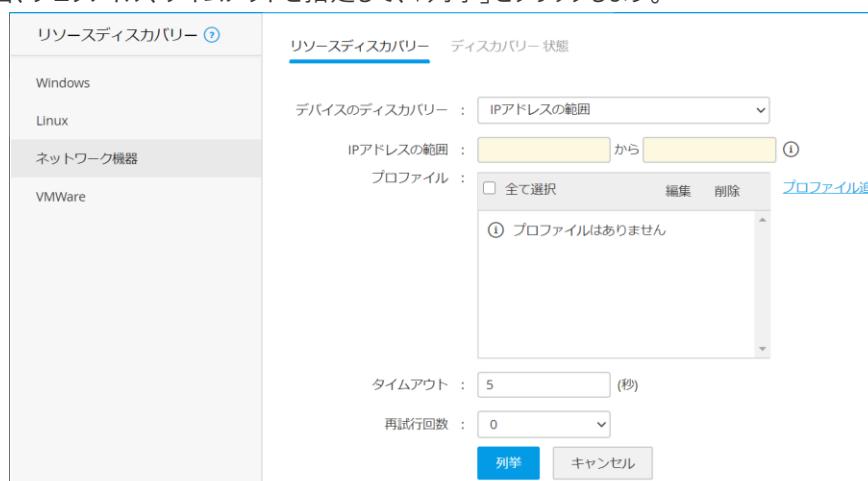
7. 「ディスクスキャナーリザルト」タブからディスクスキャナーリザルトを確認できます。



図 54 ディスクスキャナーリザルト

7-6 リソースディスクスキャナーリザルト (ネットワーク機器)

1. 「リソース」タブをクリックします。
2. 「リソースディスクスキャナーリザルト」をクリックします。
3. 「ネットワーク機器」タブをクリックします。
4. IP アドレスの範囲、プロファイル、タイムアウトを指定して、「列挙」をクリックします。



リソースディスクスキャナーリザルト (ネットワーク機器)

5. プロファイルが未作成の場合は、「プロファイル追加」をクリックし、リソース取得に必要な認証情報を追加します。

新しいディスカバリー ファイルを追加してください

名前 :	N/W_discovery
説明 :	
バージョン :	Version V3
SNMPポート :	161
ユーザー名 :	PMPUser
コンテキスト名 :	
認証プロトコル :	SHA
<input checked="" type="radio"/> 手動でパスワードを入力 <input type="radio"/> Password Manager Proに保管されているアカウントを使用 ①	
認証パスワード :	*****
Privプロトコル :	AES 128
<input checked="" type="radio"/> 手動でパスワードを入力 <input type="radio"/> Password Manager Proに保管されているアカウントを使用 ①	
Privパスワード :	*****
<input type="button" value="保存"/> <input type="button" value="キャンセル"/>	

プロファイル追加

6. 「ディスカバリーの確認」のポップアップ画面が表示されます。通知先を指定した上で、「続行」をクリックします。

ディスカバリーの確認

IPアドレス（200）を検出しようとしています。ディスカバリー プロセスは、ディスカバリーの完了まで、およそ3分20秒分かかります。

<input checked="" type="checkbox"/> すべての管理者	
<input type="checkbox"/> メールアドレスを指定	
通知先 :	
[メモ : 複数のアドレスはカンマ","で区切ります]	
<input type="button" value="続行"/> <input type="button" value="キャンセル"/>	

ディスカバリーの確認

7. 「ディスカバリー状態」タブからディスカバリーの結果を確認できます。

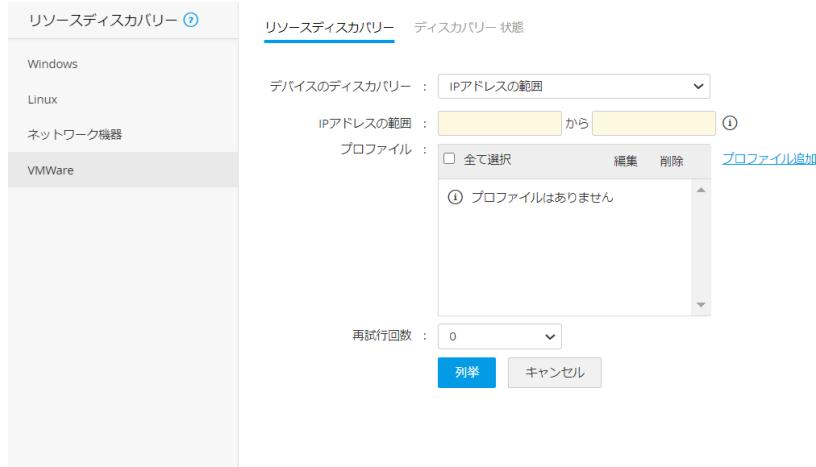
リソースディスカバリー ②

リソースディスカバリー	ディスカバリー状態															
Windows																
Linux																
ネットワーク機器																
VMWare																
<input type="button" value="ディスカバリータスクを削除"/> <input type="button" value="ディスカバリータスクのやり直し"/> <input type="button" value="ディスカバリータスクを停止"/>																
<input type="button" value="検索"/> 表示中 1 - 2 of 2 < < 1 > > 25 50 75 100																
<table border="1"> <thead> <tr> <th>タスク名</th> <th>次に起動</th> <th>完了時刻</th> <th>ディスカバリー状態</th> <th>説明</th> </tr> </thead> <tbody> <tr> <td>192.168.200.0 - 192.168.200.2...</td> <td>7/20, 2020 12:30:38 午後</td> <td></td> <td>未ディスカバリー</td> <td>Task In Progress</td> </tr> <tr> <td>192.168.200.0 - 192.168.200.2...</td> <td>7/20, 2020 12:30:38 午後</td> <td></td> <td>未ディスカバリー</td> <td>Task In Progress</td> </tr> </tbody> </table>		タスク名	次に起動	完了時刻	ディスカバリー状態	説明	192.168.200.0 - 192.168.200.2...	7/20, 2020 12:30:38 午後		未ディスカバリー	Task In Progress	192.168.200.0 - 192.168.200.2...	7/20, 2020 12:30:38 午後		未ディスカバリー	Task In Progress
タスク名	次に起動	完了時刻	ディスカバリー状態	説明												
192.168.200.0 - 192.168.200.2...	7/20, 2020 12:30:38 午後		未ディスカバリー	Task In Progress												
192.168.200.0 - 192.168.200.2...	7/20, 2020 12:30:38 午後		未ディスカバリー	Task In Progress												

ディスカバリー結果

7 - 7 リソースディスカバリー (VMware)

1. 「リソース」タブをクリックします。
2. 「リソースディスカバリー」をクリックします。
3. 「VMware」タブをクリックします。
4. IP アドレスの範囲、接続モード、プロファイル、タイムアウトを指定して、「列挙」をクリックします。



リソースディスカバリーの設定画面 (VMware)

5. プロファイルが未作成の場合は、「プロファイル追加」をクリックし、リソース取得に必要な認証情報を追加します。



プロファイル追加

6. 「ディスカバリーの確認」のポップアップ画面が表示されます。通知先を指定した上で、「続行」をクリックします。



7. 「ディスクバリーリー状態」タブからディスクバリーリーの結果を確認できます。

ディスクバリーリー結果

8 アクセス制御設定

アクセス制御を実装いただくことで申請承認のワークフローを構築できます。本章ではリソース、アカウント毎にアクセス制御を実装する手順について解説します。

8-1 アクセス制御設定項目

1. 承認管理者

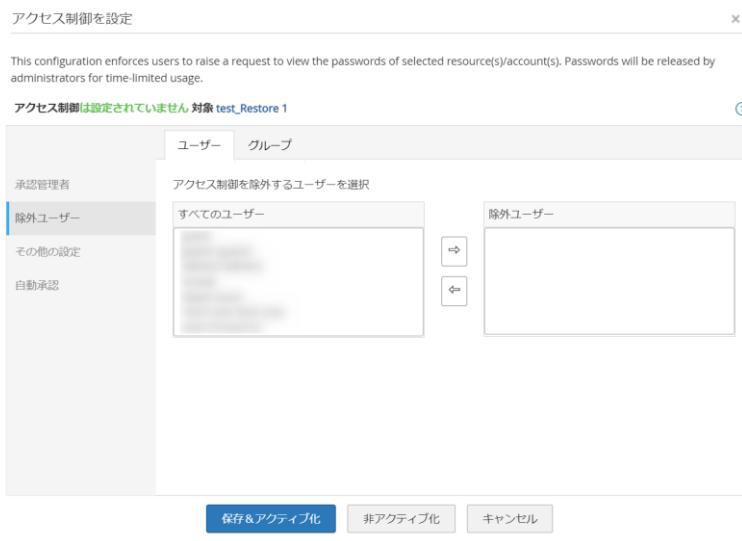
...対象のリソース/アカウントに対して承認者を選択できます。ユーザー単位、またはグループ単位で設定可能です。

