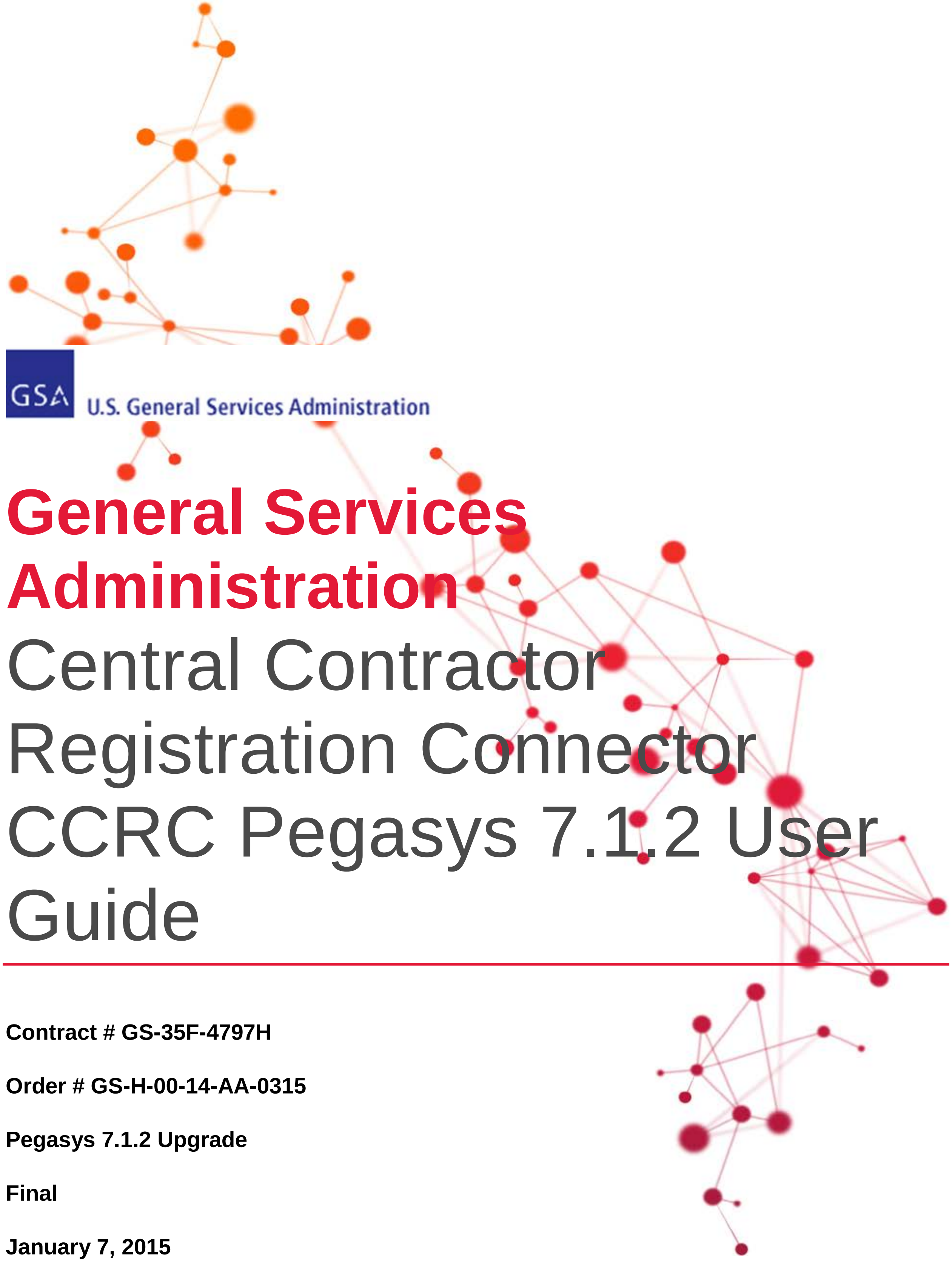
CGI

Experience the commitment®



GSA U.S. General Services Administration

General Services Administration

Central Contractor Registration Connector CCRC Pegasys 7.1.2 User Guide

Contract # GS-35F-4797H

Order # GS-H-00-14-AA-0315

Pegasys 7.1.2 Upgrade

Final

January 7, 2015

Contents

1 CCRC Introduction 1-9

2 CCRC Overview 2-10

2.1 Central Contractor Registration Connector (CCRC) 2-10

2.2 Initial Load and Initial Vendor Selection 2-10

2.3 CCRC User Interface 2-10

2.4 CCRC Import Batch Job 2-11

2.4.1 New Vendors 2-11

2.4.2 Updated Vendor 2-11

2.4.3 Inactivated/Deleted Vendors 2-11

2.5 CCRC Publishing Agent 2-12

2.6 Subscribing Agent/Agency Applications 2-12

2.7 Security 2-12

3 Loading Data from SAM 3-13

3.1 Initial SAM Data Load 3-13

3.1.1 Exporting SAM File 3-13

3.1.2 Initial SAM Data Load 3-13

3.1.2.1 Upload Parameters 3-14

3.1.3 Processing the SAM File 3-15

3.1.4 Processing Options 3-15

3.1.5 Removing the SAM File from CCRC 3-16

3.2 Initial Vendor Selection 3-16

3.2.1 Select Vendors to Enable 3-16

3.2.1.1 CCRC Data Maintenance Partners 3-17

3.2.2 Execute Initial File Creation Batch Process 3-19

3.2.3 Initial Vendor Selection Script and Synchronization 3-20

3.3 Daily Update Files 3-20

3.3.1 Daily CCRC Data Load 3-20

3.3.1.1 Parameters 3-21

3.3.2 New Vendor 3-21

3.3.3 Existing Vendor 3-21

3.3.4 Deletion and Deactivation 3-22

3.4 Supplemental Monthly Loads 3-22

3.4.1.1 Parameters 3-22

4 Searching/Publishing Vendors 4-24

4.1 Searching for Vendors 4-24

4.1.1 Vendor Information Query 4-24

4.1.2 Search Parameters 4-24

4.1.3 Search for Another Vendor 4-25

4.1.4 Case Insensitive Queries 4-26

4.2 Publishing Vendors 4-27

4.2.1 Publishing New Vendor Information 4-27

4.2.1.1 New Vendor Submissions 4-28

4.2.2 Publishing Updates 4-28

4.3 Integration 4-29

4.3.1 Audit 4-29

4.3.2 Cross References 4-30

5 System Administrator 5-31

5.1 CCRC Sign In 5-31

5.2 Data Loads 5-31

5.2.1 CCRC Holiday 5-31

5.3 Batch Execution 5-32

5.3.1 Batch Job Status 5-32

5.3.1.1 Batch Job Status Parameters 5-33

5.4 Security Policies 5-33

5.4.1.1 Adding, Deleting and Editing Policies 5-33

5.4.2 Passwords 5-35

