Entrust
Identity
Essentials

ゼロトラスト フレームワークを実現

Windows ベースの環境向けのトップクラスの MFA および VPN 保護から、オンプレミスまたはクラウドにデプロイできる高アシュアランスな認証情報ベースのパスワードレス認証まで、様々な IAM ソリューションをカバーしているのが Entrust Identity です。

ENTRUST

IDENTITY
ESSENTIALS

概要

ID - 基本

Identity Essentials は、従業員の ID を保護しつつ、リモートワークを実現するために、高速かつコスト効率に優れたサービスを求めている企業にとって理想的な多要素認証 (MFA) ソリューションです。Identity Essentials により、使いやすく、オンプレミスで簡単にデプロイできる MFA ソリューションから使用し始め、また、必要に応じて後から Identity as aService によりを使用してクラウドに移行できるようになります。Identity Essentials および Identityas a Service はシームレスに統合できるため、次のような 3 つの認証オプションを活用しつつ、手間なくハイブリッド環境を確保できます。

- デバイスのフィンガープリント認証
- モバイル プッシュ認証
- グリッド カード認証

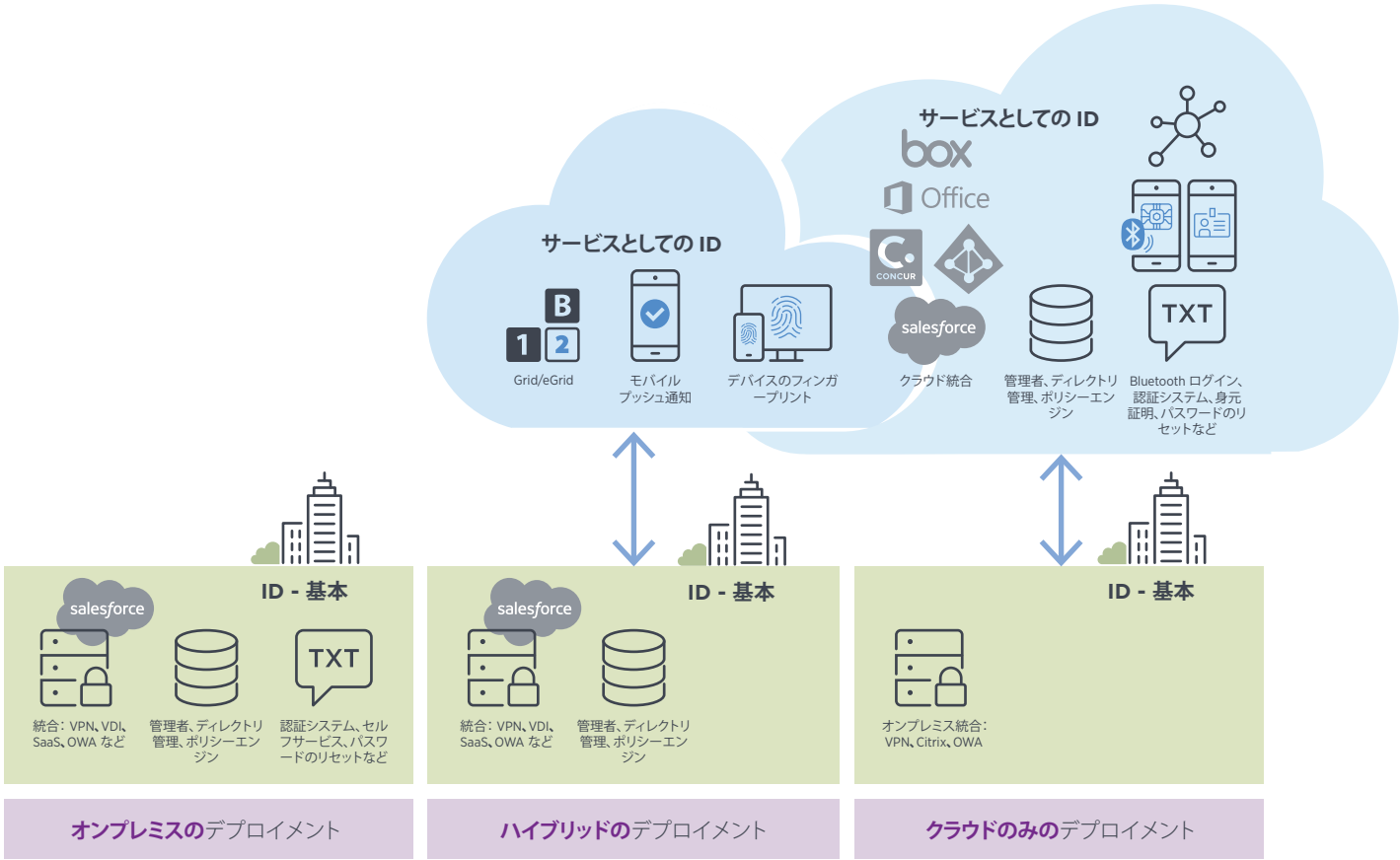
Identity Essentials は、Windows ベースの組織が Identity as a Service を使用してゼロトラスト アプローチを継続的に実現できる基盤を構築します。