承認管理者

メモ：多段承認機能はございませんが、承認者にて指定された管理者全員の承認が必要であるように設定可能です。

2. 除外ユーザー

...アクセス制御を除外するユーザーを指定します。除外ユーザーとして設定されたユーザーは申請承認のフローを経ずにリソース/アカウントに対してアクセスできるようになります。



3. その他の設定

- デフォルトではチェックされていない設定項目
- デフォルトでチェックされている設定項目、ただし無効化可能
- デフォルトでチェックされている設定項目、ただし無効化不可能

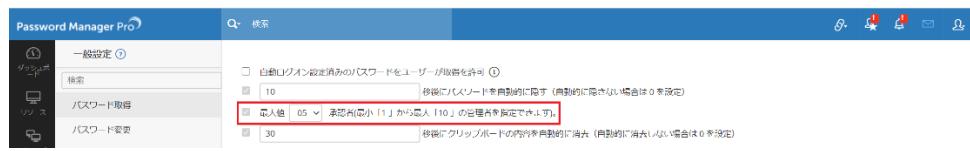
以下それぞれの設定項目について解説します。

- パスワード アクセスを承認する管理者は 2 人以上必要 () 管理者
...パスワードが払い出されるまでに必要な承認者の人数です。

メモ：デフォルトで 5 名（01～05）までの承認者を選択できます。ライセンスが 5 アドミン以上かつ承認者を 5 名以上必要と設定する場合には「管理」タブ→「セットアップ」欄一般設定→「パスワード取得」タブにて

- 最大値 () 承認者（最小「1」から最大「10」の管理者を設定できます）。

最大承認者数を変更してください。ただし、10 名が上限となります。



最大承認者数の変更

- パスワードを取得する際に理由の入力を強制

…申請する際のコメント欄にて記載が必須となります。記載なしで申請しようとした際にはエラーとなり申請処理が行われません。



コメント欄への記載

- 指定された時間の（ ）分前に、管理者にリマインドメールを送信

…時刻指定の申請に対して、開始時刻の（ ）分前に承認のリマインドメールを管理者に通知します。
- 使用時間終了後、ユーザーに（ ）分の延長時間对付与

…排他的使用時間後、セッション終了までの指定した猶予時間を設定します。
- パスワードは、承認されてから（ ）時間後に自動的にチェックイン

…パスワードを払い出した後に申請者がチェックインをし忘れた際にシステムが指定した時間を経過後自動的にチェックインします。
- 承認されない場合、要求は（ ）時間後に無効

…承認が下りない申請に対して指定された時間を経過後にその申請を無効化します。
- パスワードアクセスの排他は最大で（ ）分

…排他的に払い出されたパスワードを使用できる時間です。指定された時間を超過した瞬間にセッションは自動的に切れます。
- ✓ 排他的使用の後（他のユーザーによってチェックインする場合）に、パスワードを変更

…チェックインした後にパスワードを自動的に変更します。



その他の設定

4. 自動承認

...申請に対してシステムが自動的に承認します。以下 3 つの種類があります。

- 終日

...こちらの設定により、いかなる時間であっても申請に対しては自動的に承認されます。

- 時間帯指定

...曜日ごとに自動承認する時間帯を設定できます。一つの曜日で最大 3 つまでの時間帯を設定できます。例えば土日、祝日にて設定いただけます。

- チケット ID

...チケット管理システムと連携することで、チケット ID によって自動承認します。



自動承認

8 - 2 リソース単位でのアクセス制御設定

リソースごとにアクセス制御を設定する方法について紹介します。

1. 「リソース」タブをクリックします。
2. アクセス制御を実装したいリソースの「リソースアクション」をクリックします。

リソースアクション

3. 「アクセス制御を設定」をクリックします。
4. 8-1 アクセス制御設定項目を参照の上、要件に合った形で設定します。
5. 「保存 & アクティブ化」をクリックします。

メモ：「非アクティブ化」をクリックすることで、アクセス制御の設定内容を保持したまま無効化することができます。

8 - 3 アカウント単位でのアクセス制御設定

サーバーの特権 ID に絞ってよりセキュアなアクセス制御を設定することができます。設定方法については以下の通りです。

1. 「リソース」タブをクリックします。
2. アクセス制御を実装したいアカウントを含むリソース名をクリックします。
3. アクセス制御を実装したいアカウントの「アカウントアクション」アイコンをクリックします。
4. 「アクセス制御を設定」をクリックします。

アカウント情報 - Windowsサーバー

DEMOが動的グループの場合は、グループの条件に一致するアカウントが表示されます。リソース上の全てのアカウントを表示する場合は「すべての自分のパスワード」から確認可能です

追加 アカウントディスカバリー サービスアカウント スケジュールタスク その他の操作 [?](#)

表示中 1 - 2 合計 < 前の ページ 1 次 > 25 50 75 100

□	ユーザー アカウント	パスワード	アカウントアクション	接続をオープン	メモ
□	★ ⓘ administrator	****	🔧 🔒	接続	N/A
□	★ ⓘ demo	****	🔧 🔒	接続	N/A

アクションメニュー (demo アカウント上):

- パスワード変更
- パスワード検証
- パスワード履歴
- パスワードリンクをコピー
- アカウントを編集
- アカウントのコピー
- アカウントの移動
- アクセス制御を設定
- アクセス制御の詳細
- ユーザーに共有
- ユーザーグループに共有

アクセス制御を設定

5. 8-1 アクセス制御設定項目を参照の上、要件に合った形で設定します。

6. 「保存 & アクティビ化」をクリックします。

7. 設定内容を「アカウントアクション」アイコン→「アクセス制御の詳細」から確認します。

アクセス制御の詳細

アカウント名: demo リソースの所有者: admin アクセス制御は有効化されました: リソース単位

承認管理者: すべて (admin)

除外ユーザー: すべて ()

自動承認: 自動承認は設定されていません

その他の設定:

設定しました	状態	値
複数の管理者の承認を強制	無効	-
パスワード取得時、ユーザーに理由の入力を強制	有効	-
所定の時間までにパスワードアクセス要求への処理に対するリマインドメールを管理者に送信	無効	-
アクセス時間が一度終了しても、猶予時間をユーザーに付与する	無効	-
承認された時間外にパスワードがチェックアウトされない場合、パスワードは自動的にチェックインされます	無効	-
Requests gets void after provided time if not approved	有効	1 時間

OK

アクセス制御の詳細

メモ：アカウント単位でのアクセス制御はリソース単位のアクセス制御より優先度が高くなります。例えばあるリソースに対してアクセス制御が既に実装されていたとします。そのリソース内にてあるアカウントのみ特別に別のアクセス制御を実装したいと仮定します。その際にリソースに対して設定したアクセス制御はそのアカウントに対しては適用されず、そのアカウントに対して個別に設定したアクセス制御が適用されます。

9 リソース/リソースグループの共有

リソース/リソースグループを特定のユーザー/ユーザーグループに共有することで共有されたユーザー/ユーザーグループはそのリソースを利用することができます。

リソースの共有する際に管理者は共有するユーザー/ユーザーグループに対してどの程度の権限を与えるのか選択できます。

Password Manager Pro では 3 つの共有レベルを用意しています。

パスワードの表示

...ユーザーおよびユーザーグループ所属ユーザーは、共有リソース/リソースグループのパスワードにアクセスし、使用することができます。

パスワードの変更

...ユーザーとユーザーグループは、共有リソース/リソースグループのパスワードにアクセスし、変更を加えることができます。ただし、この権限では、ユーザー/ユーザーグループ所属ユーザーはリソースの他の属性を変更することはできません。