5.4.2.1 Invalid Passwords 5-35

5.4.3 Reset a Locked User Account 5-36

5.4.4 System Locking 5-36

5.4.5 Access Control List 5-36

5.4.5.1 ACL Descriptions 5-37

5.4.5.2 ACL Permissions 5-38

5.4.6 Secure Data 5-38

5.4.7 Dynamic Extensibility 5-40

5.5 Users and Groups 5-40

5.5.1 Users 5-40

5.5.1.1 Creating a New User 5-40

5.5.1.2 Deactivating a User 5-41

5.5.1.3 Reactivating a User 5-41

5.5.2 Groups 5-42

5.6 Security Log 5-43

5.7 Vendor Data 5-43

5.7.1 Audit 5-43

5.7.2 Cross References 5-44

5.8 CCRC Preferences 5-45

5.8.1 Themes 5-45

5.8.2 Help 5-45

5.9 Vendor Management/CCRC: SAM Entity Management Enhancements in 7.1.2 Upgrade 5-46

5.9.1 Capture Additional Data 5-46

5.9.2 Data Import Capabilities 5-47

5.9.3 Display and Search by DODAAC 5-47

List of Exhibits

Figure 2-1: CCRC Cycle 2-10

Figure 3-1: Document Management Window 3-14

Figure 3-2: File Processing 3-15

Figure 3-3: CCRC Data Maintenance Table 3-17

Figure 3-4: Available List of Vendors 3-19

Figure 3-5: SAM Extract Codes 3-21

Figure 4-1: CCRC Data Maintenance Table 4-24

Figure 4-2: Case Insensitive Query in CCRC 4-26

Figure 4-3: CCRC Vendor Detail 4-27

Figure 4-4: Webmethods Error Screen 4-29

Figure 4-5: Auditing 4-29

Figure 4-6: Cross-Reference Window 4-30

Figure 5-1: CCRC Sign In Page 5-31

Figure 5-2: CCRC Holiday Window 5-32

Figure 5-3: Batch Job Status Window 5-32

Figure 5-4: Security Maintenance Policy Window 5-33

Figure 5-5: Adding a Security Policy 5-34

Figure 5-6: Security Maintenance Information 5-34

Figure 5-7: Delete Policy 5-35

Figure 5-8: Invalid Password Window 5-36

Figure 5-9: System Lock Window 5-36

Figure 5-10: ACL Window 5-37

Figure 5-11: Valid Permissions Window 5-37

Figure 5-12: ACL Entries 5-38

Figure 5-13: Social Security Masked from User 5-39

Figure 5-14: Tax Payer ID Masked from User 5-39

Figure 5-15: Edit User Details Window 5-40

Figure 5-16: New User Fields 5-41

Figure 5-17: Group Window 5-42

Figure 5-18: Group Members Window 5-43

Figure 5-19: Security Log 5-43

Figure 5-20: Audit Window 5-44

Figure 5-21: Cross-Reference Window 5-44

Figure 5-22: Preferences 5-45

Figure 5-23: Themes 5-45

Figure 5-24: Help 5-45

Figure 5-25: Vendor Record Contains Disaster Response Information 5-46

