Entrust Identity Essentials

Logre el marco de Zero Trust

Entrust Identity cubre el espectro de soluciones de IAM, desde la mejor protección de MFA y VPN para entornos basados en Windows hasta la autenticación sin contraseña con base en credenciales de alta seguridad que pueden implementarse en las instalaciones o en la nube.

ENTRUST

IDENTITY
ESSENTIALS

DESCRIPCIÓN

Aspectos básicos de Identity

Identity Essentials es la solución ideal de autenticación multifactor (MFA) para empresas que buscan una opción rápida y rentable para proteger las identidades de los trabajadores y habilitar su fuerza de trabajo remota. Con Identity Essentials, comienza con una solución de MFA en las instalaciones fácil de usar y fácil de implementar y puede migrar a la nube con Identity as a Service a lo largo del tiempo, cuando sea necesario. La integración perfecta entre Identity Essentials e Identity as a Service garantiza una configuración híbrida sin fricciones al tiempo que se beneficia de tres opciones de autenticación:

- Autenticación de huellas digitales del dispositivo
- Autenticación push móvil
- Autenticación de tarjetas de coordenadas

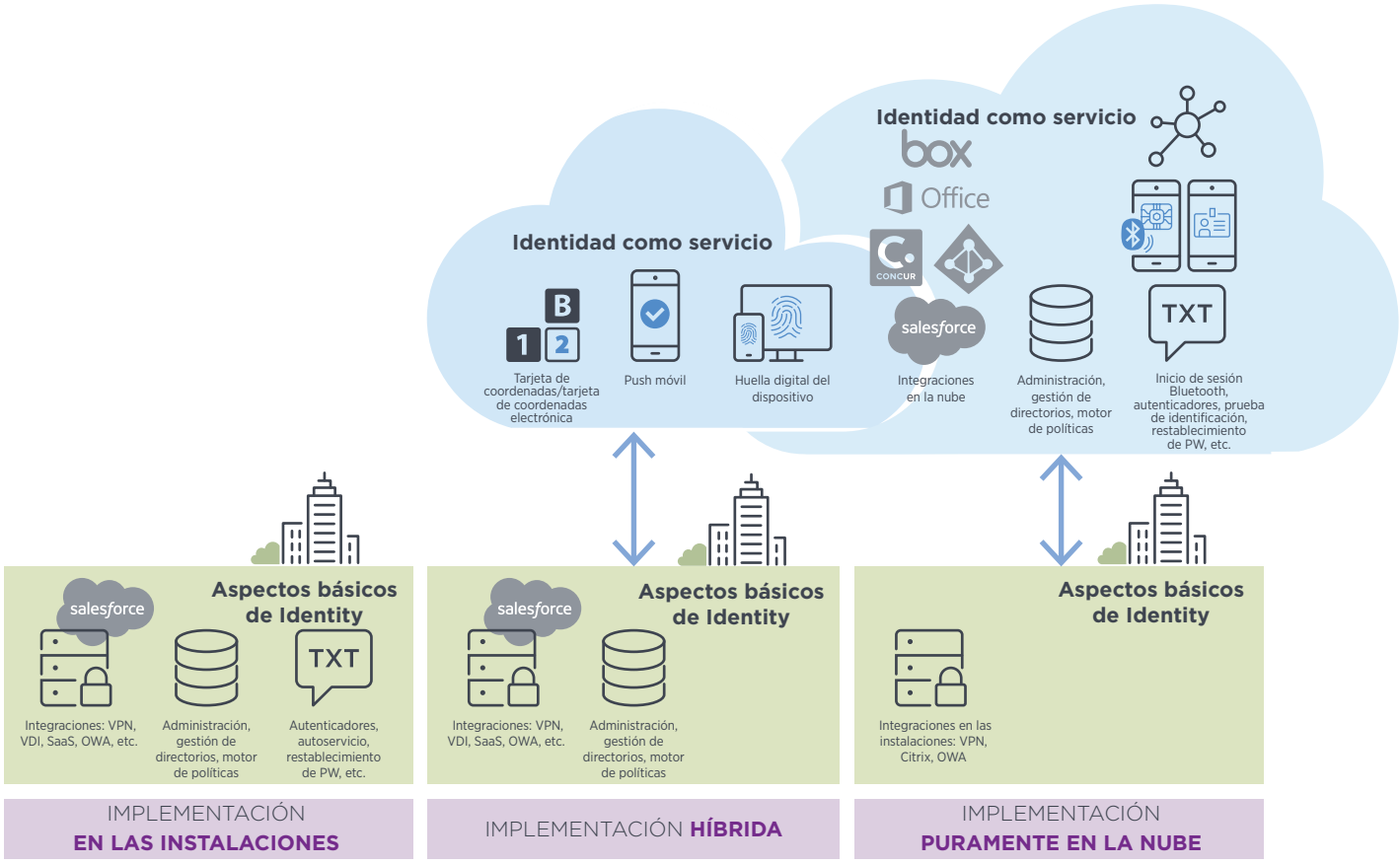
Identity Essentials proporciona la base para que las organizaciones basadas en Windows realicen una combinación de Zero Trust con Identity as a Service a lo largo del tiempo.