フルアクセス

...ユーザーとユーザーグループ所属ユーザーは、共有リソース/リソースグループを完全に管理することができます。また、リソースや関連アカウントのパスワードを他のユーザーと再共有することもできます。

注意：デフォルトグループにはフルアクセス権限を付与できません。

9 - 1 リソースを共有

1. 「リソース」タブをクリックします。
2. 共有したいリソースの「リソースアクション」アイコンをクリックします。
3. 「ユーザーに共有」または「ユーザーグループに共有」をクリックします。



ユーザーに共有

メモ：複数のリソースを一括してユーザー/ユーザーグループに共有することも可能です。その際には各リソースのチェックボックスにチェックを入れ、「リソースアクション」>>共有へと進んでください。

メモ：フルアクセスの権限で共有するためには共有されるユーザーが特権管理者、管理者、パスワード管理者であることが必要です。

4. 「アクセス権の付与」をクリックし、共有権限を選択して共有します。

アクセス権の付与

5. 共有されたユーザーでログインし、リソースを確認します。

メモ：権限に応じて共有されたリソースに対する実行可能なアクションが異なります。

パスワードの表示

パスワードの変更

パスワードの管理

9 - 2 リソースグループを共有

リソースをまとめてリソースグループとして、グループ単位で共有することも可能です。

1. 「グループ」タブをクリックします。
2. 共有したいリソースグループの「アクション」アイコンをクリックします。
3. 「ユーザーに共有」または「ユーザーグループに共有」をクリックします。

リソースグループ

グループ名: operation1

説明: あなたが作成したリソース

アクション: admin

所有者: admin

レポート: all

リソースグループの編集

- ユーザーに共有
- ユーザーグループに共有
- 所有権を移動
- 鍵のローテート
- パスワード変更を実行
- スケジュールパスワード変更
- 整合性検査
- パスワードアクションの設定
- 定期的なパスワードのエクスポート
- アカウントディスカバリーをスケジュール

ユーザーに共有

メモ：複数のリソースグループを一括してユーザー/ユーザーグループに共有することも可能です。

リソースグループ

グループ名: Linux, operation1

説明: あなたが作成したリソース

アクション: admin

所有者: admin

レポート: all

リソースグループの編集

- ユーザーに共有
- ユーザーグループに共有
- パスワード変更
- パスワードポリシーを設定
- チケット設定

一括でユーザーに共有

メモ：フルアクセスの権限で共有するためには共有されるユーザーが特権管理者、管理者、パスワード管理者であることが必要です。

4. 「アクセス権の付与」をクリックし、共有権限を選択して共有します。

adminが所有しているLinuxを他のユーザーに共有

ユーザーにLinux(リソース)のアクセスを付与するためには、表示、変更、フルアクセスのいずれかの権限で割り当てる必要があります。アクセス権の付与/削除する場合には、各ユーザーの横にある「付与」または「取り消し」ボタンをクリックして権限の設定します。複数ユーザーを一括で設定する場合には、設定するユーザーを選択しユーザーリストの上部にある「付与」または「取り消し」ボタンをクリックして権限の設定します。

フィルタ: すべてのユーザー	ユーザー名	アクセス権種別	アクション
	① auditor auditor	アクセスはありません	アクセス権の付与
	① guest	アクセスはありません	アクセス権の付与
	① admin passwd	アクセスはありません	アクセス権の付与
	① admin privileged	アクセスはありません	アクセス権の付与

アクセス権の付与

5. 共有されたユーザーでログインし、リソースグループを確認します。



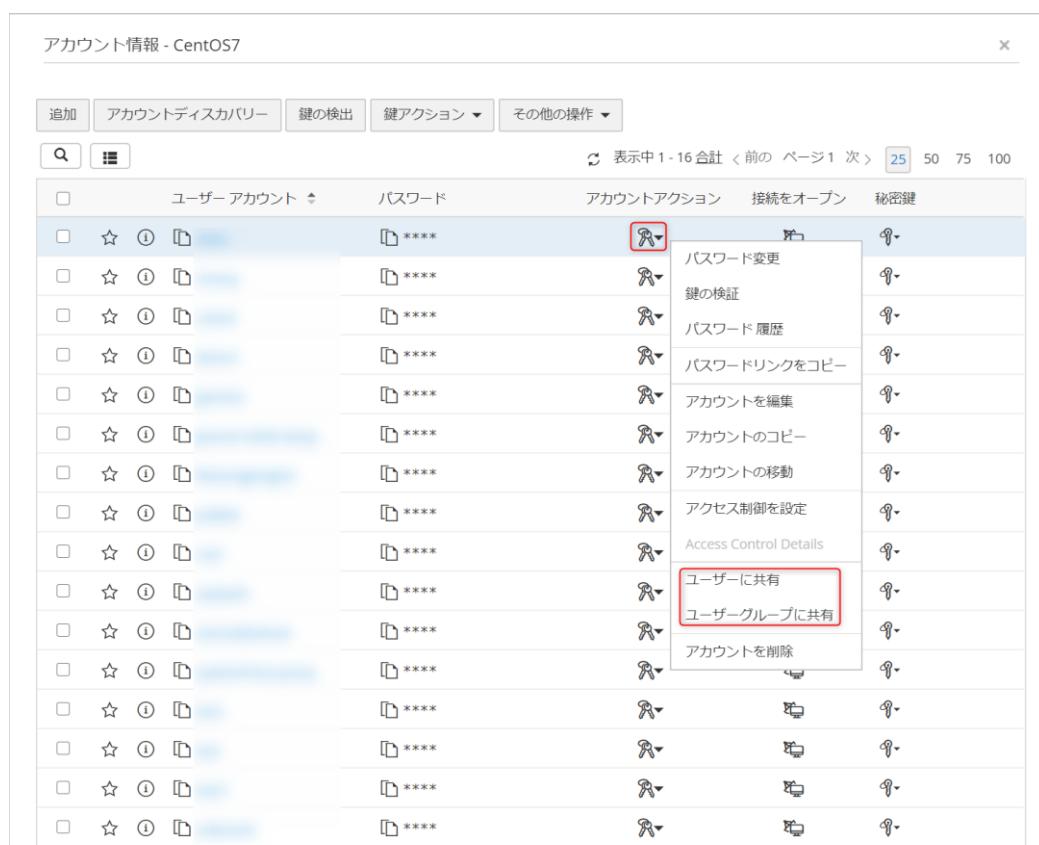
The screenshot shows the 'Password Manager Pro' application interface. On the left, there's a sidebar with icons for 'リソース' (Resources), '鍵' (Keys), and 'パスワード' (Passwords). The main area is titled 'リソース' (Resources) and shows a list of resources. A search bar at the top says '検索' (Search) and has a dropdown set to 'Linux'. Below the search bar, there are buttons for 'リソースアクション' (Resource Action) and 'パスワードのエクスポート' (Password Export). The list table has columns for 'リソース名' (Resource Name), '説明' (Description), 'リモート接続' (Remote Connection), and '種別' (Type). One entry is visible: '& CentOS7' with a 'Linux' icon. At the bottom of the list, there are buttons for '表示中 1-1 直計' (Showing 1-1 of 1 total), '前の ページ' (Previous Page), '次の ページ' (Next Page), and page numbers '25 50 75 100'.

共有されたリソースグループ

9 - 3 アカウントを共有

同じリソースの複数のアカウントをそれぞれ別のユーザーに共有することも可能です。以下の設定ではアカウントごとに共有先を設定します。

1. 「リソース」タブをクリックします。
2. 共有したいアカウントが含まれるリソース名をクリックします。
3. 共有したいアカウントの「アカウントアクション」アイコンをクリックします。



The screenshot shows the 'Account Information - CentOS7' screen. At the top, there are buttons for '追加' (Add), 'アカウントディスクアバリー' (Account Disk Quota), '鍵の検出' (Key Detection), '鍵アクション' (Key Action), and 'その他の操作' (Other Operations). Below these are search and filter buttons. The main table lists 16 accounts, each with a checkbox, a user icon, a password icon, and an 'Account Action' icon (a wrench). A context menu is open over the 'Account Action' icon of the first account. The menu items are: 'パスワード変更' (Change Password), '鍵の検証' (Key Verification), 'パスワード履歴' (Password History), 'パスワードリンクをコピー' (Copy Password Link), 'アカウントを編集' (Edit Account), 'アカウントのコピー' (Copy Account), 'アカウントの移動' (Move Account), 'アクセス制御を設定' (Set Access Control), 'Access Control Details', 'ユーザーに共有' (Share with User), 'ユーザーグループに共有' (Share with User Group), and 'アカウントを削除' (Delete Account). The 'ユーザーに共有' and 'ユーザーグループに共有' options are highlighted with a red box.