仕組み

優れたテクノロジーで大きな脅威に対処

ハッカーが従業員のパスワードを取得すると、従業員がアクセス権限を持つクラウド上やオンプレミスのあらゆるデータを悪用できるようになります。また、大抵の組織ではファイル システム、イントラネット、コラボレーション サイトなどでクラウドサービスを使用する頻度が増えているため、脅威にさらされるデータも増えています。しかし幸いなことに、ユーザーも管理者も、強力なユーザー認証を簡単に使用できるようになっています。さらに、Identity Essentials および Identity as a Service を統合することで、パスワードレス ログインやスマートログインを使用して Windows 7、8、10 や MacOS にログインすれば、クラウドをフルに利用できるようになります。

Identity as a Service とシームレスに統合できる Identity Essentials を使用すれば、クラウドをフルに利用できるようになります。*



*サブスクリプション ライセンスを持つ Identity Essentials のお客様のみ。

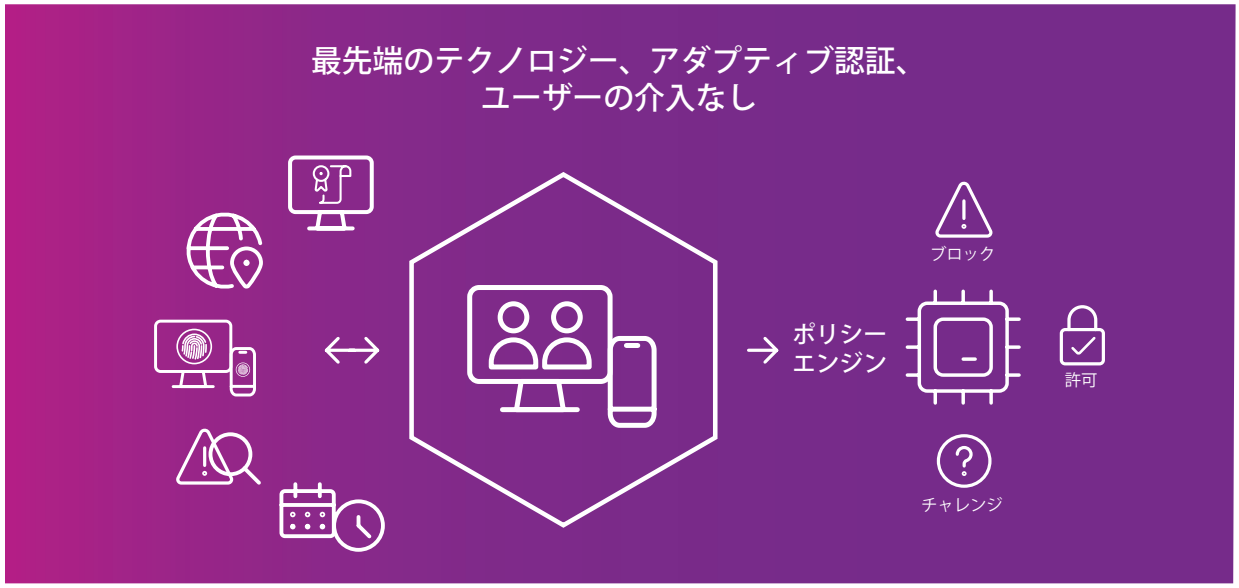
ライセンス オプション：含まれているもの*

サブスクリプション バンドルを選択した企業は、Identity Essentials と Identity as a Service の強固な統合による利点をフル活用できます。

