

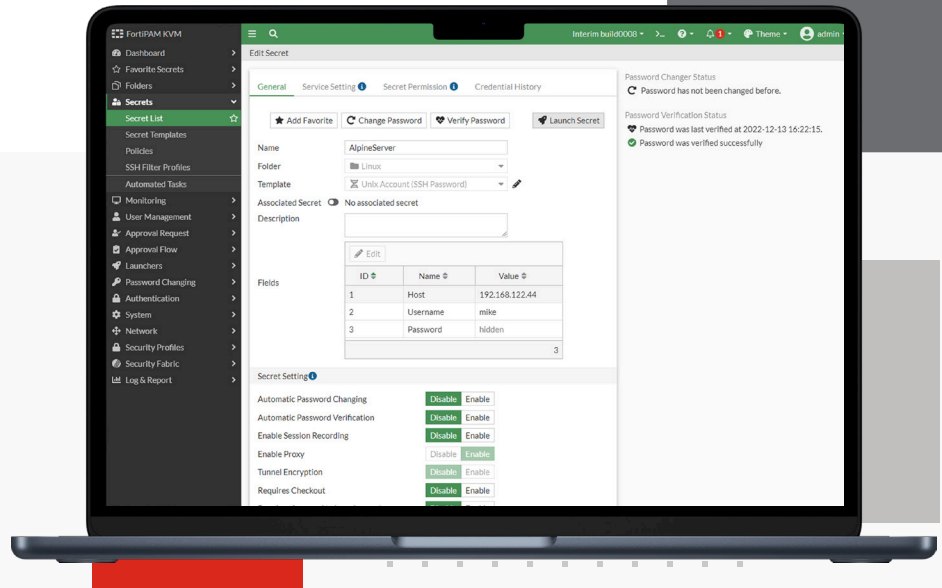
# FortiPAM

## 特権アクセスとセッションの管理

提供形態：



仮想マシン



### ハイライト

フォーティネット セキュリティ ファブリックの一部として、FortiAuthenticator、FortiToken、FortiClient と接続することで、完全な IAM ソリューションを実現

FortiClient EMS との統合により、ZTNA (ゼロトラストネットワークアクセス) の高度なアクセスのタグ付けが可能

高パフォーマンスと低遅延をビジネスクリティカルなリソースに提供

スケジュールに基づく認証情報変更が可能 (LDAPS、Samba、SSH、SSH キー)

PuTTY と RDP (FCT が必要) によるネイティブプログラムアクセスに加えて、Chrome、Firefox、Edge によるブラウザベースアクセスが可能

### アカウント認証、ユーザーアクセス、アクティビティ

特権アクセスとセッション管理により、アカウント認証情報の管理、特権ユーザーのアクセス制御、特権アカウントのアクティビティの監視を提供します。FortiPAM は、高可用性アクティブ / スタンバイ HA 機能により、アップタイムを確保します。

