ADVANCED AUTHENTICATION MODULE

KEY RESULTS

Single source of authentication across the IT resources.

Interoperability with the following multi-factor authentication methods:

- SAML (Web SSO)
- RSA SecurID®
- RADIUS
- CAC
- SMS

Centralized source of authentication

Simplified management of authentication

Manage and maintain password security in one location

Organizations need a solution that gives them more control to enforce strong passwords while providing a user-friendly solution that doesn't impede or reduce productivity. EFT™ Enterprise with Advanced Authentication module (AAM) provides support for easy-to-use authentication methods, including smart card, single sign-on, and multi-factor authentication options. By centralizing authentication methods and using an interoperable solution like AAM with EFT Enterprise, users can use a single source of authentication across the IT resources they use, including EFT. AAM includes the features and functionality described below.

Protect your organization with the powerful and convenient Advanced Authentication module (AAM) for EFT Enterprise. Improve productivity through AAM's centralized source of identity management, while also protecting your organization. AAM simplifies security measures for both administrator and end user, so you can protect your employees and customers.

SAML WEB SINGLE SIGN-ON (SSO)

Identity management is achieved through a centralized source of authentication. Single Sign-On (SSO) provides users with the ability to input their credentials once to have secure access to multiple sites, apps, or resources via SAML protocol support. EFT supports SAML v2.0 and has been verified against SafeNet Authentication Services, Shibboleth, Microsoft ADFS, and Salesforce. Web SSO support in EFT is limited to LDAP, ODBC, and Globalscape-authenticated Sites

REMOTE AUTHENTICATION DIAL-IN USER (RADIUS) INTEGRATION

In EFT Enterprise, the server has been extended for RADIUS support for RSA SecurID® two-factor authentication to send and receive RADIUS packets to/from a RADIUS server for user authentication. RADIUS authentication can be added to Globalscape, LDAP, and ODBC-authenticated Sites in EFT Enterprise's administration interface. The RADIUS settings allow you to configure EFT Enterprise as a Network Access Server (NAS).

RSA SECURID® AUTHENTICATION COMPATIBILITY

EFT Enterprise is compatible with RSA's Authentication Manager (AM), version 8.1. This guarantees interoperability with the latest supported version of EFT Enterprise and RSA AM, for two-factor authentication in conjunction with Globalscape, LDAP, and ODBC-authenticated sites. Globalscape is also an "RSA Secured" partner.

EFT

GLOBALSCAPE

ABOUT GLOBALSCAPE

Globalscape 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. Founded in 1996, Globalscape's data exchange and integration software and services are trusted by over 13,000 customers in over 150 countries worldwide, including global enterprises, governments, and small and medium enterprises. Headquartered in San Antonio, TX, Globalscape enables companies to increase business agility by unleashing the power of data. Whether you are a line-of-business stakeholder struggling to connect multiple cloud applications or an IT professional tasked with integrating partner data into homegrown or legacy systems, 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. Globalscape has consistently been named a top workplace by Computerworld, the San Antonio Business Journal, Texas Monthly, and the San Antonio Express-News, among others.

COMMON ACCESS CARD (CAC) AUTHENTICATION SUPPORT

The Common Access Card (CAC) is the standard identification for active duty uniformed service personnel, Selected Reserve, DoD civilian employees, and eligible contractor personnel in the United States. CAC authentication is available in EFT Enterprise for LDAP Sites with SSL (HTTPS or FTPS) enabled. EFT Enterprise with AAM supports CAC PIV via RFC822 Name, which provides unified access and authentication to provide physical access to buildings and computer systems.

SHORT MESSAGING SERVICE (SMS)-BASED AUTHENTICATION

The EFT platform can provide SMS authentication to using the Remote Authentication Dial-In User Service (RADIUS) implementation already built in to EFT, and Microsoft Network Policy Server (NPS) built in to Windows 2012 and later to connect to an SMS server for authentication. EFT Enterprise includes multi-factor authentication through the CensorNet MFA (formerly known as SMS PASSCODE) platform. On a local or LDAP-authenticated site, the administrator can configure EFT to connect to the SMS server to deliver a one-time-use passcode via text message (SMS), a voice call, through email, or via an app on the user's mobile phone as part of the login process for HTTP, HTTPS, or SFTP transfers.

www.globalscape.com
1.800.290.5054

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