	ソフトウェア アシュアランス	サブスクリプション バンドル
Identity Essentials の拡張機能	●	●
Windows Server 2019 のサポート	●	●
AD FS を伴うデバイスのフィンガープリント（Identity as a Service）	●	●
プッシュ認証（Identity as a Service）	●	●
Office365 およびオンプレミスの Exchange に使用する ActiveSync デバイス プロビジョニング	●	●
リスクエンジン、クラウド間認証などが含まれた Identity as a Service「Plus」		●
グローバル SMS、アプリベースおよび音声ベースの OTP 配信サービス		●
あらゆるクラウド サービスを一元的に保護する Identity as a Service シングル サインオン ポータル		●
Identity Essentials のサポート、営業時間中（延長可能）		●
グリッド カードのサポート	●	●
Windows ログオンコンソール認証の拡張機能	●	●

*Identity Smart Login は、追加料金がかかるアドオン機能です。

Entrust Identity のアダプティブ リスクベース エンジンを使用すれば、従業員が新しいデバイスを使って初めてログインする際や、平常時以外の時刻、別の場所からログインする際など、状況に応じてセキュリティをさらに強化できます。このような場合、モバイル プッシュ通知のような追加認証のみを要求することで、従業員の手間を最小限に抑えつつ、企業のリソースを保護することができるようになります。



様々な認証システムをサポート

Identity Essentials では、複数の認証方式を選択できます。アクセスするアセット、使用するデバイス、ユーザーの技術的なスキルなど、様々な要因に合わせて異なる認証方法を選択することをお勧めします。

Identity as a Service を統合することで 3 つの最新機能（以下に列挙）をすべて利用できるようになり、従業員はワークステーション、ネットワーク、アプリケーションに安全にアクセスできるようになります。パスワードを入力したり、セッションごとに従来型の 2 要素認証を使用したりする手間がなくなります。完全にパスワードレスのログインにより、一切の手間を省きつつ安全にログインできるようになります。

Identity Essentials 認証システム

プラス 3 つの認証機能
Identity as a service を使用

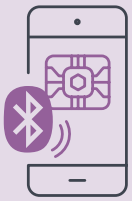
デバイスのフィンガープリント認証

AD FS を通じてクラウド アプリにアクセスする際、新しいデバイスのフィンガープリントをキャプチャして、以前に使用したデバイスを自動的に検出できます。これにより、セキュリティをさらに強化しつつ、ワンタイム パスコード（OTP）を省略できます。

Identity as a Service のリスク エンジンを使用する場合は、位置情報、IP アドレス、ログイン時間、移動速度などとともに、これを判断材料に加えることもできます。

モバイルプッシュ認証

従業員が平常時以外の時間・場所からログインする場合には、セキュリティのレベルを上げます。製品に合わせてカスタマイズできるプッシュ認証アプリを使用すれば、端末に搭載されたモバイル生体認証による保護を利用できるため、不正なアクセスを防止できます。このアプリには Confirm（確認）、Deny（拒否）、Concern（懸念事項）ボタンがあり、Concern（懸念事項）を押すと懸念事項が記録され、レポートが管理者に送信されます。



パスワードレス認証

グリッド カード認証を組織に導入すれば、シンプルでありながら効果的かつ強力な認証ツールにより、セキュリティおよび論理的なアクセス制御を強化できます。制限されたネットワーク、アプリケーション、クラウド サービス、サイトにログインしようとするユーザーに対して、認証チャレンジが表示されます。各グリッド カードは固有のものであり、シリアル番号が付いているため、すべてのユーザーを一意に識別して認証できます。ユーザーが認証するたびに異なるチャレンジが表示され、毎回異なるグリッド座標を通じて本人確認を行うよう求められます。認証チャレンジごとに、座標リクエストが変化します。

