SUM for Special Users

PIEE

Procurement Integrated
Enterprise Environment

This page intentionally left blank.

Table of Contents

1. Introduction

The Procurement Integrated Enterprise Environment application requires a varied level of involvement in the administration of the various daily activities; from simply viewing records, providing user assistance in document creation and troubleshooting production problems.

It is beyond the scope of this document to highlight the various business rules that would provide oversight to the various administrative functions and to make Standard Operating Procedures for that administration. However, this document will highlight the various functional capabilities provided for the administration of the system.

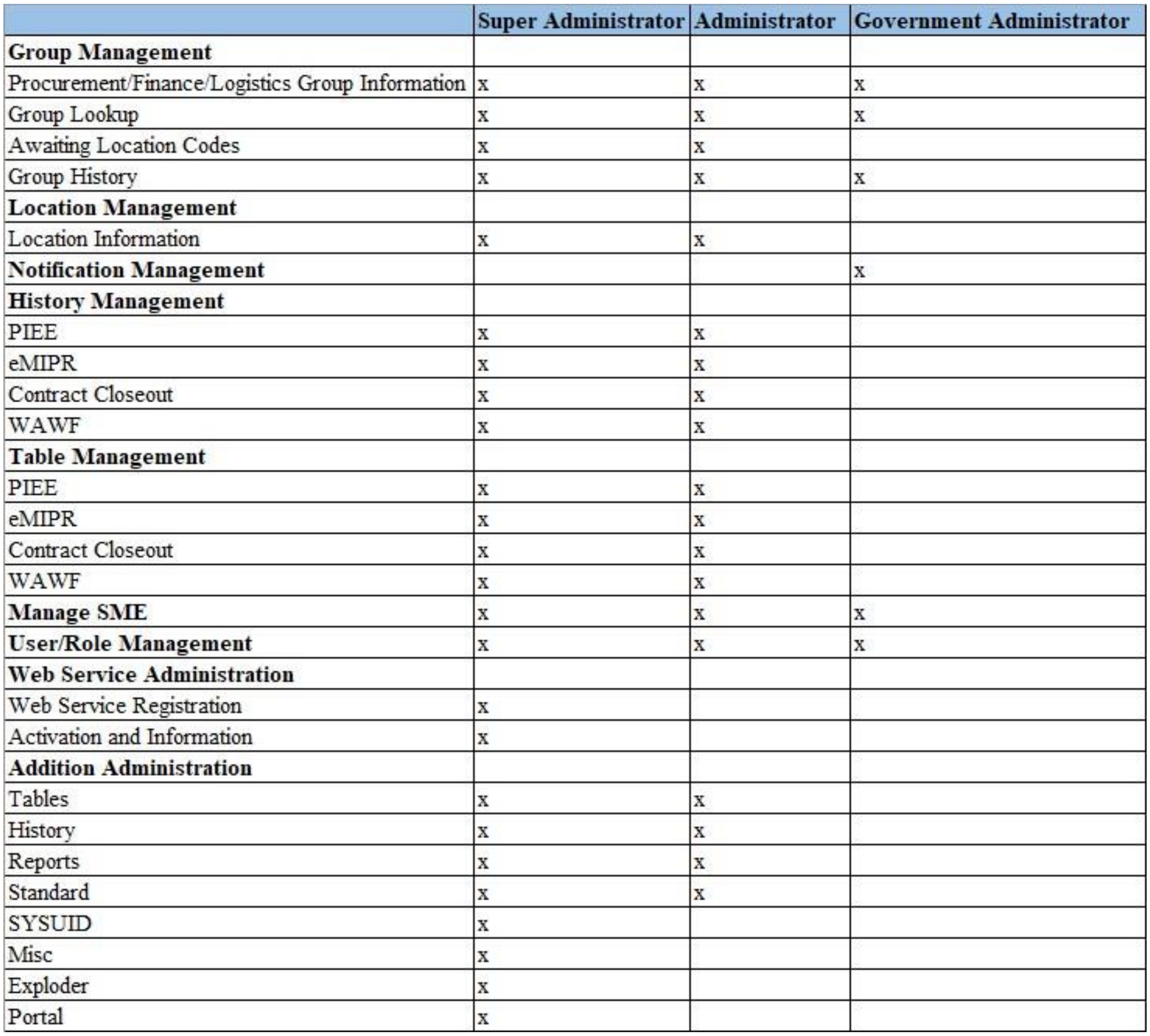
Through a series of ECPs a consolidation of Administrator Roles at the PIEE level has occurred. The functions of user and group management and system administration duties have been delegated to PIEE level administrators across PIEE.

PIEE Administrative Role	Access
PIEE Super Administrator	Highest level of access
PIEE Administrator	Subset of the PIEE Super Administrator
Government Administrator	• Administer the Group Structure (Level 2 restriction) • Administer the Location Codes in the Group (Level 2 restriction) • Manage Org. Emails and Location Notifications • User / Role Management in the Group
Contractor Administrator	

Most applications added in the PIEE Environment will have Application Level Administrators. They will manage the administrative duties within each specific application. They will not administer the PIEE Users, Roles, or Groups.

2. WAWF Administrators

This section reviews the functionalities of each of the administrators in PIEE. The table below is an overview of the level of privileges for each type of administrator.



	Super Administrator	Administrator	Government Administrator
Group Management			
Procurement/Finance/Logistics Group Information	x	x	x
Group Lookup	x	x	x
Awaiting Location Codes	x	x	
Group History	x	x	x
Location Management			
Location Information	x	x	
Notification Management			x
History Management			
PIEE	x	x	
eMIPR	x	x	
Contract Closeout	x	x	
WAWF	x	x	
Table Management			
PIEE	x	x	
eMIPR	x	x	
Contract Closeout	x	x	
WAWF	x	x	
Manage SME	x	x	x
User/Role Management	x	x	x
Web Service Administration			
Web Service Registration	x		
Activation and Information	x		
Addition Administration			
Tables	x	x	
History	x	x	
Reports	x	x	
Standard	x	x	
SYSUID	x		
Misc	x		
Exploder	x		
Portal	x		

2.1 PIEE Super Administrator / PIEE Administrator

This is the highest-level administrator in PIEE, this administrator has access to all the available function as a PIEE Super Administrator. This is reserved for a select group of personnel due to the accessibility of data and ability to make data changes. Each of the areas of functionality this administrator oversees will be reviewed in more detail in Section 4.0 PIEE Administration Categories. The other PIEE Administrators have a subset of the full set of administrative functions available for the Super Administrator.

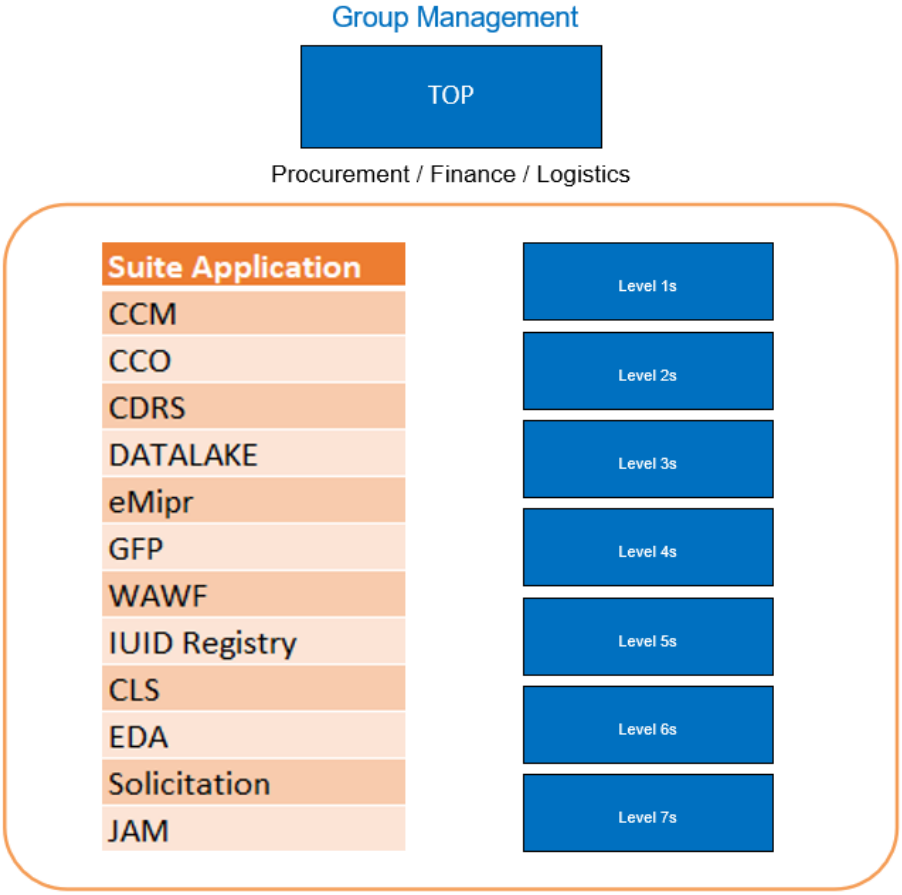
Function	Function Description	PIEE Super Admin	PIEE Admin
Group Management	Administer groups and subgroups by adding, renaming, moving / deleting groups in the group structure, and adding / moving locations in the group structure.	x	x
Location Management	Administer locations by editing locations, adding extensions, editing extensions, and viewing location and extension data.	x	x
History Management	Review historical data for database tables.	x	x
Table Management	Administer database tables by adding, editing, deleting, and viewing table data.	x	x
Subject Matter Expert (SME) Management	Manage Subject Matter Experts (SME) by Application and/or Location Code	x	x
User/Role Management	Administer database tables by adding, editing, deleting, and viewing table data.	x	x
Web Service Administration	Administer database tables by adding, editing, deleting, and viewing table data.	x	
Additional Administration	Administer database tables by adding, editing, deleting, and viewing table data.	x	Subset of the Super Admin

2.2 Government and Contractor Administrators

The Government and Contractor Administrators will have similar functions, one set of administrators will manage the Government component and the other will manage the contractors. The following four roles will manage the functions of this area:

- Government Administrator
- Contractor Administrator

Diagram 1: Group Management



Suite Application
CCM
CCO
CDRS
DATALAKE
eMipr
GFP
WAWF
IUID Registry
CLS
EDA
Solicitation
JAM

2.2.1 Government Administrator

As shown in Diagram 1, the Government Administrator will manage all the modules. The Government Administrator will oversee the function of this module. The administrator is responsible for the Government users and have the following functions available in their role:

- Level 2 Only – Move, Rename, and Delete Groups as well as Manage Location Codes within Agency.
- Level 2 Only – Deactivate Pay Location Codes within their Agency.
- Lookup Government Administrators for their structures.
- View Groups they are assigned to as well as any subgroups.
- View Location codes within their group and any subgroups.
- Manage org. emails and extensions within their group and any subgroups.
- Manage Users within their group and any subgroups including reset password / certificate.
- Manage user’s roles within their group and any subgroups.
- Send Notification emails to users within their span of control.

2.2.2 Contractor Administrator

As shown in Diagram 1, the Contractor Administrator will manage all the modules. The administrator is responsible for the contractor or non-Government users and have the following functions available in their role:

- Lookup Contractor Administrators for their structure.
- View Groups they are assigned to as well as any subgroups.
- View Location codes within their group and any subgroups.
- Manage org. emails, extensions, location notifications (only applicable to WAWF) within their group and any subgroups.
- Manage Users within their group and any subgroups including reset password / certificate.
- Manage user’s roles within their group and any subgroups.
- Send Notification emails to users within their span of control.

2.3 Functional Auditor

The Auditor role has access to information in the system for auditing purposes. Auditor Role activation is handled through the PMO Office. The Auditor has access to the following links under Reports. Only the Auditor has access to Self-Registration Events, Logon Events and Document Events. These links are described in further detail under the Reports section of the Special User's Manual.

3. PIEE Administration Categories

3.1 Group Management

The users of Wide Area Workflow e-Business Suite are broken down into groups of seven levels. Each group is administered by one or more Group Administrators (GAMs).

There will only be two groups under TOP:

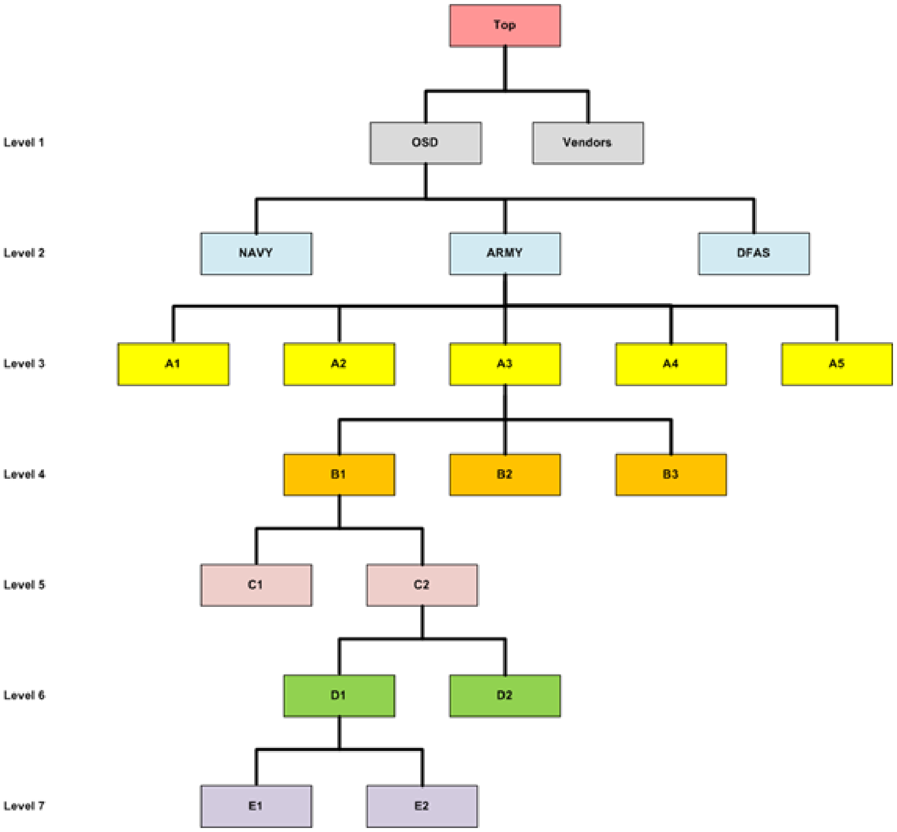
- OSD will be the root of the government group structure.
- OGDEN VENDORS will be the root of the vendor group structure. There will not be an option to add additional groups at this level.

<u>Service/Agency Level 2 GAM</u>

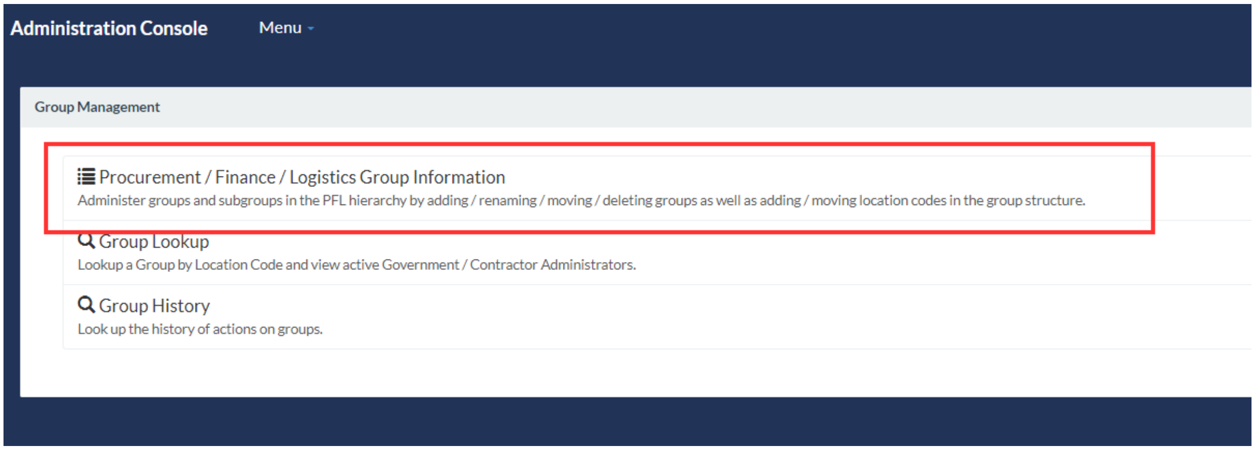
- Add a New Subgroup
- Rename a Level 2 Group
- Add Location Codes to a Level 2 group (although location codes are not required at this level). Navigate the entire group structure under the Service/Agency
- At Levels 3-6, the Service/Agency (Level 2) GAM will have options to Add Location Codes, Add Groups, Rename Groups and Move Groups. If a group does not have any subgroups, the Service/Agency GAM will have the option to delete the group.
- At Level 7, the Service/Agency GAM will have options to Add Location Codes, Rename Groups, Move Groups and Delete Groups.

<u>Service/Agency Level 3-7 GAM</u>

- Ability to navigate the entire structure under their group
- These GAMs will not be able to add new groups, delete groups or add/move location codes.



3.1.1 Procurement / Finance / Logistics Group Information



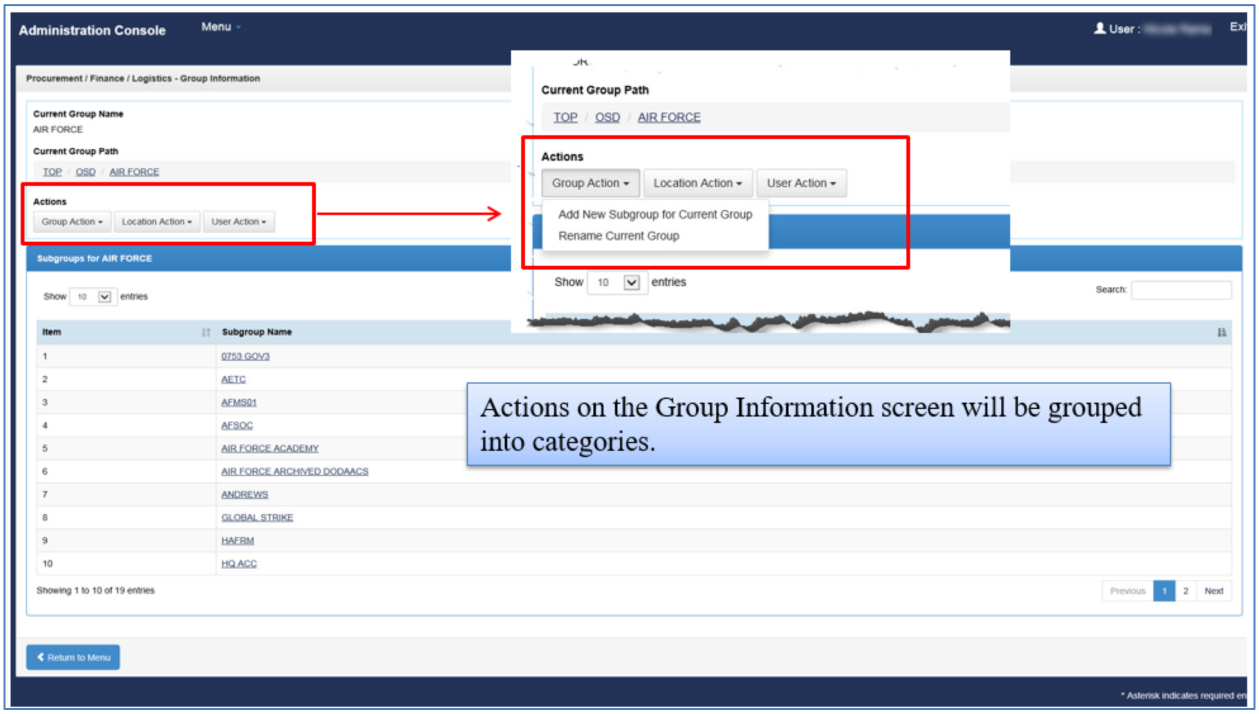
Group Management

Procurement / Finance / Logistics Group Information
Administer groups and subgroups in the PFL hierarchy by adding / renaming / moving / deleting groups as well as adding / moving location codes in the group structure.

