



GENERAL FUND ENTERPRISE BUSINESS SYSTEM

GFEBs USER PROVISIONING GUIDE

Version 6.0

April 2013

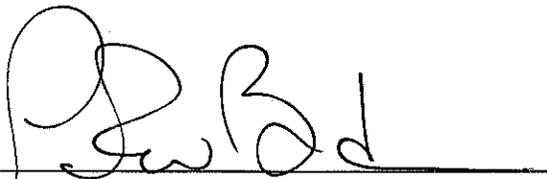
GFEBs User Provisioning Guide

SFAE-PS-GF

POLICY AND PROCEDURES

SUBJECT: GFEBs User Provisioning Guide

PURPOSE: This document establishes the General Fund Enterprise Business System (GFEBs) User Provisioning Policy and Procedures.

 3 Apr 2013

PATRICK W. BURDEN
COL, FA
Project Manager
General Fund Enterprise Business System

Date

GFEBs User Provisioning Guide

VERSION HISTORY

Version Number	Version Date	Summary of Changes
1.0		Draft Version
2.0	3/31/11	Draft Version
3.0	10/13/11	Switched to new format of document due to the old one being out of synch
	10/14/11	Continued to edit
	10/18/11	Continued to edit
	10/31/11	Continued to edit
	11/02/11	Continued to edit
	11/15/11	Continued to edit
	12/02/11	Continued to edit
	12/09/11	Continued to edit
	12/14/11	Continued to edit
3.1	12/29/11	Updates on load reconciliation
4.0	4/11/12	Updated to include SUSTAINMENT provisioning
4.0	7/06/12-7/27/12	Continue with new revisions
4.0	08/12	Review
4.0	09/01/12- 09/21/12	Continued to edit
4.0	10/19/12	Continued to edit
5.0	2/15/13	Updated for Sustainment changes, removed references to Deployment Activities
6.0	4/04/13	Added Authorizer and Command Site Level POC responsibilities

Table of Contents

GFEBs USER PROVISIONING GUIDE.....	I
1 INTRODUCTION.....	1
1.1 Purpose	1
1.2 Applicability/Scope.....	1
1.3 Applicable Federal Information System Controls Audit Manual Controls	1
2 ROLES AND RESPONSIBILITIES	3
3 USER PROVISIONING	5
3.1 Introduction	5
3.2 Four Tier Hierarchy	5
3.3 GFEBs Internal Provisioning	5
4 THE SIX STEPS OF STANDARD PROVISIONING THROUGH GRC.....	6
5 ADDITIONAL PROVISIONING CONTROLS.....	9
5.1 Risk Analysis	9
5.2 Restricted Roles.....	9
5.3 Sensitive Transactions.....	9
5.4 Miscellaneous Payment Approver	9
5.5 Personally Identifiable Information Policy	9
5.6 Non-US Citizens	10
5.7 Locking and Unlocking Users	11
5.8 Terminating GFEBs User Accounts.....	11
5.9 Changing Governance Risk and Compliance (GRC) Approvers	12
5.10 Role Removal	12
6 POST PROVISIONING.....	13
6.1 Login with Common Access Card (CAC).....	13
6.2 Termination due to Inactivity	13
6.3 Annual Role Reaffirmation.....	14
6.4 Segregation of Duties (SODs)	14
7 APPENDIX A - TERMINOLOGY AND ACRONYMS.....	15
8 APPENDIX B - REFERENCES	16

Table of Figures

Figure 1 - Provisioning Overview 1
Figure 2 - GRC Approval Flow 6
Figure 3 - GFEBS Security Investigation Requirements by Position Category 7
Figure 4 - GFEBS Single Sign On 13

Table of Tables

Table 1 - Roles and Responsibilities 4

GFEBs User Provisioning Guide

1 INTRODUCTION

1.1 Purpose

This User Provisioning Guide defines the process for managing the provisioning of end user roles in the General Fund Enterprise Business System (GFEBs). This guide is a process for ensuring user role assignments are provisioned through Systems, Applications, and Products in Data Processing (SAP) Governance, Risk and Compliance (GRC) Access Controls (AC) system. It also defines the approval steps for a user request, including the prevention of segregation of duty conflicts. This guide is not intended to replace GRC training or job aids. Figure 1 is an overview of the GFEBs Provisioning process.