アカウントアクション

4. 「ユーザーに共有」または「ユーザーグループに共有」をクリックします。

メモ：複数のアカウントを一括してユーザー/ユーザーグループに共有することも可能です。

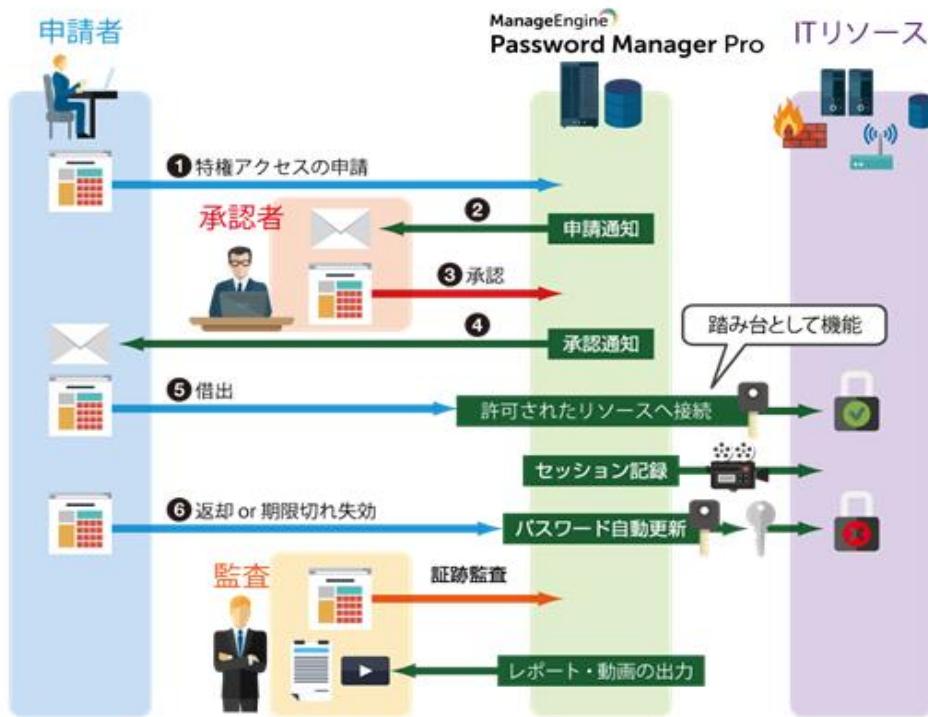
5. 「アクセス権の付与」をクリックし、共有権限を選択して共有します。

アクセス権の付与

6. 共有されたユーザーでログインし、リソースグループを確認します。

10 申請・承認のワークフローの流れ

前章まで設定いただけますと申請・承認のワークフローを運用することができます。以下実際のワークフローの流れについて説明します。



申請承認のワークフローの概要

10-1 申請者からの申請

1. 「リソース」タブをクリックします。
2. 申請したいアカウントを含むリソース名をクリックします。
3. 申請予定のアカウントのパスワード欄にて記載している[要求]をクリックします。

アカウント情報 - demo-pmp

表示中 1-1 会社 <前の ページ 1 次> 25 50 75 100

ユーザー/アカウント	パスワード	アカウントアクション	接続をオープン
☆ ① administrator	要求		

アカウント情報

4. 任意でコメントを記入し、「送信」をクリックします。即時の承認を求める場合には、「今」を選択します。

パスワードを要求

リソース名: demo-pmp アカウント名: administrator

パスワードのアクセス要求の送信先 admin に送信します。アクセス要求が承認または拒否された場合、下記のメールアドレスに送信します。送信先メールアドレス パスワードを使用する理由を入力する必要があります。

パスワードをアクセスする : 今 後で

コメント :
[Large text area]

送信 キャンセル

パスワードを要求（今）

5. 日時指定して承認する場合には、「後で」を選択します。

パスワードを要求

リソース名: demo-pmp アカウント名: administrator

パスワードのアクセス要求の送信先 admin に送信します。アクセス要求が承認または拒否された場合、下記のメールアドレスに送信します。送信先メールアドレス パスワードを使用する理由を入力する必要があります。

パスワードをアクセスする : 今 後で

開始日 : 30/01/2018

開始時刻 : 11 : 05 時間

終了日 : 30/01/2018

終了時刻 : 13 : 05 時間

サーバーの現在時刻 11:02 時間

アクセス開始の 15 分前にリマインダーメールを送信

コメント :
[Large text area]

送信 キャンセル

パスワードを要求（後で）

メモ：デフォルトの設定ではコメントは必須です。これらの設定を解除するためには、リソース/アカウントに設定されているアクセス制御設定にて「**パスワードを取得する際に理由の入力を強制**」を無効化する必要があります。詳細につきましては 8 アクセス制御の設定をご確認ください。

6. 表示が「承認待ち」に変わります。



アカウント情報 - demo-pmp

表示中 1 - 1 合計 <前の ページ 1 次> 25 50 75 100

ユーザー アカウント パスワード アカウントアクション 接続をオープン

☆ ① administrator 承認待ち

承認待ち

1 0 - 2 承認者への通知

申請者から申請されると承認者に対してメールが通知されます。その後、Password Manager Pro ログインして、その申請を処理してください。

1. 画面右上のベルアイコンをクリックします。



2. 「パスワードアクセス要求」をクリックします。

メモ：「管理」タブ→「管理」欄→「パスワードアクセス要求」からも確認できます。

1 0 - 3 承認者の承認/拒否

1. パスワードアクセス要求から申請内容を確認した後に、「要求」をクリックします。

Showing 1 - 1 of 1

リソース名 理由 ユーザー アカウント 要求者 アクション 開始時刻 終了時刻 リクエスト時刻

demo-pmp 作業ID: 1 administrator guest 要求 N/A N/A 1 30, 2018 11:14 午前

パスワードアクセス要求

2. 理由を任意で記載し、「承認」または「拒否」をクリックします。

Request Details ×

ユーザ名: [REDACTED] リソース名: Windowsサーバー

ユーザー アカウント名: administrator リクエスト時刻: [REDACTED]

使用理由: サービス停止の原因調査です。

ユーザーはパスワードへのアクセスが可能です : 今 後で

理由 :

承認 拒否

申請內容

メモ：「後で」を選択して、時刻指定した形で承認することもできます。申請者が指定した時刻とは異なる時刻を指定することもできます。

3. パスワードアクセス要求画面の[アクション]で、表示が[未使用]となります。

パスワードアクセス要求					
リソース名	理由	ユーザー アカウント	要求者	アクション	リクエスト時刻
demo-pmp	作業申請	administrator	guest	未使用 チャックイン	7/12/2017 05:33 午後

承認後のステータス

メモ：一旦承認した場合でも「チェックイン」ボタンをクリックすることでパスワードを強制的に返却させることができます。

1 0 - 4 申請者への承認/拒否通知/チェックアウト

申請が承認/拒否された際には申請者に対して通知メールが送信されます。拒否された場合はアカウントのパスワード欄にて記載しているステータスが[要求]へと代わります。以下、承認された際の手順について解説します。

1. 「リソース」タブをクリックします。
2. 申請したアカウントを含むリソース名をクリックします。
3. 申請したアカウントのパスワード欄の「チェックアウト」をクリックします。



アカウント情報 - demo-pmp

表示中 1 - 1 合計 <前の ページ 1 次 > 25 50 75 100

ユーザー アカウント	パスワード	アカウント アクション	接続をオープン
☆ ① <input type="checkbox"/> administrator	チェックアウト		

アカウント情報

4. [チェックアウト]すると当該ユーザー アカウントでリソースにアクセス可能となります。



パスワードのチェックアウト

リソース名 : **demo-pmp**

アカウント名 : **administrator**

これから 30 分間、あなたはパスワードへの排他的アクセスを有します。これは次にパスワードをチェックインすると無効になります。

チェックアウト **キャンセル**

チェックアウト

5. [パスワード]で、表示が[チェックイン]に変わります。



アカウント情報 - demo-pmp

表示中 1 - 1 合計 <前の ページ 1 次 > 25 50 75 100

ユーザー アカウント	パスワード	アカウント アクション	接続をオープン
☆ ① <input type="checkbox"/> administrator	**** チェックイン		

