AuthControl Sentry®

Protegiendo su identidad con autenticación inteligente

La solución multipremiada AuthControl Sentry®, basada en la tecnología PINsafe® y en el control dinámico de autenticación basada en riesgos, le ofrece una autenticación inteligente multifactor para su negocio.

swivelsecure

www.swivelsecure.com

USA & APAC Office
Irvine
Swivel Secure, Inc.
1340 Reynolds Ave. #116-285
Irvine, CA 92614

+1 949 480 3626 (Pacific Time)
Toll Free: 866.963.AUTH (2884)
usa@swivelsecure.com

UK & Ireland Offices
Norte
1200 Century Way
Thorpe Park,
Leeds
LS15 8ZA

HQ: +44 (0)1134 860 123
Support: +44 (0)1134 860 111
hq@swivelsecure.com

EMEA Offices
Portugal
Estrada de Alfragide,
N.º 67, Alfrapark – Lote H,
Piso 0, 2614-519 Amadora

+351 215 851 487
portugal@swivelsecure.com

Spain
Calle Punto Mobi 4,
28805 Alcala de Henares,
Madrid

+34 911 571 103
espana@swivelsecure.com

Autenticación inteligente multifactor AuthControl Sentry®

Distribuida en 54 países e implementada en diferentes sectores como: finanzas, sector público, salud, educación, fabricantes, etc.; La solución AuthControl Sentry® le ofrece una autenticación inteligente multifactor que previene accesos no autorizados a aplicaciones y datos sensibles.

Haga una captura del código QR para acceder al diagrama completo de AuthControl Sentry®, la solución de autenticación multifactor.

La flexibilidad de AuthControl Sentry® le garantiza que soporta todos los requisitos de la arquitectura de su empresa y su capacidad para adaptarse al máximo a ellos mediante el uso de una amplia variedad de factores de autenticación. No importa si usa la aplicación para móviles o la identificación biométrica para huellas dactilares, AuthControl Sentry® es la solución líder en ciberseguridad que necesita.

Lo que lo hace diferente

- Tecnología patentada PINsafe® para la máxima seguridad – ver página 8
- Arquitectura que soporta instalación local y en la nube (Cloud)
- Una única tenencia, así como una sola solución en la nube (Cloud) dividida por niveles, lo que le asegura una personalización y un control optimizados
- Autenticación basada en riesgo e inicio de sesión único como estándar
- Se integra perfectamente con cientos de aplicaciones.
- Asegura la máxima adopción con una amplia gama de métodos de autenticación. ¡Hasta diez factores!

Autentica el acceso para todas las partes interesadas, ya sea para hacer log-in en Office 365, realizar transacciones a través de comercio electrónico o acceder a su ERP de control de existencias.

✓ Empleados ✓ Clientes

✓ Proveedores

Arquitectura

Arquitectura que soporta instalación local, en la nube (Cloud) e híbrida.

No existen restricciones con AuthControl Sentry® ya que está diseñado para autenticar el acceso a todas las aplicaciones sin importar que se encuentren en la ubicación local o en la nube (Cloud), independientemente de que el usuario sea cliente, empleado o un proveedor solicitando acceso.

Arquitectura local

Acceda a los sistemas internos a través de nuestro Agente de Active Directory, una aplicación de software instalada localmente que elimina la necesidad de compartir su Active Directory a través de Internet, mientras mantiene la sincronización de la cuenta del usuario.

Arquitectura en la nube (Cloud)

IP fija: Cada cliente de AuthControl recibe una IP fija dedicada para su propia instancia virtual. No se comparten recursos, interfaz de programación de aplicaciones ni Portal de entrada o base de datos.

Dedicación exclusiva: AuthControl Cloud le ofrece una máquina virtual dedicada en exclusiva a su instalación. No se ofrecen opciones compartidas multi-tenant, por lo que puede esperar una administración y control total por su parte. Esto significa que tiene la flexibilidad de configurar la solución para satisfacer las necesidades más exigentes.

Firewall privado: Le ofrecemos firewalls privados independientes para cada cliente, permitiendo la aplicación de listas de seguridad y control de acceso a medida.