デバイスのフィンガープリント認証：安全かつ簡単にログイン

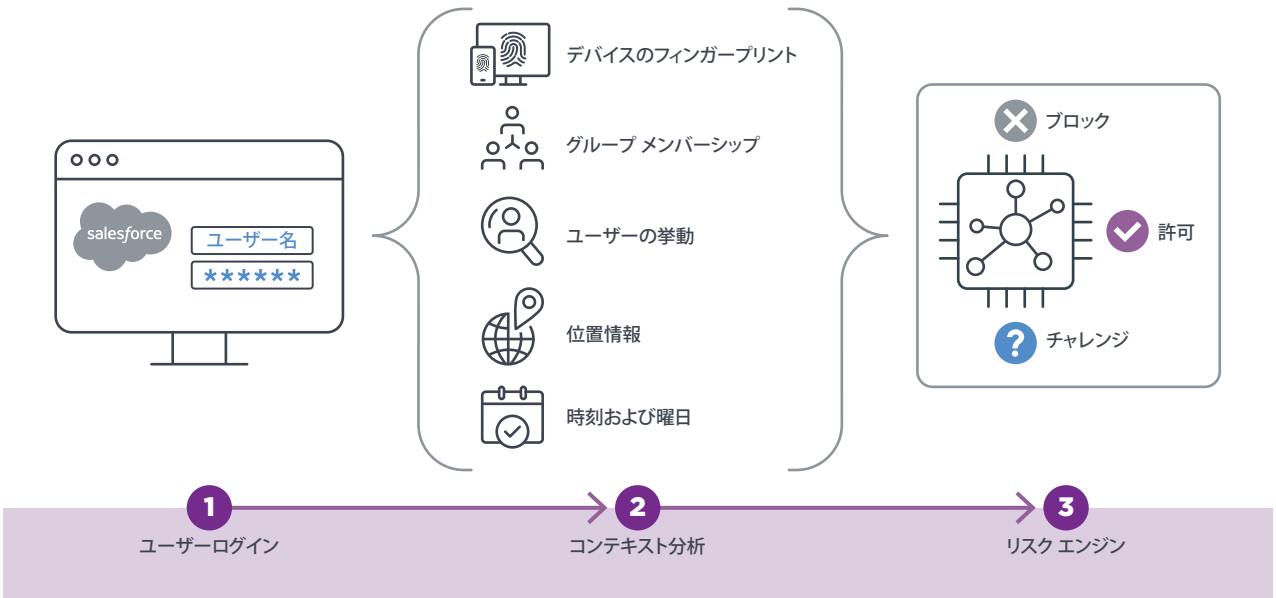
セキュリティ侵害の 80% 以上が、強力でない認証情報を使用したり、認証情報を盗まれたりしたことが原因で発生しています。すべてのサービスに MFA を追加してハッカーの攻撃から守ることで、セキュリティが大幅に向上します。

反発するユーザーがいる場合は、当社のアダプティブ/コンテキストベースのインテリジェンス機能をご確認ください。何千もの組織がすでにこの機能を使ってユーザー エクスペリエンスを向上させています。

例えばユーザーが VPN、Citrix、RDP、クラウドサービスのうちどのサービスを介してログインしているかどうかに関係なく、コンテキストに応じてログインを許可できるアダプティブ認証の先駆けとなったのがIdentity Essentials です。

最新の追加機能であるデバイス フィンガープリントを使用すれば、認証 Cookie よりも安全に、以前ログインで使用したマシンを検証することができます。

デバイスのフィンガープリント認証 – Identity as a Service を使用

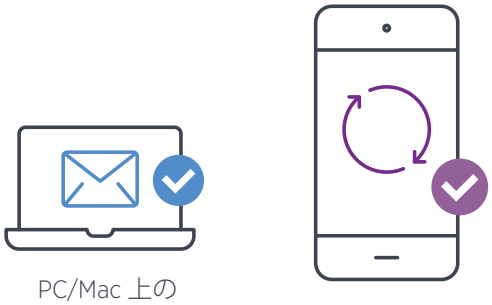


Identity Essentials は、コンテキストデータとユーザーの行動に基づいてリアルタイムにリスクを検出する、構成しやすい Identity as a Service のエンジンを活用することで、何度もログインするという手間をなくします。

ActiveSync 保護：モバイル機器の管理が不要に

ActiveSync – 見過ごされがちですが、E メールや連絡先などを簡単に同期するために使用するプロトコルにより、セキュリティ リスクが発生します。ユーザーが E メールアドレスおよびパスワードだけを使用して重要な情報に簡単にアクセスできる場合、ハッカーにとっても同じことになります。また、OWA/Office365 を MFA で保護する場合、ActiveSync が欠かせません。