パスワードの払い出し

メモ： パスワード欄の * * * * をクリックすることでパスワードが表示されます。役割が**特権管理者、管理者、パスワード管理者以外**のユーザーに対してパスワードが払い出された際に、パスワードをマスキング（# # # #）し非表示にすることも可能です。



設定方法は以下の通りです。

1. 「管理」タブ>>「セットアップ」欄>>一般設定>>「パスワード取得」タブへと進む
2. 「自動ログオン設定済みのパスワードをユーザーが取得を許可」のチェックを外す
3. 「保存」をクリックします

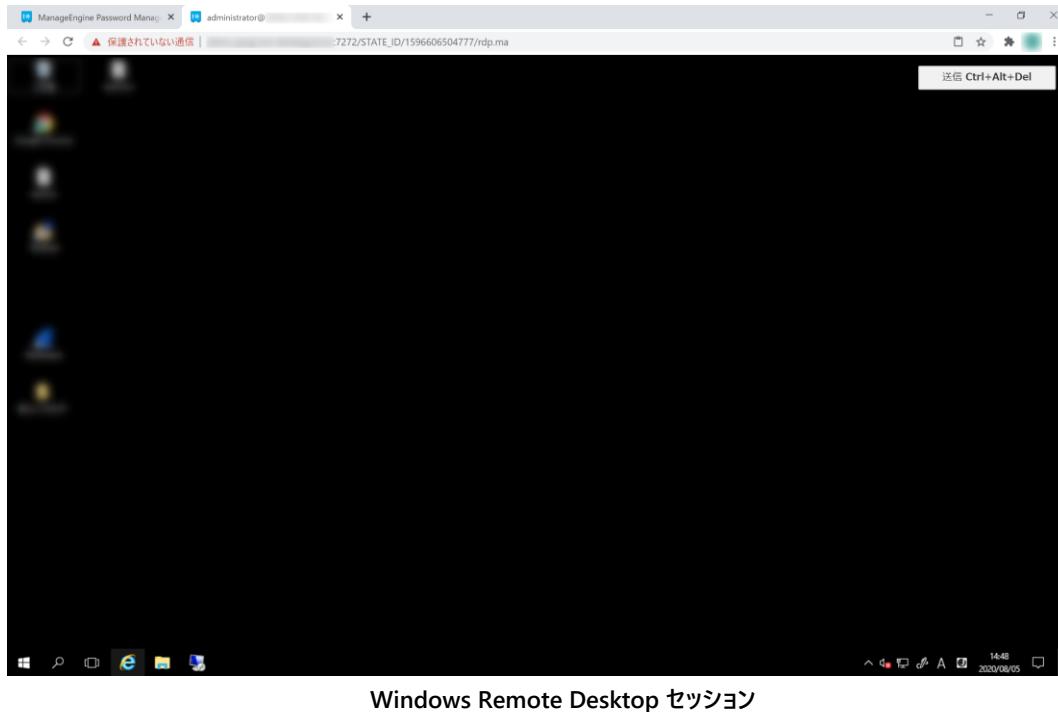
10-5 パスワードの借り出し

1.「接続をオープン」欄のマシンアイコンをクリックします。

2.[Windows Remote Desktop]をクリックします。



3. 別タブで RDP 接続が開始されます。



メモ：RDP 接続タブには「アカウント名@FQDN/IP アドレス」が記載されています。FQDN/IP アドレスはリソースを追加した際に設定した内容となります。

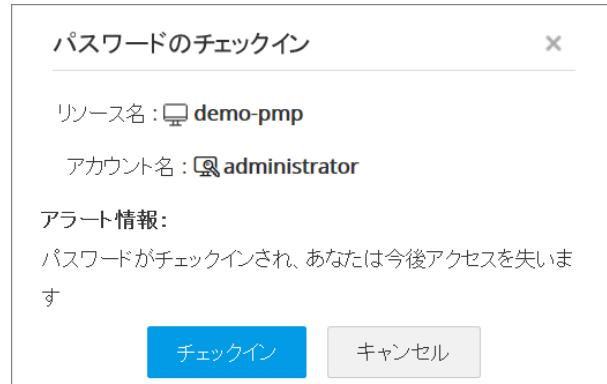
メモ：「監査」タブ>>「アクティブなリモートセッション」へ進むと、現時点で実施しているリモートセッションの一覧を確認することができます。あるセッションにて「参加」アイコンをクリックすると、当該のセッションの様子をリアルタイムで確認できます。またユーザーが不審な動作を行った際などに対して管理者は「終了」アイコンをクリックし、セッションを強制的に時刻指定した形で承認することもできます。申請者が指定した時刻とは異なる時刻を指定することもできます。



1.0 - 6 パスワードの返却

1.[パスワード]で、[チェックイン]をクリックします。

メモ：サーバー側でサインアウトする、またはブラウザーの[X]ボタンをクリックすることでもセッションを終了できます。



チェックイン

2.[パスワード]で、表示が[要求]に変わります。

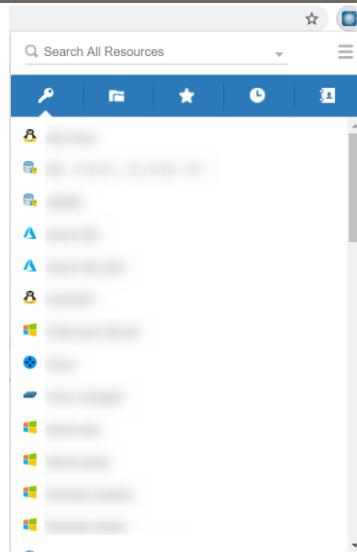


チェックイン後

メモ： チェックイン時に自動的にパスワードを変更させることもできます。アクセス制御設定のデフォルトの設定では変更するにチェックが入っています。変更する場合には以下の手順となります。

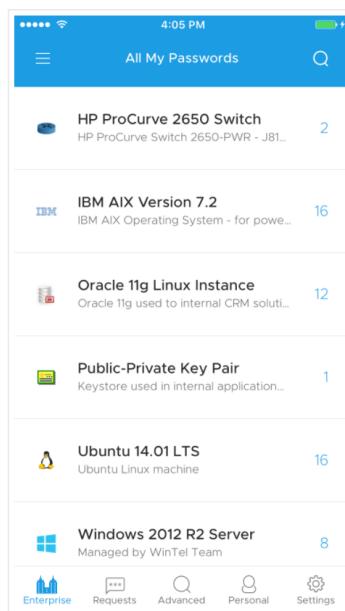
1. 当該のリソースの「リソースアクション」アイコンをクリックします。
2. 「アクセス制御を設定」をクリックします。
3. 「その他の設定」タブへ進み、「排他的使用の後（他のユーザーによってチェックインする場合）に、パスワードを変更」のチェックを外します。
4. 「保存 & アクティブ化」をクリックします。

メモ： ブラウザーの拡張機能を利用してPassword Manager ProのWebコンソールにアクセスすることなく申請承認のワークフローを回すことができます。