Figure 5-26: Fourth Address Line Added to the “Standard” Address Format 5-47

Figure 5-27: VCSS Ability to Register Vendors by DODAAC 5-48

Figure 5-28: Ability to Display and Search by DODAAC 5-49

Revision Log

Date	Version No.	Description	Author	Reviewer	Review Date
2/11/2011	Draft/Version .1	Original Draft	Danielle Becker	Tegan Dinardo, Mike Wong	1/26/2011
11/2014	Draft- version 2	Draft- 7.1.2 enhancements	Karin Keswani and Matthew Randall	Karin Keswani and Matthew Randall	11/2014
1/2015	Final	Figures were updated to reflect correct sequential order; figure numbers have been corrected in paragraphs to reference correct figures. Updated BPN to SAM in applicable areas. In section 5.4.6, Figure 5-13 and Figure 5-14 screenshots have been updated.	Karin Keswani and Benjamin Bowden	Karin Keswani and Benjamin Bowden	1/2015

1 CCRC Introduction

The Central Contractor Registration Connector (CCRC) application allows for the transfer, as well as daily updates, of vendor data from the System for Award Management (SAM) database into agency applications (i.e., the agency's financial, procurement, and/or travel applications). The SAM database is the government-wide central repository of vendors. The FAR mandates that all vendors who contract with these agencies must register with SAM and maintain updated information.

The government-wide SAM database collects, validates, stores and disseminates data in support of agency missions. Vendors complete a one-time registration to provide basic information relevant to all procurement, payment and billing transactions, and must update or renew their registration annually to maintain an active registration. SAM validates the vendor's information and electronically shares the secure data with the federal agencies' authorized offices to facilitate payments.

The CCRC application allows for a bulk load of the initial vendor data, as well as any periodic vendor additions, removal/deletions or updates from the SAM database into the customer's environment. CCRC also provides a web-based interface that enables users to select vendors and automatically transfers all relevant data elements to update Pegasys vendor data.