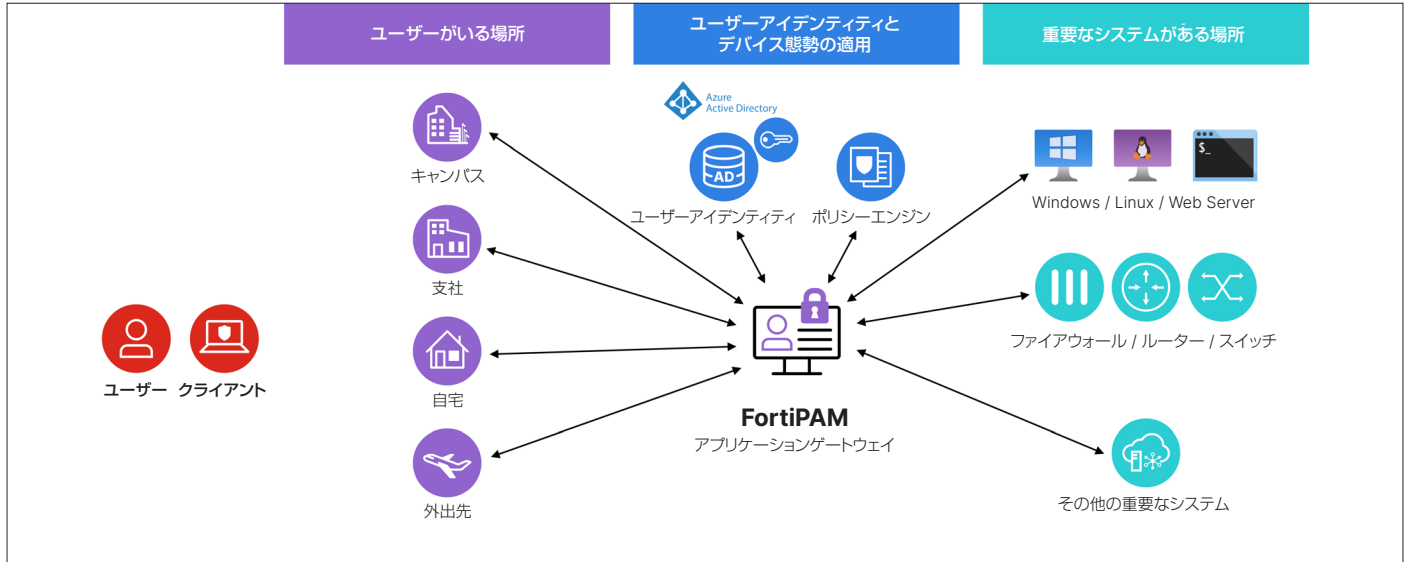
FortiPAM 特権アクセス管理は、IT 環境全体におけるユーザー、アカウント、プロセス、システム、機密データに対する昇格した特権アクセスや権限に対する制御を提供します。FortiPAM は、フォーティネットの特権アカウントと特権認証情報の厳格なセキュリティを可能にする、アイデンティティおよびアクセス管理 (IAM) ソリューションに不可欠な重要なコンポーネントです。FortiPAM は、組織内の機密度が最も高いリソースへの特権アクセスの厳格な制御を可能にし、特権アカウントのエンドツーエンドの管理、特権ユーザーのアクセス制御、監視と監査の機能を含むアカウント使用状況の可視化を実現します。これらの機能により、FortiPAM による特権アカウントへのゼロトラスト原則の導入が可能になり、組織全体の攻撃対象領域が大幅に縮小します。

IAM の近代化を目指す組織は、標準のユーザーアイデンティティだけでなく、特権アカウントの制御を PAM ソリューションという形で導入する必要があります。これらのアカウントは、機密度が最も高い情報にアクセスできるため、他より高いレベルのセキュリティが必要です。FortiPAM は、特権アカウントに関する 3 つの主なユースケースを支援します。これらのユースケースで、アカウント認証情報を管理し、特権ユーザーアクセスを制御し、特権活動を監視します。

## ハイライト

### ZTNAの要素：アクセスプロキシとしてのFortiPAM

クライアントベースの ZTNA ソリューションのコンポーネント



#### アカウント認証情報の管理

特権アカウントの管理は、特権認証情報の保管だけでなく、特権アカウントのライフサイクルの完全自動化を意味します。紐付けされていない特権アカウントの管理やそのアカウントへの最新の認証情報ポリシーの適用は、多くの組織にとって、容易なことではありません。FortiPAM は、ポリシーに基づくパスワードの自動変更を可能にすることで、特権アカウントの管理を支援します。特定のリソースの特権認証情報ポールドを FortiPAM が管理するため、リソースの認証情報をユーザーが知る必要はありません。これにより、認証情報が悪用されるリスクが少なくなります。FortiPAM はさらに、機密度の高い特権アカウント情報がエンドユーザーのデバイスにプロキシモードで配布されないようにします。

#### 特権ユーザーアクセスの制御

特権アカウントは、会社の機密度の高いリソースにアクセスが可能であるため、ゼロトラストの原則を適用する必要があります。FortiPAM は、重要なリソースへのアクセスを標準ユーザーや管理者などの役割に基づいてエンドユーザーに許可し、特権を常に最小限にすることで、これらのゼロトラストの特権アクセスを実現します。FortiPAM は、管理者が定義した中央のポリシーによる、すべてのリソースシークレットの完全制御を提供します。チェックイン後にパスワードを自動的に変更するオプションも利用できます。FortiPAM を使用して、階層型の承認システムを実装し、リスクの高いコマンドを制御することもできます。