Group Lookup
Lookup a Group by Location Code and view active Government / Contractor Administrators.

Group History
Look up the history of actions on groups.

This Group Management functionality gives the Administrator the ability manages the subgroups in the hierarchy, depending on the role they are assigned.   They have access to adding, renaming, moving or deleting groups as well as adding or moving location codes in a group structure.



Administration Console Menu

User : [redacted] Exi

Procurement / Finance / Logistics - Group Information

Current Group Name
AIR FORCE

Current Group Path
TOP / OSD / AIR FORCE

Actions
Group Action ▾ Location Action ▾ User Action ▾

Subgroups for AIR FORCE

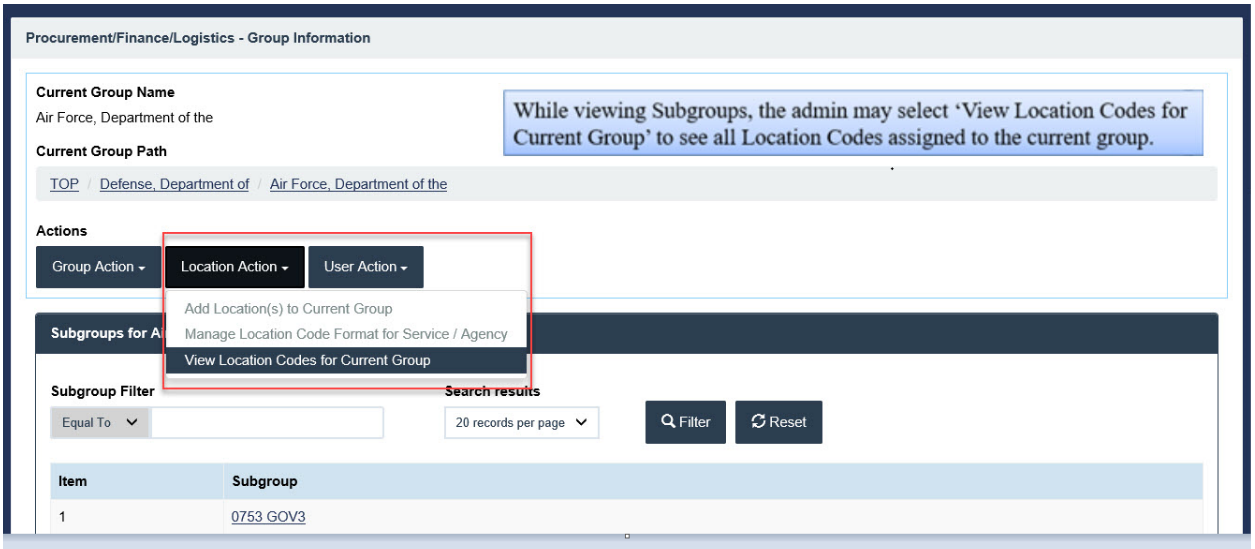
Show 10 entries Search:

Item	Subgroup Name
1	0753 GOV3
2	AETC
3	AFMS01
4	AFSOC
5	AIR FORCE ACADEMY
6	AIR FORCE ARCHIVED DODAACS
7	ANDREWS
8	GLOBAL STRIKE
9	HAFRM
10	HQ ACC

Showing 1 to 10 of 19 entries

* Asterisk indicates required en

Actions on the Group Information screen will be grouped into categories.



Procurement/Finance/Logistics - Group Information

Current Group Name
Air Force, Department of the

Current Group Path
TOP / Defense, Department of / Air Force, Department of the

Actions
Group Action ▾ Location Action ▾ User Action ▾

Add Location(s) to Current Group
Manage Location Code Format for Service / Agency
View Location Code for Current Group

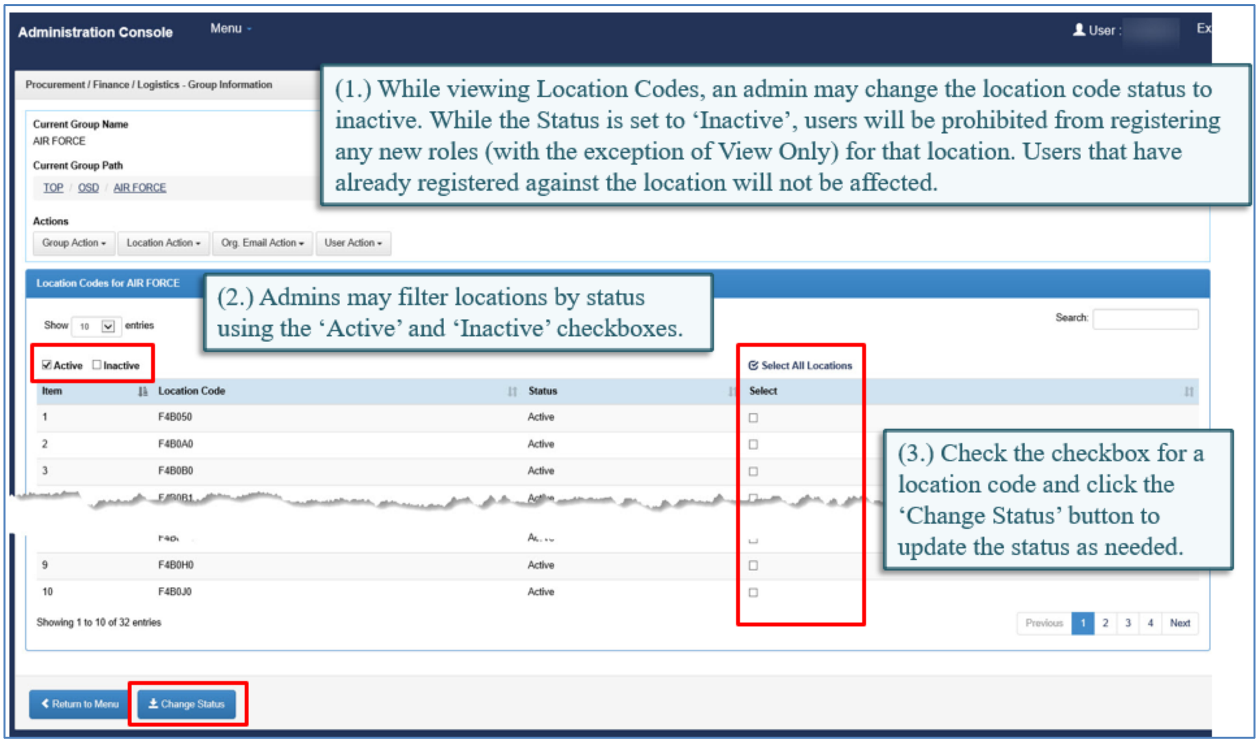
Subgroups for Ai

Subgroup Filter: Equal To

Search results: 20 records per page

Item	Subgroup
1	0753 GOV3

While viewing Subgroups, the admin may select ‘View Location Codes for Current Group’ to see all Location Codes assigned to the current group.



Procurement / Finance / Logistics - Group Information

Current Group Name
AIR FORCE

Current Group Path
TOP / OSD / AIR FORCE

Actions

Location Codes for AIR FORCE

Show 10 entries

☑ Active □ Inactive

Item	Location Code	Status	Select
1	F4B050	Active	□
2	F4B0A0	Active	□
3	F4B0B0	Active	□
	F4B0B1	Active	□
9	F4B0H0	Active	□
10	F4B0J0	Active	□

Showing 1 to 10 of 32 entries

(1.) While viewing Location Codes, an admin may change the location code status to inactive. While the Status is set to ‘Inactive’, users will be prohibited from registering any new roles (with the exception of View Only) for that location. Users that have already registered against the location will not be affected.

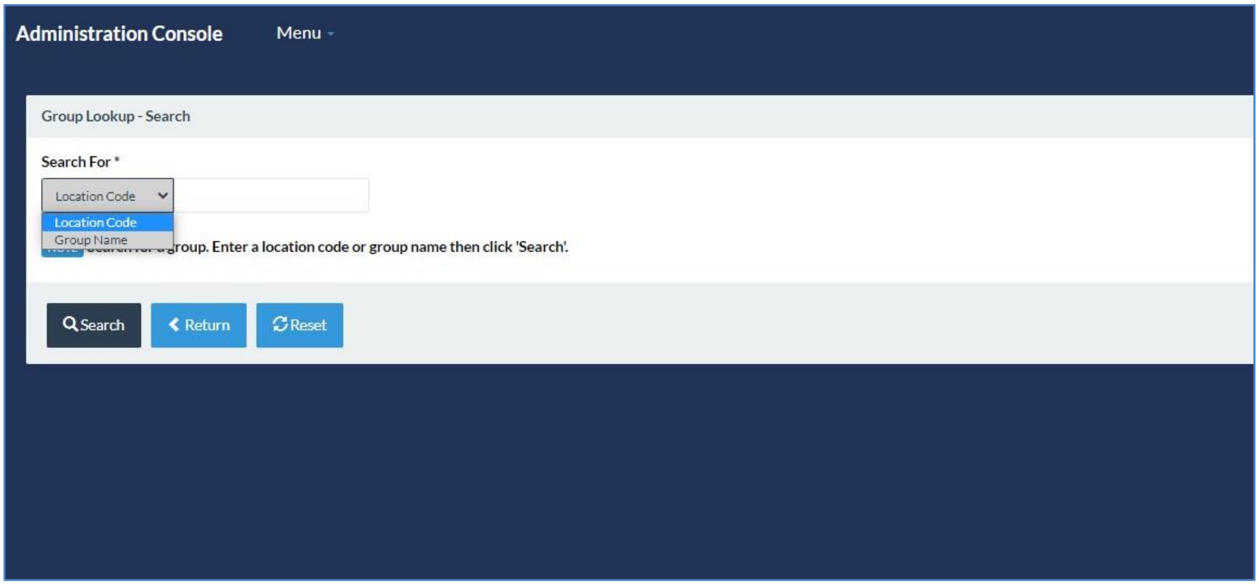
(2.) Admins may filter locations by status using the ‘Active’ and ‘Inactive’ checkboxes.

(3.) Check the checkbox for a location code and click the ‘Change Status’ button to update the status as needed.

3.1.2 Group Lookup

If Location Code is selected, the label will read "Location Code" and if Group Name is selected, the label will read "Group Name." When the user clicks Submit, the database conducts a search for a Group that matches the Group Name or Location Code.

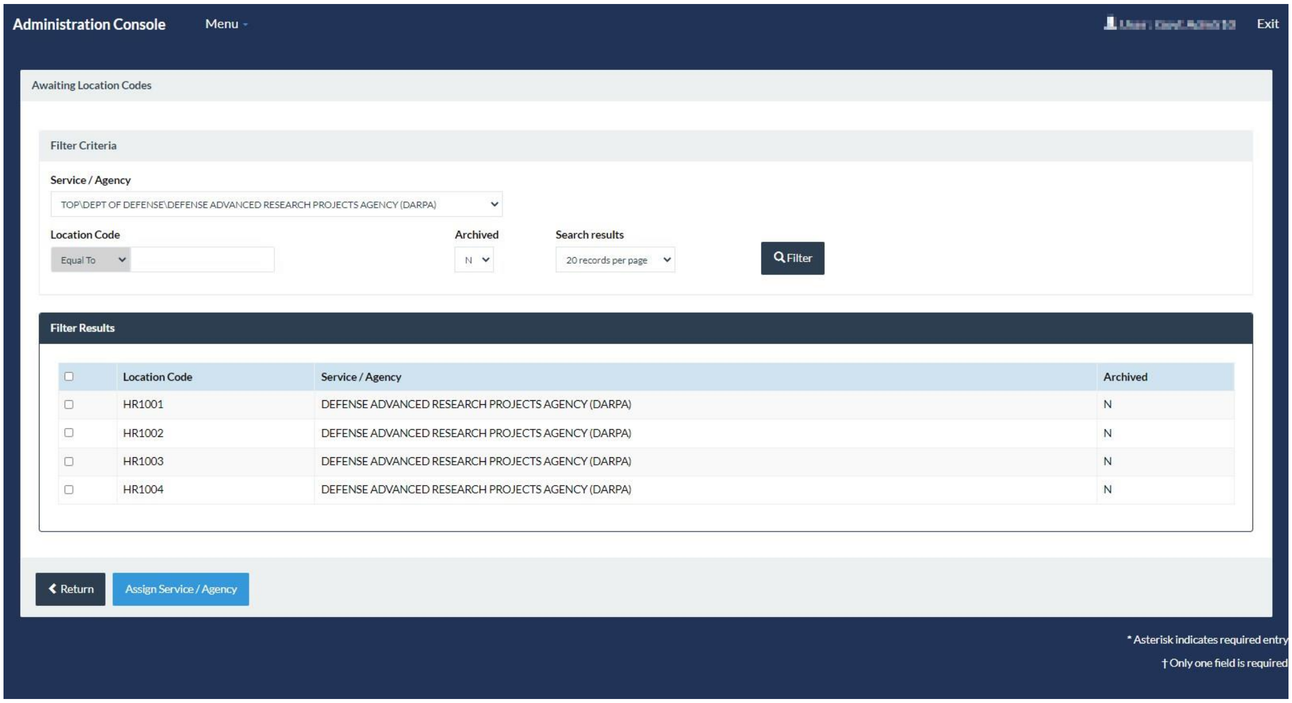
There are times when the Group may have a Location Code that is not known, but is required to perform some action such as registering a user or determining the GAM associated with a specific Location Code. The GAM has a "review only" ability to view accounts that are more than two levels below his/her groups in the hierarchy.



Search for a group. Enter a location code or group name then click 'Search'.

3.1.3 Awaiting Location Codes

Administer Awaiting Location Codes from DAASC by assigning them to a Service/Agency within the group structures. This function is now available only to the PIEE level Administrators.



Service / Agency: TOP\DEPT OF DEFENSE\DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)

Location Code: Equal To

Archived: N

Search results: 20 records per page

□	Location Code	Service / Agency	Archived
□	HR1001	DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)	N
□	HR1002	DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)	N
□	HR1003	DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)	N
□	HR1004	DEFENSE ADVANCED RESEARCH PROJECTS AGENCY (DARPA)	N

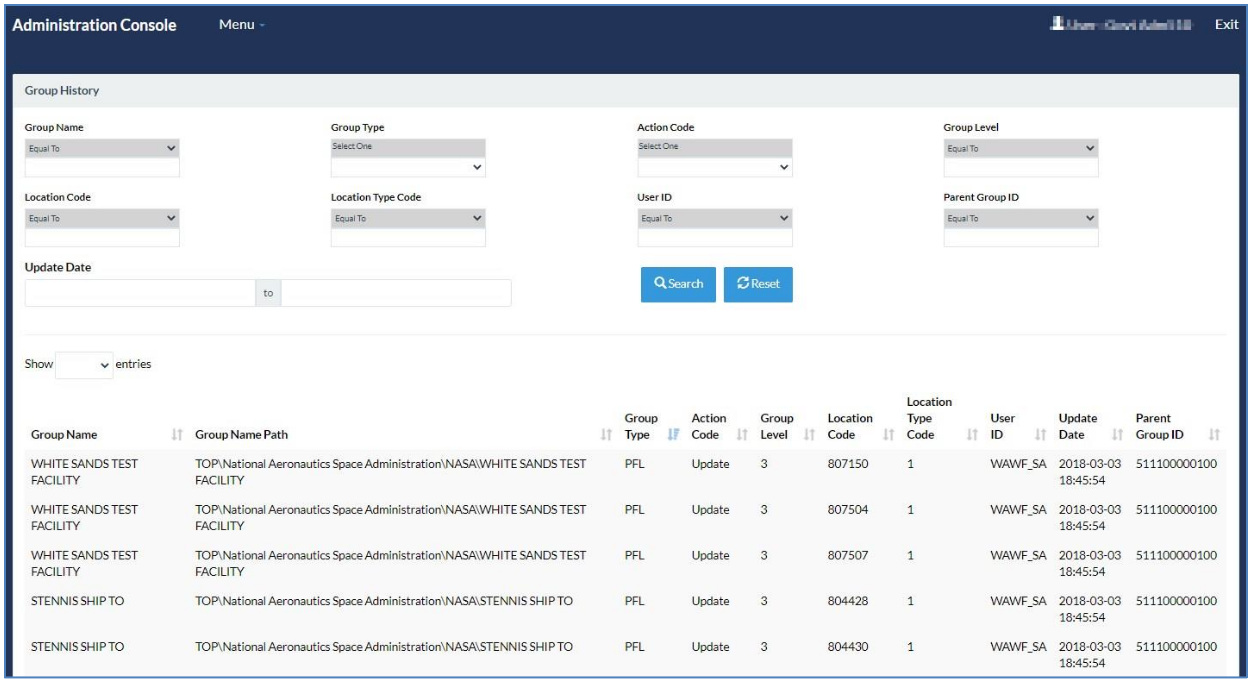
* Asterisk indicates required entry

† Only one field is required

3.1.4 Group History

This is a dashboard for the Administrator to quickly review by any of the search criteria available when records were last updated. The available criteria are:

- Group Name
- Action Code
- Group Level
- Location Code
- Location Type Code
- User ID
- Parent Group ID
- Update from and to Dates



Group History

Group Name: Equal To

Group Type: Select One

Action Code: Select One

Group Level: Equal To

Location Code: Equal To

Location Type Code: Equal To

User ID: Equal To

Parent Group ID: Equal To

Update Date to

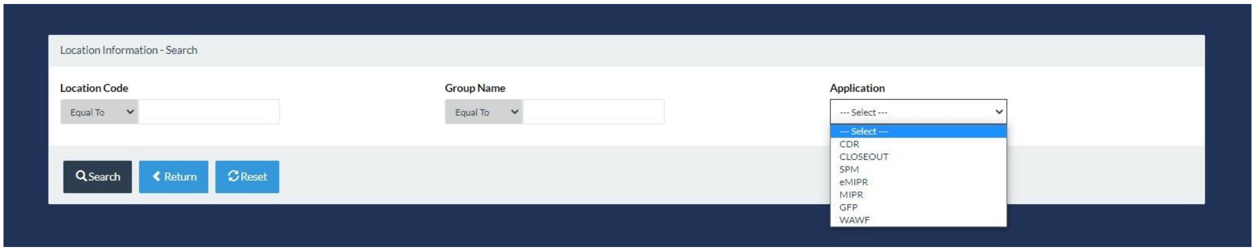
Show entries

Group Name	Group Name Path	Group Type	Action Code	Group Level	Location Code	Location Type Code	User ID	Update Date	Parent Group ID
WHITE SANDS TEST FACILITY	TOP\National Aeronautics Space Administration\NASA\WHITE SANDS TEST FACILITY	PFL	Update	3	807150	1	WAWF_SA	2018-03-03 18:45:54	511100000100
WHITE SANDS TEST FACILITY	TOP\National Aeronautics Space Administration\NASA\WHITE SANDS TEST FACILITY	PFL	Update	3	807504	1	WAWF_SA	2018-03-03 18:45:54	511100000100
WHITE SANDS TEST FACILITY	TOP\National Aeronautics Space Administration\NASA\WHITE SANDS TEST FACILITY	PFL	Update	3	807507	1	WAWF_SA	2018-03-03 18:45:54	511100000100
STENNIS SHIP TO	TOP\National Aeronautics Space Administration\NASA\STENNIS SHIP TO	PFL	Update	3	804428	1	WAWF_SA	2018-03-03 18:45:54	511100000100
STENNIS SHIP TO	TOP\National Aeronautics Space Administration\NASA\STENNIS SHIP TO	PFL	Update	3	804430	1	WAWF_SA	2018-03-03 18:45:54	511100000100

3.2 Location Management

This option is available to the Administrators under the Location tab on the Administration Console. Using these actions, the administrator may modify/update the organizational e-mail assigned to a group. This is also the location where they would add an extension to the selected location code. This option is more direct than navigating from Group to Group as with the User Administration (which is primarily focused on the users within a Group). To access these actions, the administrator enters the Location Code they want to administer.   This section also allows the administrator to deactivate a location code.