ブラウザーの拡張機能

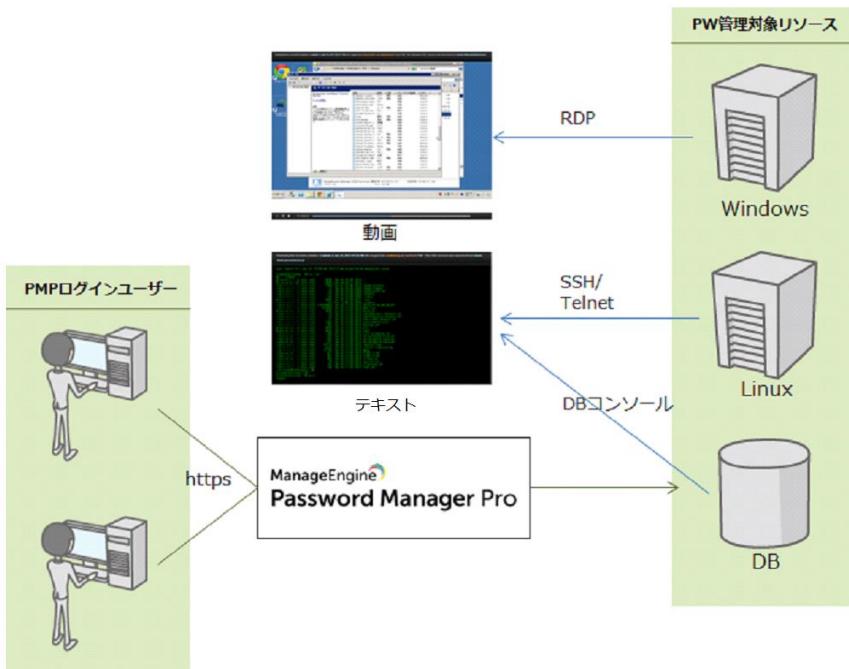
またAndroid & iOS それぞれに対応した Password Manager Pro アプリを利用することでスマートデバイス上から申請承認のワークフローを回すことができます。



モバイルアプリ

1.1 記録済みセッションの管理

下記の図のように、Password Manager Pro 経由でパスワード管理対象リソースにリモート接続し、リモート接続時の操作内容をセッション記録として取得可能です。Windows では動画、Linux、DB、ネットワーク機器等ではコマンドをテキストとして取得します。



記録済みセッションの取得

メモ： 動画ファイルは 1 分あたり約 1 MB の容量を消費します。ただし、画面操作がない場合には静止画として取得します。

1.1.1 セッションレコーディング設定

「管理」タブ→「設定」欄→セッションレコーディング（「監査」タブ→「記録済みセッション」タブ→セッションレコーディング設定）へ進みますと、セッションレコーディングに関する設定を行えます。

セッションレコーディング設定

RDPセッションの記録 SSH/Telnetセッションの記録を有効化
 VNCセッションの記録を有効化 セッション録音状態をセッションタブに表示します。

記録済みセッションの外部保存先

記録済みセッションの保存先 :

記録済みセッションのバックアップ保存先 :

日付の形式を選択する :

記録済みセッションの削除

記録済みセッションのうち 日を超えたものを削除する（削除を無効にするには、0を入力するか空白のままにします） ①

ウェルカムメッセージ

セッション開始時にウェルカムメッセージを表示します。

入力可能な残りの文字数は：です。4000

メモ: PMP経由で記録したセッションのアーカイブにより、フォレンジックによる監査に役立てることが可能です。RDP、VNC、SSH、TelnetやSQLのセッション記録を有効または無効に設定できます。

セッションレコーディング設定

設定内容としては以下の 4 つとなります。

- 各種セッション記録の有効化/無効化
...デフォルトではチェックボックスにチェックが入っている状態で、有効化されています。チェックを外すことでセッションは開始してもレコーディングはしない設定が可能です。
- 記録済みセッションの保存先
...UNC 形式で保存先パスを指定可能です。
- 記録済みセッションのバックアップ保存先
...パスが登録されている場合にのみバックアップを保存します。
- 記録済みセッションの保存期間
...日数単位で保存期間を設定できます。無期限の場合には 0 を入力してください。
- ウエルカムメッセージの表示
...セッション開始後に表示するウェルカムメッセージをカスタム可能です。

メモ： 記録済みセッションのバックアップ保存先を指定し、双方に記録済みセッションファイルを保存可能です。ただし、メインの記録済みセッション保存先のパスに保管できない場合、Password Manager Pro は記録済みセッションのバックアップ保存先に保存されず、デフォルトの保存先 (<PMP>¥recorded_files) に保管される仕様です。

1.1.2 記録済みセッションの再生方法

1. 「監査」タブをクリックします。
2. 「記録済みセッション」をクリックします。

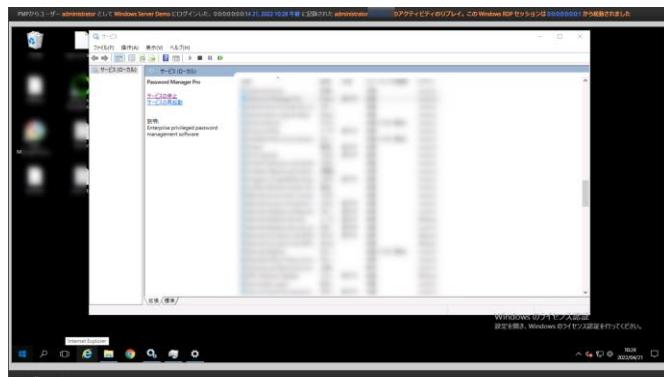


The screenshot shows the 'Recorded Sessions' list in the 'Audit' tab. The first session listed is for 'administrator' on 'admin' with a success status on '8.17.2020 10:44 年前'. The 'Actions' column for this session has a red box around the '再生' (Restart) button. The table has columns for 'リソース名', 'ユーザー アカウント', 'オペレータ', 'IP アドレス', '状態', 'タイムスタンプ', '理由', 'Actions', and 'チャットログ'.

リソース名	ユーザー アカウント	オペレータ	IP アドレス	状態	タイムスタンプ	理由	Actions	チャットログ
administrator	admin			成功	8.17.2020 10:44 年前	Windows R...	再生	
administrator	admin			成功	8.17.2020 10:42 年前	Windows R...	再生	
root	admin			成功	8.17.2020 09:36 年前	SSH 自動...	再生	
root	admin			成功	8.17.2020 09:29 年前	SSH 自動...	再生	
root	admin			成功	8.17.2020 09:21 年前	SSH 自動...	再生	

記録済みセッションの再生

3. 「再生」アイコンをクリックします。



再生画面（RDP）

メモ： 記録済みセッションファイル（.rdpv ファイル、sshv ファイル等）は生成された Password Manager Pro によって暗号化されています。つまり、Password Manager Pro のコンソール画面でのみ、記録済みセッションを再生することができるです。また他の Password Manager Pro で再生することは暗号鍵が異なるためできません。

メモ： 管理者は「削除」アイコンをクリックすることで、各々の記録済みセッションファイルを手動で削除できます。ただし、他の管理者の承認が必要です。

1.2 各タブの機能概要

1.2.1 ダッシュボードタブ

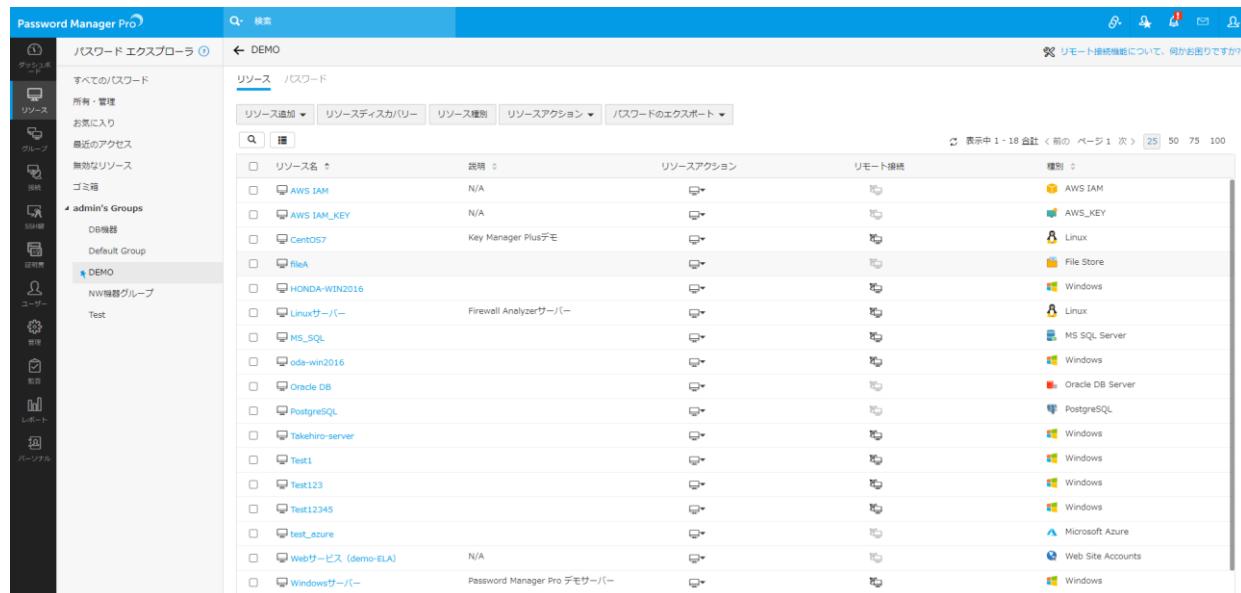
Password Manager Pro が管理するパスワード、Password Manager Pro ユーザー、SSH 鍵について、サマリーを表示します。ログイン直後に表示され、直観的に利用状況を把握できます。