主に 3 つの方法で OFFICE 365/OWA
のコンテンツにアクセス可能



PC/Mac 上の
Outlook クライアント
E メールに使った時間のうち 50%

iPhone/Android/タブレット経由の **ActiveSync**
E メールに使った時間のうち 40%

ブラウザ Office.com 、
または OWA
E メールに使った時間のうち 10%

Office365 および Exchange Server 2013/2016/2019 の Allow（許可）、Block（ブロック）、Quarantine（検疫）をサポートしている当社のソリューションは、長年にわたって何千もの組織をサポートしてきました。直感的かつ安全なデバイスのプロビジョニングによって、セキュリティを損なうことなく、またヘルプデスクに連絡してサポートを求めたりすることなく、ユーザーは新しい ActiveSync デバイスを自分で素早く簡単に登録できます。

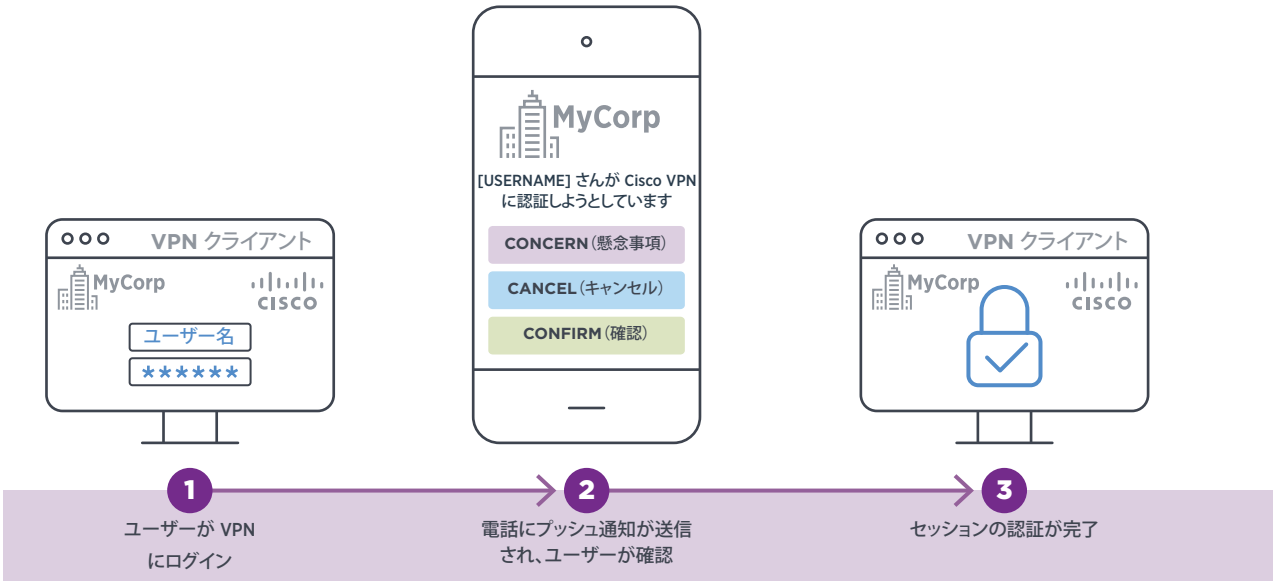
ユーザー自身が簡単かつ安全にデバイスのプロビジョニングを行えるため、BYOD を採用している組織に最適です。完全な MDM ソリューションは不要です。ユーザーが新しいデバイスを登録し、E メールを通じて手間なく、かつ非常に安全に必要なアクセスを確保できるようにすることで、ユーザーの利便性が向上します。

モバイル プッシュ認証：IT に精通した従業員に最適

Identity as a Service を統合すれば、VPN / Citrix (Radius) および AD FS を介してアクセスを得られるプッシュ認証を Identity Essentials で利用できるようになります。これを有効化すると、ユーザーのモバイル端末に「CONCERN (懸念事項)」、「CANCEL (キャンセル)」、または「CONFIRM (確認)」のプロンプトが表示されます。「CONCERN (懸念事項)」ボタンを押すとアクセスがブロックされ、システムにログインし、また管理者に通知が届きます。