#### 特権アクセスの監視

特権アカウントの管理と制御に加えて、これらの機密度の高いリソースを利用するユーザーを監視する機能を提供することも重要です。FortiPAM は、特権アカウントの使用状況のレポートをセキュリティインシデントの発生時に提供することができ、セッション全体のビデオ録画により、キーストロークやマウスイベントの監視を始めとする、特権アカウントにログインしているユーザーのビューを提供できます。監査目的で必要な場合は、すべての特権アカウントの使用状況に関する完全な監査追跡が可能です。

## 技術仕様

機能 / サービス	機能 / サービス
<b>ユーザー管理</b>	<b>ランチャー</b>
ローカルユーザー	PuTTY (FCT が必要)
リモート認証: LDAP サーバー	リモートデスク: Windows (FCT が必要)
リモート認証: Radius サーバー	Web ランチャー
SAML	Web SSH
多要素認証: FortiToken	Web RDP
多要素認証: E メールトークン	Web VNC
多要素認証: SMS トークン	VNC Viewer (FCT が必要)
管理者ロールの管理	Tight VNC (FCT が必要)
ユーザーグループ	カスタムランチャー
API ユーザー	<b>シークレットリクエストの承認</b>
ユーザートラステッドホスト	承認プロファイル (3 層まで)
FortiToken Cloud	リクエストのレビューと承認
<b>秘密フォルダー</b>	リクエストの通知
公開フォルダー	複数の承認が必要
個人フォルダー	スクリプト
フォルダーの権限の制御	<b>パスワードチェンジャー</b>
シークレットポリシーの管理	パスワードポリシー
<b>シークレットテンプレートとアクセス</b>	カスタムパスワードチェンジャー
Unix SSH (パスワードまたはキー)	<b>監視と記録</b>
Windows ドメインアカウント (LDAPS または Samba)	ユーザーの監視
テンプレート: FortiGate	アクティブセッションの監視
テンプレート: Cisco デバイス	セッションの記録
テンプレート: Web アカウント	<b>ログと監査</b>
テンプレート: マシン	イベント: システム
カスタムテンプレート	イベント: ユーザー
<b>シークレット</b>	イベント: HA
シークレットのチェックアウト / チェックイン	ログ: シークレット
シークレットのチェックアウトを更新	ログ: ビデオ (録画と再生)
承認リクエスト	<b>システム</b>
パスワードの検証	HA
定期パスワードチェンジャー	ガラスの突破
パスワードハートビート	メンテナンスモード
ビデオ録画	構成の自動バックアップ
SSH フィルター	ランチャーセッションの最長時間
ネイティブランチャーでの自動パスワード配布	vTPM: KVM
ネイティブランチャーでの Cisco デバイス自動有効化	vTPM: VMware
連携シークレットランチャー	FortiClient: カスタム FCT FortiVRS (ビデオ録画デーモン) ポート
連携シークレットパスワードチェンジャー	高可用性
ネイティブランチャーでの SSH キーボードインタラクティブ認証	ディザスタリカバリのサポート
RDP セキュリティレベル	<b>認証</b>
RDP クリップボードのブロック	アドレス (AD ターゲット制限で使用)
AD ターゲット制限	スキームとルール
シークレットの移動 / クローニング	<b>安定性</b>
シークレット権限制御	ロングセッション
お気に入りのシークレット	ストレステスト (過負荷、CPU が 70%)
	<b>インストール</b>
	アップグレード
	インストール / 管理ガイド