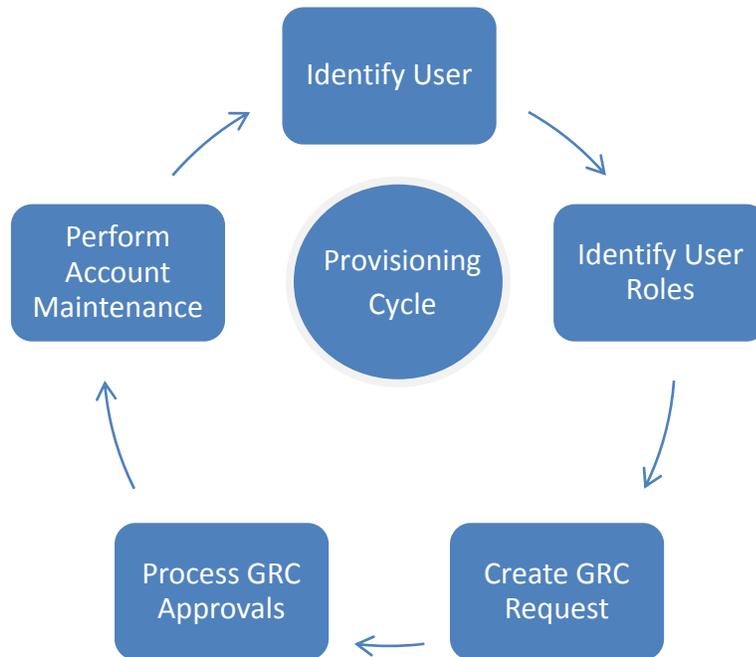


Figure 1 - Provisioning Overview

1.2 Applicability/Scope

This guide applies to all users requiring access to the production GFEBs environment and validates their initial qualification or requalification. This guide does not cover the process for a gaining organization to make role assignments, as role assignments are performed by the gaining organizations. All GFEBs production user provisioning is accomplished through the SAP GRC AC tool, which is a component of the GFEBs solution.

1.3 Applicable Federal Information System Controls Audit Manual Controls

The following Federal Information System Controls Audit Manual (FISCAM) Controls are addressed in this guide:

GFEBS User Provisioning Guide

- AC -2.1.2: Account policies (including authentication policies and lockout policies) are appropriate given the risk and enforced.
- AC-3.1.1: Resource owners have identified authorized users and the access they are authorized to have.
- AC-3.1.3. Security managers review access authorizations and discuss any questionable authorizations with resource owners.
- AC-3.1.6: Access is limited to individuals with a valid business purpose.
- AC-3.1.8. Inactive accounts and accounts for terminated individuals are disabled or removed in a timely manner.
- AS-2.4: Access to the application is restricted to authorized users.

GFEBs User Provisioning Guide

2 ROLES AND RESPONSIBILITIES

The following roles take part in the GFEBs pre-deployment provisioning process. The responsibilities listed are those related to provisioning.

Role	Summary of Responsibilities
GRC Authorizer	Approves changes to GRC Authorizers, Command Site Level POCs (cannot be a contractor), GRC Restricted Role Approvers, Miscellaneous Pay Approvers and updates GRC Hierarchy as necessary. May delegate to the Command Site Level POC to make changes for all other GRC Approvers (Supervisors, Role Approvers, Security Manager, Training Coordinators).
Command Site Level POC	Approves changes to GRC Approvers (Supervisors, Role Approvers, Security Manager, Training Coordinators).
Data Owner, Assistant Secretary of the Army, Financial Management and Comptroller (ASA (FM&C))	Responsible for approving or concurring with Non-US Citizen Access requests.
Designated Approval Authority (DAA)	Responsible for approving the Non-US Citizen Access Approval Memorandum.
Project Management Office (PMO) Non-US National Security Coordinator	Responsible for processing the data received from Non-US Citizen's packages through the Data Owner and DAA.
PMO Government Training Team	Responsible for maintaining the Army Learning Management System (ALMS) curriculum structure.
PMO GRC Support	Responsible for post deployment updates to GRC, including the application and management of help desk tickets pertaining to user GRC or Segregation of Duties (SOD) related issues.
GRC Role Approver or Site Role Approver	Approves or rejects role assignments based on the user's job responsibilities. Approvals and rejections are sent via email for initial deployment and in GRC for all others.
Site GRC Security Manager or Security Manager (at receiving organization)	Responsible for validating that the end user has a valid background investigation documented in the system of record, Joint Personnel Adjudication System (JPAS) that supports the Automated Data Processing (ADP) level documented in the User Request.
PMO GRC AC SOD Approver	Responsible for approving or rejecting GRC User Requests that contain role(s) that are forbidden by the SOD guidelines in effect at the time of the User Request. Within the PMO, the primary responsibility is to approve SOD conflicts only after an approved waiver is received from Deputy Assistant Secretary of the Army for Financial Operations (DASA-FO).
Site GRC Supervisor (at receiving organization)	Create user role assignments, create new requests in GRC.
Site GRC Training Coordinator or Training Coordinator	Responsible for validating that the end user has completed all training required for the roles assigned in the User Request; approves GRC requests, as needed.

