DATA SHEET

FortiAuthenticator

提供形態：

アプライアンス　仮想マシン　ホスティング　クラウド

ユーザーのアイデンティティ管理とシングルサインオン機能を提供

企業ネットワークにおけるアイデンティティポリシー

ネットワークおよびインターネットへのアクセスは、今や企業内のほぼすべての業務において必要不可欠になっています。しかしながら、個々の従業員のアクセス要件を設定するには、それによってもたらされるリスクとのバランスを考慮しなければなりません。すべての企業は、セキュリティ面で妥協することなく、安全にコントロールされた環境下で、業務上アクセスが必要な従業員に対して適切なタイミングで適切なアクセスを許可することを最大の目標にしています。

Fortinet Single Sign-On（FSSO）は、フォーティネット製品で接続されたネットワークに対してアイデンティティベースおよびロールベースのセキュアなアクセスを可能にする認証メソッドです。既存の Active Directory や LDAP 認証システムと統合することで、ユーザーの生産性を低下させたりネットワーク管理者の作業負荷を高めることなく、企業においてユーザーのアイデンティティベースの確実なセキュリティを実現します。

FortiAuthenticator は、セキュアな Fortinet Single Sign-on 認証システムを基盤としており、幅広いユーザー識別メソッドに対応するとともに高度な拡張性を備えています。FortiAuthenticator は、フォーティネット製品で保護されている企業ネットワークへのアクセスを許可するゲートキーパーとして機能し、ユーザーの識別やサードパーティ製システムからのアクセス許可の照会を実行するほか、このような情報を FortiGate デバイスと交信してアンデンティティベースのポリシー実施に活用することができます。

FortiAuthenticator は、次のような幅広いメソッドを用いてトランスペアレントなユーザー識別を実現します。

- Active Directory ドメインコントローラのポーリング
- ログイン、IP アドレスの変更、およびログアウトを検出する FortiAuthenticator Single Sign-On Mobility Agent との統合
- 認証の反復実行を不要にする、追跡ウィジェットを利用した FSSO ポータルベースの認証
- RADIUS アカウンティングの開始記録の監視

FSSO の特長

- Active Directory との統合により、フォーティネット製品で保護されている企業ネットワークにおいて他の認証機能を追加することなくアイデンティティベースおよびロールベースのセキュリティポリシーを実施可能
- ユーザーのアイデンティティ情報の管理と保管を簡素化および一元化することで、企業のセキュリティを強化
- セキュアな多要素 / OTP 認証と FortiToken の完全サポート
- RADIUS および LDAP 認証に対応
- 企業の VPN 導入における証明書の管理機能
- IEEE802.1X に対応し、無線 / 有線ネットワークのセキュリティを確保
- SAML SP/IdP Web SSO
- FIDO2 の特徴：パスワードレス認証として知られ、強力な単一要素（パスワードレス）、二要素、多要素での認証を使用して保護を強化する、もう 1 つ強力な認証手法

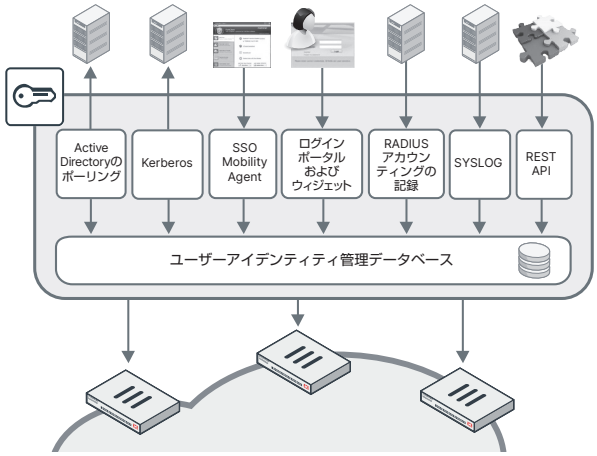
ハイライト

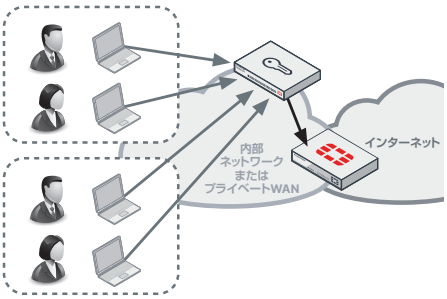
主な機能と特長

FSSO によるトランスペアレントなユーザー識別機能	企業ユーザーの生産性を低下させることが一切ありません。
LDAP および AD との統合によるグループメンバーシップの活用	既存システムを活用してネットワーク認証情報を管理することで、導入に要する時間が短縮されるとともに効率的な管理プロセスが実現します。現行のユーザー管理手順との容易な統合が可能です。
幅広いユーザー識別メソッドに対応	幅広いユーザー識別メソッドに対応しており、極めて多様性に富んだ企業環境との柔軟な統合が可能です。
アイデンティティベースおよびロールベースの確実なセキュリティを実現	セキュリティ管理者は、ユーザーの業務に応じて必要なネットワークおよびアプリケーション/リソースへのアクセスを適切に許可することが可能になると同時に、アクセスをコントロールしてリスクを最小限に抑えることができます。