ダッシュボードタブ

1.2.2 リソースタブ

Password Manager Pro で管理しているリソースの一覧を確認できます。パスワード変更やリソースの共有、アクセス制御設定などリソースの設定に関わるものは全てこちらのタブで設定します。



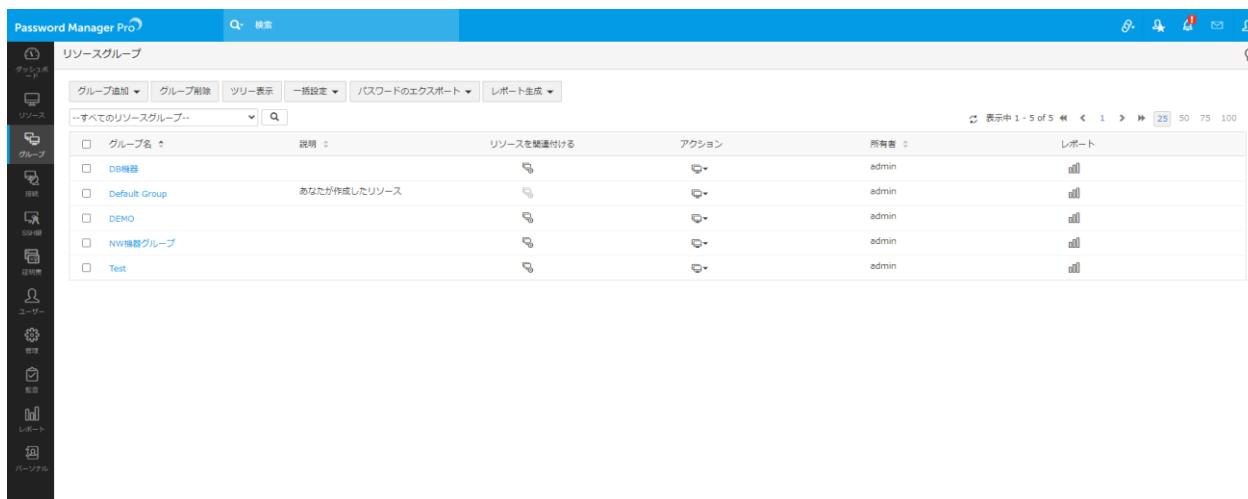
The screenshot shows the 'Resource' tab in the Password Manager Pro interface. The left sidebar shows navigation options like Dashboard, Resources, Groups, and Reports. The main area has a search bar and a toolbar with buttons for adding, deleting, and filtering resources. A table lists 18 resources, each with a checkbox, a resource icon, a name, a description, actions (edit, delete, copy, etc.), remote access (edit, delete, copy), and a type icon. The types listed are AWS IAM, AWS KEY, Linux, File Store, Windows, Oracle DB Server, PostgreSQL, Microsoft Azure, and Web Site Accounts.

リソース名	説明	リソースアクション	リモート接続	種別
AWS IAM	N/A	edit, delete, copy	edit, delete, copy	AWS IAM
AWS IAM_KEY	N/A	edit, delete, copy	edit, delete, copy	AWS_KEY
CentOS7	Key Manager Plusデモ	edit, delete, copy	edit, delete, copy	Linux
ReA		edit, delete, copy	edit, delete, copy	File Store
HONDA-WIN2016		edit, delete, copy	edit, delete, copy	Windows
Linuxサーバー	Firewall Analyzerサーバー	edit, delete, copy	edit, delete, copy	Linux
MS_SQL		edit, delete, copy	edit, delete, copy	MS SQL Server
oda-win2016		edit, delete, copy	edit, delete, copy	Windows
Oracle DB		edit, delete, copy	edit, delete, copy	Oracle DB Server
PostgreSQL		edit, delete, copy	edit, delete, copy	PostgreSQL
Takehiro-server		edit, delete, copy	edit, delete, copy	Windows
Test1		edit, delete, copy	edit, delete, copy	Windows
Test123		edit, delete, copy	edit, delete, copy	Windows
Test12345		edit, delete, copy	edit, delete, copy	Windows
test_azure		edit, delete, copy	edit, delete, copy	Microsoft Azure
Webサービス (demo-ELA)	N/A	edit, delete, copy	edit, delete, copy	Web Site Accounts
Windowsサーバー	Password Manager Pro デモサーバー	edit, delete, copy	edit, delete, copy	Windows

リソースタブ

1.2.3 グループタブ

リソースを管理区分に沿ってまとめることができます。作成されたリソースグループに対してユーザーにまとめて共有し、定期パスワード変更等のアクションを設定できます。



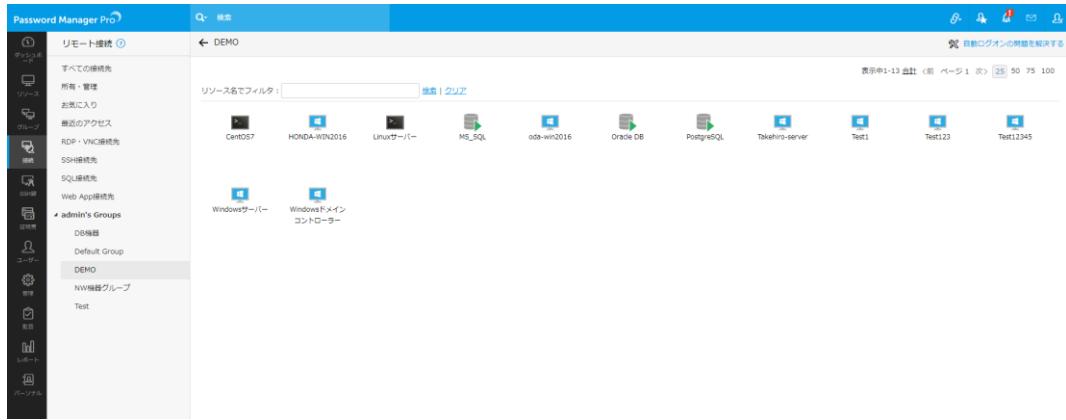
The screenshot shows the 'Group' tab in the Password Manager Pro interface. The left sidebar shows navigation options like Dashboard, Resources, Groups, and Reports. The main area has a search bar and a toolbar with buttons for adding, deleting, and filtering groups. A table lists 5 resource groups, each with a checkbox, a group icon, a name, a description, actions (edit, delete, copy), owner (admin), and a report icon.

グループ名	説明	リソースを縫接付ける	アクション	所有者	レポート
DB機器		edit, delete, copy	edit, delete, copy	admin	report
Default Group	あなたが作成したリソース	edit, delete, copy	edit, delete, copy	admin	report
DEMO		edit, delete, copy	edit, delete, copy	admin	report
NW機器グループ		edit, delete, copy	edit, delete, copy	admin	report
Test		edit, delete, copy	edit, delete, copy	admin	report

グループタブ

1 2 - 4 接続タブ

管理対象サーバーに接続する際に利用します。

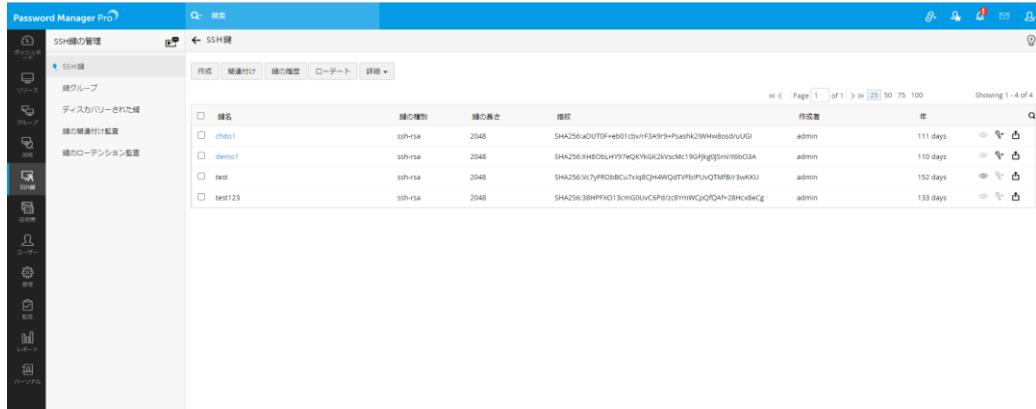


The screenshot shows the 'Connections' tab in the Password Manager Pro interface. The left sidebar has a 'Connections' icon highlighted. The main area shows a list of connections with icons: CentOS7, HONDA-WIN2016, Linuxサーバー, MS_SQL, odb-win2016, Oracle DB, PostgreSQL, Takehiro-server, Test1, Test123, and Test12345. A search bar at the top is empty. The bottom of the interface shows a navigation bar with icons for Home, Logout, and Help.