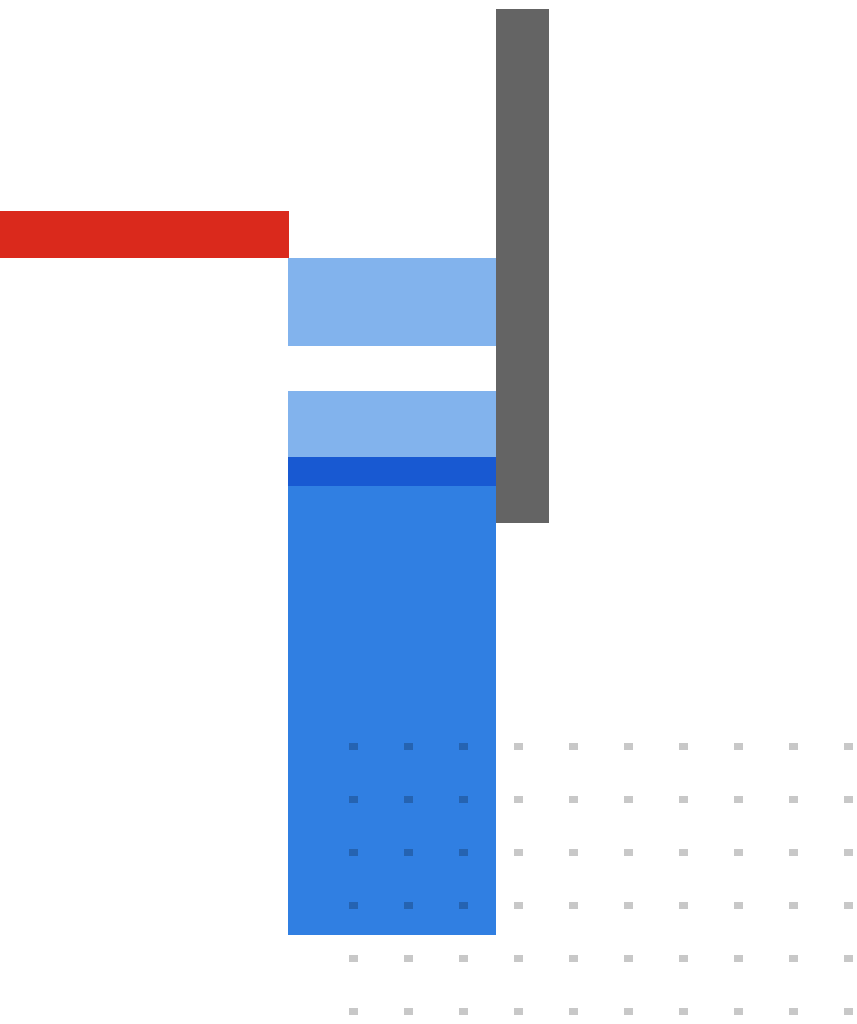


## 技術仕様

機能 / サービス
<b>セキュリティ</b>
ターゲットサーバーや PAM サーバーに対する ZTNA タグエンドポイント制御
ローカル PAM ユーザー、リモート SAML、Radius、LDAP ユーザーに対する二要素認証
Web ベースファイル転送 (Web SFTP、Web SAMBA) や SCP ベースファイル転送のアンチウイルススキャン
SSH フィルタリングプロファイルによる危険なコマンドの自動ブロック
IP やスケジュールに基づくユーザーアクセス制御
シークレットアクセスのリクエスト / 承認
シークレットチェックアウト / チェックイン保護
チェックイン後の自動パスワード変更
スケジュールに基づくパスワードの変更
強度の高い SSH 暗号化アルゴリズム
CredSSP、TLS を含む高度 RDP 認証プロトコル
ロールベースのアクセス制御
ポリシーベースのアクセスプロファイル適用
トラステッドプラットフォームモジュールによるユーザー秘密鍵の保護

## オーダー情報

Product	SKU	Description
FortiPAM-VM	FC1-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 5 to 9 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC2-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 10 to 24 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC3-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 25 to 49 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC4-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 50 to 99 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC5-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for between 100 to 249 users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
	FC6-10-PAVUL-591-02-DD	Subscription for one FortiPAM Virtual Machine seat for 250 or more users. Includes FortiClient VRS agent for FPAM. Includes 24/7 FortiCare support. HA requires additional license for an additional unit with the same user seats license on the backup unit.
FortiPAM License Options		Licensed FortiClient with PAM function activated. This is the recommended deployment as additional SSL VPN, ZTNA, SSOMA functions can also be activated. This uses the existing EMS licenses - no additional license required.
		Dedicated unlicensed standalone FortiClient with PAM function which does not require EMS. This standalone FortiClient can not be combined with other FCT standalone versions and can only be used for FortiPAM.



**FORTINET**

フォーティネットジャパン合同会社

〒106-0032

東京都港区六本木 7-7-7 Tri-Seven Roppongi 9 階

[www.fortinet.com/jp/contact](http://www.fortinet.com/jp/contact)

お問い合わせ