Entrust Identity Essentials

Mettre en place un cadre de confiance zéro

Entrust Identity englobe tout l'éventail des solutions IAM, de la meilleure protection MFA et VPN de sa catégorie pour les environnements Windows à l'authentification sans mot de passe à haute assurance basée sur des justificatifs d'identité qui peut être déployée sur site ou dans le Cloud.

ENTRUST

IDENTITY
ESSENTIALS

VUE D'ENSEMBLE

Identity Essentials

Identity Essentials est la solution d'authentification multi-facteurs (AMF) idéale pour les entreprises qui recherchent une option rapide et économique pour sécuriser l'identité des employés et permettre à leur personnel à distance de travailler. Avec Identity Essentials, vous commencez avec une solution d'AMF sur site facile à utiliser et à déployer et vous pouvez migrer vers le Cloud avec Identity as a Service dans la durée, si et quand cela s'avère utile. L'intégration transparente entre Identity Essentials et Identity as a Service garantit une configuration hybride sans problème, tout en bénéficiant de trois options d'authentification :

- l'authentification par empreinte digitale du périphérique
- l'authentification par téléphone mobile
- l'authentification par la carte en grille

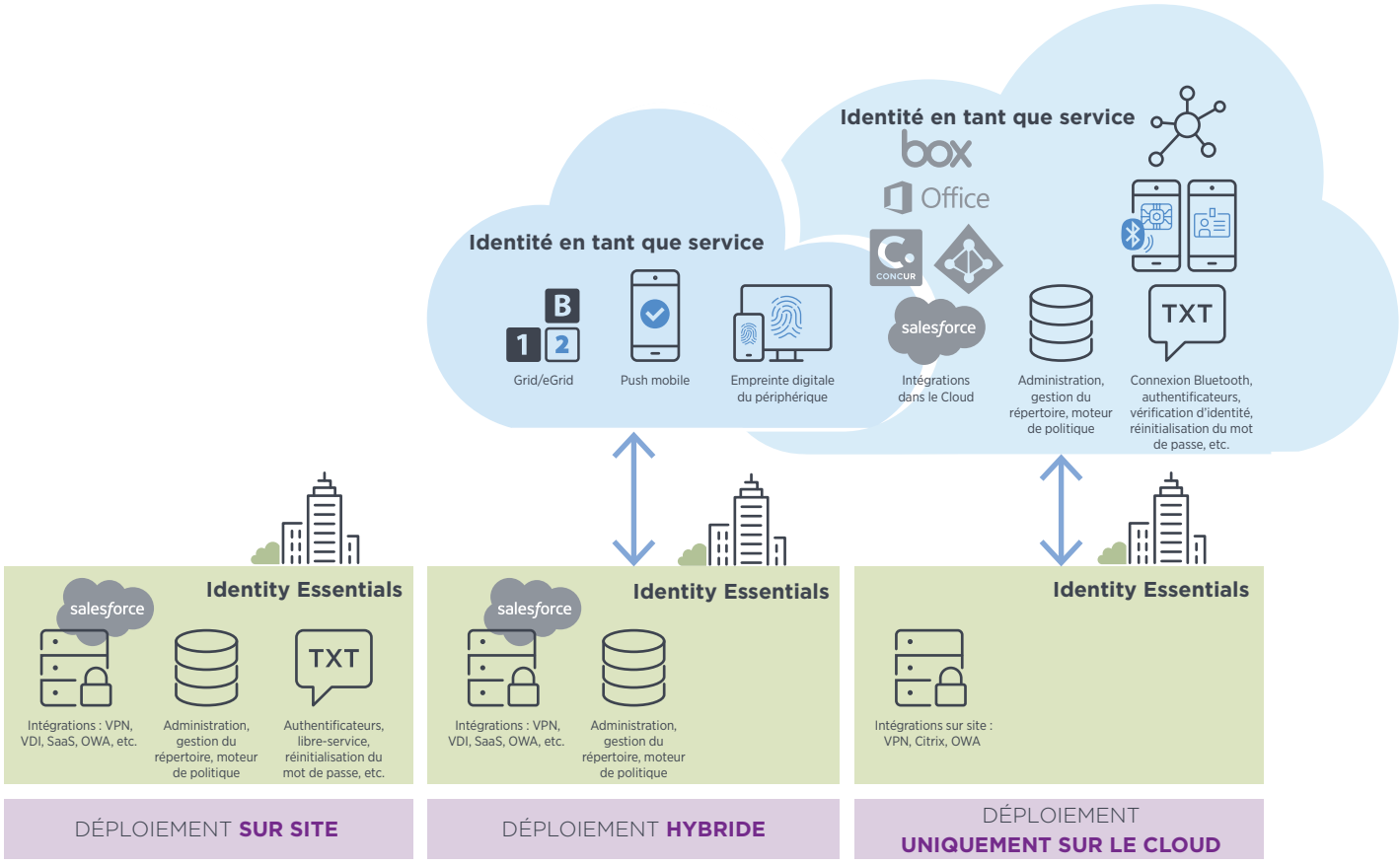
Identity Essentials fournit aux organisations sous Windows la structure de base pour réaliser une approche de confiance zéro avec Identity as a Service dans la durée.