CÓMO FUNCIONA

Luche contra amenazas más grandes con mejor tecnología

Si un hacker obtiene la contraseña de un empleado, puede vulnerar la seguridad de todo a lo que el empleado tiene acceso en la nube y en las instalaciones. Y dado que la mayoría de las organizaciones están habilitando más servicios en la nube para sistemas de archivos, intranets, sitios de colaboración, etc., ahora más datos se encuentran expuestos. Afortunadamente, una autenticación de usuario sólida es ahora menos difícil tanto para los usuarios como para los administradores de lo que solía ser antes. Y con la integración de Identity Essentials y Identity as a Service, puede adentrarse en la nube tanto como desee, con acceso inteligente y sin contraseña a Windows 7, 8, 10 y MacOS.

Identity Essentials le permite adentrarse en la nube tanto como desee mediante una integración perfecta con Identity as a Service.*



*Solo para clientes de Identity Essentials con una licencia de suscripción.

Opciones de licencia: lo que está incluido*

Las empresas que eligen el paquete de suscripción obtienen el beneficio total de una perfecta integración entre Identity Essentials y Identity as a Service.

	Garantía de software	Paquete de suscripción
Mejoras de Identity Essentials	●	●
Soporte del servidor Windows 2019	●	●
Huellas digitales del dispositivo con AD FS (Identity as a Service)	●	●
Autenticación Push (Identity as a Service)	●	●
Suministro de dispositivos ActiveSync para Office365 y Exchange en las instalaciones	●	●
Identity as a Service "Plus", incluido el motor de riesgo, la autenticación de nube a nube, etc.		●
Servicio de envío OTP global basado en SMS, aplicaciones y voz		●
Portal de inicio de sesión único de Identity as a Service para todos los servicios en la nube en un solo lugar protegido		●
Soporte de Identity Essentials, horario comercial (puede ser extendido)		●
Soporte de tarjetas de coordenadas	●	●
Funcionalidad mejorada en la autenticación de la consola de inicio de sesión de Windows	●	●

*Identity Smart Login es una función adicional que tiene un costo adicional.

El motor flexible basado en riesgos de Entrust Identity proporciona un nivel adicional de seguridad cuando las condiciones lo requieren, como cuando un trabajador inicia sesión por primera vez desde un dispositivo nuevo, en un momento anormal del día o desde una ubicación geográfica diferente. Solo requiere autenticación adicional como una notificación push en el dispositivo móvil en este tipo de situaciones disminuyendo la fricción de los trabajadores al mínimo al tiempo que protege los recursos corporativos.

Una amplia gama de autenticadores compatibles

Con Identity Essentials, tiene opciones cuando se trata de métodos de autenticación. Dependiendo de diversos factores, como el activo al que se accede, el dispositivo que se utiliza y el nivel de habilidad técnica del usuario, es posible que desee elegir diferentes métodos de autenticación.

