Fact Sheet

Extended Security

KYRIBA FACT SHEET

En raison de la plus grande sophistication et précision des fraudes et attaques informatiques, il devient plus que jamais indispensable de s'assurer que les informations de trésorerie sont protégées, même dans l'éventualité d'une découverte des identifiants utilisateurs et mots de passe.

Le pack Extended Security de Kyriba offre des fonctionnalités supplémentaires de sécurité pour l'application, afin de protéger encore davantage les workflows et informations de trésorerie. Kyriba, dans sa configuration classique, propose déjà des dispositifs de contrôle du mot de passe solides comme les limites d'expiration, les réinitialisations obligatoires, les exigences en matière de caractères alphanumériques et le clavier virtuel Kyriba. Ceux-ci peuvent être paramétrés pour satisfaire aux conditions des politiques informatiques de la trésorerie et de l'entreprise.

Kyriba Extended Security fournit des options afin d'augmenter la sécurité et la protection de l'application à propos des accès non autorisés et des activités potentiellement frauduleuses.

Authentification à deux facteurs

L'authentification à deux facteurs crée un mot de passe utilisable une fois et généré de façon aléatoire à l'aide du smartphone de l'utilisateur, d'un jeton ou d'un certificat numérique SWIFT 3SKey. Lorsque l'authentification à deux facteurs est activée, il est demandé à l'utilisateur de saisir le mot de passe utilisable une fois après avoir entré son identifiant et mot de passe classiques. Cela fait de l'authentification à deux facteurs un outil de prévention de la fraude efficace, qu'il soit utilisé seul ou mieux encore, en combinaison avec d'autres modules du pack Extended Security de Kyriba, comme le filtrage IP et le VPN.

Filtrage des adresses IP

Le filtrage d'adresses IP est une mesure de sécurité qui donne aux clients la possibilité de restreindre l'identification à une liste prédéfinie ou à des séries d'adresses IP paramétrées et conservées par l'administrateur de la sécurité du système. Lorsqu'il est utilisé seul, le filtrage IP constitue un outil de prévention de la fraude efficace. Le filtrage IP peut également être utilisé conjointement à d'autres fonctions de sécurité de Kyriba. Il est par exemple possible d'exiger que tout utilisateur ouvrant une session à partir d'une adresse IP non présente sur la liste, doive s'identifier à l'aide de l'authentification à deux facteurs.

Principales fonctionnalités:

- Authentification à deux facteurs
- Centre de contrôle Kyriba
- Signatures numériques
- Filtrage des adresses IP
- Réseau privé virtuel
- Enterprise SSO
- Conforme aux SOC 1 et SOC 2
- Redondances pour restauration en cas de sinistre
- Cryptage, authentification et administration
- Pistes d'audit

Reporting:

- Des centaines de rapports configurables
- Tableaux de bord innovants
- Traitements programmés automatiques
- Support des formats PDF,
- Excel et HTML
- Envoi des rapports par email

kyriba

Fact Sheet

Kyriba Extended Security fournit des options afin d'augmenter la sécurité et la protection de l'application à propos des accès non autorisés et des activités potentiellement frauduleuses.

Réseau privé virtuel

Kyriba peut également mettre en place et administrer un réseau privé virtuel (VPN) pour chaque client, dans le but que les utilisateurs accèdent uniquement à Kyriba par le biais d'un réseau dédié géré par la société. Le VPN est la solution idéale pour les équipes de trésorerie opérant au niveau central ou régional. Extended Security est habituellement utilisée avec le filtrage IP et l'authentification à deux facteurs, afin de personnaliser le niveau de protection pour les utilisateurs centralisés et décentralisés.

Signatures numériques

Les signatures numériques sont des outils liés à l'identité de l'utilisateur lui permettant de signer numériquement des messages et documents électroniques, ainsi que d'approuver les transactions au sein du système. Kyriba prend en charge le format de signature numérique SWIFT 3SKey. Les signatures numériques peuvent être utilisées lors des scénarios suivants:

- **Validation des paiements –** pour les paiements provenant de Kyriba ou importés à partir de systèmes externes comme un logiciel ERP.
- **Authentification des paiements envoyés à la banque à partir de Kyriba –** pour les paiements gérés au sein de Kyriba ou les lots dirigés de façon automatique à partir des logiciels ERP vers les banques en passant par le hub de paiement de Kyriba.
- **Authentification des paiements envoyés au moyen de circuits non bancaires à partir de Kyriba –** pour les paiements gérés au sein de Kyriba et les lots dirigés automatiquement à partir des logiciels ERP.
- Connexion à Kyriba, en tant que possibilité d'authentificationà deux facteurs.

Enterprise SSO

Enterprise SSO permet d'établir une connexion unique à l'environnement de sécurité interne du client. Enterprise SSO a recours au standard SAML 2.0 pour l'authentification LDAP, ce qui signifie que les informations de sécurité de chaque utilisateur (par exemple, leurs identifiants et mots de passe Windows) peuvent être utilisées pour se connecter à Kyriba et administrer l'accès utilisateur au sein de la solution. Avec Enterprise SSO, aucun identifiant et mot de passe supplémentaire n'est requis et l'ensemble des dispositifs de contrôle des mots de passe sont régulés en interne par les équipes et politiques informatiques de la société.

Centre de contrôle Kyriba

Le maintien du contrôle des workflows de trésorerie est important pour la surveillance des erreurs, perturbations et activités suspectes. Le centre de contrôle Kyriba est souvent employé pour le contrôle des workflows et des activités de trésorerie au sein de Kyriba. Extended Security peut également servir à la détection des utilisations non autorisées et des fraudes potentielles. Elle permet également de surveiller et analyser :

- Les erreurs de connexion bancaire, et notamment les fichiers attendus mais non reçus.
- Les fichiers de paiement dont l'accusé de réception n'a pas été reçu.
- Le total et le résumé des validations de workflows en attente.
- Les alertes de statut en temps réel lors de l'ajout, de la suppression ou de la modification des données.
- Le statut rouge/jaune/vert pour la surveillance des workflows, données et tâches.