生体認証 (例：touch/FaceID) を追加することで、モバイルアプリの不正使用を防いだり、誤ってユーザーがハッカーに対してアクセスを許可したりするのを防止することができます。コンテキスト情報もアプリに表示されます (例：「Login attempt from Hilton Hotel in Bangkok, Thailand (タイのバンコクのヒルトンホテルからログイン試行あり)」)。

モバイル プッシュ認証 – Identity as a Service を使用



このアプリは Android および iOS の両方で動作し、2 つの形式があります (証明書機能搭載および未搭載)。IT に精通したユーザーにとって便利なのが、プッシュ通知による認証機能です。多くの現場の従業員やあまりITに詳しくないユーザーにとっては、電話でインストールやセットアップを行う必要がない他の認証方法 (SMS/テキスト、音声通話など) も有効なソリューションになります。

パスワードレス認証：手間なくアプリにアクセス

Entrust Identity

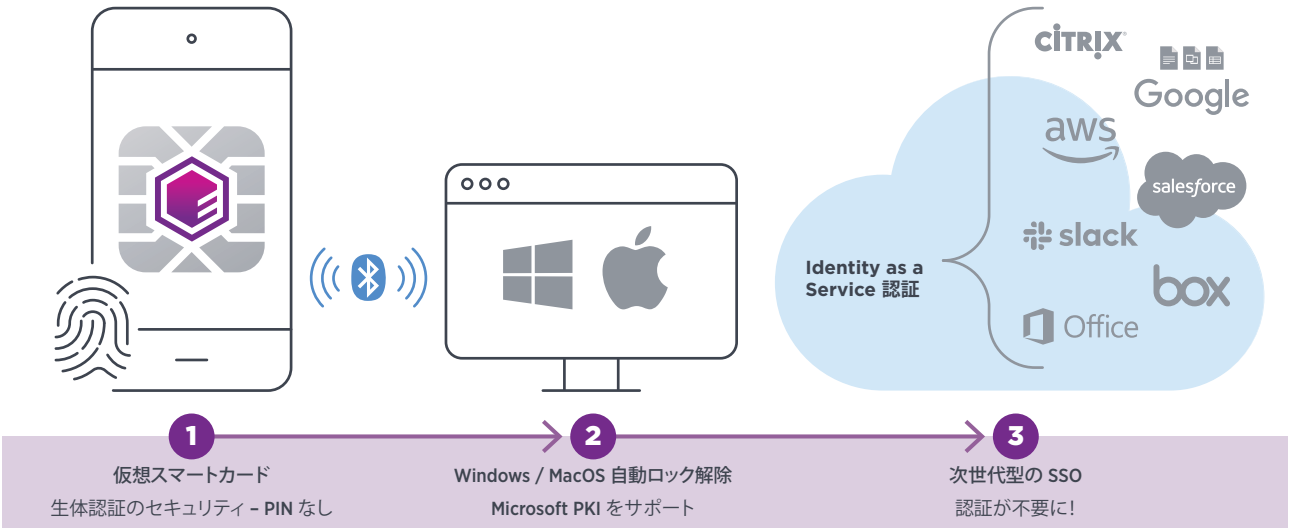
求められているセキュリティレベルをパスワードだけでは達成できない場合、長年にわたって多要素認証が使用されてきました。しかし、テクノロジーおよびサイバー攻撃の脅威がどちらも進化を続けている昨今、従来型の MFA では対応できなくなっています。

まず、ユーザーはデータ、アプリケーションに即座にアクセスしたいと思っており、手間がかかる MFA ではフラストレーションを感じます。ワンタイム パスコード（OTP）を入力したり、USB キーを持ち運んだりしなければならない MFA では、生産性が低下します。さらに、USB キーを紛失したり、ハードウェア トークンのバッテリーが切れたりすると、ユーザーはロックアウトされます。次に、ハッカーは特定の MFA 方式を回避する方法を見つけており、これが重大なセキュリティ侵害につながります。

そこでセキュリティを最大化しつつ、ユーザーの手間を最小化することで、MFA の主な問題に対処できるのがスマートログインです。デジタル証明書の安全性と携帯電話の利便性を組み合わせ、エンドユーザーにシンプルかつ高度なソリューションを提供します。