FONCTIONNEMENT

Combattre les grandes menaces avec une meilleure technologie

Si un hacker obtient le mot de passe d'un employé, il peut exploiter tout ce dont l'employé a accès - dans le Cloud et sur site. Et comme la plupart des organisations permettent davantage de services dans le Cloud pour les systèmes de fichiers, les intranets, les sites de collaboration, etc., un plus grand nombre de données sont maintenant exposées. Heureusement, l'authentification forte des utilisateurs est désormais moins pénible qu'auparavant, tant pour les utilisateurs que pour les administrateurs. Et grâce à l'intégration d'Identity Essentials et d'Identity as a Service, vous pouvez aller aussi loin dans le Cloud que vous le souhaitez - avec une connexion sans mot de passe et intelligente sous Windows 7, 8, 10 et MacOS.

Identity Essentials vous permet d'aller aussi loin dans le Cloud que vous le souhaitez grâce à l'intégration transparente d'Identity as a Service.*



*Uniquement pour les clients d'Identity Essentials avec une licence d'abonnement.

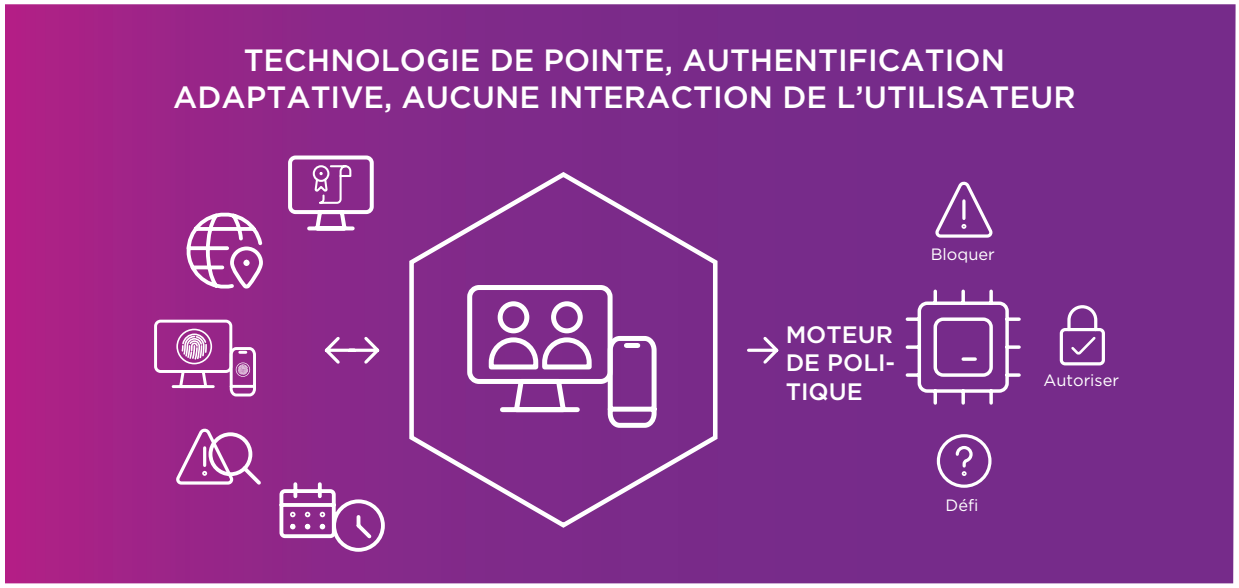
Options de licence : ce qui est inclus*

Les entreprises qui choisissent l'offre d'abonnement groupé bénéficient pleinement de l'intégration étroite entre Identity Essentials et Identity as a Service.