Tres características modernas (enumeradas a continuación) son posibles gracias a la integración de Identity as a Service, lo que permite a los empleados acceder a estaciones de trabajo, redes y aplicaciones de forma segura, sin la dificultad de ingresar una contraseña o emplear métodos tradicionales de dos factores en cada sesión. Una verdadera experiencia de inicio de sesión segura, sin contraseñas y sin fricciones.

Autenticadores de Identity Essentials

MÁS 3 FUNCIONES DE AUTENTICACIÓN
Desarrollado por Identity as a service

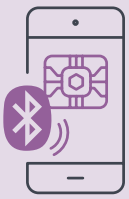
Autenticación de huellas digitales del dispositivo

Al acceder a las aplicaciones en la nube a través de AD FS, se puede capturar una nueva huella digital del dispositivo, lo que permite la detección automática de un dispositivo usado anteriormente. Esto proporciona una capa adicional de seguridad y le permite omitir las contraseñas de un solo uso (OTP).

Cuando se utiliza el motor de riesgo de Identity as a Service, esto también puede ser un factor a considerar, junto con la geolocalización, la dirección IP, la hora de inicio de sesión, la velocidad de navegación, etc.

Autenticación "push" móvil

Agregue una capa adicional de seguridad cuando los empleados quieran iniciar sesión en un momento o lugar inusual. La aplicación de autenticación push de marca proporciona seguridad biométrica utilizando su biometría móvil nativa para evitar el acceso no autorizado. La aplicación cuenta con los botones Confirmar, Denegar y Problema; los Problemas se registran y se envía un reporte a un administrador.



Autenticación sin contraseña

La autenticación con tarjeta de coordenadas proporciona a las organizaciones una herramienta de autenticación sólida, simple, pero efectiva para una mayor seguridad y control de acceso lógico. A los usuarios se les presenta un desafío de autenticación cuando inician sesión en una red, aplicación, servicio en la nube o sitio restringido. Cada tarjeta de coordenadas es única y lleva un número de serie, por lo que cada usuario puede ser identificado y autenticado de forma única. Cada vez que se le pide a un usuario que se autentique, se le presenta un desafío diferente que requiere que valide mediante un conjunto diferente de coordenadas de cuadrícula. La solicitud de coordenadas cambia para cada desafío de autenticación.

Autenticación de huellas digitales del dispositivo: un inicio de sesión seguro y fácil

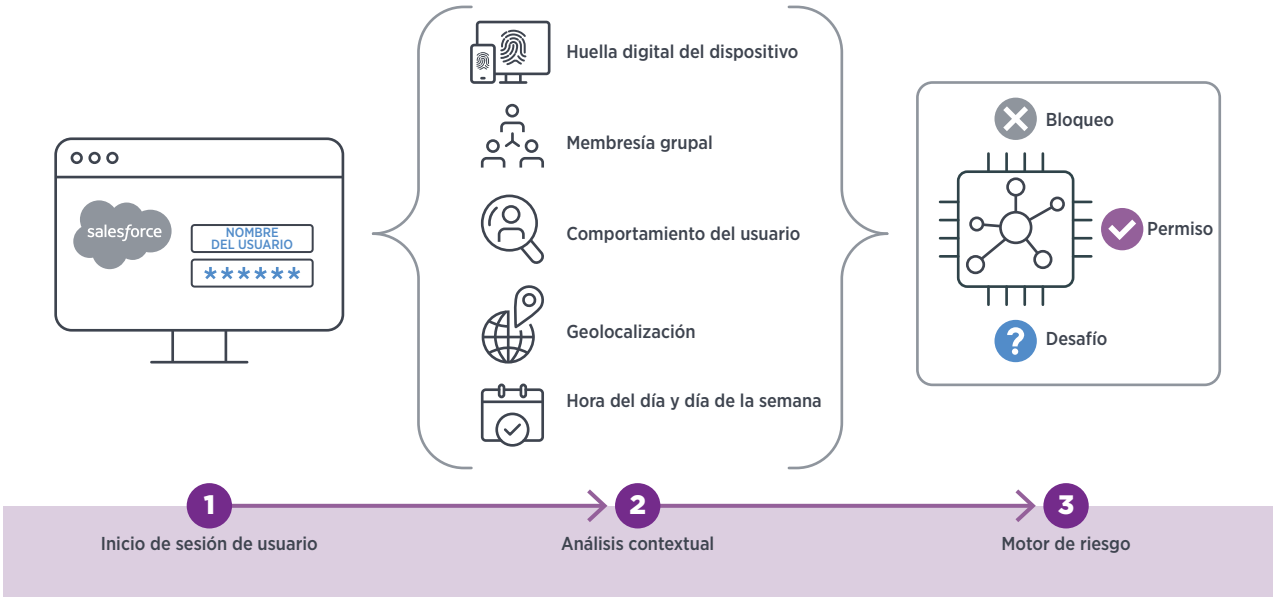
Más del 80% de todas las infracciones relacionadas con el hackeo son causadas por credenciales de usuario robadas o débiles. Agregar la MFA en todos los servicios aumentará su seguridad drásticamente al desarmar a los hackers de su arma preferida.