This manual is divided into the following sections:

- Overview
- Loading Data from SAM
- Searching/Publishing Vendors
- System Administration

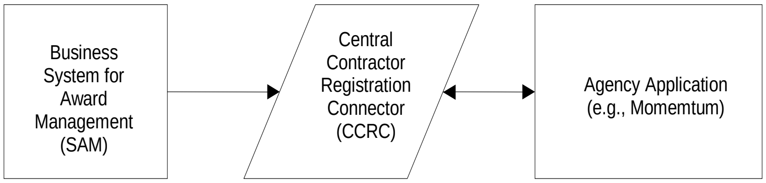
2 CCRC Overview

2.1 Central Contractor Registration Connector (CCRC)

The CCRC is a web-based application that provides the ability to store and manage SAM records before they are uploaded into Pegasys. The CCRC is populated with SAM data, which is then transferred to Pegasys and requires periodic updates to the database with changes released by SAM on an incremental basis. There are two types of updates available from CCRC.

- Daily Load File
- Monthly Load File
- The monthly load file is used for the initial load. Once the initial load has been processed, it is strongly suggested that the daily load file be used for updates to the CCRC system. This reduces the time required by the load process and ensures that vendor data remains current. The intervals between loading these updates into the CCRC are at the discretion of the agency utilizing the integration tools, based on their business practices and needs

Figure 2-1: CCRC Cycle


Business System for Award Management (SAM)
Central Contractor Registration Connector (CCRC)
Agency Application (e.g., Momemtum)

2.2 Initial Load and Initial Vendor Selection

Vendors have created 200,000+ records within the government-wide SAM database; however, not all agencies currently conduct, or are expected to conduct, business with each vendor stored in SAM. CCRC allows for one initial load, which pulls all the information collected by SAM and imports that data into the CCRC. The agency is then able to use the CCRC for the Initial Vendor Selection to select the vendors with whom they intend to do business.

Note—SAM defines vendors by their DUNS/DUNS + 4 number. The DUNS +4 is the 9-digit number assigned by Dun and Bradstreet, Inc. to identify unique business entities plus a 4-character suffix that may be assigned by a business concern for identifying alternative Electronic Funds Transfer (EFT) data. (D&B has no affiliation with the 4-character suffix).

2.3 CCRC User Interface

The CCRC User Interface enables users to specify which vendors are to be transferred from the CCRC to agency applications. In addition, this interface contains information regarding when vendor records change in the database, specifically:

- to identify when new vendor data has been received

- when an active vendor changes
- when a vendor has been inactivated or deleted.

The CCRC notifies agencies of these changes by publishing (sending their information) to Pegasys.

2.4 CCRC Import Batch Job

A CCRC Import Batch Job is used to load vendor reference data received from SAM, into the CCRC. This data may include new vendors, updated vendors, and deactivated vendors.

2.4.1 New Vendors

New Vendors are added to the CCRC during the initial load, daily loads, and monthly loads. If a vendor is added after the initial load, that vendor may be added to the CCRC through either the daily or monthly updates.

2.4.2 Updated Vendor

When vendors make changes to their SAM registration information (including annual renewal) those changes must also be updated within the CCRC. These changes will be processed as updated vendors, as their record already exists within the CCRC and Pegasys.

Updated records from SAM contain all CCR-data fields, not just the updated fields, thus the entire record of CCR-mapped fields within CCRC will be overwritten. Non-CCR fields are not updated or changed. An example of a non-CCR field that would not be overwritten is the “Transmit to Agency Application” field, which is not populated by the interface, but is part of the CCRC.

The vendor information includes the vendor's debarment status. The vendor will have a Debarred flag if the vendor has been declared ineligible from receiving Federal contracts, as shown by records at the Excluded Parties Listing System (EPLS). The purpose of the Debarred Flag is to prevent a debarred vendor from being used on financial transactions. This status and the reason will transfer to Pegasys during the Daily and Monthly Uploads.