従業員は Entrust Identity のスマートログインを使用すれば、携帯電話を所持するだけでワークステーションやアプリケーションにログインできるようになります。秘密の質問や OTP など 2FA、パスワードが不要になります。セキュリティの壁を少なくして、素早く簡単にパソコンやアプリケーションを利用できるようになるため、生産性が向上します。また、ワークステーションをロックするよう注意する必要もなくなります。スマートログインの場合、その場から離れると自動的にログアウトします。

パスワードレス認証 – Identity as a Service を使用



Identity Essentials の機能

シームレスな統合：ログイン システムおよびクラウド ソリューションに Identity Essentials MFA プラットフォームをシームレスに統合すれば、直感的かつ簡単にリモートアクセスを行えるようになります。

アダプティブ認証：ユーザーの現在の状況に基づいて認証レベルを自動的に調整することで、高度なセキュリティおよび使いやすさを両立させます。

自動フェイルオーバー：OTP が確実に届けられるよう、非常に柔軟なフェイルオーバーのメカニズムを構築することができます。ユーザーの現在のログイン状況に応じて、送信間の切り替えを行うこともできるソリューションです。

様々なディレクトリをサポート：ユーザーは、OpenLDAP や AD LDS などの一般的な LDAP ディレクトリおよび Active Directory から、同期を行うことができます。特定のユーザーグループを選択するか、LDAP フィルターを使用してユーザーをインポートできます。

リアルタイムの保護：すべての OTP コードが、ログイン時にリアルタイムで生成されます。ハッキングされるおそれがあるパスコードやシードファイルを事前に発行する必要はありません。また、リアルタイムでなければ、セッション固有の OTP を配信することができません。

PowerShell：管理者は PowerShell スクリプトを使用して、ロールベースのアクセスを作成したり、他のシステムへの統合を行ったり、ライセンスの有無の確認や国別のログインの確認など、日常的なタスクを自動化したりすることができます。

ステータスのフィードバック：ログインの進行状況を追跡できるようになるため、ユーザーの安心感が高まり、またヘルプデスクの問い合わせ件数も減ります。

位置情報と動作を認識：ログイン動作のパターンや位置情報などのコンテキスト情報に基づき、ユーザーのアクセスを許可・拒否します。ジオフェンシングにより、管理者はシステムおよび位置情報に基づくホワイトリスト、ブラックリストを使用できるようになります（例：Citrix NetScaler 経由の特定の国からのアクセスを制限）。

デバイスの安全なプロビジョニング：セキュリティを損なう、またヘルプデスクに連絡してサポートを求めることなく、ユーザーは新しい ActiveSync デバイスを自分で素早く簡単に登録できます。

OTP 配信方法：プラグインおよび標準的な OTP 配信方法（アプリ、SMS、音声通話、セキュア E メール、クラウド キー、ハード/ソフト トークンなど）により、現在および将来におけるビジネス要件に対応できます。

高度なデータベース監査：業界の厳格な規制に準拠し、監査管理要件を満たしやすくなります。

Identity as a Service を統合することで利用可能になる追加機能

モバイル プッシュ認証アプリ（ブランドに合わせてカスタマイズ可能）：従業員が平常時以外の時間・場所からログインする場合に、使いやすさを損なわずにセキュリティを強化します。ユーザーは携帯電話にポップアップ表示される通知メッセージを通じて、アクセスを求めているのが本人であることを確認します。

デバイスのフィンガープリント認証：AD FS を介してクラウドサービスに正常にログインすると、デバイスのフィンガープリントがキャプチャされ、また今後のログイン時のセキュリティ評価に使用されることからログインが簡単にできるようになります。

パスワードレス認証：従業員の携帯電話に認証情報をプロビジョニングし、その携帯電話がユーザーの近くにあり、指紋認証または顔認証によってロックが解除されている場合に、Bluetooth 経由でアプリケーション SSO（クラウドおよびオンプレミス）やワークステーション（Mac および PC）にパスワードなしでログインできるようになります。

シングルサインオン（SSO）：Identity as a Service により、従来型アプリを含むあらゆるアプリ（クラウドおよびオンプレミス）で SSO を利用できるようになります。SAML や OIDC などの規格を介してクラウドアプリと認証情報を連携します。