	Logiciel Assurance	Abonnement Groupé
Améliorations d'Identity Essentials	●	●
Prise en charge de Windows Server 2019	●	●
Empreinte digitale sur périphériquel avec AD FS (Identity as a Service)	●	●
Authentification Push (Identity as a Service)	●	●
Provisionnement de périphériques ActiveSync pour Office365 et Exchange	●	●
Identity as a Service « Plus », y compris le moteur de gestion des risques, l'authentification Cloud-à-Cloud, etc.		●
Service d'envoi d'un OTP (mot de passe à usage unique) global par SMS, application et voix		●
Portail d'authentification unique Identity as a Service pour tous les services cloud en un seul emplacement protégé		●
Assistance Identity Essentials, heures d'ouverture (peut être prolongé)		●
Prise en charge des cartes en grille	●	●
Fonctionnalité améliorée sur l'authentification de la console d'ouverture de session Windows	●	●

*Identity Smart Login est une fonctionnalité complémentaire qui entraîne des frais supplémentaires.

Le moteur adaptatif basé sur les risques d'Entrust Identity offre un niveau de sécurité supplémentaire lorsque les conditions le justifient, comme lorsqu'un employé se connecte pour la première fois à partir d'un nouveau périphérique, ou à un moment anormal de la journée, ou encore à partir d'une géolocalisation différente. Le fait de n'exiger une authentification supplémentaire, comme une notification mobile Push, que lorsque ces situations se présentent, permet de réduire au minimum les problèmes des employés tout en protégeant les ressources de l'entreprise.



Un large éventail d'authentificateurs pris en charge

Avec les Identity Essentials, vous avez le choix entre plusieurs méthodes d'authentification. En fonction de divers facteurs tels que l'accès aux ressources, le périphérique utilisé et le niveau de compétence technique de l'utilisateur, vous pouvez choisir différentes méthodes d'authentification.

Trois fonctions modernes (listées ci-dessous) sont toutes accessibles grâce à l'intégration d'Identity as a Service, qui permet aux employés d'accéder aux postes de travail, aux réseaux et aux applications en toute sécurité - sans avoir à saisir un mot de passe ou à utiliser les méthodes traditionnelles à deux facteurs à chaque session. Une véritable expérience de connexion sans mot de passe, sans problème et en toute sécurité.

Authentificateurs Identity Essentials

SMS | SMS Flash | Messagerie électronique sécurisée | Appel vocal | Identity Essentials (OTP chiffré) | Authentification mobile | Prise en charge FIDO2 | Prise en charge des jetons OATH OTP | Grid/eGrid

PLUS 3 FONCTIONNALITÉS D'AUTHENTIFICATION DÉVELOPPÉ PAR IDENTITY AS A SERVICE

Authentification par empreinte digitale du périphérique

Lors de l'accès aux applications du Cloud par le biais d'AD FS, l'empreinte digitale d'un nouveau périphérique peut être capturée, ce qui permet la détection automatique d'un périphérique utilisé antérieurement. Cela offre une couche de sécurité supplémentaire et permet de ne pas utiliser les codes d'accès à usage unique (OTP).

Lorsque vous utilisez le moteur Identity as a Service Risk Engine, ce facteur peut également être pris en compte, au même titre que la géolocalisation, l'adresse IP, l'heure de connexion, la vitesse de déplacement, etc.

Authentification mobile

Ajoutez une couche de sécurité supplémentaire lorsque les employés veulent se connecter à un moment ou un emplacement inhabituel. L'application d'authentification Push, qui porte la marque de la société, offre une sécurité biométrique utilisant la biométrie mobile d'origine pour empêcher tout accès non autorisé. L'application comporte les boutons Confirmer, Refuser et Inquiétudes ; les inquiétudes sont enregistrées et un rapport est envoyé à un administrateur.

Authentification sans mot de passe

L'authentification par carte à grille fournit aux organisations un outil d'authentification forte simple mais efficace pour une sécurité accrue et un contrôle d'accès logique. Les utilisateurs sont confrontés à un problème d'authentification lorsqu'ils se connectent à un réseau, une application, un service ou un site restreint. Chaque carte réseau est unique et porte un numéro de série, de sorte que chaque utilisateur peut être identifié et authentifié de manière unique. Chaque fois qu'un utilisateur est invité à s'authentifier, il doit relever un nouveau défi qui l'oblige à valider au moyen d'un ensemble différent de coordonnées en grille. La demande de coordonnées change pour chaque défi d'authentification.