Para superar la resistencia de sus usuarios, consulte nuestras funciones de inteligencia flexible/contextual, que ya han mejorado la experiencia del usuario para miles de organizaciones.

Identity Essentials fue pionera en la autenticación flexible, donde el inicio de sesión se otorga según el contexto, ya sea que el usuario haya iniciado sesión a través de VPN, Citrix, RDP o servicios en la nube, por ejemplo.

La huella digital del dispositivo es la última incorporación, que proporciona más seguridad que una cookie de autenticación para validar la máquina que se ha utilizado anteriormente en un inicio de sesión.

AUTENTICACIÓN DE HUELLAS DIGITALES DEL DISPOSITIVO: desarrollada por Identity as a Service



Identity Essentials elimina la necesidad de inicios de sesión repetitivos y frustrantes al aprovechar el motor fácil de configurar de Identity as a Service que detecta el riesgo en tiempo real según los datos contextuales y el comportamiento del usuario.

Protección ActiveSync: No se requiere administración de dispositivos móviles

ActiveSync: el protocolo para una sincronización sencilla de correo electrónico, contactos, etc., impone un riesgo de seguridad que a menudo se pasa por alto. Si un usuario puede configurar fácilmente el acceso a información importante utilizando solo una dirección de correo electrónico y una contraseña, también puede hacerlo un hacker. Y cuando protege OWA/Office365 con MFA, ActiveSync no debe olvidarse.

EXISTEN **TRES FORMAS PRINCIPALES**
DE ACCEDER AL CONTENIDO DE OFFICE 365/OWA

Cliente Outlook
en PC/Mac 50% del tiempo dedicado al correo electrónico

ActiveSync
a través de iPhone/Android/ Tablet 40% del tiempo dedicado al correo electrónico

Navegador
Office.com u OWA 10% del tiempo dedicado al correo electrónico

Nuestra solución ha ayudado a miles de organizaciones a lo largo de los años al admitir Permiso, Bloqueo o Cuarentena en Office servidores 365 y Exchange 2013/2016/2019. El suministro de dispositivos intuitivos y seguros permite a los usuarios incorporar rápida y fácilmente nuevos dispositivos ActiveSync por sí mismos sin comprometer la seguridad y sin tener que ponerse en contacto con la mesa de ayuda para obtener asistencia.