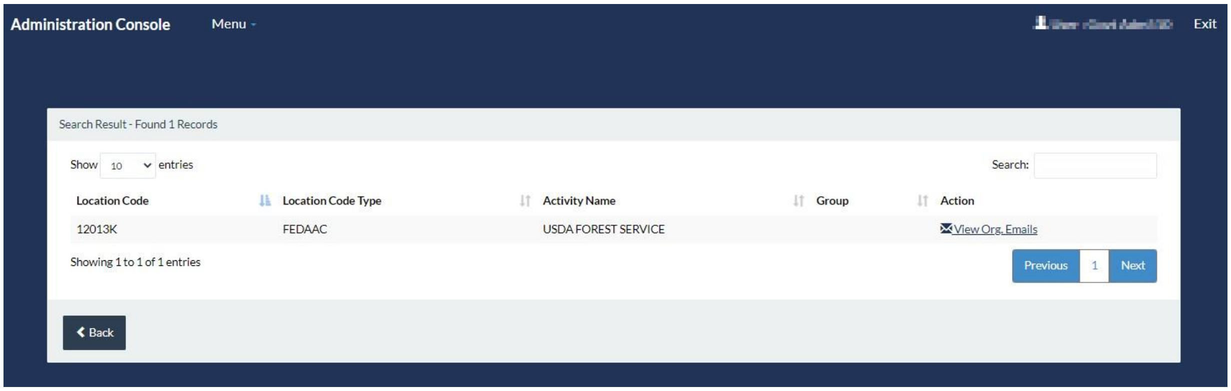
3.2.1 Location Information


Location Information - Search

Location Code: Equal To

Group Name: Equal To

Application: --- Select ---



Search Result - Found 1 Records

Show 10 entries

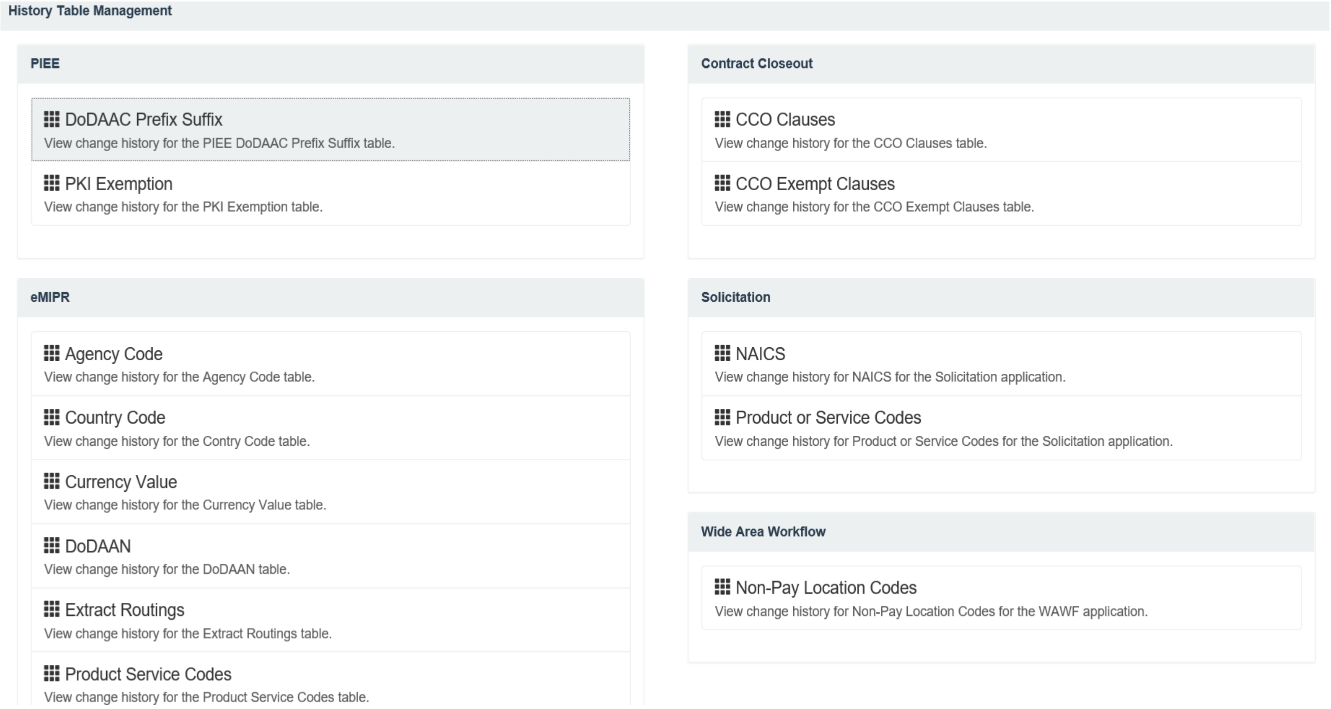
Search:

Location Code	Location Code Type	Activity Name	Group	Action
12013K	FEDAAC	USDA FOREST SERVICE		✉View Org. Emails

Showing 1 to 1 of 1 entries

3.3 History Management

This is a view only access to the records that have had a change in each of the data tables. Each of the views of the tables will all contain a Date/Time Stamp of the last time the record was modified.



History Table Management

PIEE

- DoDAAC Prefix Suffix
  View change history for the PIEE DoDAAC Prefix Suffix table.
- PKI Exemption
  View change history for the PKI Exemption table.

Contract Closeout

- CCO Clauses
  View change history for the CCO Clauses table.
- CCO Exempt Clauses
  View change history for the CCO Exempt Clauses table.

eMIPR

- Agency Code
  View change history for the Agency Code table.
- Country Code
  View change history for the Contry Code table.
- Currency Value
  View change history for the Currency Value table.
- DoDAAN
  View change history for the DoDAAN table.
- Extract Routings
  View change history for the Extract Routings table.
- Product Service Codes
  View change history for the Product Service Codes table.

Solicitation

- NAICS
  View change history for NAICS for the Solicitation application.
- Product or Service Codes
  View change history for Product or Service Codes for the Solicitation application.

Wide Area Workflow

- Non-Pay Location Codes
  View change history for Non-Pay Location Codes for the WAWF application.

3.4 Table Management

This functionality gives the administrator view only access to all the records on the data table.

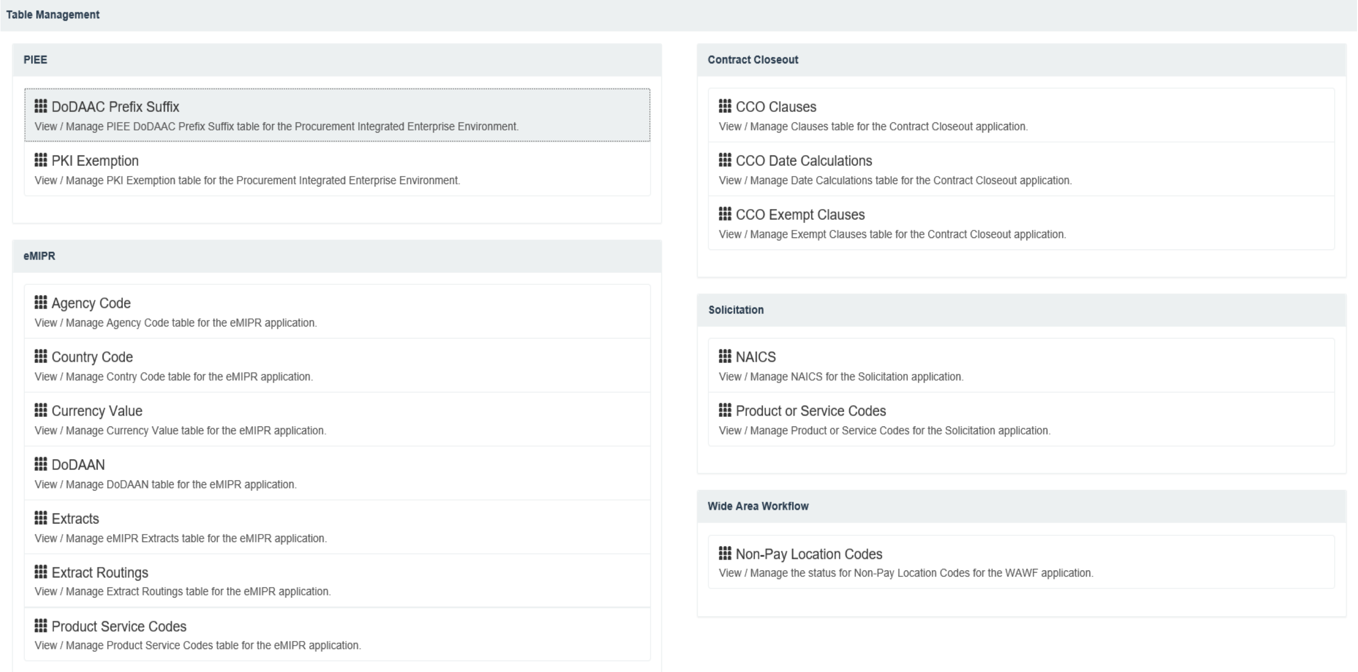


Table Management

PIEE

- DoDAAC Prefix Suffix
  View / Manage PIEE DoDAAC Prefix Suffix table for the Procurement Integrated Enterprise Environment.
- PKI Exemption
  View / Manage PKI Exemption table for the Procurement Integrated Enterprise Environment.

Contract Closeout

- CCO Clauses
  View / Manage Clauses table for the Contract Closeout application.
- CCO Date Calculations
  View / Manage Date Calculations table for the Contract Closeout application.
- CCO Exempt Clauses
  View / Manage Exempt Clauses table for the Contract Closeout application.

eMIPR

- Agency Code
  View / Manage Agency Code table for the eMIPR application.
- Country Code
  View / Manage Contry Code table for the eMIPR application.
- Currency Value
  View / Manage Currency Value table for the eMIPR application.
- DoDAAN
  View / Manage DoDAAN table for the eMIPR application.
- Extracts
  View / Manage eMIPR Extracts table for the eMIPR application.
- Extract Routings
  View / Manage Extract Routings table for the eMIPR application.
- Product Service Codes
  View / Manage Product Service Codes table for the eMIPR application.

Solicitation

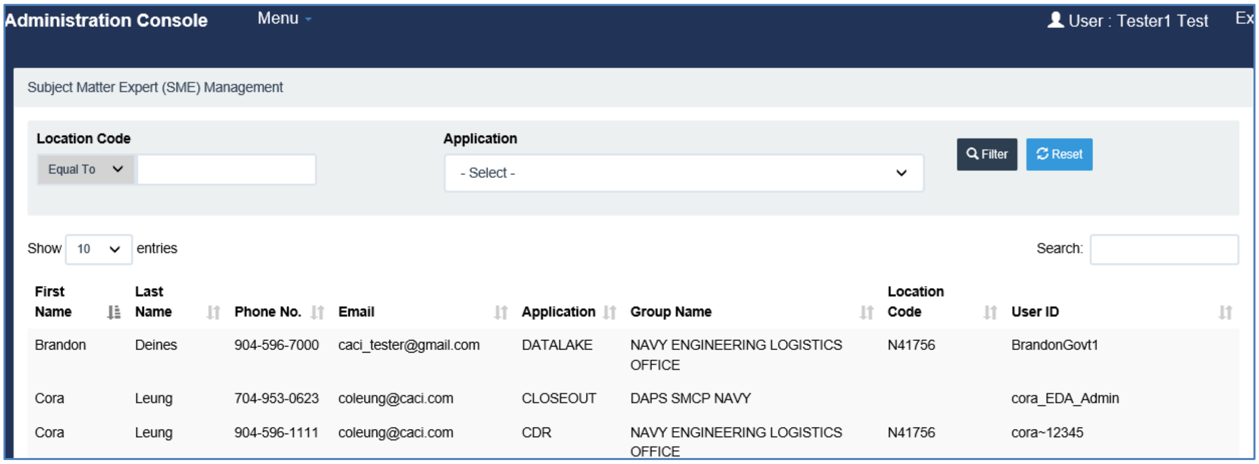
- NAICS
  View / Manage NAICS for the Solicitation application.
- Product or Service Codes
  View / Manage Product or Service Codes for the Solicitation application.

Wide Area Workflow

- Non-Pay Location Codes
  View / Manage the status for Non-Pay Location Codes for the WAWF application.

3.5 Subject Matter Expert (SME) Management

The administrators have access to this table to record the SME for each module. PIEE users have access to a lookup that utilizes this data table.



Subject Matter Expert (SME) Management

Location Code: Equal To

Application: - Select -

Show 10 entries

Search:

First Name	Last Name	Phone No.	Email	Application	Group Name	Location Code	User ID
Brandon	Deines	904-596-7000	caci_tester@gmail.com	DATALAKE	NAVY ENGINEERING LOGISTICS OFFICE	N41756	BrandonGovt1
Cora	Leung	704-953-0623	coleung@caci.com	CLOSEOUT	DAPS SMCP NAVY		cora_EDA_Admin
Cora	Leung	904-596-1111	coleung@caci.com	CDR	NAVY ENGINEERING LOGISTICS OFFICE	N41756	cora~12345

3.6 User/Role Management

User administration is the joint responsibility of the GAM/CAM and the PIEE Administrators. However, the GAM/CAM does not have access to the User Deletion link. Administrators have the option to View, Edit and Delete User profiles as well as reset passwords and certificates.

User Information

This option permits the Administrator to select a user or series of users. Once a user (or group of users) is identified, the Administrator may:

- View/Edit the profile
- View/Add to the user's roles
- Add attachments to a user's profile
- Add/Edit EDI attachment location paths (PIEE Administrator only)
- Archive any inactive accounts (This function is accessed through the Role link under the PIEE Administration Console and explained under Role Activation).

The Administrators may view the user's profile and/or the roles associated with the user, as well as view the time/date for activation/deactivation. In addition, the GAM / CAM / PIEE Administrators may edit the profile to update any portion of the information associated with that user such as telephone numbers etc.

User Deletion

This function permits the PIEE Administrators to search for and delete inactive users. Users are searched by entering a Registration Date Range.

Reset Password

Recognizing that the functional users can have occasions where they forget passwords, the Administrators all can reset the user's password. By entering in the user's user ID, the Administrator can cause the system to generate that a one-time password has been given via secure fax or by phone. This permits the user to log on to PIEE with the one-time password. The user will then be prompted to answer the three security questions, enter their new password and confirm their new password.

Reset Certificate

The Administrators as well as the CAM/GAM are provided with the capability to reset passwords for one-time use and substitute a User ID credential for a certificate when required. The most significant reason for a certificate user to have an inability to use their certificate is that they have locked their smartcard because they have forgotten or mistyped their Personal Identification Number (PIN). The PIN is the password equivalent for the CAC card. Given the potential gap in time while a CAC user waits for replacement CAC after losing it or a PIN reset after locking it, we have provided a capability for the end user to request activation of the temporary credential of a User ID with strong password.

After receiving the request, the administrator can generate a one-time password for the user and an e-mail is sent to the user letting them know that a one-time password has been given via secure fax or by phone. This permits the user to log on to PIEE with the one-time password and the user's user ID (from the expired certificate). The user will then be prompted to answer the three security questions, enter their new password and confirm their new password. After the user has replaced an expired software certificate, lost CAC, or received a PIN reset, that user can revert to the preferred credential through revised profile maintenance features.

The determination of the individual's User ID, which is system-generated for certificate users, can be made by searching the User Information using the affected user's First, Last Name, and optionally adding additional criteria such as an affiliated location code, role, or other available criteria. Resetting a certificate user changes their credential to User ID and password and all references to the previous credential are lost.

If the User being reset is a Government or Government Support Contractor, they will be allowed access to PIEE using a User Id/Password for the number of days specified in the System Properties table.

Role Administration

Role Information: View user role data, add a role, comments and attachments.

Role Activation: Activate, deactivate and archive user roles.

Role Activation Report: View role activation reports including disabled accounts.

Role Information

This option permits the administrators to select a user or series of users. Once a user (or group of users) is identified, the Administrator may:

- View and Add roles
- Add comments and attachments
- A Government Administrator can add the "Business Intelligence Access" role to existing Government users.

A Government GAM can add the new "Business Intelligence Access" role to existing Government users. The AKO E-Mail is mandatory and will be populated from the User Profile if it is there, otherwise it will have to be entered manually.

Government GAMs will also be permitted to manage the new "Business Intelligence Access" role.

Role Activation

The activation of government users is primarily the responsibility of the Government Administrator. That is the person who has the direct contact and control of their Group. However, since the Vendor community is not required to have a Contractor Administrator, the PIEE Administrator (Help Desk) also has the ability to activate users. In addition, an Administrator must activate the initial GAM/CAM in a Group.