2.4.3 Inactivated/Deleted Vendors

Any vendor that has a status change from “active” to “inactive” has been marked “deleted” within the SAM database and must also be marked inactive within the CCRC application.

However, some agency applications may still require that vendor to be “active” as there may be open obligations, receipts, or invoices that still need to be considered active for accounting purposes (e.g., within Pegasys, the ‘Prevent New Spending’ flag may be employed rather than setting that particular vendor address record to inactive).

2.5 CCRC Publishing Agent

In the CCRC application the CCRC Publishing Agent (i.e., webMethods) transforms a file containing SAM records that has been selected for use from the CCRC User Interface for publication in Pegasys. The four record status values within the CCRC are listed below:

- **Unpublished** – A new vendor that has not yet been published to Pegasys.
- **Submitted** – The vendor has been submitted to Pegasys for acceptance or rejection via a vendor form.
- **Accepted** – The vendor has been accepted by Pegasys. Once the vendor has been accepted, updates to that vendor come in from SAM, synchronization is performed, and Pegasys automatically receives the update.
- **Rejected** – The vendor has been rejected by Pegasys Advanced Workflow (which GSA does not use). Updates for rejected vendors are not transmitted.

Note—Separate status values are maintained for Financials, Procurement, and Travel applications. That being the case, it is possible that a given vendor could have different status values for each group of applications (e.g. Vendor ABC has a Financials Status of 'Accepted' while having a Travel status of 'Unpublished'). Because GSA only uses Pegasys, the Procurement and Travel status values are not relevant.

The webMethods Enterprise Adapter is an intelligent adapter that connects the Interface to the webMethods Enterprise Server, so that events can be exchanged between the two products. When the adapter is started, it logs into Pegasys using the Security services. The Metadata services are used to configure operations. These operations correspond to the Factory, Finder, Operation, and Notification services provided by the Interface. See the *Pegasys Interface User's Guide* for details on these services.

2.6 Subscribing Agent/Agency Applications

The Subscribing Agents subscribe to SAM vendor information and update Pegasys.

2.7 Security

The CCRC allows the Administrator to create and edit user accounts, including the set up of user ids and passwords and the option to associate each user with one or more groups. The Administrator can also create customized security policies that accommodate agency needs such as number of password attempts as well as length of grace periods.

3 Loading Data from SAM

Vendors have created 200,000+ records within the government-wide SAM database, however; not all vendors currently conduct, or are expected to conduct, business with each vendor stored in SAM. CCRC allows for one initial load, which pulls all the information collected by SAM and imports that data into the CCRC. The agency is then able to select the vendors that they do business with by using the CCRC for the Initial Vendor Selection.

SAM defines vendors by their DUNS/DUNS + 4 number. The DUNS +4 is the 9-digit number assigned by Dun and Bradstreet, Inc. to identify unique business entities plus a 4-character suffix that may be assigned by a business concern for identifying alternative Electronic Funds Transfer (EFT) data. (D&B has no affiliation with the 4-character suffix).

3.1 Initial SAM Data Load

3.1.1 Exporting SAM File

Before importing the file into the CCRC, the SAM extract file needs to be transferred to the agency application and vendors need to be identified. The Administrator will be granted a user id and password to access the SAM system with permissions to extract files from the SAM to the agency application server through the Secure Socket Layer (SSL).

A link is provided in CCRC which takes the user directly to SAM's website to download the file. The data obtained from this link is secure and un-encrypted.

https://ftp.SAM.gov/web_extracts/ (MS Explorer 3.0 or higher is required)

There are three types of files available:

- **FOUO (For Official Use Only)**– This file contains information available to all applications.
- **Sensitive** – This file should be used with financial applications as it contains bank information, TIN, and Lockbox.
- **Proprietary** – This file should be used with procurement/contracting applications as it does not contain sensitive information.

Once it has been determined which file is needed, the file should then be copied and placed in the C: \CCRCDocuments\CCRInput drive, which is accessible by the CCRC.