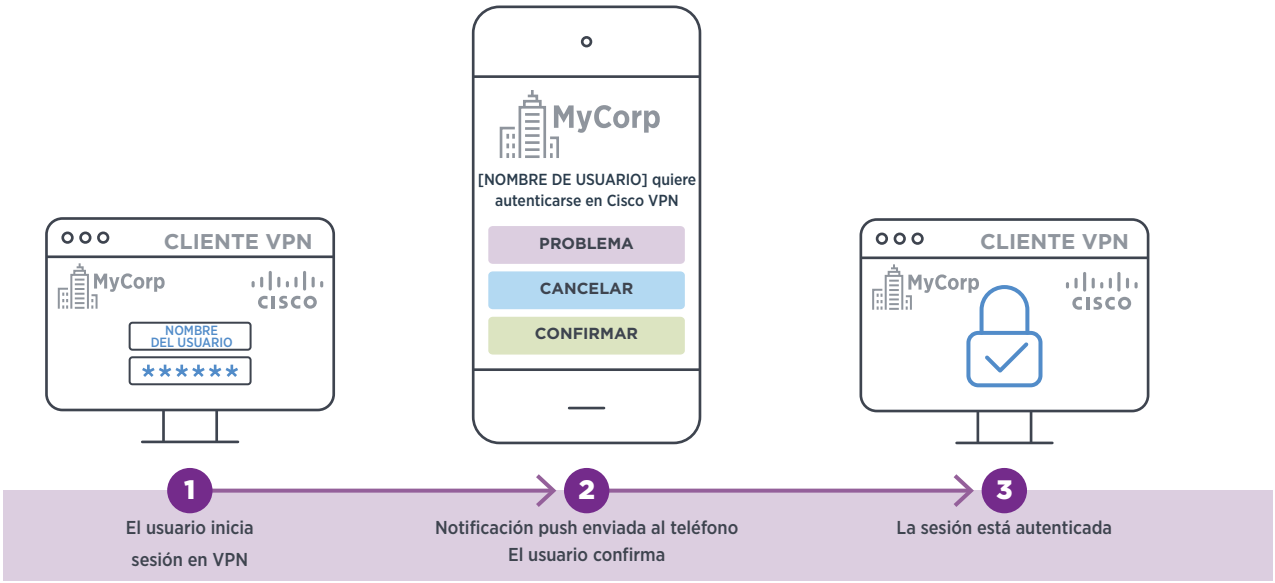
Este suministro de dispositivos simple, seguro y desarrollado por el usuario se adapta perfectamente a las culturas BYOD. No se necesita una solución MDM completa. Simplifique la vida de sus usuarios permitiéndoles incorporar su nuevo dispositivo y obtener el acceso que necesitan de una manera muy segura y sin problemas a través de su correo electrónico.

Autenticación push móvil: perfecto para trabajadores conocedores de la tecnología

Con la integración de Identity as a Service, Identity Essentials incluye autenticación push para obtener acceso a través de VPN/Citrix (Radius) y AD FS. Cuando se activa, aparecen en la pantalla del móvil del usuario "PROBLEMA", "CANCELAR" o "CONFIRMAR". Al presionar el botón "PROBLEMA" se bloquea el acceso y también se registra en el sistema para alertar al administrador.

Se puede agregar validación biométrica (por ejemplo, touch/FaceID) como protección contra el uso no autorizado de aplicaciones móviles o el usuario que accidentalmente permite el acceso a un hacker. La aplicación también muestra información contextual (p. ej., "Intento de inicio de sesión desde el Hotel Hilton en Bangkok, Tailandia").

AUTENTICACIÓN PUSH MÓVIL: desarrollada por Identity as a Service



La aplicación funciona tanto para Android como para iOS y viene en dos formas: con o sin funciones de certificado. Push es una gran característica de autenticación para los usuarios expertos en TI. Otros métodos de autenticación que no requieren instalación y configuración en el teléfono (SMS/texto, llamada de voz, etc.) siguen siendo soluciones válidas para muchos trabajadores de primera línea y una audiencia menos tecnológica.