FortiAuthenticator Single Sign-On ユーザー識別メソッド

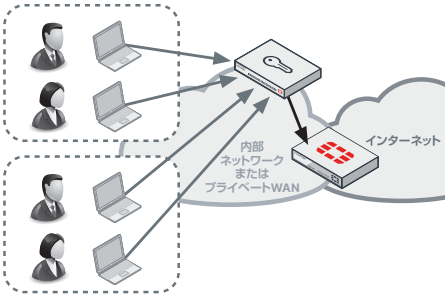
FortiAuthenticator は、さまざまなメソッドによるユーザーの識別に対応し、サードパーティ製の LDAP や Active Directory システムと統合することができます。これにより、グループやロールのデータをユーザーに適用し、FortiGate と交信してアンデンティティベースのポリシー実施に活用することが可能です。FortiAuthenticator は極めて高い柔軟性を備えており、さまざまなユーザー識別メソッドを組み合わせて利用することができます。大規模企業のお客様向けの例としては、トランスペアレントな認証を可能にするメインのメソッドとして AD ポーリングや FortiAuthenticator SSO Mobility Agent を選択し、非ドメインシステムやゲストユーザー向けには機能制限されたポータルの活用が可能です。





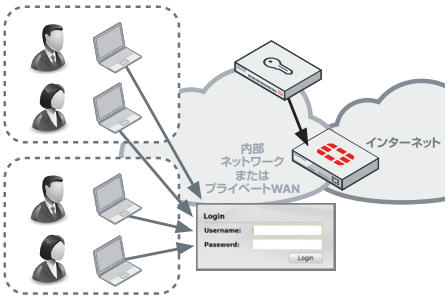
Active Directory のポーリング

Active Directory に対するユーザー認証は、ドメインコントローラの定期的なポーリングによって検出されます。ユーザーがログインしたことが検出されると、ユーザー名、IP、およびグループの詳細情報が FortiAuthenticator のユーザーアイデンティティ管理データベースに格納されます。この情報は、ローカルポリシーに基づいて複数の FortiGate デバイス間で共有されます。



FortiAuthenticator SSO Mobility Agent

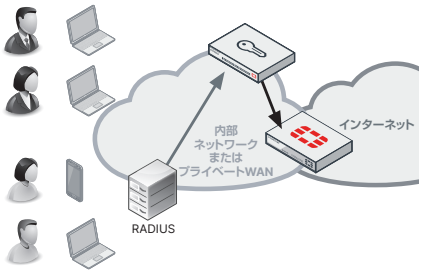
ドメイン構造が複雑に分散されているためにドメインコントローラのポーリングが難しい場合は、FortiAuthenticator SSO Client を利用することが可能です。FortiClient の一部あるいは Windows PC 向けのスタンドアロンアプリケーションとして提供されているこのクライアントは、ログイン、IP スタックの変更（有線から無線への変更、無線ネットワークローミング）、およびログアウトの各イベントを FortiAuthenticator に通知します。これにより、ポーリングが不要になります。



FortiAuthenticator ポータルおよびウィジェット

AD ポーリングがサポートされていないシステムやクライアントを実行できないシステムの場合は、FortiAuthenticator の明示的な認証ポータルを利用することができます。このポータルでは、ユーザー自身が手動で FortiAuthenticator へのアクセス、続いてネットワークへのアクセス認証を実行可能です。手動による認証ではログイン操作を繰り返す必要がありますが、その作業負荷を最小限に抑えるため、ユーザーがイントラネットのホームページにアクセスする時にブラウザの Cookie を使用した自動ログインを許可している企業イントラネットに組み込むことが可能なウィジェット群も用意されています。

ハイライト



RADIUS アカウンティングを利用したログイン機能

RADIUS 認証（無線、VPN 認証など）を使用しているネットワークの場合は、ユーザー識別メソッドとして RADIUS アカウンティングを使用することができます。この情報は、ユーザーログインのトリガーや IP 情報とグループ情報の提供に使用されるため、二次的な認証が不要になります。

