



## Entrust IdentityGuard

### Métodos de autenticación de múltiples factores

Entrust IdentityGuard es una galardonada solución de autenticación que proporciona seguridad a muchas de las principales instituciones financieras, empresas y gobiernos del mundo. Al funcionar como una plataforma de autenticación versátil, ofrece una gama de sólidas funcionalidades de autenticación para mejorar la confiabilidad de las transacciones en línea y la autenticación de identidad para otorgar acceso a aplicaciones o recursos.

Como un componente clave de un modelo de seguridad empresarial en capas, Entrust IdentityGuard puede aprovechar las capacidades actuales de detección de fraude de Entrust para ayudar a las organizaciones a crear una estrategia de autenticación basada en sus requerimientos singulares y no sufre de las limitaciones de un método de autenticación individual.

La plataforma de autenticación versátil permite que las organizaciones igualen la solidez de la autenticación y su mecanismo con el nivel del riesgo asociado, las consideraciones de costo y los requerimientos de la capacidad de uso.

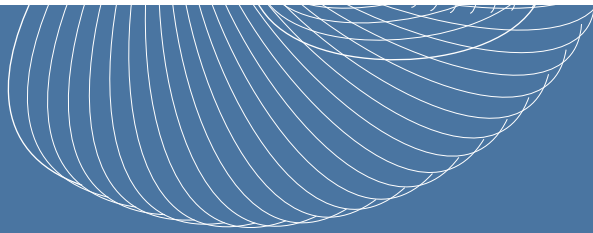
- ¿Desea que la autenticación sea transparente para el usuario?
- ¿Le gustaría que el usuario portara un dispositivo físico o que se autentique en línea?
- ¿Desea que el sitio Web además autentique al usuario por sí solo?
- ¿Cuál es el nivel de confidencialidad de la información que está protegiendo y cuál es el riesgo asociado?

La flexibilidad y el espectro de los autenticadores de Entrust IdentityGuard le permiten a las organizaciones aplicar una autenticación sólida en toda la empresa, en lugar de en un grupo determinado de usuarios. La plataforma ofrece un punto de administración único, independiente de la opción de autenticación o la combinación de opciones que se implemente, lo que permite que las organizaciones evolucionen y modifiquen los métodos de autenticación en el tiempo a medida que cambian los riesgos y el entorno operativo.

Revise la gama completa de autenticadores de la plataforma y descubra cuál puede ser el adecuado para su organización.

### Beneficios de los productos

- Componentes probados de la plataforma de autenticación versátil de Entrust IdentityGuard
- El abanico más amplio de funcionalidades de autenticación disponible en el mercado en la actualidad
- Implementación de autenticadores basada en los requerimientos del usuario, en el nivel de riesgo y en el costo
- Entrega de protección avanzada contra ataques intermediarios (man in the middle)
- Autenticadores probados en implementaciones de mercados masivos
- Precio bajo y sencillo que es una fracción del costo de las opciones tradicionales de dos factores



## Métodos de autenticación de múltiples factores de Entrust IdentityGuard

### Autenticación transparente

La autenticación transparente valida a los usuarios sin necesitar la participación de ellos en forma diaria. Entre los autenticadores transparentes se incluyen:

#### Certificados digitales

Entrust IdentityGuard puede autenticar a los usuarios usando los certificados digitales X.509 existentes emitidos por el servicio de certificados digitales administrado por Entrust o por un tercero. Los certificados se pueden almacenar de forma local o en dispositivos seguros como tarjetas inteligentes o tokens de USB. Las organizaciones que no cuenten con una infraestructura de llave pública (PKI) interna pueden obtener certificados mediante Entrust Managed Services PKI.

#### Geolocalización de IP

Los usuarios autenticados pueden registrar las ubicaciones desde las que frecuentemente obtienen acceso a la red corporativa. Durante las autenticaciones posteriores, el servidor de Entrust IdentityGuard compara la información de la ubicación actual, como país, región, ciudad, latitud y longitud, con aquella información registrada previamente. Si los valores no concuerdan, las organizaciones pueden aumentar la autenticación.

Con la geolocalización de IP, las organizaciones pueden crear listas negras de regiones, países o direcciones IP según el historial de fraudes o pueden aprovechar la Red Abierta de Información sobre Fraudes de Entrust (OFIN, Open Fraud Intelligence Network) para recibir listas actualizadas de direcciones IP que tienen antecedentes de fraude según análisis profesionales independientes.

