# EFT Server FISMA and FedRAMP Compliance

THE INFORMATION IN THIS ARTICLE APPLIES TO:

EFT v7.4.x and later

DISCUSSION

## Summary

Although and FISMA and FedRAMP are separate initiatives, with the former initially focused on on-premises governmental systems, and the latter focused on cloud-based deployments, they are both closely tied to NIST Special Publication (SP) 800-53A revision 4 controls. These controls can be leveraged by organizations seeking compliance with either standard, for planned or implemented software ecosystems that fall within the scope of these standards; however, because these ecosystems are largely comprised of a number of third party enterprise software applications and middleware, it is incumbent on the organization seeking compliance to ensure that the third-party software solutions being deployed will facilitate, rather than detract from, their compliance efforts.

## Mapping Table

| **NIST SP 800-53A Security Controls** | | **NIST 800-171** | **Globalscape Solution Mapping** |
|---|---|---|---|
| **No.** | **Control** | **CUI No.** | **EFT** |
| **AC-1** | ACCESS CONTROL POLICY AND PROCEDURES | | Customer Responsibility (**CR**) and/or Inherited Controls (**IC**) |
| **AC-2** | ACCOUNT MANAGEMENT | 3.1.1,3.1.2 | EFT provides a comprehensive set of built-in account management controls, including flexible |

| | | | |
|---|---|---|---|
| | | | authentication manager (directory) services and permissions (authorization) systems. |
| **AC-3** | ACCESS ENFORCEMENT | 3.1.1,3.1.2 | EFT provides numerous mechanisms for controlling and enforcing access. |
| **AC-4** | INFORMATION FLOW ENFORCEMENT | 3.1.3 | EFT provides a hierarchal permissions management system similar to how Active Directory permissions works. |
| **AC-5** | SEPARATION OF DUTIES | 3.1.4 | EFT separates (logically and functionality) administrator from end user (consumer) permissions. |
| **AC-6** | LEAST PRIVILEGE | 3.1.5, 3.1.6, 3.1.7 | While mainly the responsibility of the customer, EFT provides mechanisms to limit what authorized administrators can do. |
| **AC-8** | SYSTEM USE NOTIFICATION | 3.1.9 | as web client is fully customizable (ToS, |

| | | | |
|---|---|---|---|
| | | | Privacy, etc.) |
| **AC-17** | REMOTE ACCESS | 3.1.1,3.1.2 | EFT provides a number of access controls for securing remote administrative access. |
| **AC-18** | WIRELESS ACCESS | 3.1.16 | See mobile access |
| **AC-19** | ACCESS CONTROL FOR MOBILE DEVICES | 3.1.18 | EFT provides access controls for mobile users (not administrators) that control security on the native mobile app and within EFT (via authorization and ACLs) |
| **AC-20** | USE OF EXTERNAL INFORMATION SYSTEMS | 3.1.20 | CR/IC |
| **AT-1** | SECURITY AWARENESS AND TRAINING POLICY AND PROCEDURES | 3.2.1-2 | CR/IC |
| **AT-2** | SECURITY AWARENESS TRAINING | 3.2.1, 3.2.2 | CR/IC |
| **AT-3** | ROLE-BASED SECURITY TRAINING | 3.2.1, 3.2.2 | CR/IC |

| | | | |
|---|---|---|---|
| **AU-1** | AUDIT AND ACCOUNTABILITY POLICY AND PROCEDURES | | CR/IC |
| **AU-2** | AUDIT EVENTS | 3.3.1, 3.3.2,3.3.3 | EFT provides a complete audit and logging trail. |
| **AU-3** | CONTENT OF AUDIT RECORDS | 3.3.1, 3.3.2 | EFT captures all relevant metadata around transactional (end user) and administrative events. |
| **AU-4** | AUDIT STORAGE CAPACITY | | CR/IC |
| **AU-5** | RESPONSE TO AUDIT PROCESSING FAILURES | 3.3.4 | CR/IC |
| **AU-6** | AUDIT REVIEW, ANALYSIS, AND REPORTING | 3.3.1, 3.3.2, 3.3.5 | EFT offers a comprehensive set of reports as an optional component. |
| **AU-8** | TIME STAMPS | 3.3.7 | EFT audits timestamps. It is up to the customer to configure the operating system to sync with authoritative time sources. |
| **AU-9** | PROTECTION OF AUDIT INFORMATION | 3.3.8, 3.3.9 | CR/IC |