その他の機能

多要素認証による確実なユーザー識別機能

FortiAuthenticator を使用することで、複数の FortiGate アプライアンス、さらには RADIUS や LDAP 認証に対応しているサードパーティ製ソリューションでも多要素認証機能を利用できるようになります。FortiAuthenticator から取得したユーザーアイデンティティ情報と FortiToken や他の FIDO2 認証サービスから取得した認証情報を併用することにより、企業内の機密情報へのアクセスを承認されたユーザーのみに確実に制限可能になります。この強力なセキュリティレイヤーが追加されることで、企業におけるデータ漏洩のリスクが大きく低下すると同時に、プライバシーに関する法規制や企業規定に基づく監査要件を満たすことが可能になります。

FortiAuthenticator は、FIDO2 パスワードレス認証サービスを含む、可能な限り幅広い多要素認証を提供し、お客様の要件への柔軟な対応が可能です。FortiAuthenticator では、物理的な時間ベースの FortiToken 200、FortiToken Mobile（iOS、Android、Windows 向け）、E メール / SMS OTP、FIDO2 など、あらゆるユーザーや利用シナリオ向けに強力な認証オプションを提供しています。

多要素認証を利用して、FortiGate の管理、SSL と IPsec VPN、無線キャプティブポータルでのログイン、サードパーティ製の RADIUS 対応ネットワーク機器、SAML サービスプロバイダーなどのアプリケーションへのアクセスをコントロールすることが可能です。また、FortiAuthenticator は、任意の Web ベースのアプリケーションに MFA を追加するために使用できる REST API を提供しています。

FortiAuthenticator は、ユーザー自身による登録機能とパスワード復旧機能を備えており、ローカルユーザーの管理が効率化されます。

証明書ベースの企業 VPN のサポート

サイト間 VPN では、大抵の場合さまざまなリモート環境から企業ネットワークの中心部に直接アクセスすることが許可されています。このような VPN は、事前共有キーによるシンプルなセキュリティ対策が行われていることが多いため、共有キーが漏洩してしまった場合ネットワーク全体にアクセスされてしまう危険性があります。FortiOS は証明書ベースの VPN をサポートしていますが、証明書で保護されている VPN を利用している企業は一部にとどまっています。その最大の原因として挙げられるのは、証明書の管理が複雑であること、そしてそのコストです。これに対し、FortiAuthenticator は FortiManager との連携によって容易な構成が可能であると同時に、SCEP プロトコル経由でのセキュアな証明書デリバリが自動化されることで、FortiGate 環境下の VPN で使用される大量の証明書の導入作業が効率化され、管理コストが不要になります。

クライアントベースの証明書を利用する VPN の場合は、FortiToken 300 USB Certificate ストアで証明書の作成および保管が可能です。PIN で保護されているこのセキュアな証明書ストアは FortiClient との互換性があり、FortiAuthenticator との併用によってクライアントの VPN 接続のセキュリティが強化されます。

その他の機能と特長

RADIUS および LDAP によるユーザー認証	RADIUS および LDAP のインタフェースによるローカル認証データベースを使用して、ユーザーの一元管理が可能になります。
幅広い強力な認証メソッドに対応	ソフトウェアおよびハードウェアのワンタイムパスワード（OTP）トークン、E メールや SMS の OTP、デジタル証明書、FIDO キーを使用した FortiAuthenticator の強力な認証機能を使用することで、パスワードによるセキュリティが大幅に強化され、パスワードの漏洩、MITM、フィッシング、リプレイ攻撃、ブルートフォース攻撃などのリスクが軽減します。
ユーザー自身による登録機能とパスワード復旧機能	ユーザー自身による登録やパスワードに関する問題の解決が可能になることで、管理者の業務負荷が軽減し、ユーザーの満足度や生産性も向上します。
Active Directory および LDAP との統合	既存のディレクトリサービスとの統合が可能なため、導入の簡素化とインストールの所要時間短縮が実現すると同時に、既存環境の効率的な再利用も可能になります。
証明書の管理	証明書管理が効率化されることにより、VPN などの証明書ベースの認証システムの迅速な導入とコスト効果の向上が実現します。
802.1X 認証	ユーザーの LAN および無線 LAN への接続の正当性を確認するエンタープライズクラスのポートコントロール機能により、ネットワークへの不正アクセスを防止します。