Autenticación sin contraseña: acceso sin fricciones a las aplicaciones

Entrust Identity

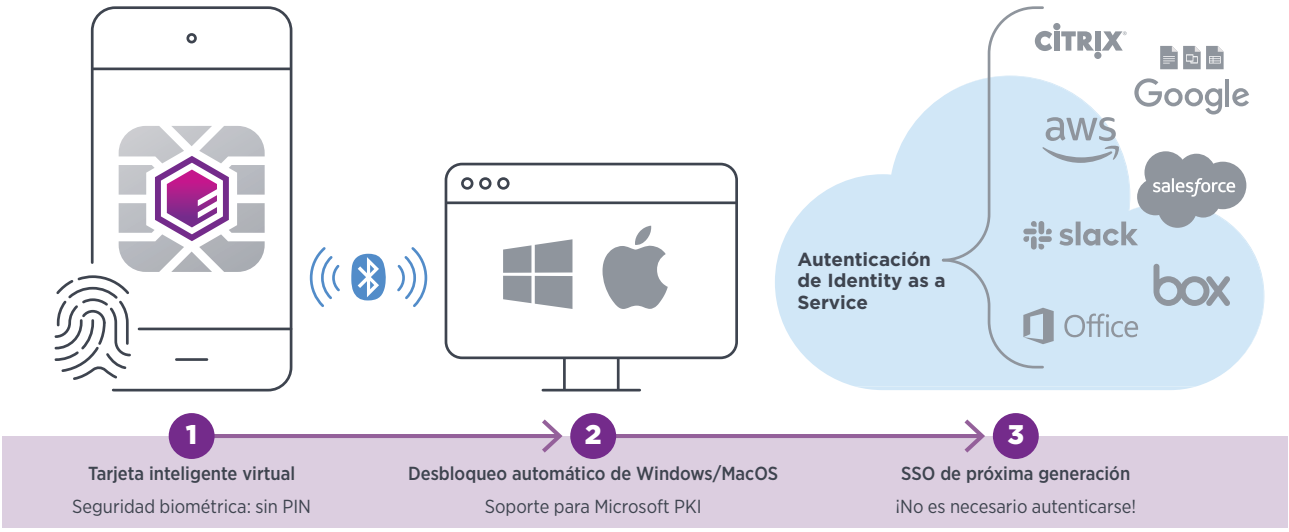
La autenticación multifactor ha proporcionado una capa de seguridad necesaria además de las contraseñas durante muchos años. Pero nuestro mundo ha seguido evolucionando, tanto desde la perspectiva de la tecnología como de las amenazas cibernéticas, creando problemas con la MFA tradicional.

En primer lugar, los usuarios esperan acceso instantáneo a datos y aplicaciones, y la MFA ha aumentado la fricción y la frustración. Desde escribir códigos de acceso de un solo uso (OTP) hasta llaves USB, la MFA ralentiza la productividad. Además, si pierde su llave USB o la batería de su token de hardware se agota, usted será bloqueado. En segundo lugar, los hackers están encontrando formas de sortear ciertos métodos de la MFA, lo que genera costosas violaciones.

El inicio de sesión inteligente aborda los problemas clave de la MFA maximizando la seguridad y minimizando la fricción del usuario. Combinando la seguridad de los certificados digitales y la conveniencia del teléfono móvil, brindamos soluciones avanzadas que son simples para los usuarios finales.

El inicio de sesión inteligente de Entrust Identity permite a los empleados iniciar sesión en su estación de trabajo y en aplicaciones simplemente con tener su teléfono en su poder. No más contraseñas y no más 2FA, como preguntas de conocimiento u OTP. Acceder a su computadora y aplicaciones es rápido y fácil con menos obstáculos de seguridad, lo que les permite ser más productivos. Además, ya no tienen que acordarse de bloquear sus estaciones de trabajo. Smart Login los desconecta automáticamente cuando se van.

AUTENTICACIÓN SIN CONTRASEÑA: desarrollada por Identity as a Service



Características de Identity Essentials

Integración sin inconvenientes: La plataforma Identity Essentials MFA se integra a la perfección con los sistemas de inicio de sesión y las soluciones en la nube para una experiencia de acceso remoto intuitivo y fácil de usar.