GFEBs User Provisioning Guide

Role	Summary of Responsibilities
Site Information Assurance Manager	Validates Users with GRC requests in JPAS.
PMO Information Assurance (IA) Team	Validates that GRC Security Managers nominated by the gaining organizations through a JPAS visit request.

Table 1 - Roles and Responsibilities

3 USER PROVISIONING

3.1 Introduction

All GFEBs user accounts are appropriately controlled through the GRC tool and require four levels of organizational approval specific to each site: GRC Supervisor, Role Approver (for non-Restricted roles), Security Manager (for US Citizens), and Training Coordinator. Requests with SOD conflicts are routed to a SOD approver at the GFEBs Program Management Office (PMO) to facilitate a waiver or reject the request so the supervisor can recreate without a SOD conflict. GFEBs uses GRC in lieu of a System Authorization Access Request (SAAR) form. This document has been written to assume an organization has already deployed to GFEBs and needs to add users, change role assignments, etc. It is not written to describe bringing an entirely new organization onto GFEBs.

3.2 FOUR TIER HIERARCHY

GFEBs GRC AC uses a four tier hierarchy to organize the users into manageable groups. The four tier hierarchy consists of:

- Command
- Sub-Command
- Organization
- Site

The GRC Authorizers manage the four-tier hierarchy and identify the Command Site-Level POCs, who maintain the four site-level approver roles for each of the hierarchies. GFEBs strongly recommended that sites identify more than one person for each role to provide coverage in case of work absences. Additionally, Security Managers are required to have access to JPAS to validate background investigations of end users. Security Managers should submit a Visit Authorization Letter (VAL) through JPAS to validate their access and confirm their position as Security Manager. Approved four-tier hierarchies are on Army Knowledge Online (AKO) at: <https://www.us.army.mil/suite/files/34822412>.

3.3 GFEBs INTERNAL PROVISIONING

The GFEBs SUSTAINMENT team and other support users requiring access to the Production environment, either through an end user role or a support role shall be provisioned through GRC, following the process described in Section 4 “The Six Steps of Standard Provisioning through GRC”. There are four-tier hierarchies established for the PMO support teams. Superuser Privileged Management (SPM), or Fire Fighter access, is covered in a separate document, GFEBs SPM Guide.

GFEBs User Provisioning Guide

4 THE SIX STEPS OF STANDARD PROVISIONING THROUGH GRC

There are six basic steps to provisioning a user. The Figure 2 process lays out the chain of events.