接続タブ

1.2.5 SSH 鍵タブ

SSH 鍵の管理をこちらのタブから行います。SSH 鍵の作成、サーバーへの関連付け等も実施することができます。

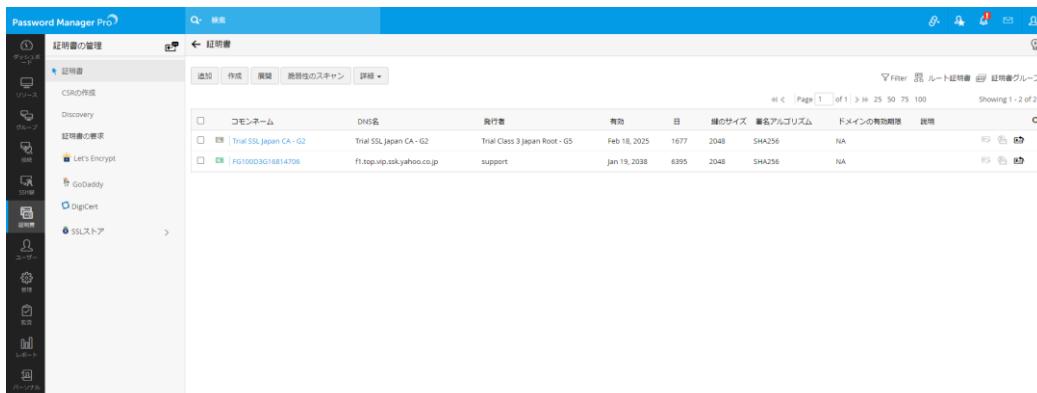


鍵名	鍵の種類	鍵の大きさ	指紋	作成者	期限
chito1	SSH-rsa	2048	SHA256:aOUT0f+e01cvfF3A5r9+PsaH2WlwBosduUGI	admin	111 days
demo1	SSH-rsa	2048	SHA256:XHB0SLH97eQKYiGK2uVscMc19GfjgSjNvWmbD3A	admin	110 days
test	SSH-rsa	2048	SHA256:Vc7yFRCB8CuzXiqCQ44VQdTVbPUQ7Mfb+r3wXU	admin	152 days
test123	SSH-rsa	2048	SHA256:3BHFFX0I3cmGUvC6p0zdBfymWCpQfQAf+28Hc84Cg	admin	133 days

SSH 鍵タブ

1.2.6 証明書タブ

SSL/TLS 証明書の管理をこちらのタブから行います。証明書の保管のみならず、既存の証明書のディスカバリー、CSR の作成、外部 CA との連携による署名等も実行できます。



コモンネーム	DNS名	発行者	有効	日	鍵のサイズ	署名アルゴリズム	ドメインの有効期限	説明
Trial SSL Japan CA - G2	Trial SSL Japan CA - G2	Trial Class 3 Japan Root - G5	Feb 18, 2025	1677	2048	SHA256	N/A	
FG10003G16814706	ft.top.ip.sks.yahoo.co.jp	support	Jan 19, 2038	6395	2048	SHA256	N/A	

証明書タブ

メモ：Password Manager Pro ではデフォルトで 25 キー分のライセンスを用意しております。SSH 鍵と証明書はそれぞれ 1 つで 1 キー分のライセンスを消費します。25 キー分以上のライセンスの追加を希望されている場合には、弊社営業部（jp-mesales@zohocorp.com）までお問い合わせください。

1.2.7 ユーザータブ

Password Manager Pro ログインするユーザーの管理をこちらのタブにて行います。各ユーザーの編集や役割の変更ができます。また Active Directory、Azure AD と連携してインポートすることもできます。

ユーザータブ

1.2.8 管理タブ

Password Manager Pro に対する各種設定を行います。このタブは原則として管理者の方のみ編集可能になります。

1. 認証

Password Manager Pro にログインする際の認証方式を強化できます。Active Directory 認証のみならず、RADIUS 認証、LDAP 認証、SAML シングルサインオン、スマートカード認証、二段階認証に対応しております。

2. リソース設定

パスワードポリシーやリソース・アカウントに関する設定を編集できます。

3. カスタマイズ

Password Manager Pro を利用するにあたって環境に即したカスタマイズ可能です。パスワードポリシー、ユーザーの役割等を編集できます。

4. セットアップ

製品全体に関わる一般的な設定はこれらから行えます。

5. SSH/SSL 変換

SSH 鍵、SSL/TLS 証明書の管理に関する設定を行えます。

6. SSL 証明書

証明書に関する設定を行えます。

7. 設定

製品のバックエンド側の設定を行えます。データベースのバックアップ、HA 構成等もこちらから確認できます。

8. 管理

本製品のセキュリティに関する設定やパスワードアクセス要求等を確認できます。

9. 連携

サードパーティ製品や他の ManageEngine 製品との連携を実施できます。

10. PMP Agents

Password Manager Pro Agent をダウンロードできます。

管理タブ

メモ：Password Manager Pro Agent を管理対象サーバーにインストールすることで https 通信によるパスワード管理が可能です。Linux サーバーに Password Manager Pro をインストールし、かつリソースとして Windows OS のパスワード管理を実施したい場合には Agent をインストールする必要があります。その他、パスワード管理に必要なポートの開放ができない場合（リソースが DMZ にある等）でもご利用可能です。

12-9 監査タブ

管理対象へのインストール状況の確認や、リモート環境へのインストール、Active Directory 環境における新規加入 PC への自動インストールなどを設定します。

監査タブ

1.2.1.0 レポートタブ

定期的にパスワードの利用状況やユーザーの活動状況をレポート化できます。また PCI DSS 等の認証機関に準拠した形式でレポートを出力することができます。クエリレポートによりカスタマイズ可能です。

レポートタブ

1.2.1.1 パーソナルタブ

Password Manager Pro ユーザー個人の情報を保管できます。デフォルトで Web アカウント情報、銀行口座、クレジットカード情報、連絡先情報を管理できます。その他のフィールドも個人でカスタマイズ可能です。

パーソナルタブ

1.2.1.2 権限毎に表示可能なタブ

権限	管理者/特権管理者	パスワード管理者	パスワード監査担当者	パスワードユーザー
ダッシュボード	○	×	○	×
リソース	○	○	○	○
グループ	○	○	×	×
接続	○	○	○	○
SSH 鍵	○	○	×	×

証明書	○	○	×	×
ユーザー	○	×	×	×
管理	○	○	×	×
監査	○	×	○	×
レポート	○	×	○	×
パーソナル	○	○	○	○

メモ：特権管理者と管理者は次の 2 点で異なります。

- 緊急対策
- IP アドレス制御

特権管理者は製品全体のセキュリティ設定に対する権限が付与されている点で管理者よりも高権限です。

1.3 製品のお問い合わせ先

評価版の使用期間 / 製品ご購入後の技術サポートは、以下のリンクよりご利用ください。

評価版サポート

<https://www.manageengine.jp/support/trial.html>

製品ご購入後のサポート

<https://www.manageengine.jp/support/purchased.html>

Password Manager Pro に関するご質問、ご購入は、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)

Web サイト: https://www.manageengine.jp/products/Password_Manager_Pro/

E-mail: jp-mesales@zohocorp.com



©ZOHO Japan Corporation. All rights reserved.