Autenticación flexible: Adapta automáticamente el nivel de autenticación en función de las circunstancias actuales del usuario, proporcionando un equilibrio de alta seguridad y una gran facilidad de uso.

Transferencia automática por falla: Es posible establecer mecanismos de conmutación por error altamente flexibles para garantizar que las OTP siempre funcionen. La solución puede incluso cambiar entre transmisiones, según el contexto de inicio de sesión actual del usuario.

Soporte de directorio amplio: Los usuarios pueden sincronizarse desde Active Directory y directorios LDAP generales como OpenLDAP o AD LDS. Los usuarios se pueden importar seleccionando un grupo de usuarios específico o mediante el uso de un filtro LDAP.

Protección en tiempo real: Todos los códigos de acceso se generan en tiempo real en el momento de inicio de sesión. No hay códigos de acceso o archivos seed emitidos previamente que se puedan hackear. Al mismo tiempo, el tiempo real es un requisito previo para la entrega de OTP específicas de la sesión.

PowerShell: Los administradores pueden usar secuencias de comandos de PowerShell para crear acceso basado en roles, integrarse a otros sistemas o automatizar tareas diarias como verificar la disponibilidad de licencias o inicios de sesión específicos del país.

Observaciones sobre la retroalimentación: Permite al usuario seguir el progreso de inicio de sesión, inspira confianza al usuario y reduce el número de llamadas al servicio de asistencia técnica.

Conciencia de la ubicación y el comportamiento: Aprovecha la información contextual, como los patrones de comportamiento de inicio de sesión y la ubicación geográfica para otorgar o denegar el acceso de los usuarios. Geofencing permite a los administradores incluir en listas blancas o negras según los sistemas y ubicaciones (por ejemplo, limitar el acceso a través de Citrix NetScaler desde ciertos países).

Suministro seguro de dispositivos: El suministro seguro de dispositivos permite a los usuarios incorporar rápida y fácilmente nuevos dispositivos ActiveSync por sí mismos sin comprometer la seguridad y sin tener que ponerse en contacto con la mesa de ayuda para obtener asistencia.

Métodos de entrega de OTP: Los complementos y los métodos de entrega de OTP estándar, como aplicaciones, SMS, llamadas de voz, correo electrónico seguro, claves en la nube y tokens físicos/blandos, respaldan sus requisitos comerciales ahora y en el futuro.

Auditoría avanzada de bases de datos: Ayuda a los clientes a cumplir con las estrictas regulaciones de la industria y cumplir con los requisitos de control de auditoría.

Funciones adicionales a través de la Integración de Identity as a Service

Aplicación de autenticación push móvil (con su propia marca): Agrega una capa adicional de seguridad cuando los empleados quieren iniciar sesión en un momento o lugar inusual. Aparece un mensaje de notificación en su teléfono móvil para confirmar que es la persona que solicita el acceso.

Autenticación de huellas digitales del dispositivo: Después de un inicio de sesión exitoso en un servicio en la nube a través de AD FS, se puede capturar una huella digital del dispositivo y usarla para futuras evaluaciones de seguridad de inicio de sesión, lo que permite un inicio de sesión más fácil.

Autenticación sin contraseña: Proporciona una credencial en el teléfono del trabajador, lo que permite el inicio de sesión sin contraseña en la estación de trabajo (Mac y PC) y el SSO de la aplicación (en la nube y en las instalaciones) a través de Bluetooth cuando el teléfono está muy cerca y es desbloqueado con la huella digital o la correspondencia facial del usuario.

Inicio de sesión único (SSO): Identity as a Service ofrece SSO a todas las aplicaciones, en la nube y en las instalaciones, incluidas las aplicaciones heredadas. Federados con aplicaciones en la nube a través de estándares como SAML y OIDC.

Integración con Azure AD: Se integra con Azure AD para la sincronización de usuarios, etc.

Cifrado de archivos y correo electrónico: La integración con los principales proveedores de MDM, incluidos Microsoft, IBM y VMware, garantiza que las comunicaciones en el lugar de trabajo sean seguras mediante correo electrónico y cifrado de archivos.