| | | | |
|---|---|---|---|
| **AU-12** | AUDIT GENERATION | 3.3.1, 3.3.2 | EFT offers all necessary controls to enable auditing, determine source of audit logs (database type), control over log level, etc. |
| **CA-1** | SECURITY ASSESSMENT AND AUTHORIZATION POLICY AND PROCEDURES | | CR/IC |
| **CA-3** | SYSTEM INTERCONNECTIONS | | Although mainly determined by customer, EFT provides a robust integration framework (Event Rules engine) that facilitates integration with 3rd party systems. |
| **CM-1** | CONFIGURATION MANAGEMENT POLICY AND PROCEDURES | | CR/IC |
| **CM-2** | BASELINE CONFIGURATION | 3.4.1, 3.4.2 | CR/IC |
| **CM-3** | CONFIGURATION CHANGE CONTROL | 3.4.3 | CR/IC |
| **CM-5** | ACCESS RESTRICTIONS FOR CHANGE | 3.1.5 | EFT utilizes access controls to restrict access; however, it is |

| | | | |
|---|---|---|---|
| | | | the customer's responsibility to establish and documents usage restrictions, configuration/connection requirements, and implementation guidance |
| **CM-6** | CONFIGURATION SETTINGS | 3.4.1, 3.4.2 | CR/IC |
| **CM-7** | LEAST FUNCTIONALITY | 3.4.6, 3.4.7,3.4.8 | for administrators via granular admin roles with diminished privileges to end user authorization and controls. |
| **CM-8** | INFORMATION SYSTEM COMPONENT INVENTORY | 3.4.1, 3.4.2 | CR/IC |
| **CM-9** | CONFIGURATION MANAGEMENT PLAN | | CR/IC |
| **CM-11** | USER-INSTALLED SOFTWARE | 3.4.9 | CR/IC |
| **CP-1** | CONTINGENCY PLANNING POLICY AND PROCEDURES | | EFT provides the ability to configure high availability active-passive (N-1) or active-active clusters, back-up and restore configuration, |

| | | | |
|---|---|---|---|
| | | | and export of configuration settings for easy migration to DR site. |
| **CP-2** | CONTINGENCY PLAN | | See CP1, but ultimately is the customer's responsibility. |
| **CP-6** | ALTERNATE STORAGE SITE | | CR/IC |
| **CP-7** | ALTERNATE PROCESSING SITE | | CR/IC |
| **CP-8** | TELECOMMUNICATIONS SERVICES | | CR/IC |
| **CP-9** | INFORMATION SYSTEM BACKUP | | CR/IC |
| **CP-10** | INFORMATION SYSTEM RECOVERY AND RECONSTITUTION | | CR/IC |
| **IA-1** | IDENTIFICATION AND AUTHENTICATION POLICY AND PROCEDURES | | CR/IC |
| **IA-2** | IDENTIFICATION AND AUTHENTICATION (ORGANIZATIONAL USERS) | 3.5.1-4 | CR/IC |

| | | | |
|---|---|---|---|
| **IA-3** | DEVICE IDENTIFICATION AND AUTHENTICATION | No map | EFT identifies all devices that connect to it via a combination of IP address, username, password, and 2nd factor authentication if configured. EFT also provides an IP access and ban list to filter unauthorized IP addresses. |
| **IA-4** | IDENTIFIER MANAGEMENT | 3.5.5,3.5.6 | Yes |
| **IA-5** | AUTHENTICATOR MANAGEMENT | 3.5.1-2, 3.5.7-10 | Yes |
| **IA-7** | CRYPTOGRAPHIC MODULE AUTHENTICATION | | EFT provides a wide variety of encryption methods for KEX, transmission, message/data encryption and signing, receipt signing, and encryption of data at rest. Standards include SSL/TLS, FIPS, PGP, and so on. |
| **IA-8** | IDENTIFICATION AND AUTHENTICATION (NON-ORGANIZATIONAL USERS) | | EFT provides mechanisms for authentication and authorizing users that are not part of the organization, including |