Implemente AuthControl Sentry® para autentificar:

- Grupos de interés, empleados, proveedores y/o clientes
- Acceso a aplicaciones como Office 365, Salesforce o SAP
- Un mercado vertical específico como los servicios financieros

Caracteristicas

swivelsecure

Inicio de sesión único como estándar

La funcionalidad de inicio de sesión único (SSO) de AuthControl Sentry® es una característica que proporciona a los usuarios la capacidad de acceder a todas sus aplicaciones con un único proceso de autenticación, asegurando que los mismos puedan trabajan de manera eficiente sin comprometer su seguridad.

Seguridad continua

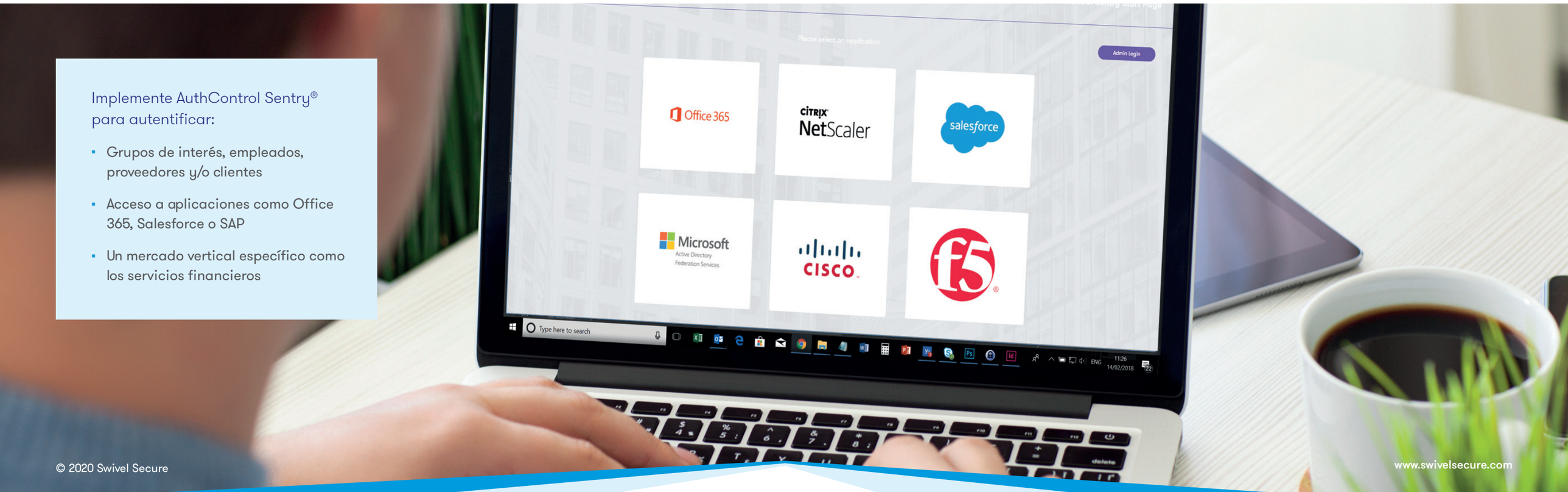
Swivel Secure proporciona un Portal Unificado para que sus usuarios puedan acceder sin problemas. Mediante este punto de acceso único, los privilegios de los usuarios pueden ser gestionados y su comportamiento puede ser rastreado en casos de auditoría, mejora de la seguridad y aumento de responsabilidad.

Económico

Puede lograr ahorros significativos utilizando SSO, por ejemplo, eliminando la necesidad de llamadas relacionadas con problemas con la contraseña al soporte IT. La productividad aumenta al facilitar que los usuarios, a través de un único inicio de sesión y un único punto de registro, puedan acceder a todas sus aplicaciones, con el consiguiente ahorro de tiempo.

Intuitivo

Si los usuarios están accediendo a aplicaciones a través de una VPN, tanto en las intalaciones locales como en la nube, éstos serán automáticamente dirigidos a la autenticación mediante la intuitiva funcionalidad SSO dentro del Portal unificado.



Caracteristicas

Autenticación basada en el riesgo como estándar

La autenticación basada en el riesgo (RBA) es un proceso dinámico de AuthControl Sentry®, diseñado para solicitar automáticamente el nivel apropiado de autenticación para acceder a las aplicaciones. Basado en los parámetros establecidos en el sistema de políticas, RBA solicita el nivel adecuado de autenticación para acceder a aplicaciones basadas en el usuario, sus dispositivos y la aplicación.