Note— In order for the upload to the CCRC to be successful, the file must meet three specific criteria. First, the file must be named with the Julian date (Month + actual day of the year the file was created) in the name (SAM extract files are automatically named this way). Second, all alphabetical characters in the filename must be capitalized. Third, the file must be zipped.

3.1.2 Initial SAM Data Load

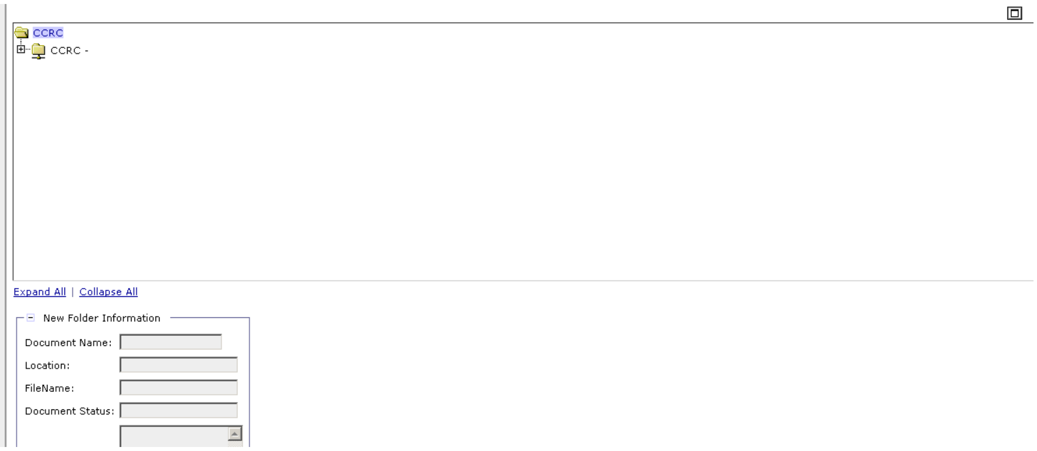
For the Initial SAM Data Load, the CCRC should be a blank database. The CCRC is initially loaded with a monthly extract file before daily update files can be applied.

The SAM File Upload can be accessed through the following path:

CCRC File Handler/Process CCR File/Document Management

Figure 3-1 Document Management Window Displays the Document Management Window.

Figure 3-1: Document Management Window



CCRC
CCRC -

Expand All | Collapse All

New Folder Information

Document Name:

Location:

FileName:

Document Status:

Steps to Upload a SAM Extract File:

1. Click the CCRC subfolder, which will activate the **Upload** button.
2. Click the **Upload** button
3. Browse for the desired SAM Extract file and click the **Upload** button

3.1.2.1 Upload Parameters

Field	Field Description
Description	The user has the ability to enter a description of the file for future reference.
Document	The filename/path of the extract file to be loaded. This parameter is required.

The Initial Load verifies the extract file layout by ensuring the SAM Extract Code of each record is set to 'A'.

The Initial Load sequentially reads each record from the initial monthly extract file and inserts into the appropriate CCRC table. Each insert includes the timestamp of when the record was loaded, the user id of the Administrator running the load and any additional information required.

Note — The CCRC system must be locked while uploading the file to the CCRC.

3.1.3 Processing the SAM File

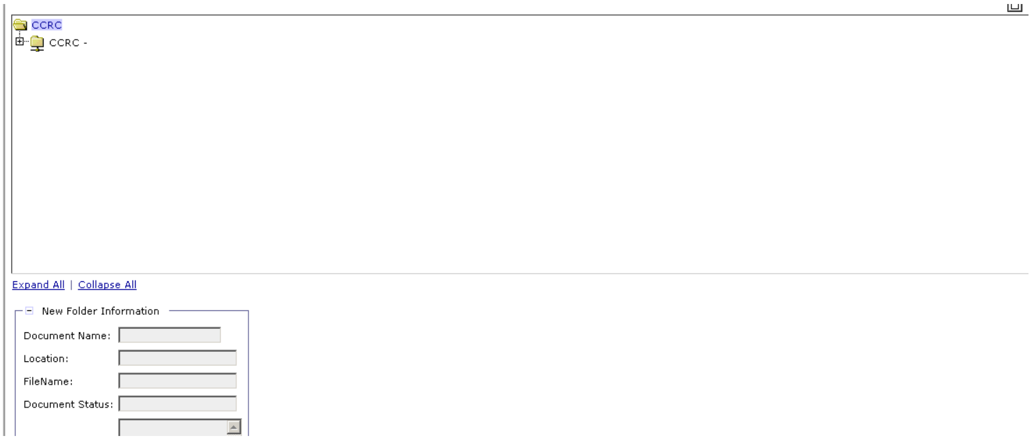
Although the Administrator has uploaded the SAM data file into the CCRC database, the file still needs to be processed in order for the data to be fully accepted into the CCRC.