Authentification des empreintes digitales du périphérique : une connexion facile et sécurisée

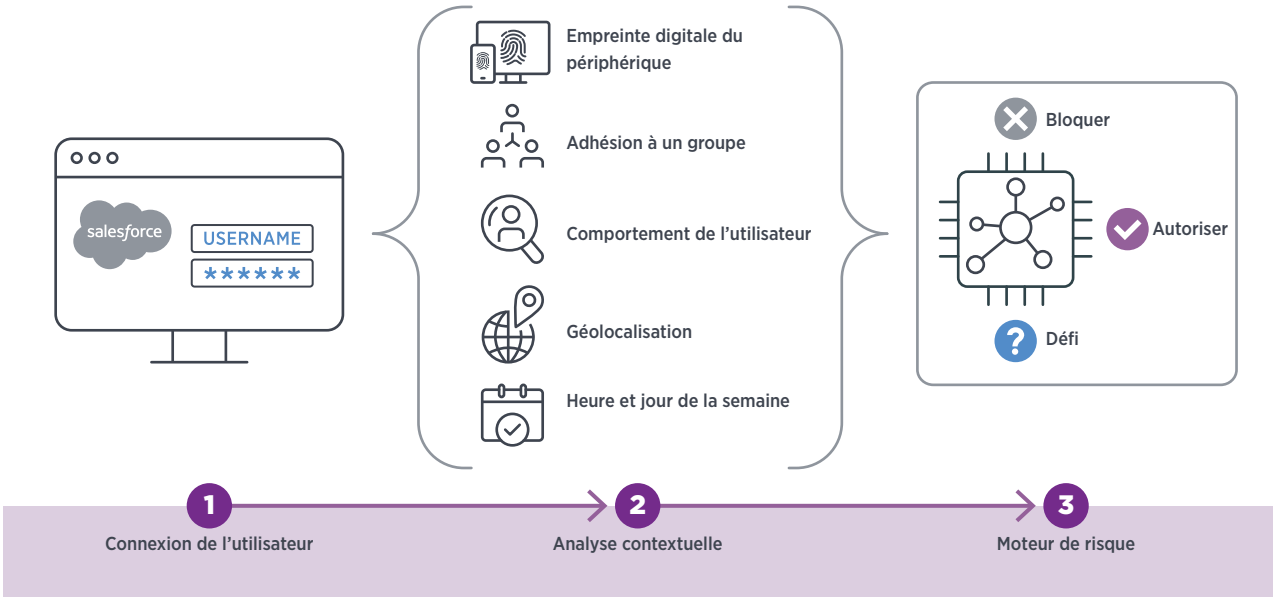
Plus de 80 % de toutes les infractions liées au piratage sont causées par des identifiants d'utilisateur faibles ou volés. L'ajout de l'AMF (Authentification multifactorielle) sur tous les services renforcera considérablement votre sécurité en désarmant les pirates de leur arme préférée.

Pour contrer le retour d'information de la part de vos utilisateurs, consultez nos capacités d'intelligence adaptative/contextuelle, qui ont déjà amélioré l'expérience utilisateur de milliers d'organisations.

Identity Essentials est le pionnier de l'authentification adaptative, où la connexion est accordée en fonction du contexte - que l'utilisateur soit connecté par VPN, Citrix, RDP ou des services en ligne par exemple.

L'empreinte digitale du périphérique est la dernière nouveauté, offrant plus de sécurité qu'un cookie d'authentification pour valider la machine qui a été utilisée précédemment lors d'une connexion.

AUTHENTIFICATION D'EMPREINTES DIGITALES DU PÉRIPHÉRIQUE - Développé par Identity as a service



Identity Essentials élimine le besoin de connexions frustrantes et répétitives en exploitant le moteur facile à configurer d'Identity as a Service qui détecte les risques en temps réel sur la base de données contextuelles et du comportement de l'utilisateur.

Protection ActiveSync : aucune gestion des périphériques mobiles n'est requise

ActiveSync - le protocole permettant de synchroniser facilement les courriers électroniques, les contacts, etc., impose un risque de sécurité souvent négligé. Si un utilisateur peut facilement configurer l'accès à des informations importantes en utilisant uniquement une adresse électronique et un mot de passe, un pirate informatique peut en faire autant. Et lorsque vous protégez OWA/Office365 avec l'authentification MFA, ActiveSync ne doit pas être oublié.