Dinámico e inteligente

Se adapta a las circunstancias del usuario incluyendo:

- A qué aplicaciones está tratando de hacer acceder
- A qué grupo pertenece
- Desde dónde está accediendo a las aplicaciones
- Qué dispositivo está usando

Sistema o motor de políticas

El sistema de políticas de autenticación adaptativa está basado en un sistema de puntos, que permite establecer parámetros por usuario y por aplicación.

- Pertenencia a un grupo
- Aplicación a la que se accede
- Dirección IP
- Última autenticación
- Certificación X.509
- Dispositivo
- Ubicación física (GeoIP)
- Geo Velocidad

Autenticación basada en el riesgo: Ejemplo 1

Un Asistente de Compras vuela al sureste de Asia para visitar a un proveedor junto con el Gerente de Compras. Acaba de terminar de comer en un restaurante y se da cuenta de que se olvidó comprobar el stock de algunos componentes para una reunión al día siguiente. El Asistente cree que se puede conectar rápidamente al sistema ERP usando su dispositivo móvil de la compañía.

Sistema ERP	
Requiere 120 puntos	
LAN	0
IP conocido	0
Dispositivo	50
Rango de IP (Asia)	-100
Se requiere autenticación	
U&P	10
Aplicación móvil	60
Huella dactilar	20

Resultado: Sin éxito (no puede acceder)
Aunque el Asistente está tratando de usar un dispositivo de su compañía para acceder al ERP, el rango de IP le resta -100 puntos por su ubicación. No tendrá acceso al ERP esta vez, independientemente de su deseo de usar autenticación multifactor.

Autenticación basada en el riesgo: Ejemplo 2

El Gerente de Ventas está trabajando en la oficina y quiere acceder al CRM para crear una oportunidad después de una reunión. Está usando su portátil de empresa y está accediendo a la aplicación localizada dentro de sus instalaciones.

Sistema CRM	
Requiere 120 puntos	
LAN	50
IP conocido	50
Dispositivo	50
Rango de IP (España)	50
Se requiere autenticación	
U&P	10
Aplicación móvil	60
Huella dactilar	20

Resultado: Autenticación con éxito (puede acceder)
El Director de Ventas supera con creces los puntos mínimos necesarios para acceder al CRM. Una vez que esté autentificado, puede usar el single Sign-on (SSO) para acceder a otras aplicaciones. Recibe una llamada del Asistente de Compras para acceder al sistema ERP y puede acceder con el número de puntos que recibe al ser contactado.

Máxima flexibilidad y control

El sistema de políticas le permite crear nuevas normas y combinarlas con las normas ya existentes, así como proporcionar un mecanismo para soportar una serie de escenarios de creciente complejidad.

Caracteristicas

Portal del Usuario

El Portal del Usuario es una característica de AuthControl Sentry®, diseñada para proporcionar a los administradores de una solución configurable y que ofrece autonomía a los usuarios para tareas básicas de autoadministración.

El Portal del Usuario proporciona a los administradores servicios como la capacidad de dar acceso directo a los usuarios, permitiendo a estos últimos satisfacer necesidades básicas como el cambio o restablecimiento del PIN o aprovisionar la aplicación móvil.

Aprovisionamiento de la aplicación móvil

Además de permitir a los usuarios cambiar y reiniciar su PIN, la aplicación móvil también puede ser aprovisionada sin esfuerzo. Se envía un correo electrónico al usuario detallando los pasos para aprovisionar la aplicación móvil y un QR para facilitar la configuración. Una vez implementados, los usuarios pueden autenticar el acceso a todos sus servicios habituales utilizando: El código de una sola vez (OTC) o la notificación PUSH.

Autoservicio

La función de autoservicio del Portal del Usuario reduce y/o suprime los costes asociados con la prestación del servicio de soporte para estas acciones.

Mayor eficiencia

El Portal del Usuario de Swivel Secure está diseñado para ofrecer una mayor eficiencia a los usuarios y que puedan ejecutar requisitos básicos, incluyendo:

- Cambiar su PIN
- Restablecimiento de su PIN
- Aprovisionamiento de la Aplicaciones Móvil
- Resincronización de tokens hardware.

Se pueden implementar restricciones para asegurar políticas específicas, asegurando que las acciones son conformes a los protocolos de seguridad.