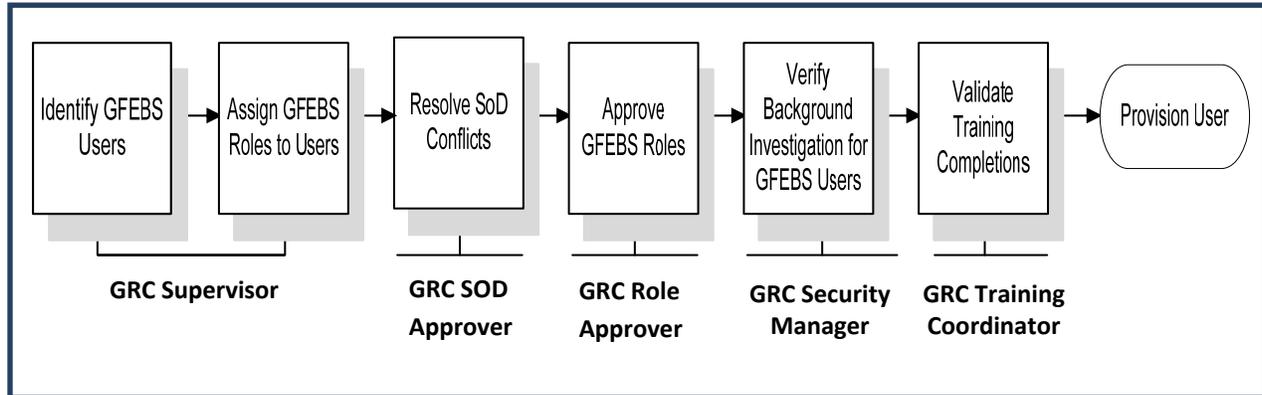


Figure 2 - GRC Approval Flow

1. The provisioning process begins with the GRC Supervisor. The process is the same for a new user, or a user needing to change role assignments. The Supervisor starts the GRC Workflow activities by identifying the correct individual based on Electronic Data Interchange Personal Identifier (EDIPI), then ensuring the correct role is assigned to the correct user based on the user's job responsibilities. Supervisors should adhere to the policy of least privilege and only assign those roles required for the user to perform their job. **If no SOD conflicts move the request to Step 3.** For guidance is assigning roles, Supervisors can use the Role Assignment Guidance spreadsheet on AKO at: <https://www.us.army.mil/suite/doc/36346049>. GRC AC is configured to allow only one request per user at a time. If a Supervisor needs to make a change to a request, they will need to contact the GRC Approver with the request in their queue and ask them to cancel the request. Supervisors should copy an existing request and modify it to reduce the chances of the request going to an 'Approver not found' state.
2. If SODs are found, the request will move to the SOD Approver stage. If not, proceed to Step 3. The SOD Approver will either reject the request or ask the user to remediate the roles before resubmitting (remove roles to clean-up SODs) or mitigate (put a waiver control in place to manage the risk). Remediation is the first choice. Mitigation requires approval of a waiver by DASA-FO. The GFEBs SOD policy is on AKO at: <https://www.us.army.mil/suite/doc/26006383>.
3. After the GRC Supervisor approves the request, it moves to the Role Approver who validates the roles assigned by the GRC Supervisor. Role Approvers have the right and responsibility to remove roles they own from a request if the user does not have a need for the role. A request may go to multiple Role Approver queues in the event one or more of the roles assigned is a restricted role. The Role Approver is the process owner for approving access to the role (resource). The request will not move to the Security Manager stage until all roles (i.e. restricted and non-restricted roles) have been approved or rejected. Once the request has passed the Role Approver stage, the role assignments flow to ALMS for training registration.

GFEBs User Provisioning Guide

4. The Security Manager validates the user’s background investigation (BI) in the Joint Personnel Adjudication System (JPAS). The required BI is dependent on the Information Technology (IT)/Automated Data Processing (ADP) level that is selected by the supervisor based on level of risk. If a user works with several other people on different steps in the business process there is less risk than an employee working in a small office performing multiple steps of the business process. GFEBs does not map roles to IT/ADP levels. ADP levels are described in DoD 5000.2 and IT levels in AR25-2. If a user maps to more than one IT or ADP level, the more restrictive BI applies. Figure 3 describes the GFEBs Security Investigation Requirements by Employee Type. The Security Manager should address questionable authorizations with the supervisors or process owners as appropriate.

ADP Levels are broken out as follows:

ADP Level I - critical to sensitive positions; has a high risk for causing grave damage or realizing a personal gain. ADP Level I is required if a user is in a position that involves the accounting, disbursement, or authorization of disbursements greater than \$10M per year.

ADP Level II - noncritical to sensitive positions; work is reviewed by a higher authority. ADP Level II is required if a user is in a position that involves the accounting, disbursement, or authorization of disbursements less than \$10M per year.

ADP Level III - non-sensitive positions, and is the minimum requirement for all GFEBs users

<i>Position Category</i>	<i>Civilians</i>	<i>Military</i>	<i>Contractor</i>	<i>Non-U. S. Citizens</i>
IT/ADP-I	SSBI	SSBI	SSBI	Host Nation Agreements or host investigation that meets requirements to access classified information.
IT/ADP-II	ANACI	NACLCL	NACLCL	Host Nation Agreement
IT/ADP-III	NACI	NACLCL	NACI	Host Nation Agreement

Figure 3 - GFEBs Security Investigation Requirements by Position Category

5. The final site controlled stage is the Training Coordinator stage. ALMS is the system of record for GFEBs training. GFEBs has implemented an interface to ALMS to record role attainment. Once all roles for a request have been attained, the request is automatically approved. Training policy regarding users unable to complete training prior to provisioning is on AKO at <https://www.us.army.mil/suite/files/32983830>.
6. The GFEBs PMO manages the final provisioning step, “SAP Security”. This stage is used to verify user and role validity dates and role correctness prior to provisioning. This step may be removed if the Provisioning team determines there are not changes being made at this step.

Please note that any open GRC request that is older than six months will be subject to deletion.

GFEBs User Provisioning Guide

5 ADDITIONAL PROVISIONING CONTROLS

There are numerous circumstances where additional or alternate controls are required over and above the standard provisioning controls.

5.1 Risk Analysis

The GRC tool has been configured with a set of approved risks to conduct a risk analysis prior to approval at the Supervisor stage. No request will be provisioned with a SOD conflict unless a waiver has been received from DASA-FO. Army organizations are expected to adapt organizational structures and legacy processes to comply with the SOD risks identified as applicable to GFEBs or obtain a waiver from DASA-FO.