| | | | |
|---|---|---|---|
| | | | self-provisioning, with full control and audit trail for administrator control. |
| **IR-1** | INCIDENT RESPONSE POLICY AND PROCEDURES | | CR/IC |
| **IR-4** | INCIDENT HANDLING | 3.6.1-2 | CR/IC |
| **IR-5** | INCIDENT MONITORING | 3.6.1-2 | CR/IC |
| **IR-6** | INCIDENT REPORTING | 3.6.1-2 | CR/IC |
| **IR-8** | INCIDENT RESPONSE PLAN | | CR/IC |
| **MA-1** | SYSTEM MAINTENANCE POLICY AND PROCEDURES | | CR/IC |
| **MP-1** | MEDIA PROTECTION POLICY AND PROCEDURES | | CR/IC |
| **MP-2** | MEDIA ACCESS | 3.8.1-3 | CR/IC |
| **MP-4** | MEDIA STORAGE | 3.8.1-3 | CR/IC |
| **MP-5** | MEDIA TRANSPORT | 3.8.5-6 | CR/IC |
| **MP-6** | MEDIA SANITIZATION | 3.8.1-3 | CR/IC |

| | | | |
|---|---|---|---|
| **MP-7** | MEDIA USE | 3.8.7-8 | CR/IC |
| **PE-1** | PHYSICAL AND ENVIRONMENTAL PROTECTION POLICY AND PROCEDURES | | CR/IC |
| **PE-2** | PHYSICAL ACCESS AUTHORIZATIONS | 3.10.1, 3.10.2 | CR/IC |
| **PE-3** | PHYSICAL ACCESS CONTROL | 3.10.3-5 | CR/IC |
| **PE-4** | ACCESS CONTROL FOR TRANSMISSION MEDIUM | 3.10.1, 3.10.2 | CR/IC |
| **PE-6** | MONITORING PHYSICAL ACCESS | | CR/IC |
| **PE-9** | POWER EQUIPMENT AND CABLING | | CR/IC |
| **PE-10** | EMERGENCY SHUTOFF | | CR/IC |
| **PE-11** | EMERGENCY POWER | | CR/IC |
| **PE-12** | EMERGENCY LIGHTING | | CR/IC |
| **PE-13** | FIRE PROTECTION | | CR/IC |
| **PE-14** | TEMPERATURE AND HUMIDITY CONTROLS | | CR/IC |

| | | | |
|---|---|---|---|
| **PE-15** | WATER DAMAGE PROTECTION | | CR/IC |
| **PL-1** | SECURITY PLANNING POLICY AND PROCEDURES | | CR/IC |
| **PL-2** | SYSTEM SECURITY PLAN | | CR/IC |
| **PL-8** | INFORMATION SECURITY ARCHITECTURE | | While this is a customer responsibility, EFT security features support a defense-in-depth strategy. |
| **PS-1** | PERSONNEL SECURITY POLICY AND PROCEDURES | | CR/IC |
| **PS-2** | POSITION RISK DESIGNATION | | CR/IC |
| **PS-3** | PERSONNEL SCREENING | | CR/IC |
| **PS-4** | PERSONNEL TERMINATION | | CR/IC |
| **PS-7** | THIRD-PARTY PERSONNEL SECURITY | | CR/IC |
| **RA-1** | RISK ASSESSMENT | | CR/IC |

