



HOJA DE DATOS DE KYRIBA

Seguridad en tesorería

Tomando en cuenta que los fraudes y ataques cibernéticos se ejecutan cada día con mayor sofisticación y precisión, actualmente es de vital importancia garantizar que la información de la tesorería de su organización esté protegida, inclusive en el caso poco probable que los IDs de usuario y contraseñas se vean amenazados.

El paquete de Seguridad de Kyriba brinda capas adicionales de seguridad de aplicaciones para una mejor protección de la información y los flujos de trabajo de la tesorería. De hecho, la configuración estándar de Kyriba ofrece sólidos controles de contraseña, tales como tiempos de espera, reinicios obligatorios, requisitos alfanuméricos y el Teclado Virtual de Kyriba – todos los cuales se pueden configurar para cumplir con las políticas corporativas de TI y de tesorería.

La Seguridad de Kyriba ofrece funciones opcionales para llevarla protección y la seguridad de las aplicaciones al siguiente nivel a fin de evitar cualquier acceso no autorizado y posibles actividades fraudulentas.

Autenticación de Doble Factor

La autenticación de doble factor crea una contraseña única generada de manera aleatoria usando el teléfono inteligente del usuario, un token o un certificado digital SWIFT 3SKey. Cuando la autenticación de doble factor se activa, se solicita al usuario ingresar la contraseña única después de enviar su ID de usuario y contraseña normales. Esto hace de la autenticación de doble factor una eficaz herramienta para la prevención de fraudes cuando se utiliza por sí sola o en combinación con otros módulos de Seguridad Extendida de Kyriba, tales como el Filtrado de IP y VPN.

Filtrado de IP

El filtrado de IP es un método de seguridad que permite a los clientes restringir el acceso a un conjunto de direcciones IP predeterminadas – o rangos de direcciones – que el administrador de seguridad del sistema configura y mantiene. Si se utiliza por sí solo, el filtrado de IP es una eficaz herramienta para la prevención de fraudes. Además, el filtrado de IP puede usarse en combinación con otras funcionalidades de seguridad de Kyriba – por ejemplo, para cualquier usuario que ingrese fuera del conjunto predeterminado de direcciones IP es necesario utilizar la autenticación de doble factor.

Principales Funcionalidades:

- Autenticación de doble factor
- Centro de Control de Kyriba
- Firmas Digitales
- Filtrado de IP
- Red Privada Virtual
- Inicio de Sesión Único (SSO) Empresarial

Software como servicio (SaaS):

- Sin cargos de mantenimiento – basado en suscripción

Seguridad:

- Compatible con SOC 1 y SOC 2
- Recuperación de desastres redundante
- Cifrado, autenticación y administración
- Seguimientos de auditorías

Informes:

- Cientos de informes configurables
- Tableros de control predefinidos
- Programación automatizada
- Formatos PDF, Excel HTML
- Distribución de informes por medio de correo electrónico

La Seguridad Extendida de Kyriba ofrece funciones opcionales para llevarla protección y la seguridad de las aplicaciones al siguiente nivel a fin de evitar cualquier acceso no autorizado y posibles actividades fraudulentas.

Red Privada Virtual

Kyriba puede crear y mantener una red privada virtual (VPN) para cada cliente de manera que los usuarios puedan tener acceso a Kyriba a través de una red dedicada mantenida por Kyriba. La VPN es ideal para equipos de tesorería centralizados o regionales. Se utiliza comúnmente en combinación con el filtrado de IP y la autenticación de doble factor para personalizar el nivel de protección de los usuarios centralizados y descentralizados.

Firmas Digitales

Las firmas digitales son herramientas de identidad personal que permiten al usuario firmar mensajes y documentos electrónicos de manera digital, así como aprobar operaciones dentro del sistema. Kyriba admite el formato de firma digital SWIFT 3SKey. Las firmas digitales pueden utilizarse en los siguientes casos:

- Aprobación de pagos – aquellos pagos que se originan dentro de Kyriba o se importan de sistemas externos como ERP
- Autenticación de pagos enviados al banco a través de Kyriba – pagos gestionados dentro de Kyriba o lotes ciegos enviados mediante ERP al banco a través del Nodo de Pagos de Kyriba
- Autenticación de pagos enviados por canales no bancarios a través de Kyriba – para pagos gestionados dentro de Kyriba y lotes ciegos enviados mediante ERP
- Acceso a Kyriba como una opción la autenticación de doble factor

Inicio de Sesión Único (SSO) Empresarial

El SSO Empresarial permite al usuario acceder una única vez con un entorno de seguridad interna del cliente. El SSO Empresarial utiliza SAML 2.0 para la autenticación LDAP, lo cual significa que las credenciales de seguridad de cada usuario (por ejemplo, su ID de usuario y contraseña de Windows) pueden usarse para iniciar sesión en Kyriba y controlar el acceso dentro de Kyriba. Con el SSO Empresarial no se requiere ningún ID de usuario y contraseña adicional, y todos los controles de contraseña son gestionados internamente por el equipo de TI de la corporación de conformidad con sus políticas.

Centro de Control de Kyriba

Es fundamental mantener el control de los flujos de trabajo de tesorería para efectuar el seguimiento de errores, interrupciones y actividades sospechosas. Con frecuencia, se utiliza el Centro de Control de Kyriba para monitorear los flujos y la actividad de la tesorería dentro de Kyriba. El centro también puede usarse para detectar oportunamente usos no autorizados y fraudes potenciales. Ofrece la capacidad de monitorear y analizar:

- Fallas de conectividad con los banco, incluyendo archivos esperados pero no recibidos
- Archivos de pago sin recepción de acuse de recibo final
- Escalamiento y resumen de aprobaciones de flujo de trabajo pendientes
- Alertas de estado en tiempo real de inclusiones, eliminaciones o modificaciones de datos
- Estado de la luz de alerta (rojo / amarillo / verde) para el monitoreo del flujo, datos y tareas

Acerca de Kyriba

Kyriba es líder mundial en soluciones de gestión financiera en la nube que permite a los equipos de finanzas y tesorería con visión de futuro optimizar la gestión de activos monetarios y riesgos, pagos y estrategias de capital de trabajo. Kyriba ofrece una plataforma de SaaS 100% segura, excelente conectividad con los bancos y un conjunto de soluciones perfectamente integradas para hacer frente a muchos de los desafíos financieros más complejos de la actualidad. Con Kyriba, las organizaciones mundiales pueden hacer más eficientes sus procesos, elevar el nivel de protección de fraudes y cumplimiento e impulsar más oportunidades de crecimiento a través de un mejor pronóstico y apoyo de decisiones. Kyriba goza de la confianza de sus más de 1,600 clientes, entre los que se encuentran muchas de las marcas más grandes y reconocidas a nivel mundial. Con sede en Nueva York, Kyriba cuenta con oficinas en San Diego, París, Londres, Tokio y Dubái, además de otras importantes ciudades.

Para mayor información, por favor visite nuestro sitio: www.kyriba.com.