5.2 Restricted Roles

Certain GFEBs roles require restriction to selected users and the roles are owned by specific organizations (e.g., Defense Finance and Accounting Service (DFAS), Army Budget Office (ABO), Site-level). In order to be provisioned with a restricted role, GFEBs users must obtain approval from the organization(s) that owns the role prior to requesting the role through GRC. GRC Authorizers manage the restricted role approvers for their command. A list of restricted roles and their approvers is available in the Role Approver tab of the GRC Master List of Approvers posted on AKO for reference at: <https://www.us.army.mil/suite/files/34109846>.

5.3 Sensitive Transactions

Sensitive transactions are those transactions which could affect the financial information in GFEBs. The users provisioned to these transactions will be monitored each month by the transaction owners. At the direction of the transaction owner, the GFEBs Sustainment team will remove the role with the sensitive transaction. The list of sensitive transactions is posted on AKO at: <https://www.us.army.mil/suite/files/37449439>.

5.4 Miscellaneous Payment Approver

The Miscellaneous Payment Approver role conveys pecuniary liability to a user. As such, any GRC AC request that includes the Miscellaneous Payment Approver role must have a signed, valid DD Form 577 with the social security number redacted to show only the last four digits. Any user assignment without a valid, redacted DD Form 577 will have the role removed by the GFEBs Sustainment team. The "Miscellaneous Payments Certification in GFEBs" memo provides guidance on actions required to request the Miscellaneous Pay Approver role, and is available on AKO at: <https://www.us.army.mil/suite/doc/36591751>. GRC Authorizers manage the Miscellaneous Payment Approver role approvers for their command.

5.5 Personally Identifiable Information Policy

Certain GFEBs roles provide access to Personally Identifiable Information (PII). GFEBs defines PII data as:

Information about an individual that identifies, links, relates or is unique to, or describes him/her (e.g., a social security number; age; marital status; race; salary; home telephone

GFEBs User Provisioning Guide

number; other demographic, biometric, personnel, medical, and financial information). Also, information that can be used to distinguish or trace an individual's identity, such as his or her name; social security number; date and place of birth; mother's maiden name; and biometric records, including any other personal information that is linked or linkable to a specified individual.

These roles require approval from a role approver that confirms a "need to know" the PII data.

5.6 Non-US Citizens

GFEBs allows Non-US Citizens to be provisioned to Non-US citizen roles. Non-US citizen roles provide the same access to data as normal roles, but end with a suffix to indicate the country the Non-US citizen works in. Per AR25-2, Non-US citizen access requests must be approved by the Data Owner and DAA prior to provisioning. GFEBs PMO acts as the Security Manager for all Non-US Citizen requests, and will process the Non-US citizen packages off-line through the Data Owner and DAA, then approve the GRC requests after approval is received. A Job Aid, sample memo, and Information Assurance Manager Form, as well as the list of approved Non-US citizens are on AKO at:

<https://www.us.army.mil/suite/files/26178968>.

If a Non-US Citizen is from those countries that do not have Status of Forces Agreements (SOFA) agreements with the United States he or she will not be approved for access to the GFEBs application. The employing organization can request an exception to this policy if they require these Non-US Citizens to use GFEBs. The exception will require increased scrutiny of their statement of compelling need and background investigation. This will include a review of local national background investigation procedures, GFEBs role assignments and organization staffing levels. The Center for Law and Military Operations (CLAMO) maintains a list of countries with SOFA agreements. The link for the site is: <https://www.jagcnet.army.mil/8525751D00557EFF/0/5E8CD0C5A611B3DD852577620060B8AA?opendocument>. North Atlantic Treaty Organization (NATO) SOFA, NATO Partnership for Peace and Individual SOFA agreements are considered SOFA agreements.

The following roles, which convey pecuniary liability and/or inherently governmental functions, have certain restrictions for provisioning to Non-US Citizens:

- Purchase Order Processor
- Miscellaneous Payment Approver
- Payment Certifier

Direct hire non-U.S. citizens may be provisioned to the Payment Certifier role in GFEBs in accordance (IAW) Department of Defense Financial Management Regulation (DoDFMR), Volume 5, Chapter 33 (dated August 2010), Paragraph 330204. Commanders must consider that non-U.S. citizens may not be subject to pecuniary liability based on the applicable Status of Forces (SOFA) agreement. Direct hire non-U.S. citizens may also be provisioned to the Purchase Order Processor role, which conveys inherently governmental functions, and duties subject to the provisions of the Anti-Deficiency Act (ADA). In each instance, the designating authority will submit a delegation memorandum with the Statement of Compelling Need for each direct hire non-U.S. citizen provisioned to one of the aforementioned roles.