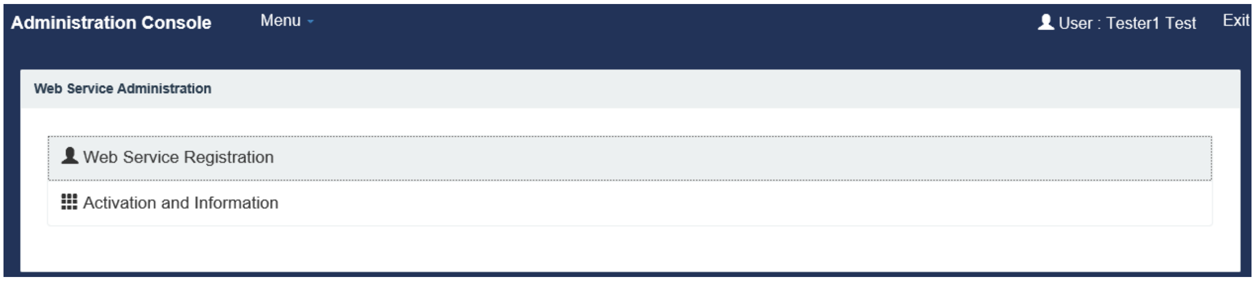
By entering a variety of search criteria, a single user may be selected or a series of users may be selected from within a Group. At this point, his/her status may be changed from Inactive to Active, or Active to Inactive, and comments can be logged or files attached, as to the reason for the change. The Administrators may also archive inactive accounts. NOTE: The Functional Auditor Role can only be activated by the PMO.

Role Activation Report

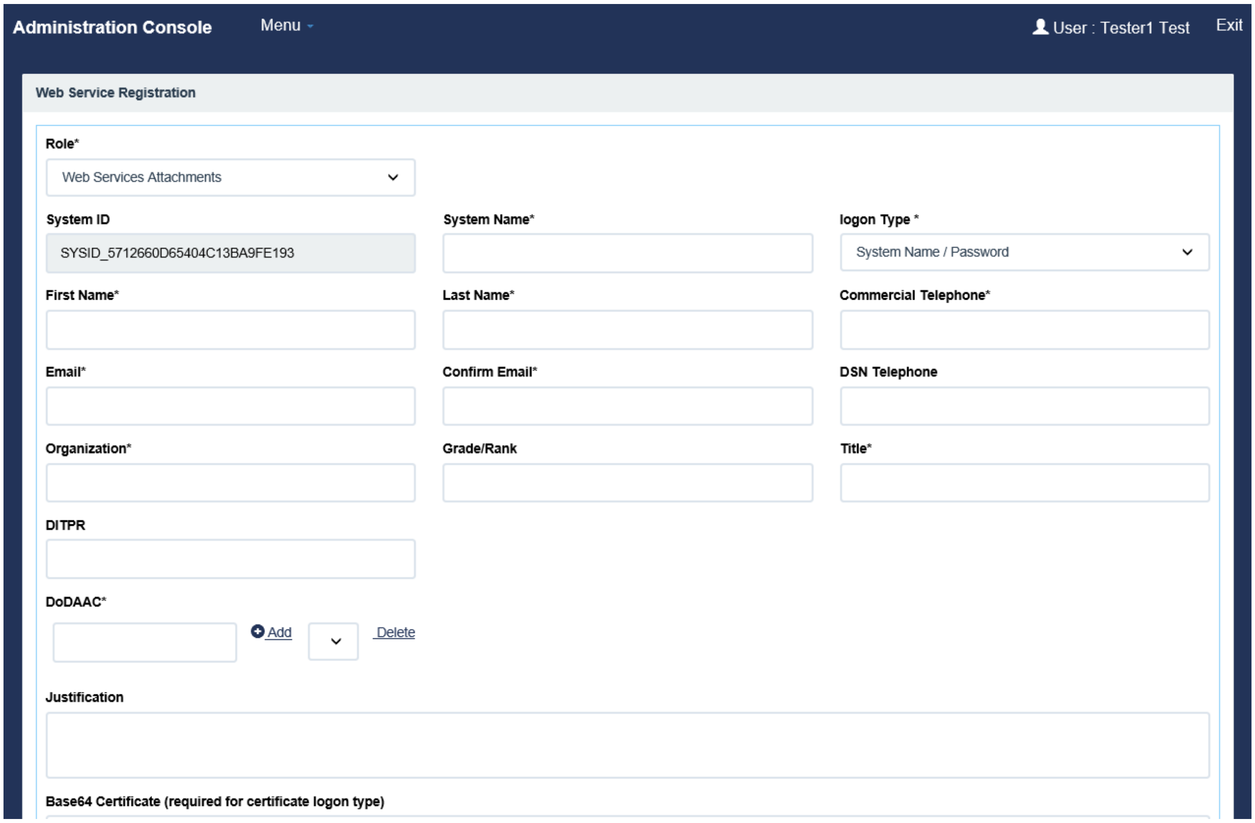
This option permits the GAM to view role activation reports as well as information on disabled accounts. Filtered results provide the GAM with access to User ID history, roles and comments.

3.7 Web Service Administration

The functionalities of the Web Service Administration are available only to the PIEE Super Administrator.



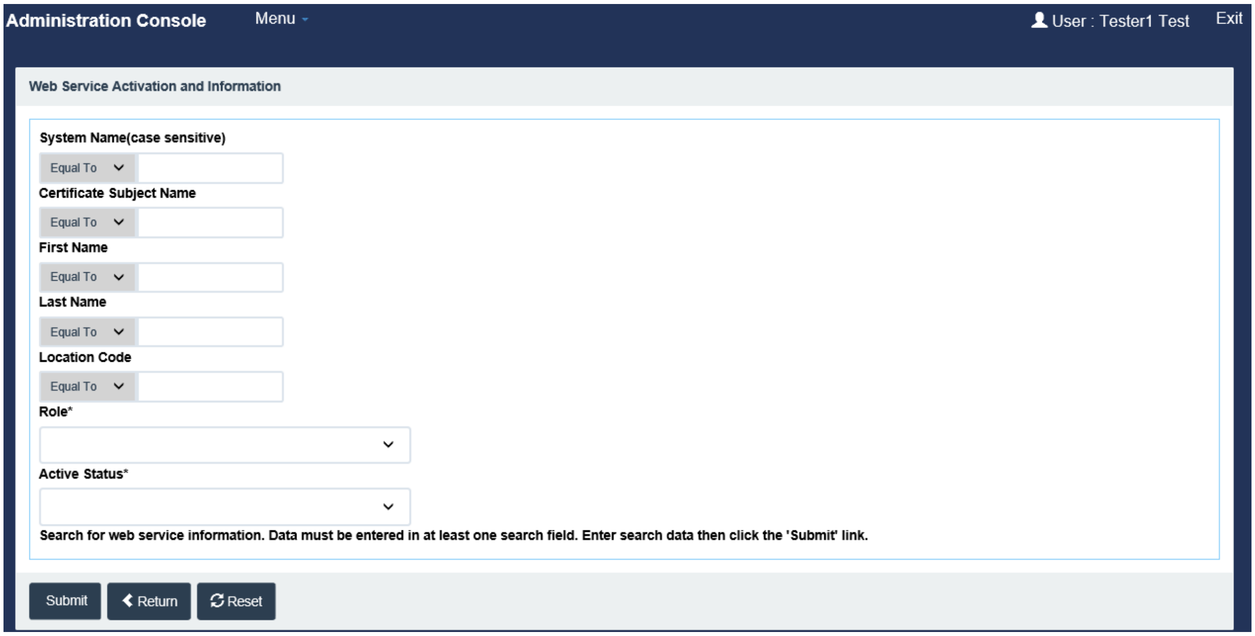
Web Service Registration



Web Service Registration

Role*		
Web Services Attachments		
System ID	System Name*	logon Type *
SYSID_5712660D65404C13BA9FE193		System Name / Password
First Name*	Last Name*	Commercial Telephone*
Email*	Confirm Email*	DSN Telephone
Organization*	Grade/Rank	Title*
DITPR		
DoDAAC*		
Justification		
Base64 Certificate (required for certificate logon type)		

The PIEE Super Administrator will log on to the WAWF application via the PIEE Home Page.



Search for web service information. Data must be entered in at least one search field. Enter search data then click the 'Submit' link.

Activation

The activation of government users is primarily the responsibility of the Group Administrator. That is the person who has the direct contact and control of their Group. However, since the government users who intend on viewing WAWF attachments using Web Services, are not required to have a WAWF user account, the PIEE Super Administrator must activate the Web Service user. The PIEE Super Administrator will enter the appropriate data to search for the Web Service User to be activated and click the Submit link.

Information

When PIEE Super Administrator clicks on the System Name link for a particular user, a Web Service – Manage System Profile page will be displayed with 3 tabs:

- Profile
- Justification/Attachments
- Reset Password / Certificate

On the Profile tab, PIEE Super Administrator can view the Web Service user profile information, such as System ID, System Name, and Logon Type. The Admin user can also edit the profile information such as user's name, phone number, organization and add/deleted a DoDAAC.

On the Justification/Attachments tab, the Admin user can view/add/delete system attachments and view/add justification.

Reset Web Service Password tab

Recognizing that the Web Service users can have occasions where he/she forgets his/her password, the PIEE Super Administrator has the ability to reset the user's password. By entering a value in the System Name field, the Admin can cause the system to generate a one-time password for the user and have that password sent to the email address that is contained in the user's system profile.

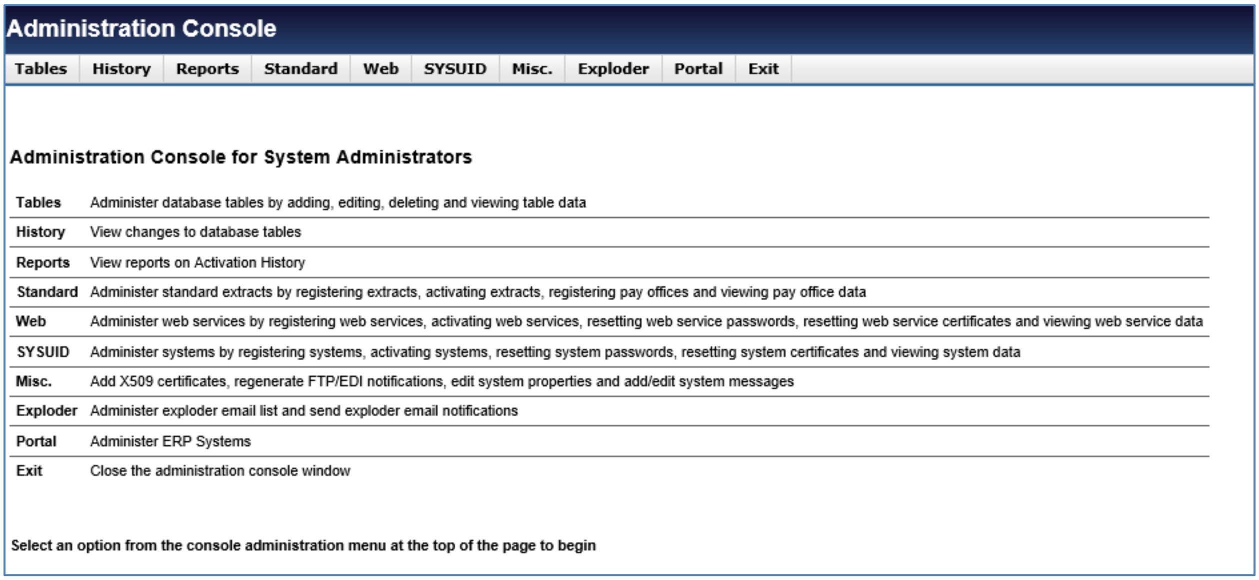
Reset Web Service Certificate tab

The PIEE Super Administrator is provided with the capability to reset passwords and substitute a System ID credential for a certificate when required. The most significant reason for a certificate user to have an inability to use their certificate is that they have locked their smartcard because they have forgotten or mistyped their Personal Identification Number (PIN). The PIN is the password equivalent for the CAC card. Given the potential gap in time while a CAC user waits for replacement CAC after losing it or a PIN reset after locking it, we have provided a capability for the end user to request activation of the temporary credential of a User ID with strong password.

After receiving the request, the PIEE Super Administrator is able to generate and transmit a password to be paired with the new Web Service ID for viewing documents. After the user has replaced an expired software certificate, lost CAC, or received a PIN reset, that user can revert to the preferred credential through revised profile maintenance features.

Recognizing that the Web Service users can have occasions where their certificates expire and need to transfer their user ID to a new certificate, the Admin has the ability to reset the user's certificate. By entering in the user's Web Service ID (from the expired certificate), the Admin can cause the system to reset the user's certification.

3.8 Additional Administration



Administration Console for System Administrators

Tables	Administer database tables by adding, editing, deleting and viewing table data
History	View changes to database tables
Reports	View reports on Activation History
Standard	Administer standard extracts by registering extracts, activating extracts, registering pay offices and viewing pay office data
Web	Administer web services by registering web services, activating web services, resetting web service passwords, resetting web service certificates and viewing web service data
SYSUID	Administer systems by registering systems, activating systems, resetting system passwords, resetting system certificates and viewing system data
Misc.	Add X509 certificates, regenerate FTP/EDI notifications, edit system properties and add/edit system messages
Exploder	Administer exploder email list and send exploder email notifications
Portal	Administer ERP Systems
Exit	Close the administration console window

Select an option from the console administration menu at the top of the page to begin

3.9 Additional Administration Console Overview

System Tables are accessible by the WAWF PMO, Administrators and Auditor roles through the PIEE Administration Console menu. Tables are located under the 'Tables' and 'History' menu links. User privileges for these tables are based upon the assigned role of the logged in user.

There are four actions that may be taken on the system tables depending on the user role logged in:

- Search
- Add
- Edit
- Delete

Each system table has a matching history table where every action taken on the system table is recorded. The history tables have the same name as the system tables with a suffix of '_HST'.

Table Administration Menu

- Agency Help Desk
- Certificate Authorities
- Contract Closeout
- Contract Information
- Contract Number Type
- Contractor DoDAACs
- Currency Codes
- DCAA Direct Bill Authorization Codes
- DCMA Direct Bill Authorization Codes
- DCMA Administration Location Codes
- DCMA Cost Voucher Processing Location Codes
- DFAS Pay Codes
- DoDAAC Prefix Suffix
- DSS Acceptor
- EDI Location Codes
- EDI Extracts
- EEBP Locations Codes
- Energy Tests - Master List
- Energy Commodities
- Energy Sub Commodities
- Energy Tests - Add/Edit/Delete

- Order Energy Tests
- Energy Test Categories
- Group Energy Tests
- Energy Test Types
- Energy Issue By DoDAACs
- Energy Signature NSNs
- Entitlement Status Update
- Extract Suppression
- File Extensions
- Foreign Military Sales Codes
- Group Role Id
- IUID Data Correction Locations
- IUID DoDAAC Prefix Suffix
- Legacy AAI Codes
- Matching DUNS/CAGE
- Misc. Fee Type Codes
- Misc. Pay DBS
- Misc. Pay Type Codes
- Navy ERP Ship To Codes
- One-Pay AAIs
- One-Pay TFS AAIs
- ONR Cost Voucher Processing Location Codes
- Org Location Codes
- Org Location Notifications
- PKI Constrained Policy Sets
- PKI Exemption
- PKI Policy Configurations
- Pay System Misc. Tax and Fee Codes
- QCTS DoDAACs
- Payment and Accounting Systems
- System Extracts
- System Misc. Pay Types
- Receiving Activities
- Reference Taxes
- Restricted Currency Codes
- Special Package Markings
- Standard Extracts
- Standard Systems
- SUPSHIP DoDAACs
- Tax Type Codes

- Unit Of Measure
- WAWF Extra Data

The History Administration option is available to the Administrators, WAWF PMO and Auditor roles. This allows the administrator to view changes to database tables.

Each system table has a matching history table where every action taken on the system table is recorded. The history tables have the same name as the system tables with a suffix of '_HST'.

History Table Administration Menu

- Agency Help Desk
- Certificate Authorities
- Contract Closeout
- Contract Number Type
- Currency Codes
- DCAA Direct Bill Authorization Codes
- DCMA Direct Bill Authorization Codes
- DCMA Administration Location Codes
- DCMA Cost Voucher Processing Location Codes
- DFAS Pay Codes
- DoDAAC Prefix Suffix
- DSS Acceptor
- EDI Location Codes
- EDI Extracts
- EEBP Locations Codes
- Energy Test Master
- Energy Results Dropdown Master
- Energy Test Categories
- Energy Results Dropdown
- Energy Issue By DoDAACs
- Energy Signature NSNs
- Energy Test
- Energy Test Codes
- Energy Test Types
- Entitlement Status Update
- Extract Suppression
- File Extensions
- Foreign Military Sales Codes
- Group Role Id
- IUID Data Correction Locations
- IUID DoDAAC Prefix Suffix

- Legacy AAI Codes
- Misc. Fee Type Codes
- Misc. Pay DBS
- Misc. Pay Type Codes
- Navy ERP Ship To Codes
- One-Pay AAIs
- One-Pay TFS AAIs
- ONR Cost Voucher Processing Location Codes
- Org Location Codes
- Org Location Notifications
- QCTS DoDAACs
- Payment and Accounting Systems
- System Extracts
- System Misc. Pay Types
- Pay System Misc. Tax and Fee Codes
- Receiving Activities
- Reference Taxes
- Restricted Currency Codes
- Standard Extracts
- Standard Systems
- SUPSHIP DoDAACs
- Tax Type Codes
- Unit Of Measure
- WAWF Extra Data

Reports

- User Activation History
- Administrator Activation History

Standard

This allows administrators to administer standard extracts by registering extracts, activating extracts, registering pay offices and viewing pay office data.

Standard Extract Registration -Provides the administrator the ability to sign up External Entities to receive Standard Extracts.

Standard Extract Activation - Provides the administrator the ability to activate and deactivate Standard Extracts.

Pay Office Registration - Prior to the administrator signing up External Entities to receive Standard Extracts they must ensure that the External Entity has a Standard Pay DoDAAC within the WAWF program.

Pay Office Information -Allows administrators to Editing Standard Pay Office Information.

Misc Administration

The Miscellaneous Administration option is available to the PIEE Super Administrator and PIEE Administrator. This allows the administrator to add X509 certificates and regenerate FTP/EDI notifications.

In addition, the PIEE Super Administrator, PIEE Administrator and WAWF PMO are responsible for the System Properties and System Messages sections.

Add Certificate

The System Administrators are provided with the capability to save the Root and the Root Issuer certificate authority details into the database by using the application.

FTP/EDI Notification Regeneration

This option is available to the PIEE Super Administrator and PIEE Administrator only. This allows the administrator to regenerate FTP/EDI notifications.

System Properties

The SYSTEM_PROPERTIES entity stores all the FTP/EDI and some of the property file parameters. It has all the sensitive data stored and is an editable PMO table.

System Messages

The SYSTEM_MESSAGES entity stores all the system messages and can be added to and edited by the WAWF PMO.

Exploder

The administrator exploder email lists and send exploder email notifications using the Exploder Information link. The information can be edited and deleted as well.

Portal Administration

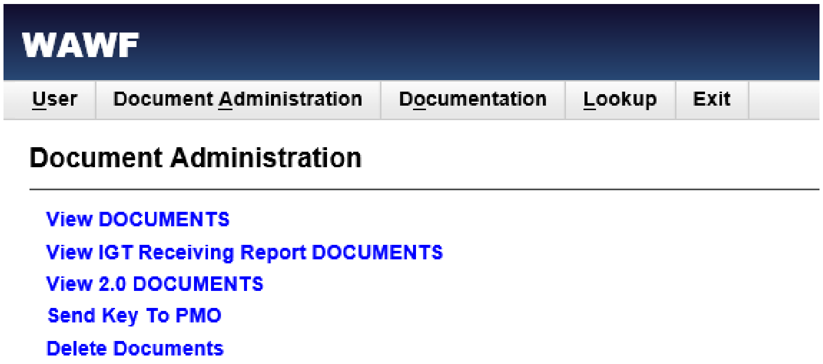
The Portal Administration menu is available to select administrators. ERP Systems Administration manages ERP systems that are registered with PIEE. ERP CAGE Administration manages CAGEs that are assigned to ERP Systems.