| | | | |
|---|---|---|---|
| | POLICY AND PROCEDURES | | |
| **RA-2** | SECURITY CATEGORIZATION | | CR/IC |
| **RA-3** | RISK ASSESSMENT | 3.11.1 | CR/IC |
| **RA-5** | VULNERABILITY SCANNING | 3.11.2,3.11.3 | CR/IC |
| **SA-1** | SYSTEM AND SERVICES ACQUISITION POLICY AND PROCEDURES | | CR/IC |
| **SA-2** | ALLOCATION OF RESOURCES | | CR/IC |
| **SA-3** | SYSTEM DEVELOPMENT LIFE CYCLE | | While this is a customer responsibility, EFT, as part of broader system, is based on a "security by design" principle. When configured properly and used with the corresponding DMZ Gateway product, the solution can be deployed in a matter that significantly reduces attack vectors, thus complying with this directive. |

| | | | |
|---|---|---|---|
| **SA-4** | ACQUISITION PROCESS | | CR/IC |
| **SA-8** | SECURITY ENGINEERING PRINCIPLES | | CR/IC |
| **SA-9** | EXTERNAL INFORMATION SYSTEM SERVICES | | Globalscape's EFT software complies with many organizational information security requirements as defined in applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance; |
| **SA-10** | DEVELOPER CONFIGURATION MANAGEMENT | | Globalscape's EFT software repository is subject to formal configuration management controls for source control, including revisions, access, builds, commits, etc. |
| **SA-11** | DEVELOPER SECURITY TESTING AND EVALUATION | | Globalscape's EFT software undergoes security testing and evaluation by nature of all new feature designs or refactors being subjected to |

| | | | |
|---|---|---|---|
| | | | architectural oversight committees, code peer reviews, adherence to standards such as OWASP, and post build security assessment tools such as HTBridge and Qualsys |
| **SC-1** | SYSTEM AND COMMUNICATIONS PROTECTION POLICY AND PROCEDURES | | CR/IC |
| **SC-2** | APPLICATION PARTITIONING | | While this is a customer responsibility, EFT separates admin and user functionality |
| **SC-4** | INFORMATION IN SHARED RESOURCES | | if configured properly, EFT's access controls prevent unauthorized information transfer. EFT also supports the ICAP protocol for integrating with 3rd party data loss prevention and classification systems, to further control information sharing. |
| **SC-5** | DENIAL OF SERVICE PROTECTION | | EFT provides built in controls for mitigating the effects of DoS and Flood attacks. |

| | | | |
|---|---|---|---|
| **SC-7** | BOUNDARY PROTECTION | | While this is a customer responsibility, Globalscape provides a secure smart proxy solution that can be coupled with EFT to protect the network boundary (DMZ). |
| **SC-8** | TRANSMISSION CONFIDENTIALITY AND INTEGRITY | | EFT uses secure protocols to protect the confidentiality and integrity of transmitted information. |
| **SC-12** | CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | | Yes |
| **SC-13** | CRYPTOGRAPHIC PROTECTION | | Yes |
| **SC-15** | COLLABORATIVE COMPUTING DEVICES | | CR/IC |
| **SC-17** | PUBLIC KEY INFRASTRUCTURE CERTIFICATES | | Yes |
| **SC-19** | VOICE OVER INTERNET PROTOCOL | | CR/IC |
| **SC-20** | SECURE NAME / ADDRESS RESOLUTION SERVICE | | CR/IC |

| | | | |
|---|---|---|---|
| | (AUTHORITATIVE SOURCE) | | |
| **SC-21** | SECURE NAME / ADDRESS RESOLUTION SERVICE (RECURSIVE OR CACHING RESOLVER) | | CR/IC |
| **SC-22** | ARCHITECTURE AND PROVISIONING FOR NAME / ADDRESS RESOLUTION SERVICE | | CR/IC |
| **SC-23** | SESSION AUTHENTICITY | | EFT provides numerous internal controls for establishing and maintaining session authenticity and integrity, including support for various secure headers in compliance with OWASP recommended practices to mitigate against XFS, XSS, CRSS, etc. |
| **SC-28** | PROTECTION OF INFORMATION AT REST | | Yes |
| **SC-39** | PROCESS ISOLATION | | Yes |
| **SI-1** | SYSTEM AND INFORMATION | | CR/IC |