Tecnología

swivelsecure

Tecnología patentada PINsafe®

PINsafe® es la tecnología patentada que da soporte a los factores de autenticación de imagen PINpad®, PICpad y TURing, todos dentro del rango de factores de autenticación disponibles con AuthControl Sentry®, la solución de autenticación multifactor diseñada para proteger a las organizaciones del acceso no autorizado a sus aplicaciones, redes y datos.

¿Cómo funciona PINsafe®?

A cada usuario se le asigna un número de identificación personal (PIN). No obstante, el PIN exacto nunca se teclea.

Cuando un usuario necesita autenticarse de forma segura, se les envía una cadena de seguridad de 10 dígitos, que consiste en una secuencia de caracteres o números. La cadena de seguridad se puede mostrar en forma de gráfico (TURing, PINpad® o PICpad) o puede ser recibido como un correo electrónico o a través de un SMS de verificación al móvil.

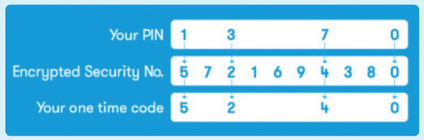
Al utilizar el PIN como indicador de posición, se extræ un código de un solo uso para la autenticación.

¿Puede mostrarme un ejemplo?

El siguiente ejemplo muestra que su PIN es 1370. En esta ocasión, la cadena de seguridad es 572169494380, por lo que su código es 5240.

La cadena de seguridad se puede integrar con muchos dispositivos y aplicaciones, en una variedad de formas para una flexibilidad completa. Incluyendo:

- Inicio de sesión en Windows
- Acceso remoto con F5, Citrix Netscaler y Cisco VPN
- Acceso a la Web con OWA, Apache y Microsoft ILS



Puesto que PINsafe® evita que el usuario tenga que introducir su PIN, se evita cualquier infiltración como en el caso de los ataques ‘man-in-the-middle’.

Factores

Factores de autenticación

Swivel Secure ofrece una amplia gama de factores de autenticación para garantizar que cada implementación resulte en la máxima adopción en toda su organización.

Tanto si decide autenticarse utilizando el OTC en la aplicación móvil (AuthControl Mobile®), un token hardware tradicional o incluso usando su huella dactilar, AuthControl Sentry® de Swivel Secure le proporciona la máxima seguridad y configurabilidad para adaptarse a las necesidades de seguridad de su empresa.

AuthControl Mobile®: OTC (código de un solo uso)

Cada vez que la aplicación le reta a autenticarse, simplemente utilice el OTC que se muestra en la pantalla de la App. Dado que existen 99 códigos, la función OTC es suficientemente versátil para poder ser usada offline. Una vez que el código ha sido introducido de forma correcta, se le concederá el acceso a la aplicación.

Factor de imagen: PINpad®

Se presenta como un código de 10 dígitos en forma de una cuadrícula numérica en el navegador del usuario. El usuario simplemente hace clic en las imágenes que representan su PIN. Cada imagen en la que hizo clic transmite un código TC diferente a AuthControl Sentry® para de ese modo autenticar al usuario.

Factor de imagen: PICpad

PICpad es un factor de autenticación que trasciende las opciones habituales del lenguaje de diversificación tanto de empleados como de clientes.

Usando los mismos principios que PINpad®, PICpad muestra símbolos en lugar de números, proporcionando de este modo un significado comprensible para entornos multinacionales.

AuthControl Mobile®: PUSH

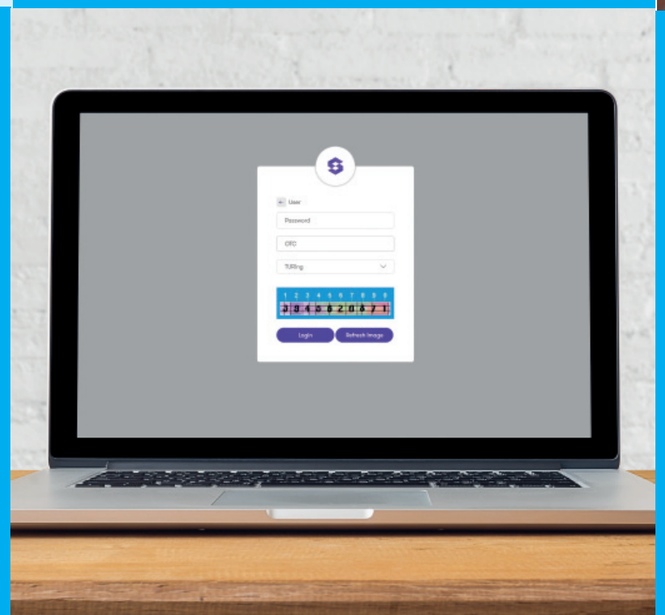
Simplemente presionando un botón en el móvil puede confirmar la autenticación al recibir la notificación enviada directamente a su móvil.