GFEBs User Provisioning Guide

Indirect hire non-U.S. citizens or contractors cannot perform roles conveying pecuniary liability (IAW the DoDFMR, Volume 5, Chapter 33, Paragraphs 330202 and 330204 respectively). DoDFMR, Volume 5, Chapter 1 (dated August 2010), Paragraph 010304, states: “(Inherently governmental) functions include activities that require making value judgments regarding monetary transactions and entitlement involving the collection, control, or disbursement of appropriated and other Federal funds.” Indirect hire non-U.S. citizens or contractors may be provisioned to all other GFEBs roles that are not inherently governmental. Indirect hire non-U.S. citizens or contractors may not be provisioned to the following GFEBs roles: Purchase Order Processor and Payment Certifier.

Non-US Citizens should only be assigned to those roles ending with the country name where the Non-US Citizen is working (e.g. Purchase Requisition Processor – Germany). Non-US Citizens working in Embassies should select the Department of State role. If the role required does not exist, select the base role without country (e.g. Purchase Requisition Processor) and open a GFEBs Help Desk trouble ticket requesting creation of the country-specific role. GFEBs may remove any incorrectly assigned roles.

Non-US Citizen access will be recertified annually. Commanders and Security Managers are required to restate the compelling need and favorability for each Non-US Citizen. GFEBs accounts for Non-US Citizens will be locked if the recertification is not complete within 30 days.

When a Non-US citizen user package has been approved but the user has not been provisioned, or if their account has been locked for inactivity, their Data Owner approval for access to the system will be terminated after 180 days of approval or locking. If access is needed in the future, a new GRC request will be created. A revised Non-US Citizen package will be required if the last package was approved more than one year prior to the new request date.

5.7 Locking and Unlocking Users

A GRC Request is required to deactivate a GFEBs User. GFEBs User Accounts are not deleted from the GFEBs system; instead User Accounts are deactivated via the Request Type “Lock Account”.

If a user has transferred to your organization and the account has not been locked, for auditing purposes (1) the GRC Supervisor of the initial organization must to be contacted and (2) informed to remove ALL GFEBs roles (Common Roles and Portal Groups/Roles are to remain) from the account and (3) once ALL GFEBs roles are removed a Lock Account Request is to be issued for the User Account.

A GFEBs User Account is to be deactivated / lock when a user:

- Transfers organizations
- Retires from the organization
- Experiences a revocation of security clearance
- No longer needs access to GFEBs

Job aids to lock and unlock user accounts are on AKO at: <https://www.us.army.mil/suite/files/20728625>.

5.8 Terminating GFEBs User Accounts

GFEBs User Provisioning Guide

Army policy as described in AR25-2 and Army ERP policy on AKO at:

<https://www.us.army.mil/suite/files/32983830> requires organizations de-provision users within 48 hours of departure. This is captured in the Commander's Checklist. OASA(FM&C) monitors the compliance with the Commander's Checklist. Additionally, users leaving the Army organization will have their Common Access Card (CAC) revoked, restricting their access to GFEBs.

Each organization that needs to terminate users already provisioned in GFEBs creates two GRC requests to fully remove access. The first request is required to remove the roles from the user and the second request is required to lock their account. The requests will have to be processed sequentially as only one request is allowed per user at a time. For additional information, please refer to the following job aid on AKO: <https://www.us.army.mil/suite/doc/31676808>.

5.9 Changing Governance Risk and Compliance (GRC) Approvers

For auditing purposes GRC Approver changes must be emailed to: GFEBs.HELPDESK@accenture.com by the GRC Authorizer with the subject line of the email stating "GRC Approver Change" and include a completed template with the four-tier hierarchy (Command, Sub-Command, Site, and Organization), the AKO email address, and the EDIPI of the GRC Approver(s) to be added or deleted. GRC Approvers must be GS-15 or O-6 level civilian/military. Exceptions are worked with the GFEBs Sustainment Director and Director, Transformation and Communication, GFEBs. The GRC Approver Changes Template is on AKO at: <https://www.us.army.mil/suite/doc/30589157> and the GRC Org Hierarchy Changes Template is on AKO at: <https://www.us.army.mil/suite/doc/30589158>.

5.10 Role Removal

During routine maintenance, GFEBs may find roles incorrectly assigned to users. After coordination with the Role Owner, GFEBs may remove the role from the user via a GRC removal request or directly from the user in the event the role is not available in GRC. The user will be sent an email alerting them to the fact a role has been removed from their account.