IL Y A **TROIS FAÇONS PRINCIPALES**
D'ACCÉDER AU CONTENU OFFICE 365/OWA

Client Outlook
sur PC/Mac 50 % du temps passé sur la messagerie électronique

ActiveSync
via iPhone/Android/Tablette 40 % du temps passé sur la messagerie électronique

Navigateur
Office.com ou OWA 10 % du temps passé sur la messagerie électronique

Notre solution a aidé des milliers d'organisations au fil des ans en prenant en charge l'autorisation, le blocage ou la quarantaine dans Office 365 et Exchange Server 2013/2016/2019. Le provisionnement intuitif et sécurisé des périphériques permet aux utilisateurs d'intégrer rapidement et facilement de nouveaux périphériques ActiveSync par eux-mêmes sans compromettre la sécurité - et sans avoir à contacter le service d'assistance pour obtenir de l'aide.

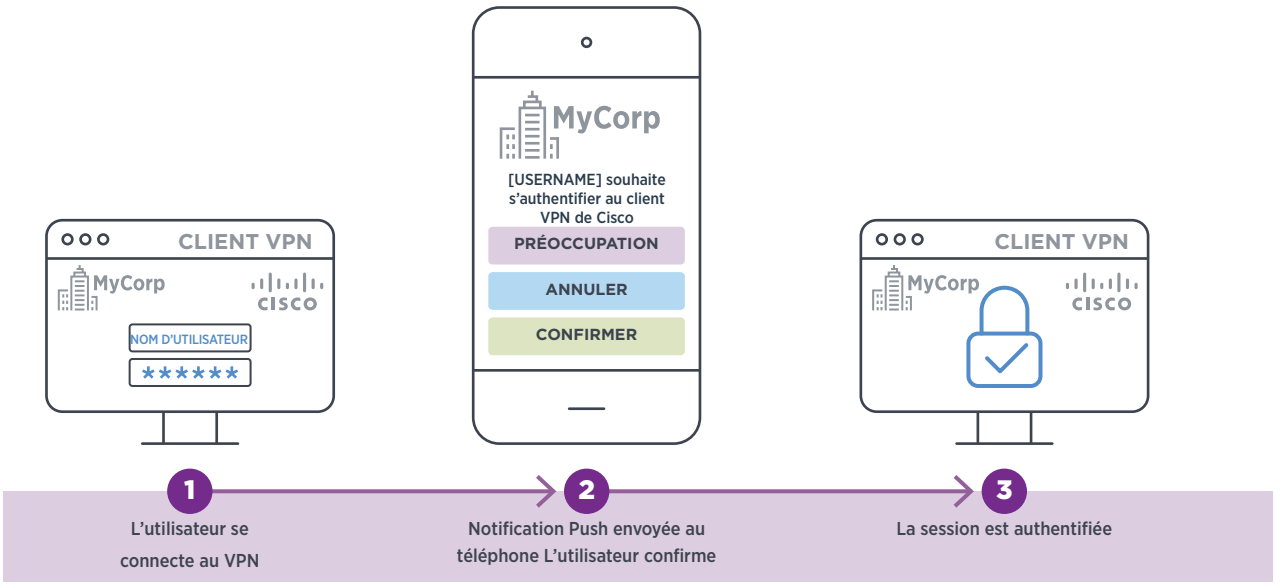
Ce système simple, sécurisé et adapté à l'utilisateur s'inscrit parfaitement dans la culture de BYOD. Pas besoin d'une solution MDM complète. Simplifiez les tâches de vos utilisateurs en leur permettant de se connecter à leur nouveau périphérique et d'obtenir l'accès dont ils ont besoin de manière simple et très sécurisée par le biais de leur messagerie électronique.

Authentification mobile Push : parfaite pour les employés à la pointe de la technologie

Avec l'intégration d'Identity as a Service, Identity Essentials comprend l'authentification Push pour obtenir un accès par le VPN/Citrix (Radius) et AD FS. Lorsqu'ellel est activée, l'utilisateur est invité sur son écran mobile avec « INQUIÉTUDE », « ANNULER » ou « CONFIRMER ». Le fait d'appuyer sur le bouton « INQUIÉTUDE » bloque l'accès et est également connecté au système pour alerter l'administrateur.

La validation biométrique (par exemple, l'identification tactile/faciale) peut être ajoutée pour protéger contre l'utilisation non autorisée d'une application mobile ou contre une autorisation accidentelle d'accès à un pirate informatique par l'utilisateur. Des informations contextuelles sont également affichées dans l'application (par exemple, « Tentative de connexion depuis l'hôtel Hilton à Bangkok, Thaïlande »).