4. WAWF Administrator Roles

4.1 WAWF System Administrator

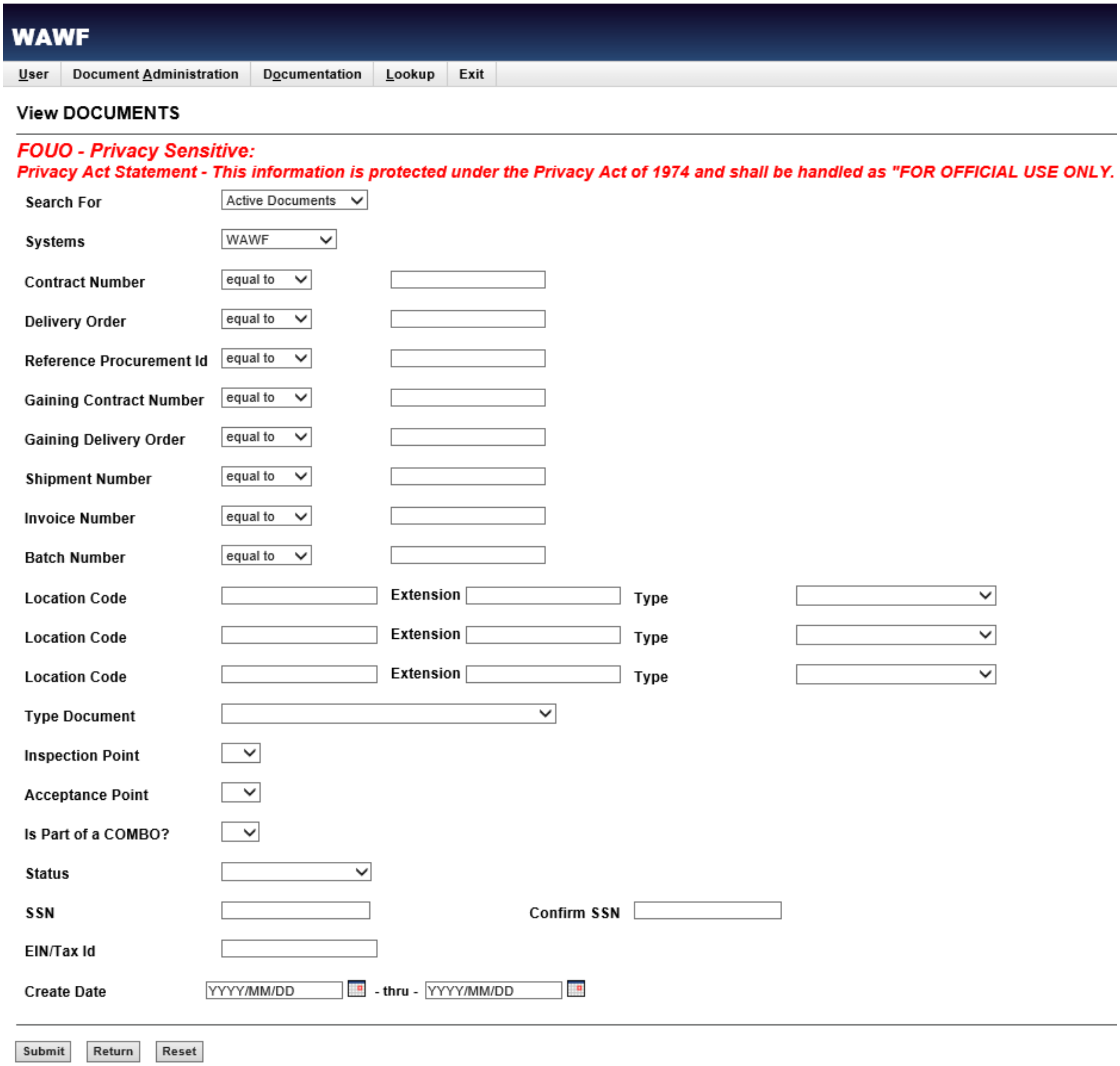
The WAWF System Administrator (formerly the WAWF SAM/HAM) will have the following functions available:

- View Documents in WAWF



Document Administration

View DOCUMENTS
View IGT Receiving Report DOCUMENTS
View 2.0 DOCUMENTS
Send Key To PMO
Delete Documents

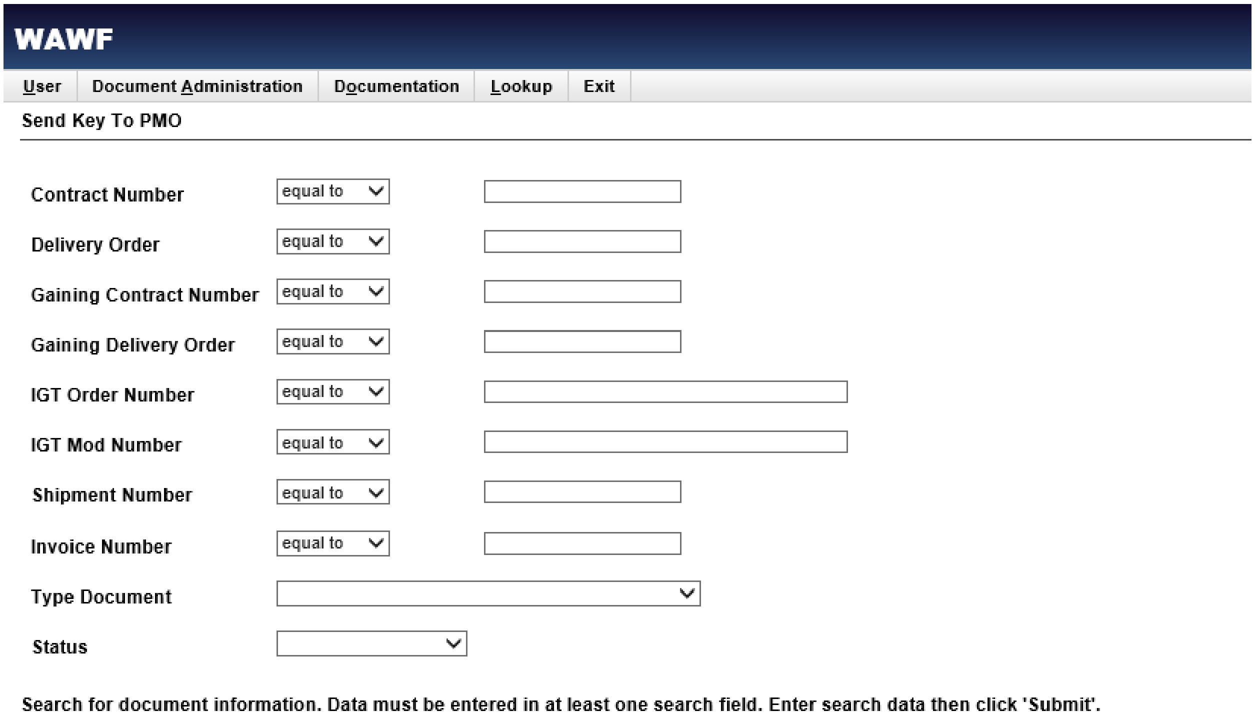


View DOCUMENTS

FOUO - Privacy Sensitive:
Privacy Act Statement - This information is protected under the Privacy Act of 1974 and shall be handled as "FOR OFFICIAL USE ONLY.

Search For	Active Documents				
Systems	WAWF				
Contract Number	equal to				
Delivery Order	equal to				
Reference Procurement Id	equal to				
Gaining Contract Number	equal to				
Gaining Delivery Order	equal to				
Shipment Number	equal to				
Invoice Number	equal to				
Batch Number	equal to				
Location Code		Extension		Type	
Location Code		Extension		Type	
Location Code		Extension		Type	
Type Document					
Inspection Point					
Acceptance Point					
Is Part of a COMBO?					
Status					
SSN		Confirm SSN			
EIN/Tax Id					
Create Date	YYYY/MM/DD	- thru -	YYYY/MM/DD		

- Send Key To PMO to request document deletion

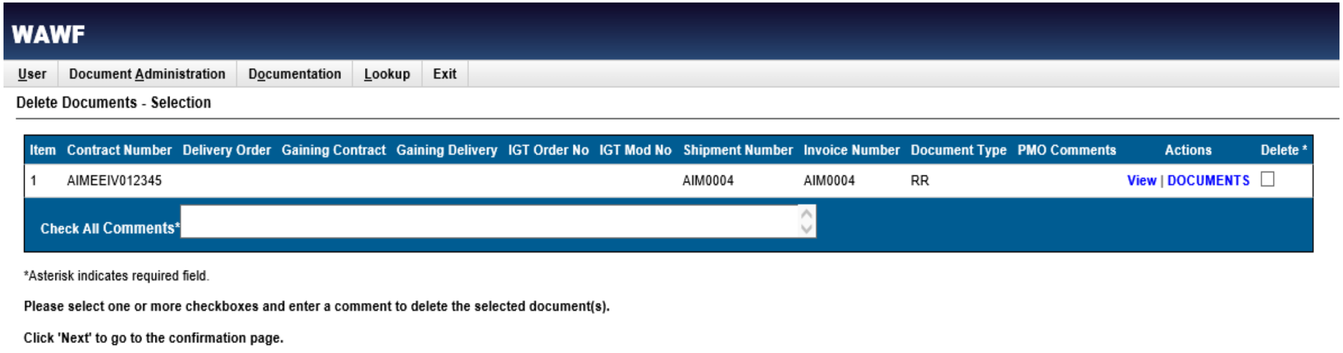


Send Key To PMO

Contract Number	equal to	
Delivery Order	equal to	
Gaining Contract Number	equal to	
Gaining Delivery Order	equal to	
IGT Order Number	equal to	
IGT Mod Number	equal to	
Shipment Number	equal to	
Invoice Number	equal to	
Type Document		
Status		

Search for document information. Data must be entered in at least one search field. Enter search data then click 'Submit'.

- Delete WAWF documents that have been approved by PMO



Delete Documents - Selection

Item	Contract Number	Delivery Order	Gaining Contract	Gaining Delivery	IGT Order No	IGT Mod No	Shipment Number	Invoice Number	Document Type	PMO Comments	Actions	Delete *
1	AIMEEIV012345						AIM0004	AIM0004	RR		View | DOCUMENTS	☐

Check All Comments*

*Asterisk indicates required field.

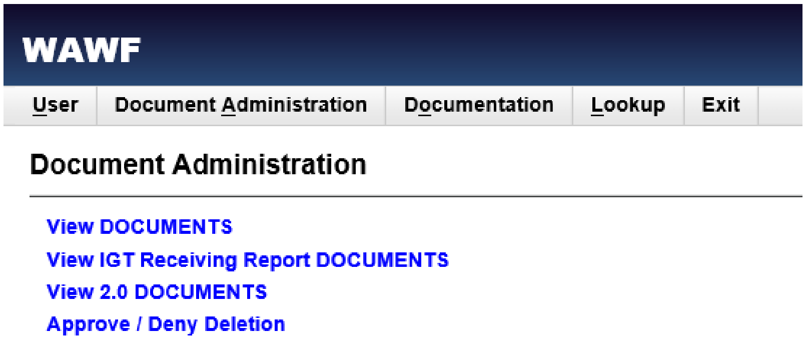
Please select one or more checkboxes and enter a comment to delete the selected document(s).

Click 'Next' to go to the confirmation page.

4.2 WAWF PMO

The WAWF PMO administrator has accessibility to the following functions:

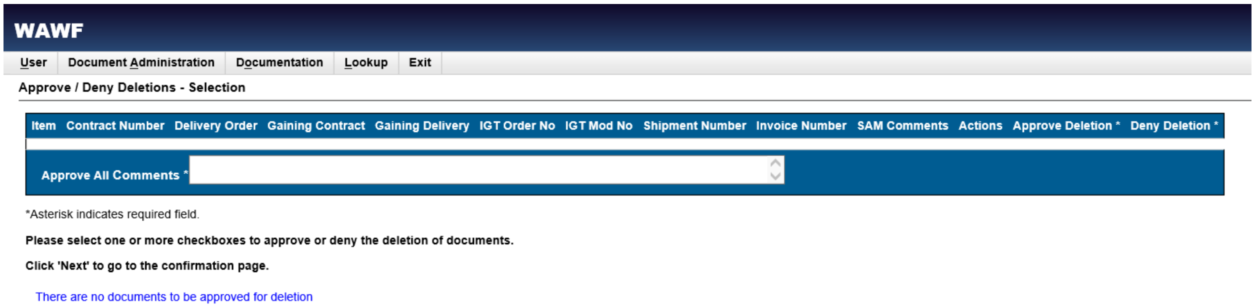
- View Documents in WAWF



Document Administration

View DOCUMENTS
View IGT Receiving Report DOCUMENTS
View 2.0 DOCUMENTS
Approve / Deny Deletion

- Approve or Deny Documents that have been requested for deletion



Approve / Deny Deletions - Selection

Item	Contract Number	Delivery Order	Gaining Contract	Gaining Delivery	IGT Order No	IGT Mod No	Shipment Number	Invoice Number	SAM Comments	Actions	Approve Deletion *	Deny Deletion *

Approve All Comments *

*Asterisk indicates required field.

Please select one or more checkboxes to approve or deny the deletion of documents.

Click 'Next' to go to the confirmation page.

There are no documents to be approved for deletion

- Manage / View history for DLA Energy tables

Additionally, the WAWF PMO administrator has access to the following select functions in the PIEE Administration Console:

Role Management: Administer roles by activating, deactivating, and archiving user roles.

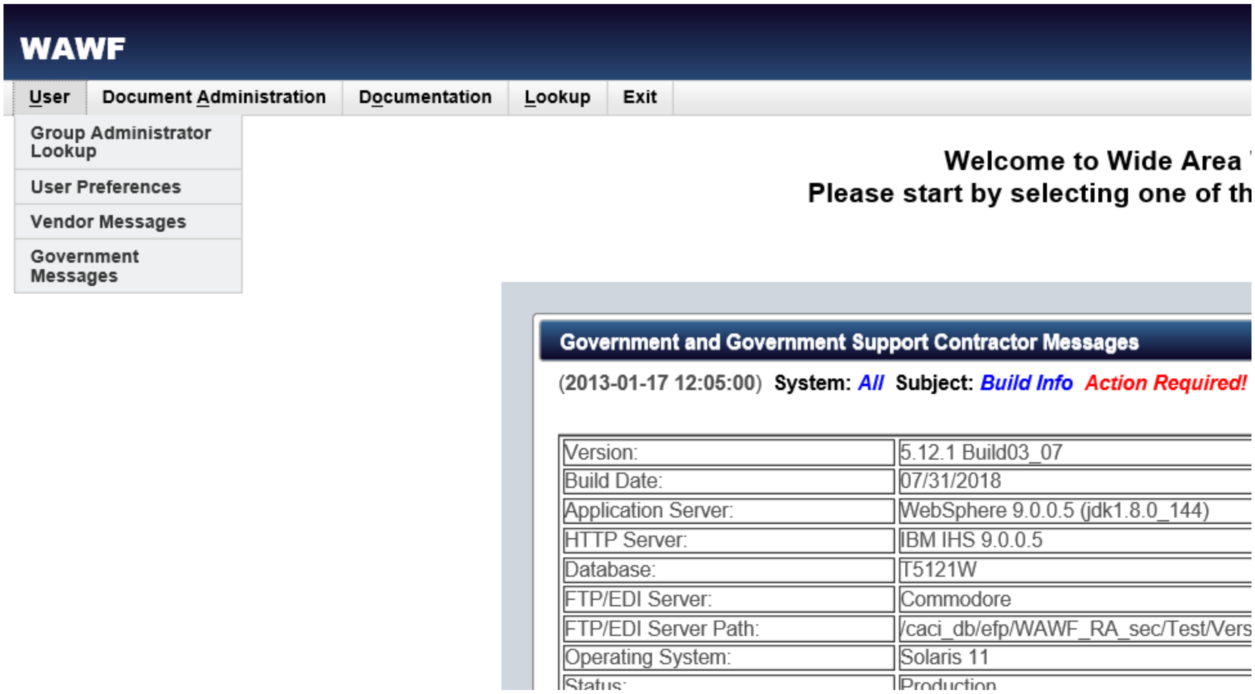
History Management: Review historical data for database tables.

Table Management: Administer database tables by adding, editing, deleting and viewing table data.

Additional Administration

4.3 Group View All

The Group View All Administrator will have view only capabilities to a set of documents in WAWF. It will be based on the location codes in the Group as well as any subgroups.



Welcome to Wide Area '
Please start by selecting one of th

Government and Government Support Contractor Messages

(2013-01-17 12:05:00) System: *All* Subject: *Build Info* *Action Required!*

Version:	5.12.1 Build03_07
Build Date:	07/31/2018
Application Server:	WebSphere 9.0.0.5 (jdk1.8.0_144)
HTTP Server:	IBM IHS 9.0.0.5
Database:	T5121W
FTP/EDI Server:	Commodore
FTP/EDI Server Path:	/caci_db/efp/WAWF_RA_sec/Test/Vers
Operating System:	Solaris 11
Status:	Production

4.4 DLA Energy Table Administrator

The DLA Energy Table Administrator will have access to edit or delete data on the DLA Energy tables. This administrator also has the ability to view the history of changes to the DLA Energy tables.

