DATA SHEET

EXPRESS SECURITY MODULE FOR EFT™ EXPRESS

KEY RESULTS

- Achieve or exceed industry, government, and corporate security standards
- Actively monitor PCI DSS compliance requirements
- Warnings when security configuration is changed to non-compliant settings
- Industry-standard secure protocols, strong ciphers, encryption keys
- Minimized attack vector
- Easy security configuration
- Protection of data at rest
- Protection of data in transit
- Centralized control of access to data
- Capture all of this activity in a relational database.

The Express Security module (ESM) for EFT Express secures sensitive data, provides secure authentication options, and achieves or exceeds security practices mandated by the most rigorous standards.

Securing sensitive company data requires continuous monitoring and validation of security policies and controls. Globalscape makes it easy for an administrator to create and maintain file-transfer services that meet or exceed these standards with a simple set-up wizard. Once enabled, the ESM is an ever-vigilant security tool that disallows low-security options, captures compensating controls, and generates reports for auditing the system's compliance status.

COMPLY WITH REQUIREMENTS

Whether your business is obligated to comply with standards and regulations such as GDPR, PCI DSS, FIPS 140-2, HIPAA, HITECH, SOX, GLBA/FFEIC, DIACAP, or simply want a strict security configuration, a setup wizard provides you with an easy, step-by-step method to configuring a security-enabled site, with each page describing the requirement and what you need to do to meet that requirement, or to provide a compensating control (workaround).

The ESM also eliminates the need to create, maintain, and track standards compliance of built-in administrator accounts and maintain and ensure compliance of accounts in one location by using existing Active Directory infrastructure for EFT account creation.

The ESM, in concert with EFT and DMZ Gateway®, helps organizations comply with data storage requirements—including not storing data in the network DMZ—using repository encryption and securely sanitizing (wiping) deleted data so that it cannot be reconstituted.

SECURE SENSITIVE DATA

By enforcing the use of secure protocols, strong ciphers, encryption keys, and password policies, data transfers strictly follow all security guidelines. With support for multiple secure protocols, including FIPS 140-2 certified protocols, the ESM protects data in transit.

The ESM actively monitor PCI DSS and strict security settings by alerting on non-compliance, identifying the cause of non-compliance, allowing reverting of security controls, implementing mitigation/workaround techniques.

The Auditing and Reporting module (ARM) captures all of this activity in a relational database, including any administrator changes to settings.

EFT

GLOBALSCAPE

AUTOMATICALLY ENFORCE POLICY

The ESM enforces account access policy controls such as the automatic lock out of accounts after a set amount of incorrect login attempts and the removal of inactive accounts after a certain period of inactivity. Additional security controls can be set to expire passwords automatically on certain dates, and notifications such as emails and banners can be configured accordingly. For user authentication, you can use an AD, NTLM, LDAP, or ODBC-compatible database, or the local authentication manager built into EFT Express.

EFT SECURITY FEATURES

The ESM layers on top of EFT Express built-in security features, including:

- Extensive options for secure transport protocols
- User-friendly interfaces for sending and receiving files
- Data encryption and security, including OpenPGP
- Industry-leading authentication and user account controls
- Event-based automation and processing

ESM SECURITY FEATURES MAPPED TO PCI DSS REQUIREMENTS

- Automatically redirects HTTP to HTTPS (PCI DSS 2.2.3)
- Forces password reset on initial use (PCI DSS 8.2.6)
- Expires user and/or Admin passwords after 90 days (PCI DSS 8.2.4)
- Enables password expiration reminders (e-mail, banner)
- Removes old data automatically Data sanitization/wiping (PCI DSS 9)
- Removes inactive accounts after 90 days (PCI DSS 8.1.4)
- Hides or disables non-allowed cipher or SSL versions, key lengths <128 bits, anonymous account type, and warns when importing certificates with weak keys (PCI DSS 4.1)
- Warns if password complexity is disabled (PCI DSS 8.2.3)
- Warns if insecure protocols are in use (PCI DSS 2.2.2)
- Warns if user disk quota is not set (PCI DSS 3.1)
- Warns if secure remote administration not set (PCI DSS 2.3)
- Warns if Encrypting File System (EFS) in use (PCI DSS 3.4.1)
- Warns if weak SSL or SFTP keys are in use (PCI DSS 3.6.1)
- Warns if weak SSL versions and ciphers are in use (PCI DSS 4.1)
- Warns if DoS and flood settings are too low (PCI DSS 2.2.4)
- Warns if vendor defaults remain unchanged (PCI DSS 2.1)
- Warns if expired keys present (PCI DSS 3.6.5)
- Warns if multiple administrator roles present (PCI DSS 7.1)
- Warns if anonymous account type in use (PCI DSS 8.5)
- Causes idle sessions to automatically timeout (PCI DSS 8.1.8)
- Limits repeated invalid login attempts (PCI DSS 8.1.6)

ABOUT GLOBALSCAPE

Globalscape, Inc. (NYSE MKT: GSB) is a pioneer in securing and automating the movement and integration of data seamlessly in, around and outside your business, between applications, people and places, in and out of the cloud. Globalscape provides cloud services that automate your work, secure your data and integrate your applications – while giving visibility to those who need it. Globalscape makes business flow brilliantly. For more information, visit http://www.globalscape.com or follow the blog and Twitter updates.

Contact Globalscape to find out more about EFT™ Express and the Express Security Module.

GLOBALSCAPE

www.globalscape.com
1.800.290.5054

4500 Lockhill-Selma Rd, Suite 150
San Antonio, TX 78249
United States