Azure AD の統合：Azure AD を統合してユーザーを同期することができます。

E メールおよびファイルの暗号化：主要な MDM ベンダー（Microsoft、IBM、VMware など）を統合し、E メールおよびファイルを暗号化することで、業務中の通信を保護できます。

ドキュメント署名：MDM ベンダーの統合は、ドキュメント署名による Non-Repudiation および業務トランザクションの保護をサポートしています。

身元証明：従業員、契約者、パートナーなどの身元を安全に確認します。

消費者認証：Identity as a Service は、従業員の認証以外にも使用できます。これを使用して、消費者認証のあらゆるニーズに対応することもできます。

Entrust Identity ポートフォリオ：Identity Essentials は、Identity as a Service および Identity Enterprise なども含む Entrust Identity ポートフォリオ一式の一部です。従業員の ID およびアクセス管理（IAM）ソリューションを提供する Entrust Identity は、ユーザー数 50 から 100 万以上に至るまで、様々な規模の組織に対応できます。

サポートされているシステム

Identity Essentials は、リモートアクセスに使用する様々なログイン システムをサポートしています。このプラットフォームは何百もの VPN にシームレスに統合できるよう設計されており、安全かつ直感的なログインプロセスを可能にします。サポートされているリモートアクセス システムの一部を以下にリストアップしています。

RADIUS VPN/SSL VPN クライアント

- Check Point
- Cisco ASA
- Citrix Netscaler（Citrix ADC）
- Juniper
- Pulse Secure
- Barracuda NG ファイアウォール
- VMware Horizon View
- Netop Remote Control
- Palo Alto
- F5 BIG-IP
- NCP VPN
- その他の RADIUS クライアント

インターネットインフォメーションサービス（IIS）ウェブサイト

次の種類のウェブサイトのサポート：

- Outlook Web Access 2010 / 2013 / 2016 / 2019
- Remote Desktop Web Access（Windows Server 2012 R2 / 2016 / 2019）
- ベーシック認証、統合 Windows 認証、ASP.NET フォームベース認証を使用する IIS ウェブサイト

Windows ログオン、リモートデスクトップ サービス

次の種類のサーバーおよびサービスのサポート：

- リモートデスクトップ サービス（RDP 接続）
- Windows Server / 2012 / 2012 R2 / 2016 / 2019
- Windows 8、Windows 8.1、および Windows 10
- VMware Virtual Desktop Portal および Client Access

デバイスのセキュアなプロビジョニング

次のシステム上の ActiveSync デバイスの保護：

- Exchange 2010 SP3
- Exchange 2013
- Exchange 2016
- Exchange 2019
- Exchange Online

Microsoft AD FS 保護

- 多要素認証用の AD FS 3.0/4.0/5.0 アダプタ

次の多要素認証のサポート：

- Salesforce.com、Microsoft Office 365、Google Apps などのクラウド アプリケーションへのアクセス（AD FS 3.0/4.0/5.0）
- Outlook Web Access など、Microsoft Web Application Proxy（AD FS 3.0/4.0/5.0）を介して公開されたウェブサイトへのアクセス
- Workplace Join に関連するデバイスの承認（AD FS 3.0/4.0/5.0）

詳細はこちらから

888.690.2424
+1 952 933 1223
sales@entrust.com
entrust.com

ENTRUST CORPORATIONについて

Entrust は、信頼できるID、支払い、およびデータ保護を可能にすることで、急速に変化する世界を守ります。国境の有無に関係なく、商品やサービスの購入、電子政府サービスへのアクセス、企業ネットワークへのログインなど、今日ますますシームレスで安全な体験が求められています。Entrustは、こうしたやり取りのすべてのまさに核心部において、非常に幅広いデジタルセキュリティやクレデンシャルの発行ソリューションを提供しています。Entrustは世界150ヶ国以上において、2,500名の社員とグローバルパートナーネットワークを擁しています。そのため、世界で最も信頼される組織が当社に信頼を寄せていることは驚きではありません。

詳細はこちら:
entrust.com

ENTRUST

米国内 フリーダイヤル：888 690 2424
国際電話：+1 952 933 1223
info@entrust.com