The File Processing can be accessed through the following path:

CCRC File Handler/Process CCR File/Document Management

Figure 3-2 ***File Processing*** displays the Document Management window.

Figure 3-2: File Processing



Steps to Process a SAM Extract File:

1. Click the plus expansion button next to the CCRC subfolder
2. Select the file intended for processing
3. Click the **Process** button
4. Go to Batch Jobs/Batch Job Status to check the result of the processing or processed SAM Extract File

There are five possible status values in the File Processing window:

- **Failed**—The initial/daily/monthly upload has failed.
- **Loading**—The upload is in the process of loading the file to the CCRC.
- **Pending**—The upload file is pending.
- **Processing**—The upload file is processing.
- **Processed**—The upload file has been uploaded successfully and has been processed. All of the data contained in the SAM extract file is now in the CCRC.

Once the extract file has been loaded and processed, the CCRC will contain all data, valid or invalid, contained in those SAM extract files.

3.1.4 Processing Options

There are three possible ways to process the data in CCRC.

- Download a monthly extract each month – the monthly will always override all of the data in the CCRC database
- Download the monthly once in the beginning to load initial data, then process daily files to incorporate changes into the CCRC database
- A combination of the above two ways where you process an initial monthly load file, process daily files to incorporate changes, and also periodically process monthly refresh files to ensure that data is in sync with SAM. – each monthly will override all of the data in the CCRC database (including any changes made through the dailys)

3.1.5 Removing the SAM File from CCRC

This is not advised, but a user can remove a file from the file list or entirely remove the file from the system. To delete a file entry from the file list or remove the file from the system, select the desired file by following the same steps when processing the file, except click the delete or download button respectively, instead of the process button.

3.2 Initial Vendor Selection

After the initial load has occurred, initial vendors need to be selected for publication to Pegasys. The initial selection of vendors can be accomplished in a variety of ways:

- Select Vendors to Enable from Pegasys
- Execute Batch Process (GSCCRI)
- Run Initial Vendor Selection script

Example: ABC Agency has performed the SAM load and has ensured that all of the vendors that it needs to enable for SAM have a unique DUNS/DUNS + 4 Number. The agency needs to select numerous vendors to be enabled for SAM, so the SAM information for these vendors can be obtained from the CCRC.