AUTHENTIFICATION MOBILE PUSH - Développé par Identity as a Service



L'application fonctionne à la fois pour Android et iOS, et se présente sous deux formes : avec ou sans certificat. La fonction Push pour s'authentifier est une fonction très utile pour les utilisateurs avertis en matière de technologies de l'information. D'autres méthodes d'authentification qui ne nécessitent pas d'installation et de configuration sur le téléphone (SMS/texte, appel vocal, etc.) restent des solutions valables pour de nombreux employés de première ligne et un public moins technique.

Authentification sans mot de passe : accès sans problèmes aux applications

Entrust Identity

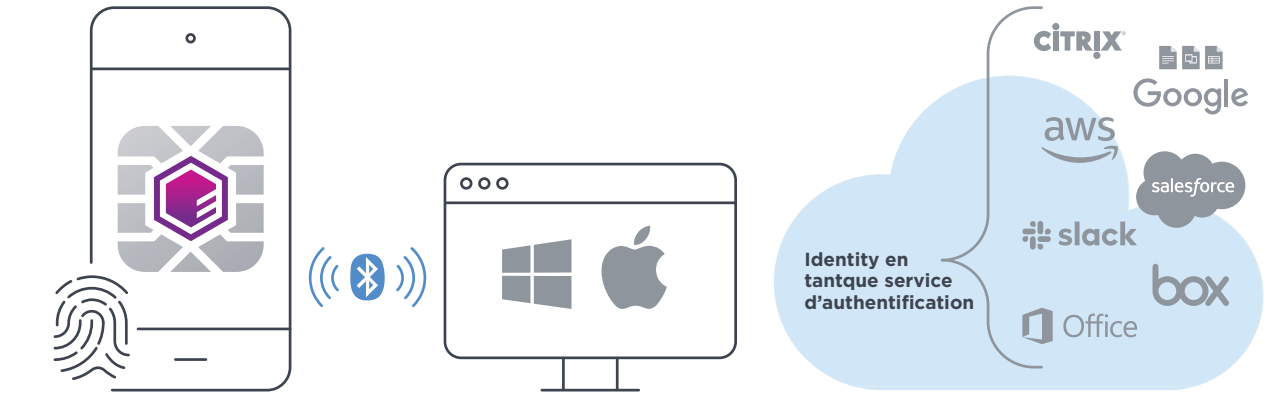
Depuis de nombreuses années, l'authentification multifactorielle offre une couche de sécurité nécessaire en complément des mots de passe. Mais notre monde a continué d'évoluer - tant du point de vue technologique que de celui des cybermenaces - ce qui a créé des problèmes avec l'AMF traditionnelle.

Tout d'abord, les utilisateurs s'attendent à un accès instantané aux données et aux applications et l'AMF a accru les difficultés et la frustration. De la saisie de codes d'accès à usage unique (OTP) au transport de clés USB, l'AMF ralentit la productivité. De plus, si vous perdez votre clé USB ou si la batterie de votre jeton matériel est déchargée, vous êtes bloqué. Deuxièmement, les pirates informatiques trouvent des moyens de contourner certaines méthodes d'AMF, ce qui entraîne des violations coûteuses.

Smart Login s'attaque aux problèmes clés de l'AMF en maximisant la sécurité et en minimisant les difficultés des utilisateurs. En associant la sécurité des certificats numériques et le confort du téléphone portable, nous proposons des solutions avancées et simples pour les utilisateurs finaux.

Le Smart Login d'Entrust Identity permet aux employés de se connecter à leur poste de travail et à leurs applications simplement en ayant leur téléphone en leur possession. Plus de mots de passe et plus d'authentification à 2 facteurs (2FA), comme les questions de connaissance ou les OTP. L'accès à leur ordinateur et à leurs applications est rapide et facile, avec moins de contraintes de sécurité, ce qui leur permet d'être plus productifs. De plus, ils n'ont plus besoin de se souvenir de verrouiller leur poste de travail. Smart Login les déconnecte automatiquement lorsqu'ils quittent les lieux.

AUTHENTIFICATION SANS MOT DE PASSE - Développé par Identity as a Service



Caractéristiques d'Identity Essentials

Une intégration sans problème : la plateforme d'AMF Identity Essentials s'intègre de manière transparente aux systèmes de connexion et aux solutions du Cloud pour une expérience d'accès à distance intuitive et conviviale.