Tables:

- Table Administration
- Energy Tests - Master List
- Energy Commodities
- Energy Sub Commodities
- Energy Tests - Add/Edit/Delete
- Order Energy Tests
- Energy Test Categories
- Group Energy Tests
- Energy Test Types
- Reference Taxes

History:

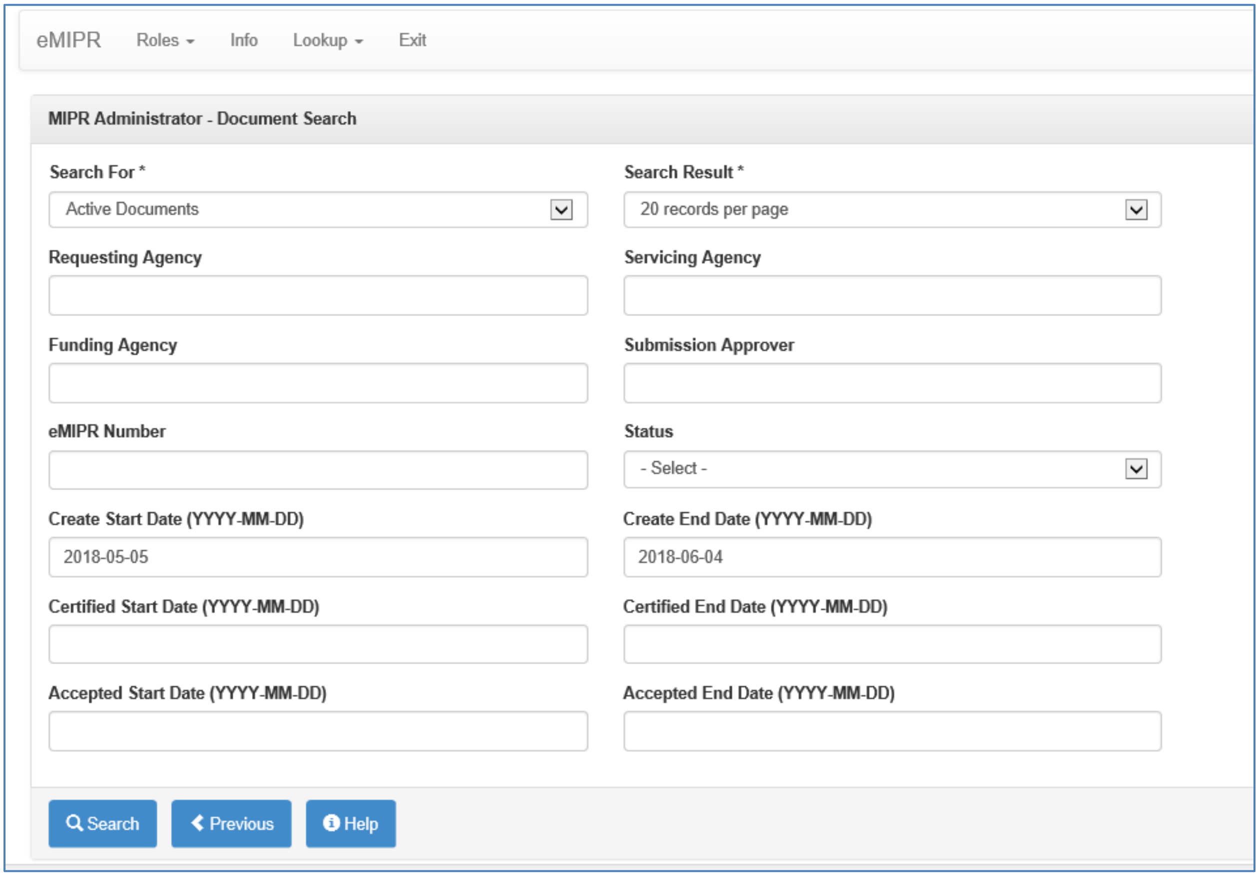
- History Table Administration
- Energy Test Master
- Energy Results Dropdown Master

- Energy Test Categories
- Energy Results Dropdown
- Energy Test
- Energy Test Codes
- Energy Test Types

5. MIPR Administrator Roles

5.1 MIPR Administrator

The eMIPR Administrator will have access to view Purchase Request documents. The screenshot below are the available search criteria available.



Search For * Active Documents

Search Result * 20 records per page

Requesting Agency

Servicing Agency

Funding Agency

Submission Approver

eMIPR Number

Status - Select -

Create Start Date (YYYY-MM-DD) 2018-05-05

Create End Date (YYYY-MM-DD) 2018-06-04

Certified Start Date (YYYY-MM-DD)

Certified End Date (YYYY-MM-DD)

Accepted Start Date (YYYY-MM-DD)

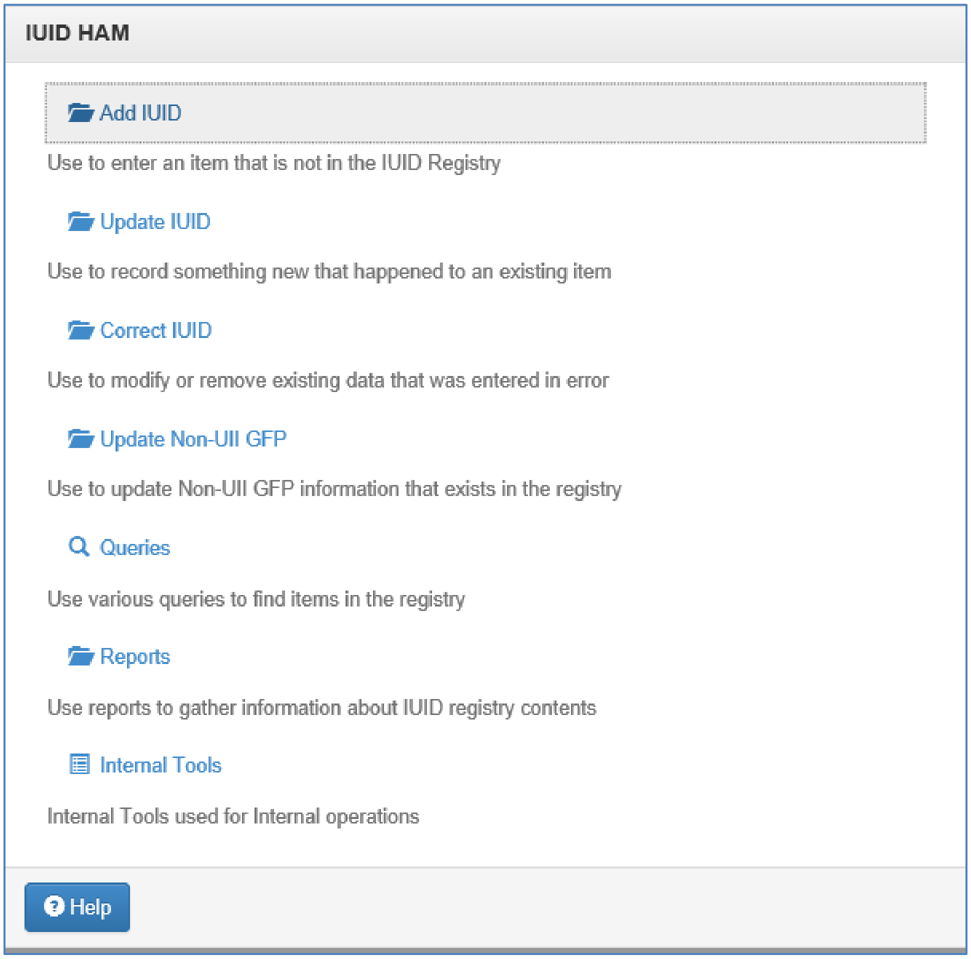
Accepted End Date (YYYY-MM-DD)

6. IUID Administrator Roles

6.1 IUID Help Administrator

Many of the administrative role privileges for the IUID module have been elevated to the PIEE level administrators. The remaining Help Administrator has access to the following duties for the module:

- Add new IUID records
- Update all existing IUID records
- Correct all existing IUID records
- Query all IUID records
- Run all Reports for IUID records.



IUID HAM

Add IUID

Use to enter an item that is not in the IUID Registry

Update IUID

Use to record something new that happened to an existing item

Correct IUID

Use to modify or remove existing data that was entered in error

Update Non-UII GFP

Use to update Non-UII GFP information that exists in the registry

Queries

Use various queries to find items in the registry

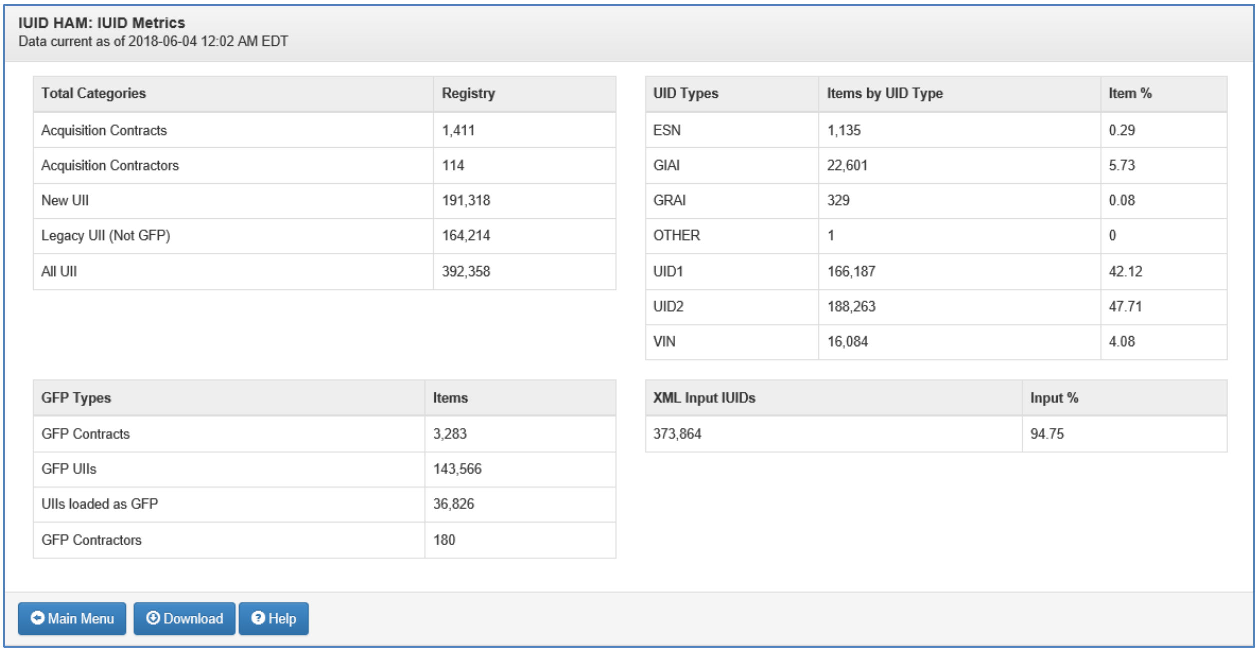
Reports

Use reports to gather information about IUID registry contents

Internal Tools

Internal Tools used for Internal operations

Additionally, the administrator has access to a metrics view and the IUID documentation.



IUID HAM: IUID Metrics
Data current as of 2018-06-04 12:02 AM EDT

Total Categories	Registry
Acquisition Contracts	1,411
Acquisition Contractors	114
New UII	191,318
Legacy UII (Not GFP)	164,214
All UII	392,358

UID Types	Items by UID Type	Item %
ESN	1,135	0.29
GIAI	22,601	5.73
GRAI	329	0.08
OTHER	1	0
UID1	166,187	42.12
UID2	188,263	47.71
VIN	16,084	4.08

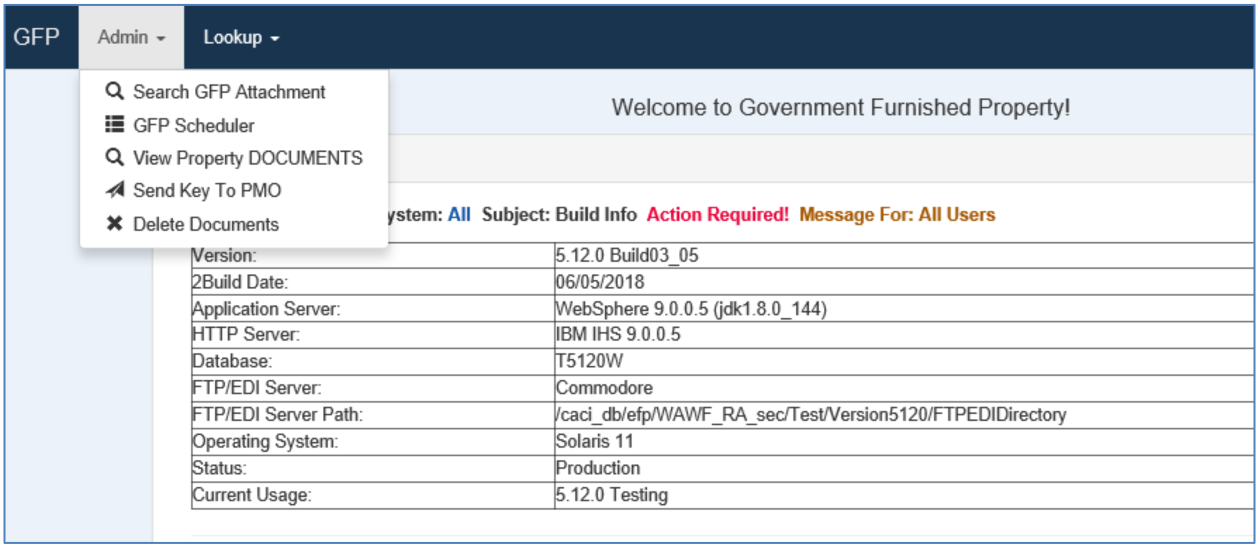
GFP Types	Items
GFP Contracts	3,283
GFP UIIs	143,566
UIIs loaded as GFP	36,826
GFP Contractors	180

XML Input IUIDs	Input %
373,864	94.75

7. GFP Administrator Role

The GFP System Administrator has the following administrative functionalities available.

- Search GFP Attachment
- GFP Scheduler
- View Property Documents
- Send Key to PMO
- Delete Documents



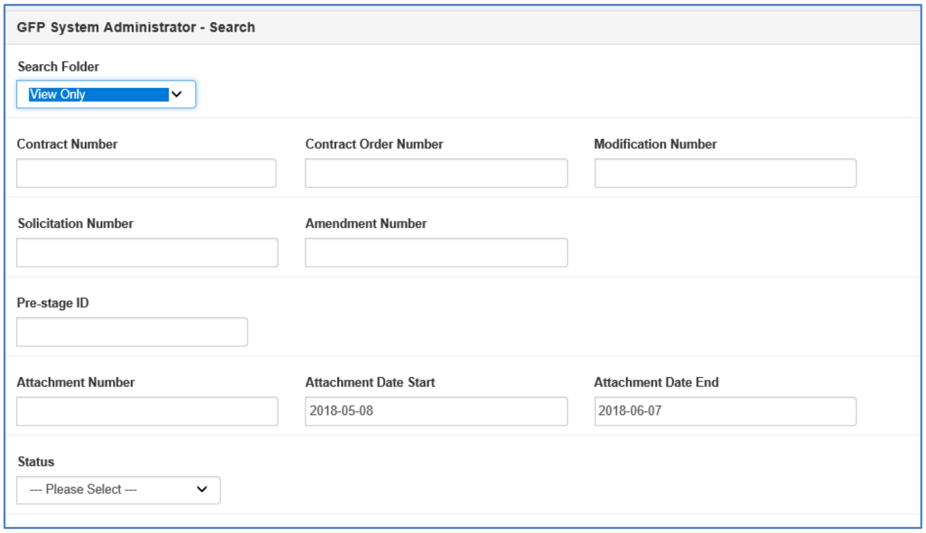
Welcome to Government Furnished Property!

ystem: All Subject: Build Info Action Required! Message For: All Users

Version:	5.12.0 Build03_05
2Build Date:	06/05/2018
Application Server:	WebSphere 9.0.0.5 (jdk1.8.0_144)
HTTP Server:	IBM IHS 9.0.0.5
Database:	T5120W
FTP/EDI Server:	Commodore
FTP/EDI Server Path:	/caci_db/efp/WAWF_RA_sec/Test/Version5120/FTPEDIDirectory
Operating System:	Solaris 11
Status:	Production
Current Usage:	5.12.0 Testing

7.1 GFP System Administrator

The GFP System Administrator has access to search and view the GFP Attachments.



GFP System Administrator - Search

Search Folder: View Only

Contract Number:

Contract Order Number:

Modification Number:

Solicitation Number:

Amendment Number:

Pre-stage ID:

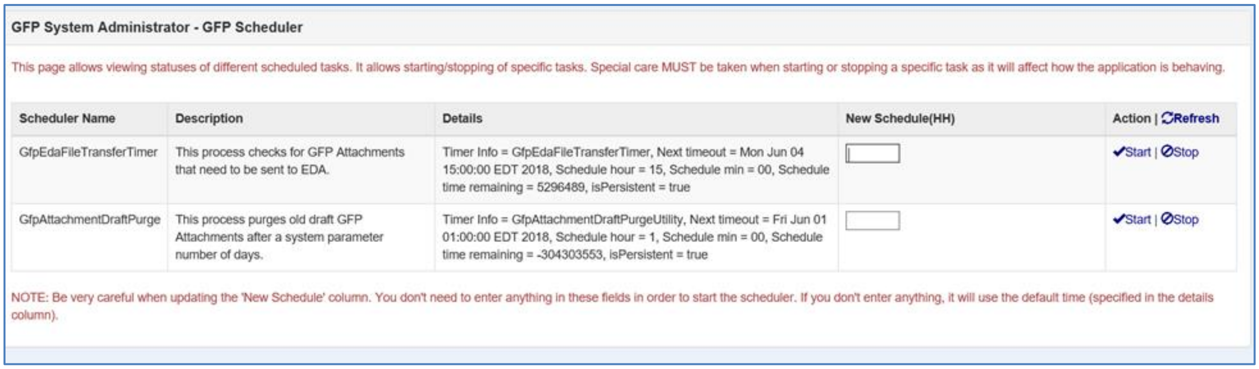
Attachment Number:

Attachment Date Start: 2018-05-08

Attachment Date End: 2018-06-07

Status: --- Please Select ---

This administrator can also view statuses of different scheduled tasks. It allows starting/stopping of specific tasks. Special care MUST be taken when starting or stopping a specific task as it will affect how the application is behaving.



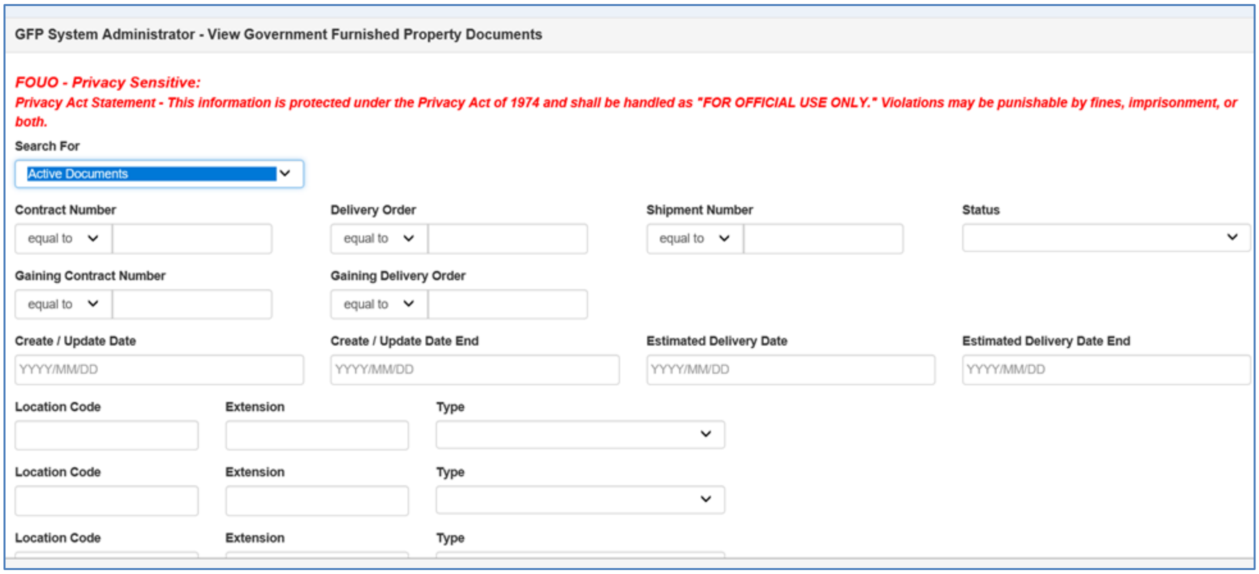
GFP System Administrator - GFP Scheduler

This page allows viewing statuses of different scheduled tasks. It allows starting/stopping of specific tasks. Special care MUST be taken when starting or stopping a specific task as it will affect how the application is behaving.