#### Autenticación de dispositivos

Los usuarios autenticados pueden registrar un equipo o dispositivo que usen frecuentemente para entrar a la red corporativa. Para esto, se crea y se almacena un sofisticado perfil encriptado del equipo registrado. Durante autenticaciones posteriores, el servidor de Entrust IdentityGuard crea un nuevo perfil y lo compara con el valor almacenado. Si los valores no concuerdan, se debe aplicar una mayor autenticación.

La geolocalización de IP y la autenticación de equipos, implementadas en conjunto, ofrecen un método de autenticación transparente y efectivo para los usuarios.

### Autenticadores de factor de forma físicos

Los factores de forma físicos son dispositivos tangibles que el usuario porta y utiliza para autenticarse. Entrust ofrece una variedad de dispositivos de autenticación física para satisfacer los diversos requerimientos de los usuarios corporativos. Entre los autenticadores de factor de forma físicos se incluyen:

#### Tokens con código de acceso de un solo uso

Entrust ofrece dos versiones del popular token con código de acceso de un solo uso (OTP). Desde sólo US\$5, el Mini Token de Entrust IdentityGuard cumple con los estándares OATH y genera un código de acceso seguro de ocho dígitos al presionar un botón. El Token de bolsillo, que cumple con los estándares OATH, ofrece características adicionales entre las que se incluyen un desbloqueo mediante PIN antes de la generación del código de acceso, además de un modo con preguntas de comprobación.

#### DisplayCard

La tarjeta DisplayCard de Entrust proporciona la misma funcionalidad que el popular token en forma de tarjeta de crédito. Además de cumplir con el estándar OATH y proporcionar un código de un solo uso, la tarjeta DisplayCard incluye una banda magnética y opcionalmente puede incluir un chip PKI o EMV para brindar una mayor versatilidad.

#### Autenticación en cuadrícula

La tarjeta de cuadrícula patentada de Entrust es un autenticador del tamaño de una tarjeta de crédito que contiene números y caracteres en un formato de filas y columnas. En el inicio de sesión, se les presenta a los usuarios una pregunta acerca de coordenadas, la que se debe responder usando la información correspondiente en las celdas de la tarjeta de cuadrícula única que poseen.



### **Lista de código de acceso de un solo uso**

Los usuarios finales cuentan con una lista de códigos de acceso generados o números de transacción (TAN) generados de forma aleatoria, los que por lo general se imprimen en una hoja de papel y se distribuyen a los usuarios finales. Cada código de acceso se utiliza sólo una vez.

### **Autenticadores de factor de forma no físicos**

La autenticación de factor de forma no física proporciona métodos para verificar la identidad del usuario sin la necesidad de que porten un dispositivo físico adicional. Entre los autenticadores de factor de forma no físicos se incluyen:

#### **Autenticación basada en el conocimiento**

La autenticación basada en el conocimiento solicita a los usuarios que proporcionen información que es poco probable que un intruso posea. Las preguntas que se presentan al usuario en el momento del inicio de sesión se basan en la información (a la que se refiere como secretos de autenticación) que el usuario suministró en el momento del registro o en transacciones o relaciones anteriores. Entrust IdentityGuard permite que el administrador determine la cantidad y el tipo de preguntas que se presentan.

#### **Autenticación fuera de banda**

La autenticación fuera de banda usa medios independientes y que existen con anterioridad para comunicarse con el usuario para proteger de ataques comprometan el canal principal. Entrust IdentityGuard admite esta opción al permitir la generación de números de confirmación de un solo uso que se pueden transmitir al usuario junto con un resumen de la transacción. Esto se puede hacer directamente mediante correo electrónico o mensaje de texto (SMS) o se puede enviar mediante un mensaje de voz a un número de teléfono registrado. Cuando recibe el número de confirmación, el usuario simplemente debe ingresarlo y la transacción se aprueba.

#### **Tokens de software por SMS**

Similar a las funcionalidades de autenticación fuera de banda de la plataforma, Entrust IdentityGuard también incluye tokens de software por SMS, los que permiten la transmisión de una cantidad

determinable de códigos de acceso de un solo uso (OTP) a un dispositivo móvil para usarlo durante la autenticación. Este enfoque del token de software dinámico, que se repone automáticamente según sea necesario, otorga la solidez de una autenticación fuera de banda sin la preocupación por la disponibilidad constante de la red, el tiempo de entrega o la instalación del software en un dispositivo móvil.