Authentification adaptative : adapte automatiquement le niveau d'authentification en fonction de la situation actuelle de l'utilisateur, offrant un équilibre entre sécurité élevée et grande convivialité.

Commutation automatique : il est possible d'établir des mécanismes de commutation très souples pour garantir la réception permanente des OTP. La solution peut même passer d'une transmission à l'autre, en fonction du contexte de connexion actuel de l'utilisateur.

Prise en charge étendue d'annuaires : les utilisateurs peuvent être synchronisés à partir d'Active Directory et d'annuaires LDAP généraux comme OpenLDAP ou AD LDS. Les utilisateurs peuvent être importés en sélectionnant un groupe d'utilisateurs spécifique, ou en utilisant un filtre LDAP.

Protection en temps réel : Tous les codes OTP sont générés en temps réel au moment de la connexion. Il n'y a pas de codes pré-délivrés ou de fichiers de démarrage qui pourraient être piratés. En même temps, le temps réel est une condition préalable à la fourniture d'un OTP (mot de passe à usage unique) spécifiques à une session.

PowerShell : les administrateurs peuvent utiliser les scripts PowerShell pour créer des accès basés sur des rôles, s'intégrer à d'autres systèmes ou automatiser des tâches quotidiennes telles que la vérification de la disponibilité des licences ou des connexions spécifiques à un pays.

Retour d'information sur le statut : permet à l'utilisateur de suivre la progression de la connexion ; inspire confiance à l'utilisateur et réduit le nombre d'appels au service d'assistance.

Connaissance de l'emplacement et du comportement : cette fonctionnalité exploite des informations contextuelles telles que les modèles de comportement de connexion et la géolocalisation pour autoriser ou refuser l'accès à l'utilisateur. La géolocalisation permet aux administrateurs d'établir une liste blanche ou une liste noire en fonction des systèmes et des lieux (par exemple, limiter l'accès via Citrix NetScaler à partir de certains pays).

Mise à disposition de dispositifs sécurisés : Permet aux utilisateurs d'enregistrer eux-mêmes rapidement et facilement de nouveaux périphériques ActiveSync sans compromettre la sécurité et sans avoir à contacter le service d'assistance pour obtenir de l'aide.

Méthodes de délivrance des OTP : les plug-ins et les méthodes de diffusion OTP standard - comme les applications, les SMS, les appels vocaux, les courriers électroniques sécurisés, les clés dans le Cloud et les jetons matériels et logiciels - répondent aux besoins de votre entreprise aujourd'hui et demain.

Audit de base de données avancé : Aide les clients à se conformer aux réglementations strictes du secteur et à satisfaire aux exigences de contrôle des audits.

Fonctions supplémentaires par l'intégration d'Identity as a Service

Application d'authentification Push mobile (avec votre propre marque) : ajoute un niveau de sécurité convivial lorsque les employés veulent se connecter à un moment ou un lieu inhabituel. Un message de notification s'affiche sur leur téléphone portable pour confirmer que c'est bien eux qui demandent l'accès.

Authentification des empreintes digitales du périphérique : après une connexion réussie à un service du Cloud par le biais d'AD FS, une empreinte digitale du périphérique peut être capturée et utilisée pour de futures évaluations de la sécurité de la connexion, ce qui permet une connexion plus facile.

Authentification sans mot de passe : fournit un justificatif d'identité sur le téléphone de l'employé, permettant une connexion sans mot de passe à un poste de travail (Mac et PC) et à l'application SSO (Sur le Cloud et sur site) par l'intermédiaire de Bluetooth lorsque le téléphone est à proximité et déverrouillé avec l'empreinte digitale ou la correspondance faciale de l'utilisateur.

Authentification unique SSO (Single Sign-on) : Identity as a Service permet de fournir un service d'authentification unique SSO à toutes les applications Cloud et sur site, y compris les anciennes applications. Fédération avec les applications sur le Cloud via des standards comme SAML et OIDC.

Intégration Azure AD : s'intègre à Azure AD pour la synchronisation des utilisateurs, etc.

Chiffrement des courriers électroniques et des fichiers : l'intégration avec les principaux fournisseurs de MDM - y compris Microsoft, IBM et VMware - garantit la sécurité des communications sur le lieu de travail grâce au chiffrement des courriers électroniques et des fichiers.

