Scheda informativa

Extended Security

SCHEDA INFORMATIVA DI KYRIBA

Con l'avvento di frodi e attacchi informatici sempre più complessi e precisi, diventa sempre più importante mettere al sicuro le informazioni della tesoreria, anche nell'improbabile evento di una compromissione di UserID e password della tesoreria.

Il pacchetto Extended Security di Kyriba fornisce ulteriori livelli di sicurezza delle applicazioni per meglio proteggere i flussi di lavoro e i dati della tesoreria. La configurazione standard di Kyriba offre già potenti strumenti di controllo basati su password come timeout, ripristini obbligatori, requisiti alfanumerici e Virtual Keyboard di Kyriba, il tutto impostabile secondo le politiche IT aziendali e della tesoreria.

Extended Security di Kyriba offre funzionalità aggiuntive per offrire misure di sicurezza e protezione delle applicazioni di livello superiore e prevenire accessi non autorizzati e attività potenzialmente fraudolenti.

Autenticazione a due fattori

L'autenticazione a due fattori crea una password monouso generata casualmente utilizzando lo smartphone dell'utente, un token o un certificato digitale SWIFT 3SKey. Quando l'autenticazione a due fattori viene attivata, all'utente viene chiesto di inserire prima il nome utente e la password ordinaria e poi la password monouso. Ciò rende l'autenticazione a due fattori uno strumento di prevenzione delle frodi efficace sia se utilizzata da sola, sia se usata in combinazione con altri moduli di Extended Security di Kyriba, come il filtro IP e la VPN.

Filtro IP

Il filtro IP è una funzionalità di sicurezza che consente ai client di limitare l'accesso a un set predefinito o a una gamma di indirizzi IP, impostati e gestiti dall'amministratore della sicurezza del sistema. Anche se utilizzato da solo, il filtro IP è uno strumento di prevenzione delle frodi efficace. Esso però può essere usato anche in combinazione con altre funzionalità di sicurezza di Kyriba: per esempio, agli utenti che cercano di effettuare l'accesso da un indirizzo IP diverso da quelli predefiniti potrebbe essere chiesto di usare l'autenticazione a due fattori.

Funzionalità chiave:

- Autenticazione a due fattori
- Centro di controllo Kyriba
- Firme digitali
- Filtro IP
- Virtual Private Network
- SSO aziendale
- Conformità SOC 1 e SOC 2
- Ripristino di emergenza con ridondanza
- Crittografia, autenticazione e amministrazione
- Audit trail

Reporting:

- Centinaia di report configurabili
- Dashboard pronti all'uso
- Pianificazione automatizzata
- Formati PDF, Excel e HTML
- Report distribuiti mediante e-mail

kyriba

Scheda informativa

Extended Security di Kyriba offre funzionalità aggiuntive per offrire misure di sicurezza e protezione delle applicazioni di livello superiore e prevenire accessi non autorizzati e attività potenzialmente fraudolenti.

Virtual Private Network

Kyriba può configurare e gestire una virtual private network (VPN, rete privata virtuale) per ciascun client. In questo modo, gli utenti accedono a Kyriba unicamente tramite una rete dedicata e gestita da Kyriba. La VPN è una soluzione ideale per le squadre di tesoreria centralizzate o regionalizzate. Normalmente viene utilizzata insieme al filtro IP e all'autenticazione a due fattori per personalizzare il livello di protezione rispetto sia agli utenti centralizzati che a quelli decentralizzati.

Firme digitali

Le firme digitali sono strumenti di identificazione personale che consentono all'utente di firmare digitalmente messaggi e documenti elettronici, nonché approvare le transazioni internamente al sistema. Kyriba supporta il formato di firma digitale SWIFT 3SKey. Le firme digitali possono essere usate nei seguenti scenari:

- **Approvazione dei pagamenti** - i pagamenti generati all'interno del sistema di Kyriba o importati da sistemi esterni come l'ERP
- **Autenticazione dei pagamenti inviati alle banche da Kyriba** - i pagamenti gestiti internamente al sistema di Kyriba o quelli semplicemente inviati alle banche dall'ERP tramite l'hub dei pagamenti di Kyriba
- **Autenticazione dei pagamenti inviati da Kyriba tramite canali non bancari** - sia nel caso di pagamenti gestiti internamente al sistema di Kyriba che in quello di pagamenti inviati alle banche dall'ERP
- Accesso a Kyriba come uno dei due fattori dell'autenticazione a due fattori

SSO aziendale

Il single sign-on (SSO) aziendale aiuta a snellire l'ambiente di sicurezza interno dei client. L'SSO aziendale sfrutta il SAML 2.0 per l'autenticazione LDAP. Questo significa che le credenziali di sicurezza di ciascun utente (per esempio, nome utente e password su Windows) possono essere usate per effettuare l'accesso a Kyriba e limitarne l'attività all'interno del sistema di Kyriba. Con l'SSO aziendale, non servono altri nomi utente e password. Tutti i controlli tramite password vengono gestiti internamente dalla squadra IT e dalle politiche aziendali.

Centro di controllo Kyriba

Poter tenere sotto controllo tutte le fasi dei flussi di lavoro della tesoreria è importante per monitorare errori, problemi e attività sospette. Il centro di controllo Kyriba viene spesso usato per monitorare i flussi di lavoro e le attività della tesoreria all'interno del sistema di Kyriba. Il centro può essere usato anche per rilevare tempestivamente attività non autorizzate e potenziali frodi. Esso offre la possibilità di monitorare e analizzare:

- Gli errori nella connettività bancaria, inclusi i file attesi ma non ricevuti
- I file di pagamento di cui non è stata ricevuta la conferma finale
- L'escalation e il riepilogo delle approvazioni dei flussi di lavoro in sospeso
- Gli avvisi in tempo reale in caso di aggiunta, rimozione e modifica di dati
- Gli status verde/giallo/rosso del monitoraggio dei flussi di lavoro, dei dati e dei compiti

kyriba

kyriba.it infokyriba@kyriba.com