Implemente la funcionalidad One Touch® de forma rápida y con la configuración mínima requerida.

Factor de imagen: TURing

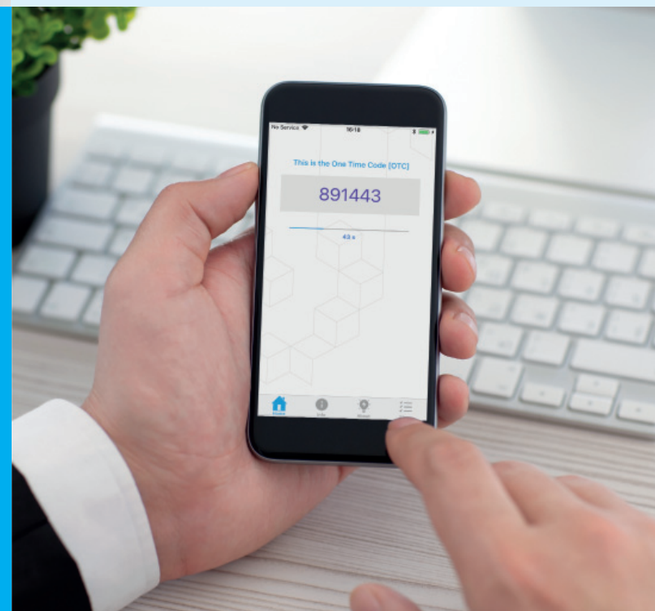
Se presenta con la forma de un código de 10 dígitos dentro de una imagen rectangular en la web del navegador. El usuario tiene que extræer de él el código representado en forma de números haciendo uso de su PIN.

Ejemplo: Si su PIN es 1370, entonces debe extræer el 1.º, 3.º, 7.º y 10.º número de la imagen.



AuthControl Mobile®: OATH

El token OATH es un token basado en el tiempo de 0 a 60, similar al token hardware tradicional usado para acceder a la VPN. El token OATH es compatible y proporciona al usuario un código de seis dígitos para autentificar.



Móvil: SMS

Para proteger el OTC (a través de SMS) de interceptación fraudulenta, el SMS se protege con PINsafe®. Esto significa que el SMS contiene una cadena de seguridad de dos secuencias alfanuméricas, y cuando se combina con el PIN del usuario se le proporciona su OTC.

Biometría: huella dactilar

El reconocimiento de huellas dactilares está disponible en el AuthControl Credential® Provider del marco biométrico de Windows 10 y para el controlador de acceso de huellas dactilares NITGEN. Los usuarios pueden autenticarse utilizando el controlador de huellas dactilares NITGEN o el lector de huellas dactilares integrado en su portátil.

AuthControl Voice

Mediante una llamada al usuario, AuthControl Voice vocaliza un código de una sola vez (OTC) o una notificación PUSH (SÍ o NO) para autenticar el acceso a las aplicaciones. El OTC que se entrega vocalmente por teléfono se debe escribir en la ventana si se solicita.

Token hardware

El token hardware proporciona a los usuarios un código de una sola vez (OTC) para que puedan acceder de forma segura a su aplicación. Cada vez que se presiona el botón del token hardware se proporciona un nuevo código, asegurando el este modo el acceso no autorizado.

swivelsecure

Integraciones

AuthControl Sentry® es una de las soluciones más flexibles del mercado, integrándose con cientos de aplicaciones y dispositivos de software a través de RADIUS, ADFS, SAML y con nuestra propia API - AgentXML.

No importa que necesite acceder a Salesforce, autenticarse con la aplicación móvil o iniciar sesión en el Proveedor de Credenciales de Windows usando una imagen de autenticación, AuthControl Sentry® es compatible con una amplia gama de aplicaciones y dispositivos, proporcionando la flexibilidad y la eficiencia necesarias para una autenticación sin riesgos en toda su organización.