Scheduler Name	Description	Details	New Schedule(HH)	Action | Refresh
GfpEdaFileTransferTimer	This process checks for GFP Attachments that need to be sent to EDA.	Timer Info = GfpEdaFileTransferTimer, Next timeout = Mon Jun 04 15:00:00 EDT 2018, Schedule hour = 15, Schedule min = 00, Schedule time remaining = 5296489, isPersistent = true		✓Start | ⊘Stop
GfpAttachmentDraftPurge	This process purges old draft GFP Attachments after a system parameter number of days.	Timer Info = GfpAttachmentDraftPurgeUtility, Next timeout = Fri Jun 01 01:00:00 EDT 2018, Schedule hour = 1, Schedule min = 00, Schedule time remaining = -304303553, isPersistent = true		✓Start | ⊘Stop

NOTE: Be very careful when updating the 'New Schedule' column. You don't need to enter anything in these fields in order to start the scheduler. If you don't enter anything, it will use the default time (specified in the details column).

The GFP System Administrator has access to search and view the GFP Documents.



GFP System Administrator - View Government Furnished Property Documents

FOUO - Privacy Sensitive:
Privacy Act Statement - This information is protected under the Privacy Act of 1974 and shall be handled as "FOR OFFICIAL USE ONLY." Violations may be punishable by fines, imprisonment, or both.

Search For: Active Documents

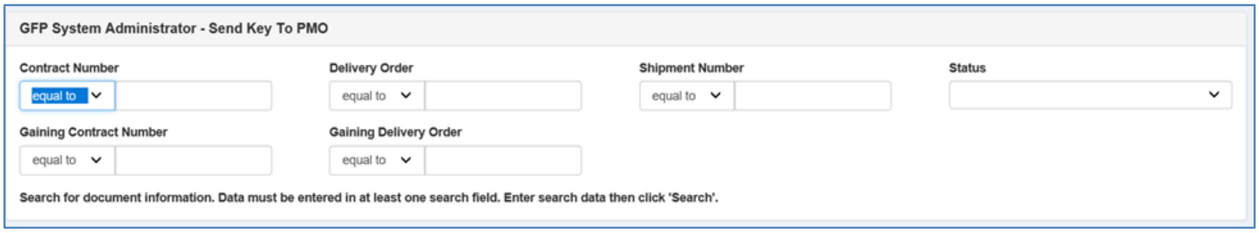
Contract Number: equal to
Delivery Order: equal to
Shipment Number: equal to
Status:

Gaining Contract Number: equal to
Gaining Delivery Order: equal to

Create / Update Date: YYYY/MM/DD
Create / Update Date End: YYYY/MM/DD
Estimated Delivery Date: YYYY/MM/DD
Estimated Delivery Date End: YYYY/MM/DD

Location Code | Extension | Type
Location Code | Extension | Type
Location Code | Extension | Type

The GFP System Administrator will have privileges to Send Key to PMO.



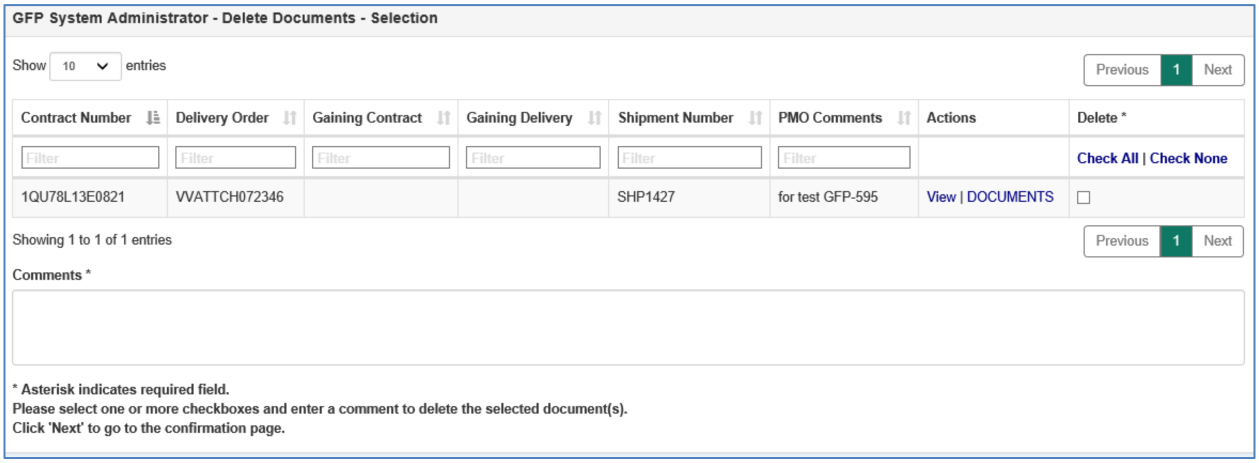
GFP System Administrator - Send Key To PMO

Contract Number: equal to
Delivery Order: equal to
Shipment Number: equal to
Status:

Gaining Contract Number: equal to
Gaining Delivery Order: equal to

Search for document information. Data must be entered in at least one search field. Enter search data then click 'Search'.

The GFP System Administrator will also have the rights to delete GFP Documents.



GFP System Administrator - Delete Documents - Selection

Contract Number	Delivery Order	Gaining Contract	Gaining Delivery	Shipment Number	PMO Comments	Actions	Delete *
Filter	Filter	Filter	Filter	Filter	Filter		Check All | Check None
1QU78L13E0821	VVATTCH072346			SHP1427	for test GFP-595	View | DOCUMENTS	□

Showing 1 to 1 of 1 entries

Comments *

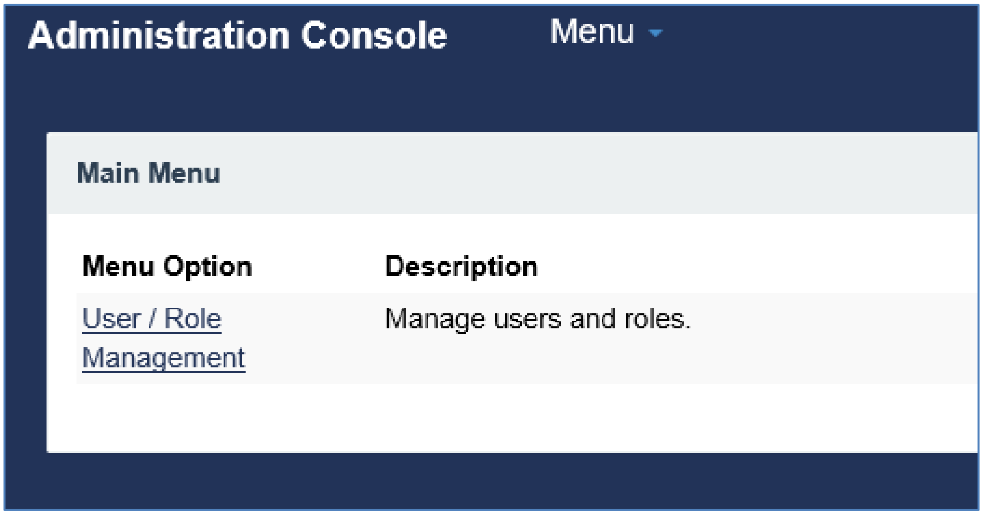
* Asterisk indicates required field.
Please select one or more checkboxes and enter a comment to delete the selected document(s).
Click 'Next' to go to the confirmation page.

8. CLS Administrator Roles

The other administrative roles within the CLS module has automatic access to EDA Contracts role. They can access the CLS application but has no access to the PIEE Administration Console.

8.1 Program Management Office (PMO)

The Program Management Office Administrator for the CLS module has access to the PIEE Administration Console to manage the users of the CLS Module only.



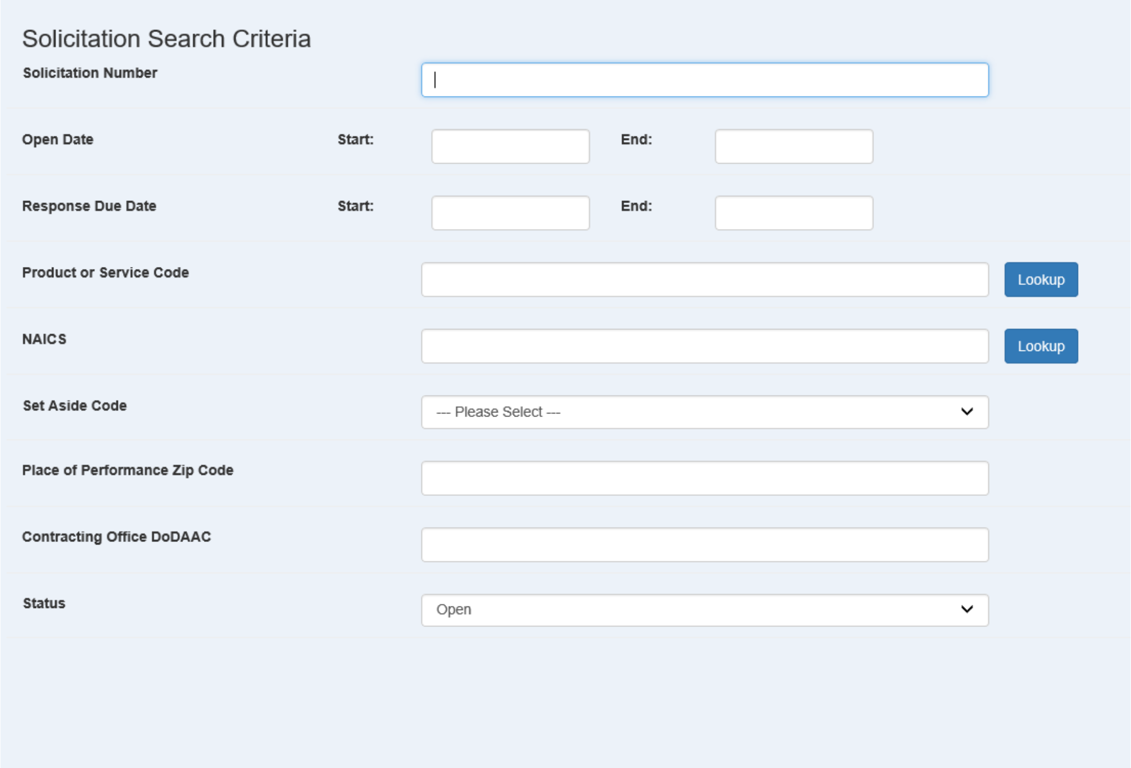
Main Menu

Menu Option	Description
User / Role Management	Manage users and roles.

9. Solicitation Administrator Roles

9.1 Solicitation Administrator

The Solicitation Administrator has access to search and view the solicitations. There is also the capability to search for the available Product/Service Codes and NAICS.



Solicitation Search Criteria

Solicitation Number

Open Date Start: End:

Response Due Date Start: End:

Product or Service Code

NAICS

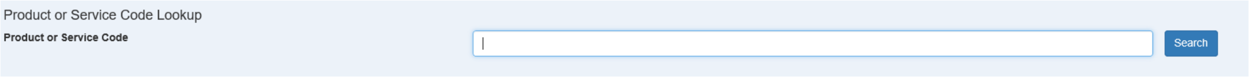
Set Aside Code: --- Please Select ---

Place of Performance Zip Code

Contracting Office DoDAAC

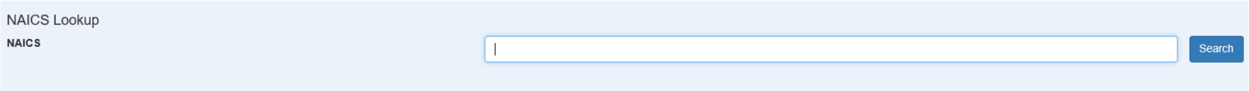
Status: Open

Lookup Functionality



Product or Service Code Lookup

Product or Service Code



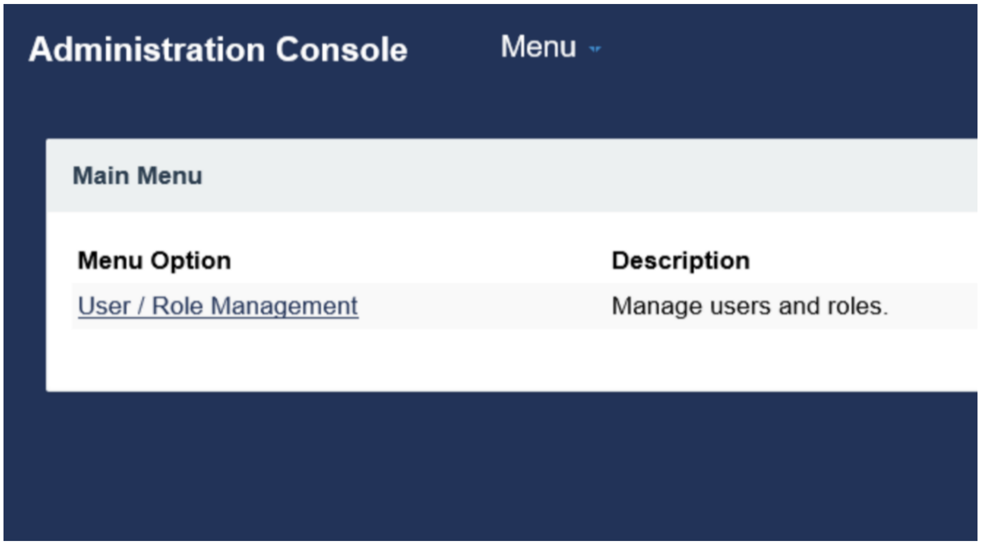
NAICS Lookup

NAICS

10. PPML Administrator Roles

10.1 PPML PMO

The Program Management Office Administrator for the PPML application has access to the PIEE Administration Console to manage the users of the PPML module only.



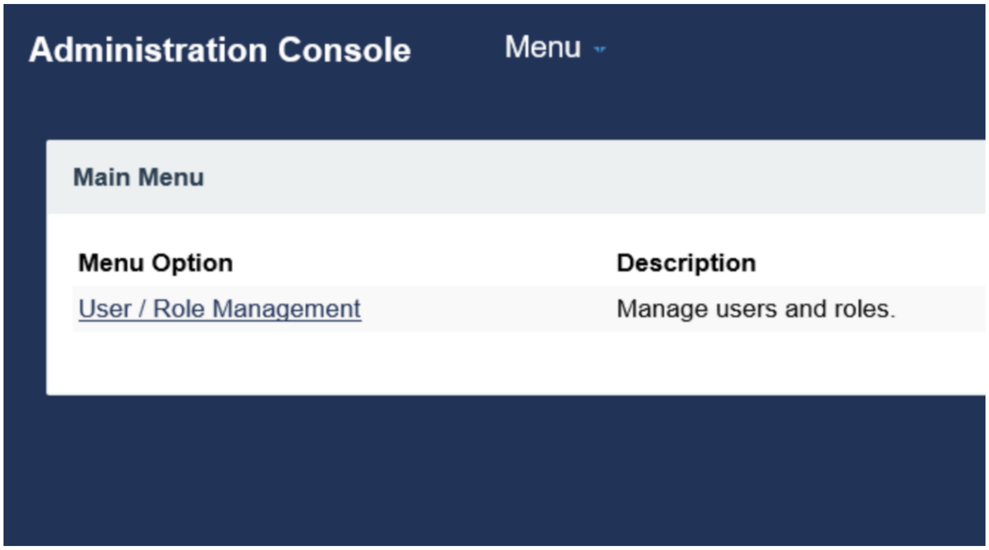
Main Menu

Menu Option	Description
User / Role Management	Manage users and roles.

11. PC Administrator Roles

11.1 GPC DoD PMO

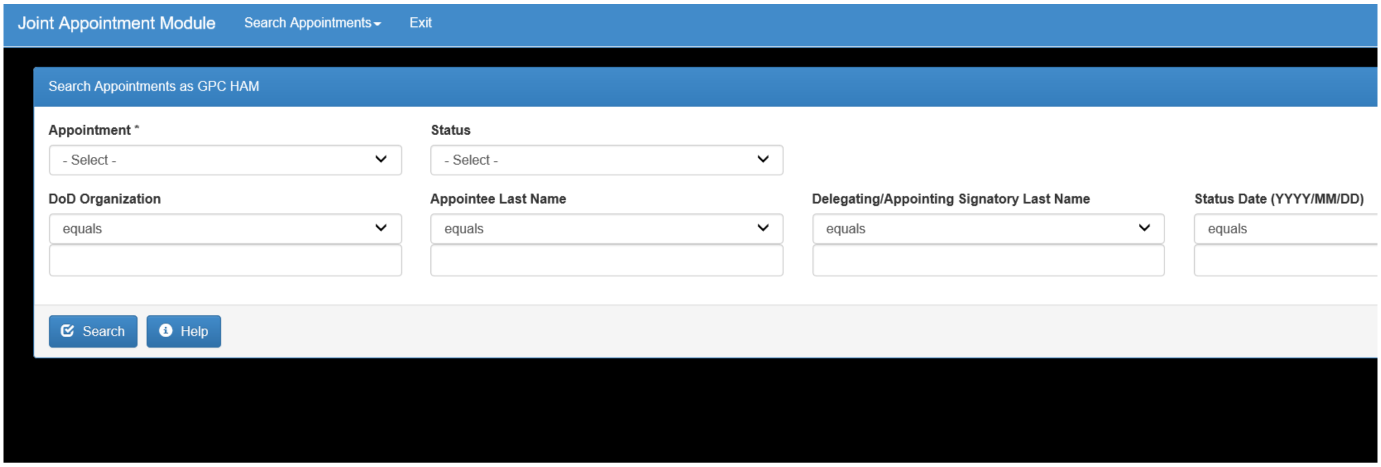
The GPC DoD Program Management Officer for the PC application has access to the PIEE Administration Console to manage the users of the PC module only.



Menu Option	Description
User / Role Management	Manage users and roles.

11.2 GPC HAM

The GPC HAM user for the PC application has the capability to search appointments in JAM.