Signature de documents : l'intégration avec les fournisseurs de MDM permet de sécuriser les transactions sur le lieu de travail et d'assurer la non-répudiation grâce à la signature de documents.

Vérification de l'identité : vérifie en toute sécurité l'identité des employés, des entrepreneurs, des partenaires et autres.

Authentification des consommateurs : Identity as a Service va au-delà de l'authentification des employés. L'application peut également être utilisée pour répondre à tous vos besoins d'authentification des consommateurs.

Solutions Entrust Identity : Identity Essentials fait partie de notre gamme unifiée de solutions Entrust Identity qui comprend également Identity as a Service et Identity Enterprise. Entrust Identity offre des solutions de gestion des identités et des accès des employés (IAM) pour soutenir une variété de tailles d'organisations, de 50 à plus d'un million d'utilisateurs.

Systèmes pris en charge

Identity Essentials prend en charge divers systèmes de connexion utilisés pour l'accès à distance. La plateforme est conçue pour s'intégrer de manière transparente dans des centaines de VPN, offrant un processus de connexion sécurisé et intuitif. Vous trouverez ci-dessous une liste d'exemples de systèmes d'accès à distance pris en charge.

Clients VPN RADIUS/SSL VPN

- Check Point
- Cisco ASA
- Citrix Netscaler (Citrix ADC)
- Juniper
- Pulse Secure
- Barracuda NG firewalls
- VMware Horizon View
- Netop Remote Control
- Palo Alto
- F5 BIG-IP
- NCP VPN
- Autres clients RADIUS

Sites web des services d'information sur Internet (IIS)

Prise en charge des types de sites Web suivants :

- Outlook Web Access 2010/2013/2016/2019
- Accès à distance au bureau par le Web (Windows Server 2012 R2/2016/2019)
- Sites web IIS utilisant l'authentification de base, l'authentification intégrée de Windows et l'authentification basée sur un formulaire ASP.Net

Connexion à Windows, services de bureau à distance

Prise en charge des serveurs et services suivants :

- services de bureau à distance (connexions RDP)
- serveurs Windows/2012/2012 R2/2016/2019
- Windows 8, Windows 8.1 et Windows 10
- Portail du bureau virtuel VMware et accès client

Mise à disposition de périphériques sécurisés

Protection des dispositifs ActiveSync sur les systèmes suivants :

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

Protection Microsoft AD FS

- Adaptateur AD FS 3.0/4.0/5.0 pour l'authentification multifactorielle

Prise en charge de l'authentification multifactorielle pour :

- àccès aux applications du Cloud telles que Salesforce.com, Microsoft Office 365, Google Apps, etc. (AD FS 3.0/4.0/5.0)
- accès à des sites Web publiés par le biais de Microsoft Web Application Proxy (AD FS 3.0/4.0/5.0), tels que Outlook Web Access
- Homologation des périphériques en rapport avec les jonctions sur le lieu de travail (AD FS 3.0/4.0/5.0)

Pour plus d'informations

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

À PROPOS D'ENTRUST CORPORATION

Entrust sécurise un monde en rapide évolution en assurant des identités, des paiements et une protection des données fiables. Aujourd'hui plus que jamais, les personnes exigent des expériences transparentes et sécurisées, qu'elles traversent les frontières, fassent un achat, accèdent à des services d'administration en ligne ou se connectent à des réseaux d'entreprise. Entrust offre une gamme inégalée de solutions de sécurité numérique et d'émission de titres de compétences au cœur même de toutes ces interactions. Avec plus de 2 500 collègues, un réseau de partenaires mondiaux et des clients dans plus de 150 pays, il n'est pas étonnant que les organisations les plus confiantes au monde nous fassent confiance.

Pour en savoir plus, consultez le site
entrust.com

Entrust et le logo Hexagon sont des marques commerciales, des marques déposées et/ou des marques de service d'Entrust Corporation aux États-Unis et/ou dans d'autres pays. Tous les autres noms de marques ou de produits sont la propriété de leurs propriétaires respectifs. En raison de l'amélioration constante de nos produits et services, Entrust Corporation se réserve le droit de modifier les spécifications sans préavis. Entrust est un employeur garantissant l'égalité des chances.
©2020 Entrust Corporation. Tous droits réservés. IA21Q2-Entrust-Identity-Essentials-BR

ENTRUST

É.-U. Téléphone gratuit : 888 690 2424
Téléphone international : +1 952 933 1223
info@entrust.com