Licencias

Disponemos de planes de licencia flexibles y modelos de precios adecuados para todas las organizaciones. El plan de licencias se cobra en base a usuario individual.

Licencias de usuario

Planes de licencias flexibles y modelos de precios adecuados para todas las organizaciones.

- Las licencias para AuthControl Sentry® son por usuario único
- Todas las licencias incluyen TODOS los factores de autenticación
- MFA, SSO y RBA se incluyen en AuthControl Sentry®
- Disponible en contratos de 1, 3, 5 ó 7 años o a perpetuidad.

Aplicación local

Las licencias perpetuas están disponibles para el uso local o para ser alojadas en una nube (Cloud) privada. El precio es por usuario, en una escala proporcional y decreciente, a partir de un mínimo de solo 10 usuarios. La política de precios es acumulativa, por lo que ésta es una forma extremadamente rentable para comprar un elevado volumen de licencias, en lugar de un modelo escalonado. Este sistema es adecuado para organizaciones que quieren invertir el costo de un servicio por adelantado y con un número de usuarios estables.

Aplicación en la nube (Cloud)

La licencia de suscripción está disponible para la nube (Cloud) y permite a las organizaciones cumplir con sus requisitos de usuario a medida que se modifica la demanda. Sin costes por adelantado y con un contrato flexible y sin penalizaciones por fin de uso. Es una solución ideal para organizaciones que quieren optimizar el coste de un servicio y con un número de usuarios variables.

Opciones de licencias

Utilice la siguiente tabla para comparar las opciones de licencias locales y en la nube (Cloud).

Tipo de licencia	On-Premise (local)	Nube (Cloud)
Autenticación basada en el riesgo	✓	✓
Integraciones (SAML/ADFS/RADIUS)	✓	✓
Aplicaciones On-Premise (local) y en la nube (Cloud)	✓	✓
Todos los factores de autenticación	✓	✓
Agente y Sincronización AD	✓	✓
Portal unificado con inicio de sesión único	✓	✓
Informes	✓	✓
Dispositivo (Físico/Virtual)	✓	✗
Imagen Amazon AWS	✗	✓
24x7x365	Opcional	✓

Servicio y soporte

Para asegurar que las organizaciones tengan acceso a la formación técnica y a las últimas funcionalidades, le ofrecemos distintos niveles de soporte: Standard y Premium. También disponemos de servicios profesionales para actualizar, desplegar, migrar y para integraciones complejas.

Contrato de mantenimiento (nivel de entrada)

Horario de soporte: 8/5. Acceso a actualizaciones de software, upgrades y correcciones de errores.

Contrato de Mantenimiento Estándar

Horario de soporte: el servicio estándar de Swivel Secure le ofrece soporte 24 horas al día, los 5 días laborables de la semana.

Contrato de Mantenimiento Premium

Horario de soporte: servicio 24 horas al día, 7 días a la semana, ideal par organizaciones empresariales que requieren un apoyo experto de inmediato.

Servicios Profesionales

Swivel Secure ofrece una amplia gama de productos profesionales: servicios para las organizaciones que requieren servicios adicionales o recursos técnicos a medida que se implementa la autenticación multifactor, garantizándole la compatibilidad con sistemas, conexiones y hardware existente.

Servicio de Technical Account Manager (TAM)

Nuestro servicio TAM le ofrece una guía proactiva y la gestión centralizada de servicios, garantizando beneficios y un apoyo prioritario dentro del canal de mantenimiento.

¿Necesita actualizar su dispositivo Swivel Secure?

Swivel Secure reconoce los problemas que pueden surgir durante una actualización y le ofrece un servicio de actualización desarrollado para garantizar que el servicio y su empresa sufran una interrupción mínima.

¿Su infraestructura de red es altamente compleja y requiere de numerosas integraciones?

Nuestro equipo de ingenieros expertos trabaja en estrecha colaboración con los equipos de Arquitectos Técnicos y de Servicios para garantizar que:

- Cualquier diseño propuesto se adapta a la arquitectura de su red
- El diseño cumple con sus requisitos de arquitectura organizacional y control de cambios

¿Necesita integrar un nuevo dispositivo RADIUS o SAML sin integración previa contra la que trabajar?

Nuestro equipo de desarrolladores de software está disponible para:

- Evaluar y desarrollar nuevas integraciones
- Facilitar nuevos plugins
- Responder a las solicitudes de funciones para mejorar el software.