技術仕様

	FortiAuthenticator 300F	FortiAuthenticator 800F
インタフェースとモジュール		
10 / 100 / 1000 インタフェース（カッパー、RJ45）	4	4
GbE SFP インタフェース	—	2
内蔵ストレージ	2 × 1 TB	2 × 2 TB
トラステッドプラットフォームモジュール（TPM）	○	○
電源装置	300 W 冗長オートレンジ（100 V ～ 240 V）、オプション冗長電源（1 + 1）	冗長（1 + 1）300 W 冗長オートレンジ（100 V ～ 240 V）
システム性能		
ローカル + リモートユーザー（ベース / 上限）	1,500 / 3,500	8,000 / 18,000
FortiToken サポート数	3,000	16,000
RADIUS クライアント（NAS デバイス）	500	2,666
ユーザーグループ	150	800
CA 証明書サポート数	10	50
クライアント証明書サポート数	7,500	40,000
サイズ		
高さ x 幅 x 奥行	44 × 438 × 422 mm	44 × 438 × 701.2 mm
重量	8.2 kg	15.0 kg
動作環境		
形状	ラックマウント（1 RU）	ラックマウント（1 RU）
電源	100 ～ 240 V AC、50 ～ 60 Hz 300 W、冗長電源（1 + 0）	100 ～ 240 V AC、50 ～ 60 Hz
最大電流	5 A / 100 V、2.5 A / 240 V	5 A / 100 V、2.5 A / 240 V
消費電力（平均 / 最大）	82.35 W / 131.23 W	154 W / 196.04 W
放熱	482 BTU/h	703 BTU/h
エアフロー	前面 ～ 背面	前面 ～ 背面
動作温度	0 ～ 40 ºC	0 ～ 40 ºC
保管温度	-20 ºC ～ 70 ºC	-20 ºC ～ 70 ºC
湿度	5 ～ 90%（結露しないこと）	5 ～ 95%（結露しないこと）
システム仕様		
サポートする標準	10 / 100 / 1000 Base-TX（GbE）、IP、Telnet、HTTP 1.0 / 1.1、SSL、RS232、NTP クライアント（RFC1305）、RADIUS（RFC2865）、LDAP（RFC4510）、x.509（RFC5280）、証明書失効（RFC3280）、PKCS#12 証明書インポート、PKCS#10 CSR インポート（RFC2986）、Online Certificate Status Protocol（RFC 2560）、EAP-TLS（RFC2716）、Simple Certificate Enrollment Protocol（SCEP）、oAuth、OIDC、SAML2.0	
管理	CLI、Direct Console DB9 CLI、HTTPS	
高可用性	アクティブ / パッシブ高可用性および構成同期機能による高可用性	
準拠規格・認定		
準拠規格	FCC Part 15 Class A、RCM、VCCI、CE、UL / cUL、CB	FCC Part 15 Class A、RCM、VCCI、CE、BSMI、KC、UL / cUL、CB、GOST

FortiAuthenticator 300F

FortiAuthenticator 800F

技術仕様

	FortiAuthenticator 3000F
インタフェースとモジュール	
10 / 100 / 1000 インタフェース（カッパー、RJ45）	4
GbE SFP インタフェース	2
内蔵ストレージ	2 × 2 TB SAS
トラステッドプラットフォームモジュール（TPM）	—
電源装置	冗長（1 + 1）1000 W オートレンジ（100 V ～ 240 V）
システム性能	
ローカル + リモートユーザー（ベース / 上限）	40,000 / 240,000
FortiToken サポート数	480,000
RADIUS クライアント（NAS デバイス）	80,000
ユーザーグループ	24,000
CA 証明書サポート数	300
クライアント証明書サポート数	1,200,000
サイズ	
高さ x 幅 x 奥行	88 × 438 × 601 mm
重量	20 kg
動作環境	
形状	ラックマウント（2 RU）
電源	100 ～ 240 V AC、50 ～ 60 Hz
最大電流	100 ～ 127 / 200 ～ 240 VAC、50 / 60 Hz、10 / 5 A
消費電力（平均 / 最大）	193.30 W / 236.28 W
放熱	1325 BTU/h
エアフロー	前面 ～ 背面
騒音レベル	49.8 db
動作温度	0 ～ 40 ºC
保管温度	-40 ～ 70 ºC
湿度	5 ～ 90%（結露しないこと）
システム仕様	
サポートする標準	10 / 100 / 1000 Base-TX（GbE）、IP、Telnet、HTTP 1.0 / 1.1、SSL、RS232、NTP クライアント（RFC1305）、RADIUS（RFC2865）、LDAP（RFC4510）、x.509（RFC5280）、証明書失効（RFC3280）、PKCS#12 証明書インポート、PKCS#10 CSR インポート（RFC2986）、Online Certificate Status Protocol（RFC 2560）、EAP-TLS（RFC2716）、Simple Certificate Enrollment Protocol（SCEP）、oAuth、OIDC、SAML2.0
管理	CLI、Direct Console DB9 CLI、HTTPS
高可用性	アクティブ / パッシブ高可用性および構成同期機能による高可用性
準拠規格・認定	
準拠規格	FCC Part 15 Class A、RCM、VCCI、CE、BSMI、KC、UL / cUL、CB、GOST