Firma de documentos: La integración de proveedores de MDM admite transacciones seguras en el lugar de trabajo y la no resistencia a la firma de documentos.

Acreditación de identidad: Verifica de forma segura las identidades de empleados, contratistas, socios y otros.

Autenticación del consumidor: Identity as a Service va más allá de la autenticación de la fuerza laboral. También se puede utilizar para abordar todas las necesidades de autenticación de sus consumidores.

Activación de la cartera de Entrust Identity: Identity Essentials es parte de nuestra cartera unificada de Entrust Identity que también incluye Identity as a Service y Identity Enterprise. Entrust Identity ofrece soluciones de gestión de acceso e identidad de la fuerza laboral (IAM) para admitir una variedad de tamaños de organización, desde 50 hasta más de 1 millón de usuarios.

Sistemas compatibles

Identity Essentials admite una variedad de sistemas de inicio de sesión utilizados para acceso remoto. La plataforma está diseñada para integrarse sin problemas en cientos de VPN, lo que proporciona un proceso de inicio de sesión seguro e intuitivo. A continuación, se muestra una lista de ejemplos de sistemas de acceso remoto compatibles.

Clientes VPN RADIUS SSL/VPN

- Check Point
- Cisco ASA
- Citrix Netscaler (Citrix ADC)
- Juniper
- Pulse Secure
- Cortafuegos Barracuda NG
- VMware Horizon View
- Mando a distancia Netop
- Palo Alto
- F5 BIG-IP
- NCP VPN
- Otros clientes RADIUS

Sitios web de Internet Information Services (IIS)

Soporte para los siguientes tipos de sitios web:

- Outlook Web Access 2010/2013/2016/2019
- Acceso web a escritorio remoto (servidor Windows 2012 R2/2016/2019)
- Sitios web de IIS que utilizan autenticación básica de Windows integrada y autenticación basada en formularios ASP.Net

Inicio de sesión de Windows, servicios de escritorio remoto

Soporte para los siguientes servidores y servicios:

- Servicios de escritorio remoto (conexiones RDP)
- Servidores Windows 2012/2012 R2/2016/2019
- Windows 8, Windows 8.1 y Windows 10
- Portal de escritorio virtual de VMware y acceso de cliente

Aprovisionamiento seguro de dispositivos

Protección para dispositivos ActiveSync en los siguientes sistemas:

- Exchange 2010 SP3
- Exchange 2013
- Exchange 2016
- Exchange 2019
- Exchange en línea

Protección de Microsoft AD FS

- Adaptador AD FS 3.0/4.0/5.0 para autenticación multifactor

Soporte de autenticación multifactor para:

- Acceso a aplicaciones en la nube como Salesforce.com, Microsoft Office 365, Google Apps, etc. (AD FS 3.0/4.0/5.0)
- Acceso a sitios web publicados a través de Microsoft Web Application Proxy (AD FS 3.0/4.0/5.0), como Outlook Web Access
- Aprobación de dispositivos en relación con los ingresos en el lugar de trabajo (AD FS 3.0/4.0/5.0)

Para obtener más información

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

ACERCA DE ENTRUST CORPORATION

Entrust se dedica a asegurar un mundo en movimiento al permitir el uso de identidades, pagos y protección de la información confiables. Hoy más que nunca, las personas demandan experiencias seguras y sin obstáculos, ya sea que estén cruzando las fronteras, haciendo una compra, accediendo a los servicios electrónicos del gobierno o iniciando sesión en las redes corporativas. Entrust ofrece una incomparable amplitud de soluciones de seguridad digital y emisión de credenciales basadas en todas estas interacciones. Al contar con más de 2500 colegas, una red de socios globales y clientes en más de 150 países, no es de extrañar que las organizaciones más confiables del mundo confíen en nosotros.

Para más información visite
entrust.com

ENTRUST

E.E. U.U. Línea telefónica gratuita: 888 690 2424
Teléfono internacional: +1 952 933 1223
info@entrust.com