| | | | |
|---|---|---|---|
| | INTEGRITY POLICY AND PROCEDURES | | |
| **SI-2** | FLAW REMEDIATION | | CR/IC |
| **SI-3** | MALICIOUS CODE PROTECTION | | EFT includes built-in Known-Answer-Tests (KAT), and CRC checksums on application startup for valid configuration. |
| **SI-4** | INFORMATION SYSTEM MONITORING | | CR/IC |
| **SI-5** | SECURITY ALERTS, ADVISORIES, AND DIRECTIVES | | CR/IC |
| **SI-7** | SOFTWARE, FIRMWARE, AND INFORMATION INTEGRITY | | CR/IC |
| **SI-10** | INFORMATION INPUT VALIDATION | | EFT provides comprehensive checks around input validation for both user and administrative functions. |
| **SI-16** | MEMORY PROTECTION | | EFT includes several measures to protect against memory corruption as afforded by the compilation |

| | | | |
|---|---|---|---|
| | | | software which builds the object code that comprises the EFT solution. |

```
.telerik-reTable-1 { border-width: 0px; border-style: none; border-collapse: collapse;
font-family: Tahoma; } .telerik-reTable-1 tr.telerik-reTableHeaderRow-1 { margin: 10px;
padding: 10px; color: #3F4D6B; background: #D6E8FF; text-align: left; font-style: normal;
font-family: Tahoma; text-transform: capitalize; font-weight: bold; border-spacing: 10px;
line-height: 14pt; vertical-align: top; } .telerik-reTable-1 td.telerik-reTableHeaderFirstCol-1
{ padding: 0in 5.4pt 0in 5.4pt; color: #3a4663; line-height: 14pt; } .telerik-reTable-1
td.telerik-reTableHeaderLastCol-1 { padding: 0in 5.4pt 0in 5.4pt; color: #3a4663;
line-height: 14pt; } .telerik-reTable-1 td.telerik-reTableHeaderOddCol-1 { padding: 0in
5.4pt 0in 5.4pt; color: #3a4663; line-height: 14pt; } .telerik-reTable-1
td.telerik-reTableHeaderEvenCol-1 { padding: 0in 5.4pt 0in 5.4pt; color: #3a4663;
line-height: 14pt; } .telerik-reTable-1 tr.telerik-reTableOddRow-1 { color: #666666;
background-color: #F2F3F4; vertical-align: top; } .telerik-reTable-1
tr.telerik-reTableEvenRow-1 { color: #666666; background-color: #E7EBF7; vertical-align:
top; } .telerik-reTable-1 td.telerik-reTableFirstCol-1 { padding: 0in 5.4pt 0in 5.4pt; }
.telerik-reTable-1 td.telerik-reTableLastCol-1 { padding: 0in 5.4pt 0in 5.4pt; }
.telerik-reTable-1 td.telerik-reTableOddCol-1 { padding: 0in 5.4pt 0in 5.4pt; }
.telerik-reTable-1 td.telerik-reTableEvenCol-1 { padding: 0in 5.4pt 0in 5.4pt; }
.telerik-reTable-1 tr.telerik-reTableFooterRow-1 { background-color: #D6E8FF; color:
#4A5A80; font-weight: 500; font-family: Tahoma; line-height: 11pt; } .telerik-reTable-1
td.telerik-reTableFooterFirstCol-1 { padding: 0in 5.4pt 0in 5.4pt; border-top: solid gray
1.0pt; text-align: left; } .telerik-reTable-1 td.telerik-reTableFooterLastCol-1 { padding: 0in
5.4pt 0in 5.4pt; border-top: solid gray 1.0pt; text-align: left; } .telerik-reTable-1
td.telerik-reTableFooterOddCol-1 { padding: 0in 5.4pt 0in 5.4pt; text-align: left;
border-top: solid gray 1.0pt; } .telerik-reTable-1 td.telerik-reTableFooterEvenCol-1 {
padding: 0in 5.4pt 0in 5.4pt; text-align: left; border-top: solid gray 1.0pt; }
```

GlobalSCAPE Knowledge Base
https://kb.globalscape.com/Knowledgebase/11518/EFT-Server-FISMA-and-FedRAMP...