FortiAuthenticator 3000F

技術仕様

FortiAuthenticator仮想アプライアンス

仮想アプライアンス	FortiAuthenticator VM Base	FortiAuthenticator VM-100-UG	FortiAuthenticator VM-1000-UG	FortiAuthenticator VM-10000-UG
システム性能				
ユーザー数（ローカル / リモート）	100	+100	+1,000	+10,000
FortiToken サポート数	200	+200	+2,000	+20,000
NAS デバイス	33	+33	+333	+3,333
ユーザーグループ	10	+10	+100	+1,000
CA 証明書サポート数	5	+5	+50	+500
クライアント証明書サポート数	100	+500	+5,000	+50,000
仮想マシン				
サポートするハイパーバイザー	VMware ESXi / ESX 6 / 7 / 8、Microsoft Hyper-V Server 2010、2012 R2、および 2016、 Nutanix AHV（Acropolis Hypervisor）、KVM、Xen、Microsoft Azure、AWS、Oracle OCI、Alibaba Cloud			
仮想 CPU 数（最大）	64			
仮想 NIC 数（最小 / 最大）	1 / 4			
ストレージ容量（最小 / 最大）	60 GB / 16 TB			
メモリ（最小 / 最大）	2 GB / 1 TB			
高可用性（HA）	アクティブ / パッシブ高可用性および構成同期機能による高可用性			

オーダー情報

Product	SKU	Description
FortiAuthenticator 300F		4x GE RJ45 ports, 2× 1 TB HDD. Base License supports up to 1500 users. Expand user support to 3500 users by using FortiAuthenticator Hardware Upgrade License.
FortiAuthenticator 800F		4x GE RJ45 ports, 2x GE SFP, 2× 2 TB HDD. Base License supports up to 8000 users. Expand user support to 18 000 users by using FortiAuthenticator Hardware Upgrade License.
FortiAuthenticator 3000F		4x GE RJ45 ports, 2× 10GE SPF, 2× 2TB SAS Drive. Base License supports up to 40 000 users. Expand user support to 240 000 users by using FortiAuthenticator Hardware Upgrade License
FortiAuthenticator-VM License	FAC-VM-Base	VM Base License supports 100 users. Expand user support to 1 million plus users by using FortiAuthenticator VM Upgrade License.
	FAC-VM-100-UG	FortiAuthenticator-VM 100 user license upgrade.
	FAC-VM-1000-UG	FortiAuthenticator-VM 1000 user license upgrade.
	FAC-VM-10000-UG	FortiAuthenticator-VM 10 000 user license upgrade.
	FC1-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–500 users).
	FC2-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–1100 users).
	FC3-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–5100 users).
	FC4-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–10 100 users).
	FC8-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–25 100 users).
	FC5-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–50 100 users).
	FC6-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–100 100 users).
	FC9-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–500 100 users).
	FC7-10-0ACVM-248-02-12	1 Year 24×7 FortiCare Contract (1–1M users).
FortiClient SSO License for FortiAuthenticator	FCC-FAC2K-LIC	FortiAuthenticator FortiClient SSO Mobility Agent License for 2000 FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate)
	FCC-FAC10K-LIC	FortiAuthenticator FortiClient SSO Mobility Agent License for 10 000 FortiClient connections (does not include FortiClient Endpoint Control License for FortiGate)
	FCC-FACUNL-LIC	FortiAuthenticator FortiClient SSO Mobility Agent License for unlimited FortiClient connections(does not include FortiClient Endpoint Control License for FortiGate)
Hardware Upgrade Licenses for FAC-300F, FAC-800F, and FAC-3000F	FAC-HW-100UG	FortiAuthenticator 300F, 800F, 3000E, or 3000F, 100 user upgrade
	FAC-HW-1000UG	FortiAuthenticator 300F, 800F, 3000E, or 3000F, 1000 user upgrade
	FAC-HW-10KUG	FortiAuthenticator 800F, 3000E, or 3000F, 10 000 user upgrade
	FAC-HW-100KUG	FortiAuthenticator 3000F, 100 000 user upgrade
Optional Accessories		
Power Supplies	SP-FML900F-PS	AC power supply for FAC-300F.
	SP-FML900F-PS	AC power supply for FAC-800F.

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

お問い合わせ