6 POST PROVISIONING

6.1 Login with Common Access Card (CAC)

GFEBs access is CAC based and leverages the AKO single sign on (SSO). The user's EDIPI is their application user ID, and is bound to all transactions executed in the system. There are no passwords to remember or reset. The user logs on to AKO using their CAC, and clicks the GFEBs Home Page to access the GFEBs Portal. Access is granted to the GFEBs application based on the roles associated with the user ID. Figure 4 shows how a user is authenticated with AKO.

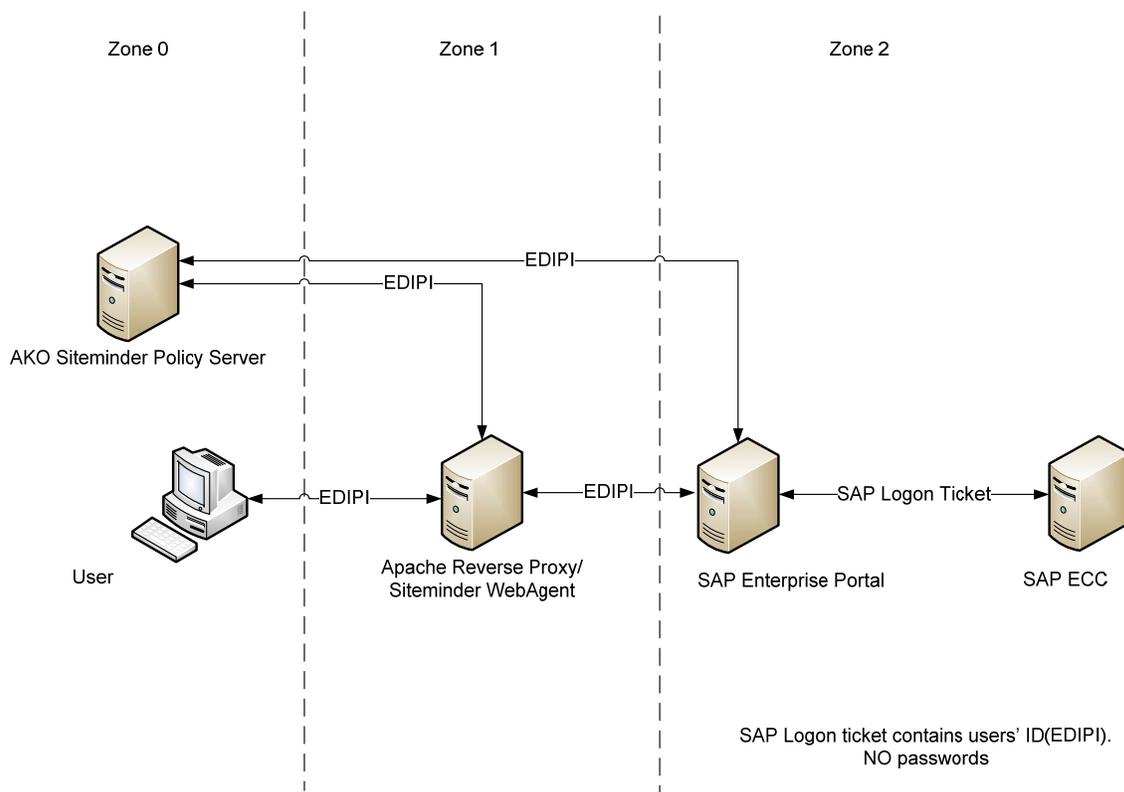


Figure 4 - GFEBs Single Sign On

6.2 Termination due to Inactivity

Army and DoD policy requires accounts to be locked if they are inactive for a period of time. The Army policy is 45 day inactivity for account lockout and the Defense Information System Agency (DISA) Enterprise Resource Planning (ERP) Security Technical Implementation Guide (STIG) sets the lockout at 60 days. GFEBs warns users of account inactivity at 45 days, and then locks users after 60 days of inactivity. GFEBs uses the ERP STIG as it is more specific to the GFEBs application than the generic Army regulation as approved by the GFEBs DAA. GFEBs has implemented this policy via twice a month reports and once a month locking of accounts. Activity is measured through the most recent logon into either the GFEBs Enterprise Core Component (ECC) or Business Intelligence (BI) logon by the account. In order to keep year end activities moving smoothly, no accounts are disabled between 15 August and 15

GFEBs User Provisioning Guide

October. Roles are removed from users that have been locked, for any reason after the account has been locked for 60 days.

6.3 Annual Role Reaffirmation

In accordance with Army Auditability Requirement (FISCAM control AC-3.1.5) all GFEBs user accounts will be revalidated (reaffirmed) no less than annually. The GFEBs Sustainment team works with the commands to reaffirm an entire command at a time. GRC Supervisors, Role Approvers and Restricted Role Approvers are required to re-authorize (reaffirm) each role that is assigned to GFEBs users.

