Fact Sheet

Extended Security

KYRIBA FACT SHEET

With fraud and cyberattacks being executed with greater sophistication and precision, it is even more important to ensure that treasury information is protected, even in the unlikely event that treasury's user IDs and passwords are compromised.

Kyriba's Extended Security package offers additional layers of application security to better protect treasury workflows and information. Kyriba's standard configuration already offers strong password controls such as timeouts, mandatory resets, alphanumeric requirements and Kyriba's Virtual Keyboard – all of which can be set up to meet treasury and corporate IT policies.

Kyriba's Extended Security delivers optional features to take application security and protection to the next level in preventing unauthorized access and potential fraudulent activity.

Dual-Factor Authentication

Dual-factor authentication creates a randomly generated one-time password using the user's smartphone, a token or a SWIFT 3SKey digital certificate. When dual-factor authentication is activated, the user is prompted to enter the one-time password after submitting their normal user ID and password. This makes dual-factor authentication an effective fraud prevention tool when used on its own or in combination with other Kyriba Extended Security modules such as IP Filtering and VPN.

IP Filtering

IP filtering is a security feature that allows clients to restrict login to a pre-defined set of IP addresses – or ranges of addresses – which are set up and maintained by the system security administrator. If used on its own, IP filtering is an effective fraud prevention tool. IP filtering can also be used in combination with other Kyriba security capabilities – for example any user logging in outside of the pre-defined set of IP addresses is required to use dual-factor authentication.

Key Capabilities:

- Dual-factor authentication
- Kyriba Control Center
- Digital signatures
- IP filtering
- Virtual private network
- Enterprise SSO
- SOC 1 and SOC 2 compliant
- Redundant disaster recovery
- Encryption, authentication and administration
- Audit trails

Reporting:

- Hundreds of configurable reports
- Out-of-the-box dashboards
- Automated scheduling
- PDF, Excel and HTML formats
- Distribute reports via email

kyriba

Fact Sheet

Kyriba's Extended Security delivers optional features to take application security and protection to the next level in preventing unauthorized access and potential fraudulent activity.

Virtual Private Network

Kyriba can set up and maintain a virtual private network (VPN) for each client so that users only access Kyriba through a dedicated network maintained by Kyriba. The VPN is ideal for centralized or regionalized treasury teams. It is commonly used in combination with IP filtering and dual-factor authentication to customize the level of protection for both centralized and decentralized users.

Digital Signatures

Digital signatures are personal identity tools that allow the user to digitally sign messages and electronic documents, as well as approve transactions within the system. Kyriba supports the SWIFT 3SKey digital signature format. Digital signatures can be used in the following scenarios:

- **Approve payments** – those payments originating within Kyriba or imported from external systems such as ERP
- **Authenticate payments sent to bank from Kyriba** – payments managed within Kyriba or batches blind routed from ERP to the bank via Kyriba's Payment Hub
- **Authenticate payments sent via non-bank channels from Kyriba** – for both payments managed within Kyriba and batches blind routed from ERP
- Login to Kyriba as one option for dual-factor authentication

Enterprise SSO

Enterprise single sign-on (SSO) helps streamline a client's internal security environment. Enterprise SSO uses SAML 2.0 for LDAP authentication, meaning that each user's security credentials (for example, their Windows user ID and password) can be used to log in to Kyriba and drive user access within Kyriba. With Enterprise SSO, no additional user ID and password is required, and all password controls are managed internally by the corporate IT team and policies.

Kyriba Control Center

Maintaining control of treasury workflows is important for monitoring of errors, disruptions and suspicious activity. Kyriba Control Center is often used for monitoring workflows and treasury activity within Kyriba. The center can also be used for early detection of unauthorized usage and potential fraud. It offers the ability to monitor and analyze:

- Bank connectivity failures, including files expected, but not received
- Payment files where final acknowledgement was not received
- Escalation and summary of pending workflow approvals
- Real-time status alerts of additions, deletions or modifications of data
- Red/yellow/green status for workflow, data and task monitoring

kyriba