#### **eGrid**

Como alternativa para los tokens de hardware, las tarjetas de cuadrículas eGrid se envían al usuario mediante la Web o como un archivo PDF, las que pueden almacenarse fácilmente en un equipo o dispositivo móvil para otorgar un acceso conveniente y, de este modo, eliminar la necesidad de portar un factor de forma físico.

#### **Nombre de usuario y contraseña seguros**

Entrust IdentityGuard generalmente proporciona un segundo factor de autenticación sólido a la infraestructura de nombre de usuario y contraseña existente de la organización. La plataforma de autenticación versátil puede proporcionar nombres de usuario y contraseñas para inicio de sesión seguras para las empresas que no cuentan con una solución.

#### **Autenticación mutua**

Su organización necesita confiar en la identidad del usuario. Asimismo, los usuarios deben confiar que están realizando transacciones con el sitio Web de la organización y no con una organización fraudulenta o un sitio falso. La autenticación mutua proporciona métodos para que la organización confirme su legitimidad a los usuarios.

Entrust le proporciona a las organizaciones una variedad de opciones para autenticación mutua con sus clientes, entre las que se incluyen:

#### **Presentación de imagen y mensaje**

Cuando el usuario se registra, selecciona una imagen de un extenso banco de imágenes que proporciona Entrust IdentityGuard. El usuario también crea un mensaje. En inicios de sesiones posteriores, se muestra la imagen y el mensaje al usuario.



### **Presentación de número de serie de la cuadrícula**

En el inicio de sesión, se le presenta al usuario el número de serie de su tarjeta de cuadrícula única.

### **Presentación de ubicación de la cuadrícula**

En el inicio de sesión, se le presenta al usuario los valores de una cantidad de celdas de su tarjeta de cuadrícula única.

### **Certificados SSL de validación extendida (EV)**

Las organizaciones pueden implementar certificados SSL de validación extendida, los que confirman la autenticidad del sitio Web al mostrar una barra de direcciones verde, un indicador claro de confianza para el usuario final.

Cada método está diseñado para presentar al usuario información identificable que sólo puede venir desde la organización legítima, lo que permite a los usuarios confirmar rápida y fácilmente que el sitio Web es auténtico.

### **Entrust y usted**

La plataforma de autenticación versátil de Entrust IdentityGuard ofrece el más amplio rango de autenticadores disponibles en el mercado en la actualidad. Desde tarjetas de cuadrícula fáciles de usar, pasando por opciones de geolocalización de IP, hasta tokens de códigos de acceso de un solo uso, la solución proporciona a cualquier organización, institución financiera, empresa y agencia gubernamental métodos fluidos y eficientes para implementar una autenticación sólida de múltiples factores como parte de una estrategia de seguridad en capas.

Para descubrir cómo Entrust IdentityGuard puede ayudar a asegurar las identidades digitales y la información de su organización, llámenos al 613-270-3400 (ext. 5). También puede comunicarse con nosotros en [entrust@entrust.com](mailto:entrust@entrust.com) y en [www.entrust.com](http://www.entrust.com).

### **Acerca de Entrust**

Entrust provee soluciones de seguridad basadas en la identidad, que posibilita a empresas, consumidores, ciudadanos y sitios web en más de 4000 organizaciones en 60 países. El enfoque de seguridad basada en la identidad de Entrust permite el balance correcto entre servicio, experiencia y costo. Para autenticación robusta, detección de fraude, certificados digitales, SSL y PKI, llame al 613-270-3400 (ext. 5) correo electrónico [entrust@entrust.com](mailto:entrust@entrust.com) o visite [www.entrust.com](http://www.entrust.com).

**Entrust®** Securing Digital Identities & Information

Entrust es una marca comercial registrada de Entrust, Inc. en Estados Unidos y otros países. En Canadá, Entrust es una marca comercial registrada de Entrust Limited. Los demás nombres de productos y nombres de servicios de Entrust son marcas comerciales o marcas comerciales registradas de Entrust, Inc. o Entrust Limited en determinados países. Los demás nombres de empresas, de productos y logotipos son marcas comerciales o marcas comerciales registradas de sus respectivos propietarios. © Copyright 2010 Entrust. Todos los derechos reservados.