Appointment * - Select -

Status - Select -

DoD Organization equals

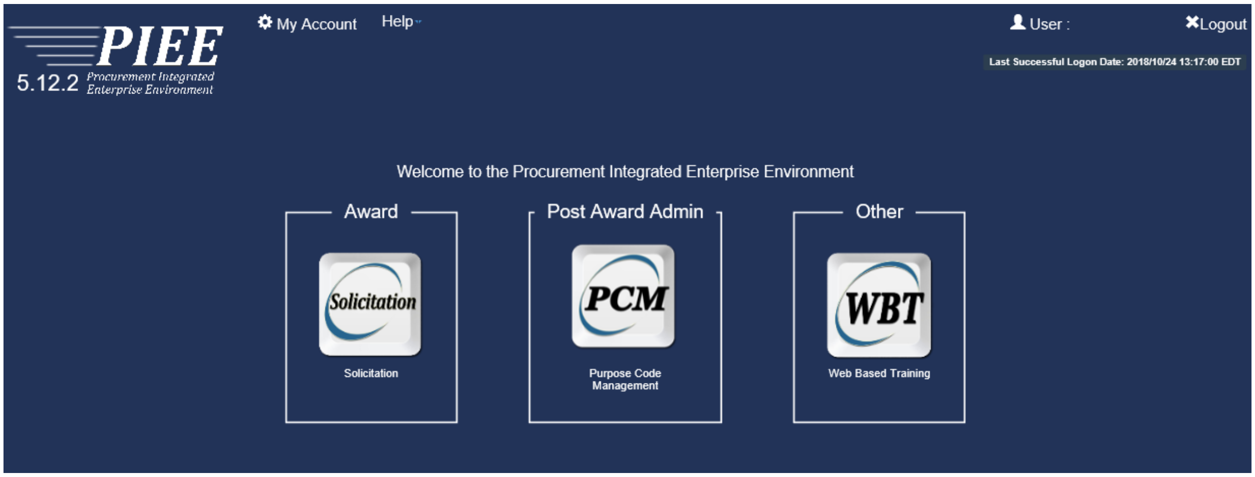
Appointee Last Name equals

Delegating/Appointing Signatory Last Name equals

Status Date (YYYY/MM/DD) equals

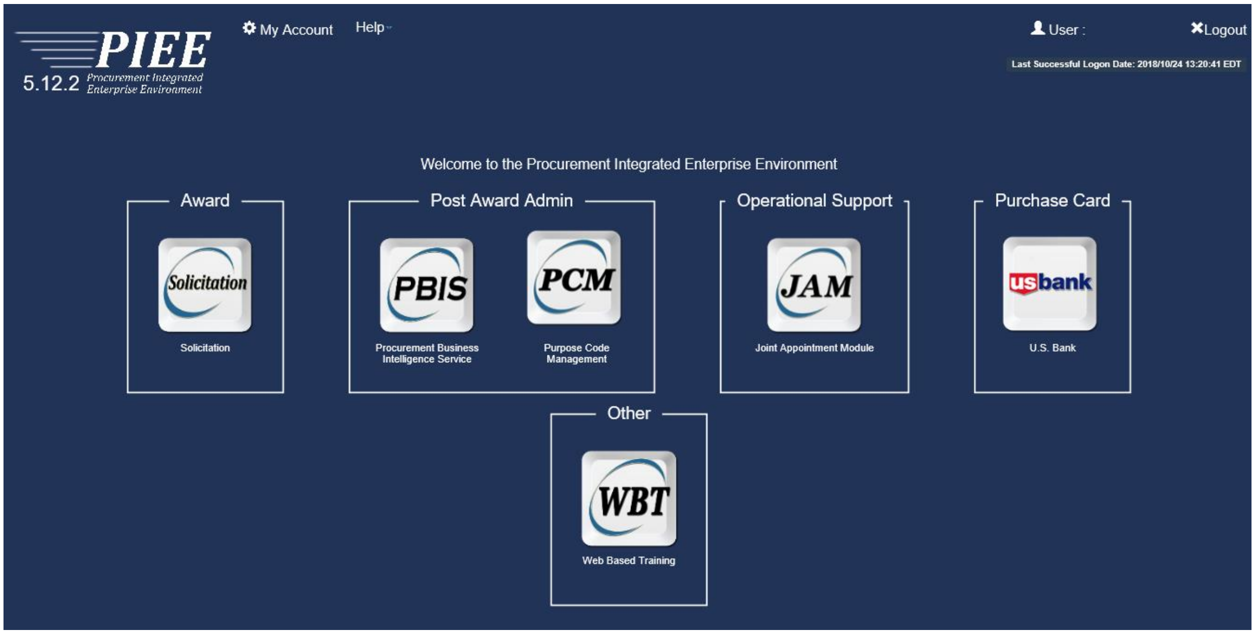
11.3 GPC Auditor

The GPC Auditor user for the PC application has access to the Solicitation and PCM modules.


PIEE
5.12.2 Procurement Integrated Enterprise Environment
My Account
Help
User :
Logout
Last Successful Logon Date: 2018/10/24 13:17:00 EDT
Welcome to the Procurement Integrated Enterprise Environment
Award
Solicitation
Post Award Admin
Purpose Code Management
Other
Web Based Training

11.4 GPC Support View Only

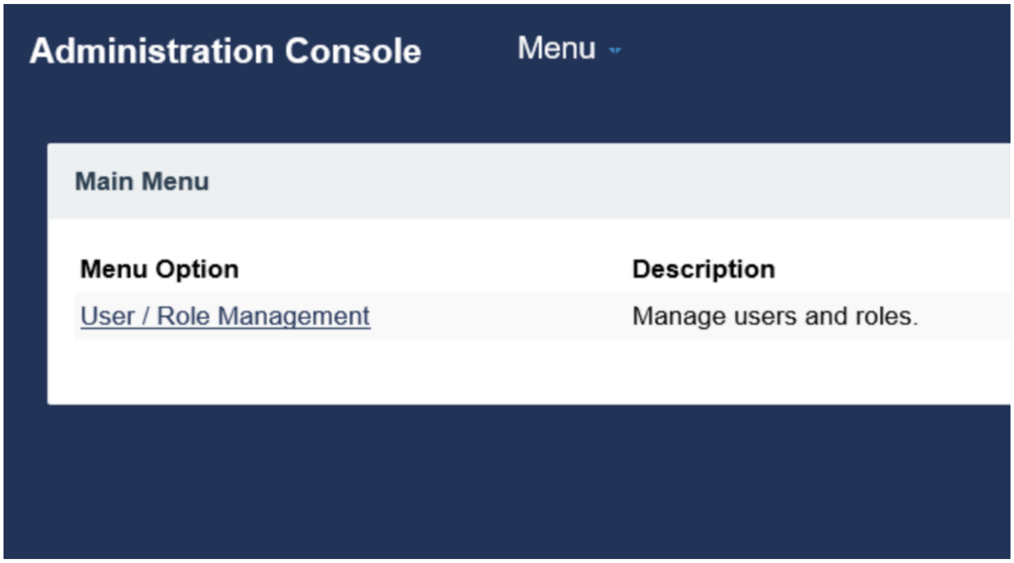
The GPC Support View Only user for the PC application has access to the following modules: Solicitation, PBIS, PCM, JAM, and U.S. Bank.


PIEE
5.12.2 Procurement Integrated Enterprise Environment
My Account
Help
User :
Logout
Last Successful Logon Date: 2018/10/24 13:20:41 EDT
Welcome to the Procurement Integrated Enterprise Environment
Award
Solicitation
Post Award Admin
Procurement Business Intelligence Service
Purpose Code Management
Operational Support
Joint Appointment Module
Purchase Card
U.S. Bank
Other
Web Based Training

12. SPRS Administrator Roles

12.1 SPRS HAM

The SPRS HAM user for the SPRS application has access to the PIEE Administration Console to manage the users of the SPRS module only.



Menu Option	Description
User / Role Management	Manage users and roles.

13. Contract Deficiency Report Administrator Roles

Please refer to the PIEE Admin section for more detailed descriptions of the functions listed below.

13.1 Administration

- Account Information/Activation
- Government Support Contractor Request
- Reset Password
- Reset Certificate
- EDA POC Assignments
- Account Activation History

13.2 C/S/A Administration

13.3 Location Administration

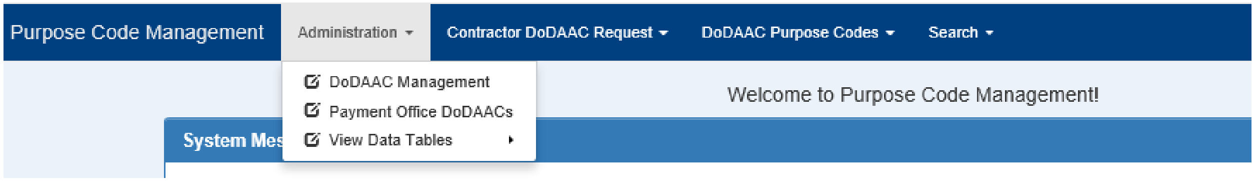
14. Purpose Code Management (PCM)

The Purpose Code Management (PCM) Module will provide three main functionalities:

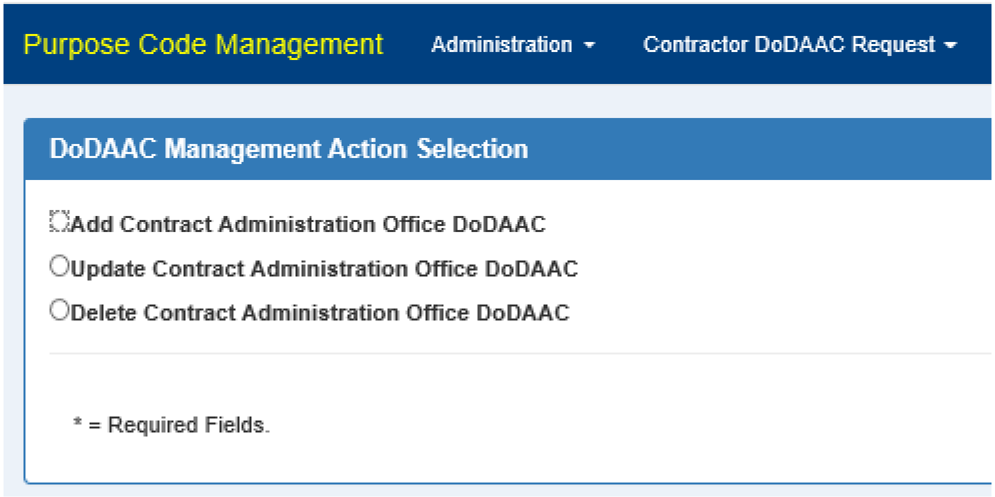
- Contract Administration Office(CAO) DoDAAC and Pay Office(PO) DoDAAC Tool
  - DCMA Contract Administration Office Manager – manage the relationships between the CAO and PO DoDAACs with zip codes and CAGE codes.
  - Users – will have the ability to select zip codes or CAGE codes and retrieve the corresponding CAO and PO DoDAACS
- Contract Administration DoDAAC Requests – Registered and non-Registered PIEE users
- Purpose Code Flag Administration

14.1 DCMA Contract Admin Office (CAO) Manager

The DCMA CAO Manager is the administrator of the Contract Admin Office and Pay Office DoDAACs. A user with this role will manage the relationship of the CAO and Pay Office DoDAACs with zip codes and countries. They will also manage any CAGE codes with exceptions to the standard assignments by zip code or country.



Welcome to Purpose Code Management!



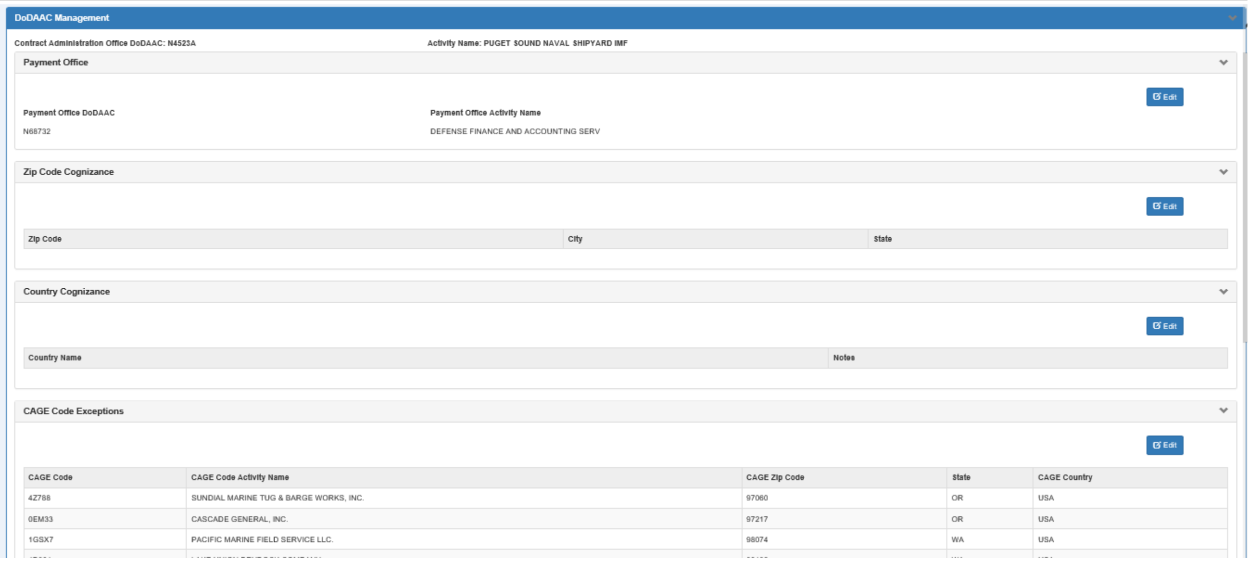
DoDAAC Management Action Selection

○Add Contract Administration Office DoDAAC

○Update Contract Administration Office DoDAAC

○Delete Contract Administration Office DoDAAC

* = Required Fields.



DoDAAC Management

Contract Administration Office DoDAAC: N4523A

Activity Name: PUGET SOUND NAVAL SHIPYARD IMF

Payment Office

Payment Office DoDAAC	Payment Office Activity Name
N68732	DEFENSE FINANCE AND ACCOUNTING SERV

Zip Code Cognizance

Zip Code	City	State

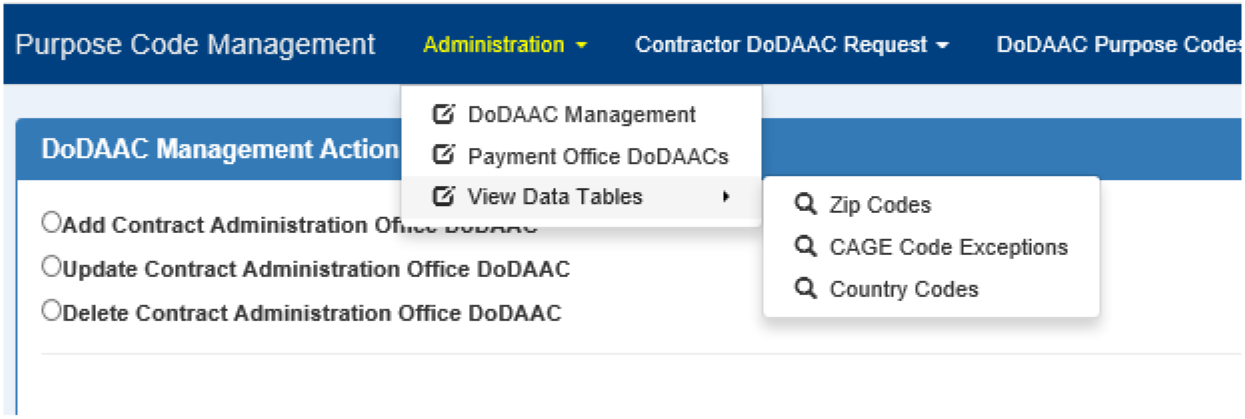
Country Cognizance

Country Name	Notes

CAGE Code Exceptions

CAGE Code	CAGE Code Activity Name	CAGE Zip Code	State	CAGE Country
4Z788	SUNDIAL MARINE TUG & BARGE WORKS, INC.	97060	OR	USA
0EM33	CASCADE GENERAL, INC.	97217	OR	USA
1GSX7	PACIFIC MARINE FIELD SERVICE LLC.	98074	WA	USA

Additionally, the DCMA CAO Manager also has access to a list of data tables. These data tables are a convenient way for this administrator to view key data elements on one spreadsheet. These spreadsheets can be downloaded for further analysis by the DCMA CAO Manager.



DoDAAC Management Action

○Add Contract Administration Office DoDAAC

○Update Contract Administration Office DoDAAC

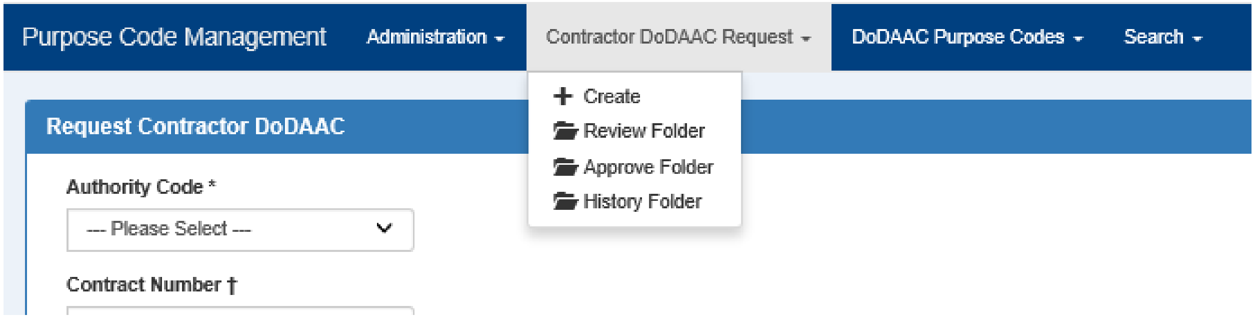
○Delete Contract Administration Office DoDAAC

14.2 Contractor DoDAAC Manager

The Contractor DoDAAC Manager role serves as the approver for the Contractor DoDAAC Requests.

- The current PIEE Users that belong in the Job Series 1102 (includes ACO, Contract Specialist ACO, PCO, and Contract Specialist PCO) will automatically be granted this role.
- Job Series 1102 Users with this role may submit a Contractor DoDAAC request and can self-approve the request, they will also have the ability to approve other requests within their DoDAAC.

Non-1102 Series PIEE users may register for this role, however they will not have the ability to approve their own requests. They can only approve the requests within their DoDAAC.

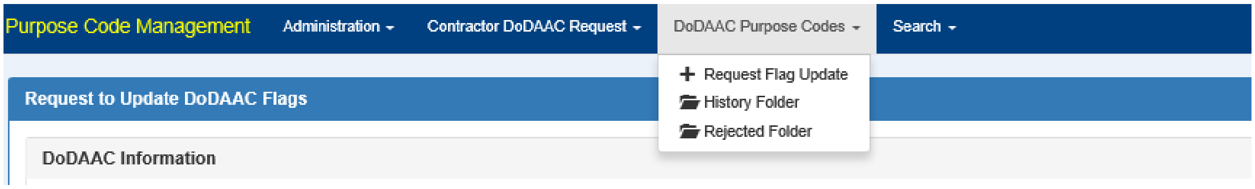


14.3 Purpose Code Flag Administrator

The following roles have been added for the Purpose Code Management application:

- Payment Office Purpose Code Manager
- Procurement & Grant Purpose Code Manager
- Contract Admin Purpose Code Manager
- Contractor Admin Purpose Code Manager

As PIEE users submit requests for purpose code flag updates these managers will have the ability to approve or reject the requests.


Purpose Code Management
Administration
Contractor DoDAAC Request
DoDAAC Purpose Codes
Search
Request Flag Update
History Folder
Rejected Folder
Request to Update DoDAAC Flags
DoDAAC Information