To streamline the process, a special 2 stage reaffirmation workflow named User Access Reaffirmation, has been created and will be pre-loaded with GRC Requests for users that need to be reaffirmed. Reaffirmation involves accessing, reviewing, and approving GRC Reaffirmation Requests. These Requests will be mass loaded to the GRC Supervisor Stage and require action by the GRC Supervisor and GRC (Restricted) Role Approver. For assistance with the reaffirmation process please reference the job aid 'How to Process User Access Reaffirmation Requests' available via AKO link at: <https://www.us.army.mil/suite/doc/36420879>. Users whose accounts are not reaffirmed will be expired at the end of the revalidation period and a change request will be required to process through all stages in order to regain access.

6.4 SEGREGATION OF DUTIES (SODs)

The SOD/Internal Controls team reviews the GRC User Analysis Report on a weekly basis for all end-users. End-users with SOD violations are identified by business area, and team leads are subsequently informed to remediate their SOD violations in a timely manner. If a business must operate with an existing SOD deficiency due to resource constraints or some other valid reason, then a SOD waiver must be requested and submitted to DASA-FO for formal approval. In addition, compensating controls must be in place to ensure that the underlying risk for the SOD violation is adequately mitigated.

The SOD/Internal Controls team also performs a weekly trend analysis to continuously monitor end-users with SOD violations that have mitigating controls and those that do not have mitigating controls in place. The trend statistics are communicated during periodic collaboration team meetings. In addition, e-mail communications are sent to the team leads to ensure that their SOD violations are remediated in a timely manner. If the business areas fail to remediate their SOD violations in a timely manner, then the SOD/Internal Controls & Security will coordinate and take necessary action to mitigate the underlying risk (s) for SOD violation(s).

GFEBs User Provisioning Guide

7 APPENDIX A - TERMINOLOGY AND ACRONYMS

AC	Access Control
ADA	Anti-Deficiency Act
ADP	Automated Data Processing
AKO	Army Knowledge Online
ALMS	Army Learning Management System
ANACI	Access National Agency Check with Inquiries
ASA (FM&C)	Assistant Secretary of the Army, Financial Management and Comptroller
BI	Background Investigation, Business Intelligence
CAC	Common Access Card
CBT	Computer Based Training
CLAMO	Center for Law and Military Operations
DAA	Designated Approval Authority
DASA-FO	Deputy Assistant Secretary of the Army for Finance Operations
DD Form 577	Appointment/Termination Record – Authorized Signature form
DFAS	Defense Finance and Accounting Service
DoD FMR	Department of Defense Financial Management Regulation
ECC	Enterprise Core Component
EDIPI	Electronic Data Interchange Personal Identifier
ERP	Enterprise Resource Planning
FISCAM	Federal Information System Controls Audit Manual
GAI	GRC ALMS Interface
GFEBs	General Fund Enterprise Business System
GRC	Governance, Risk, and Compliance Tool
IA	Information Assurance
IAW	In Accordance With
IT	Information Technology
JPAS	Joint Personnel Adjudication System
NACI	National Agency Check with Inquiries
NACLCLC	National Agency Check with Local Agency Check
PII	Personally Identifiable Information
PMO	Project Management Office
SAP	Systems, Applications, and Programs in Data Processing (Enterprise Resource Management solution on which GFEBs resides)
SOD	Separation of Duties or Segregation of Duties, terms used synonymously
SOFA	Status of Forces Agreements
SPM	Superuser Privileged Management
SSBI	Single Scope Background Investigation
Stage	Identifies in whose control the User Request resides; synonymous with the GRC approver that currently has the User Request in their workflow inbox
STIG	Security Technical Implementation Guide
TC	Training Coordinators
User Request	Electronic record that contains user information, organizational information, and the roles to be provisioned for an end user
VAL	Visit Authorization Letter

8 APPENDIX B - REFERENCES

1. Execution Order: Implementing General Fund Enterprise Business System (GFEBs), 10 December 2009
2. GFEBs Material Fielding Plan V 3.0, PM GFEBs, 13 February 2009
3. Governance, Risk and Compliance (GRC) Functional Design V 7.0, May 2010
4. Assistant Secretary of the Army for Financial Management and Comptroller, 27 September 2010, subject: Delegation of Authority to Sign Segregation of Duty Waivers.
5. Assistant Secretary of the Army for Financial Management and Comptroller, 27 September 2010, subject: General Fund Enterprise Business System (GFEBs) Separation of Duties (SOD) Waiver Policy.
6. Non-Citizen Provisioning Process-Standard Operating Procedure, 13 May 2011
7. Federal Information System Controls Audit Manual (FISCAM), February 2009