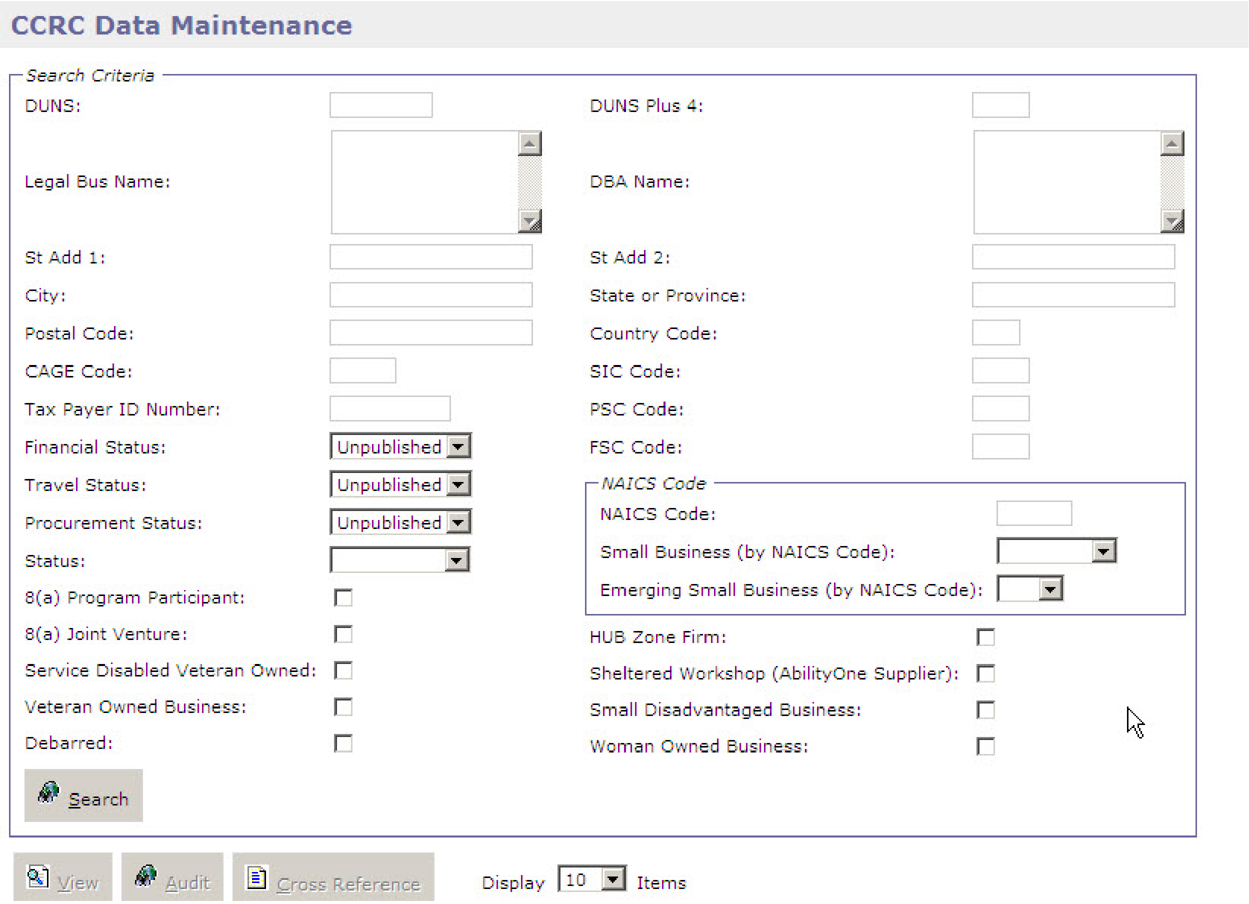
3.2.1 Select Vendors to Enable

Selecting vendors for the transfer to Pegasys can also be accomplished through the CCRC Data Maintenance Table (see ***Figure 3-3: CCRC Data Maintenance*** Table).

The CCRC Data Maintenance Table Window can be accessed through the following path:

Reference Data/CCRC Data/CCRC Data Maintenance

Figure 3-3: CCRC Data Maintenance Table



CCRC Data Maintenance

Search Criteria

DUNS:		DUNS Plus 4:	
Legal Bus Name:		DBA Name:	
St Add 1:		St Add 2:	
City:		State or Province:	
Postal Code:		Country Code:	
CAGE Code:		SIC Code:	
Tax Payer ID Number:		PSC Code:	
Financial Status:	Unpublished	FSC Code:	
Travel Status:	Unpublished	*NAICS Code*	
Procurement Status:	Unpublished	NAICS Code:	
Status:		Small Business (by NAICS Code):	
8(a) Program Participant:	□	Emerging Small Business (by NAICS Code):	
8(a) Joint Venture:	□	HUB Zone Firm:	□
Service Disabled Veteran Owned:	□	Sheltered Workshop (AbilityOne Supplier):	□
Veteran Owned Business:	□	Small Disadvantaged Business:	□
Debarred:	□	Woman Owned Business:	□

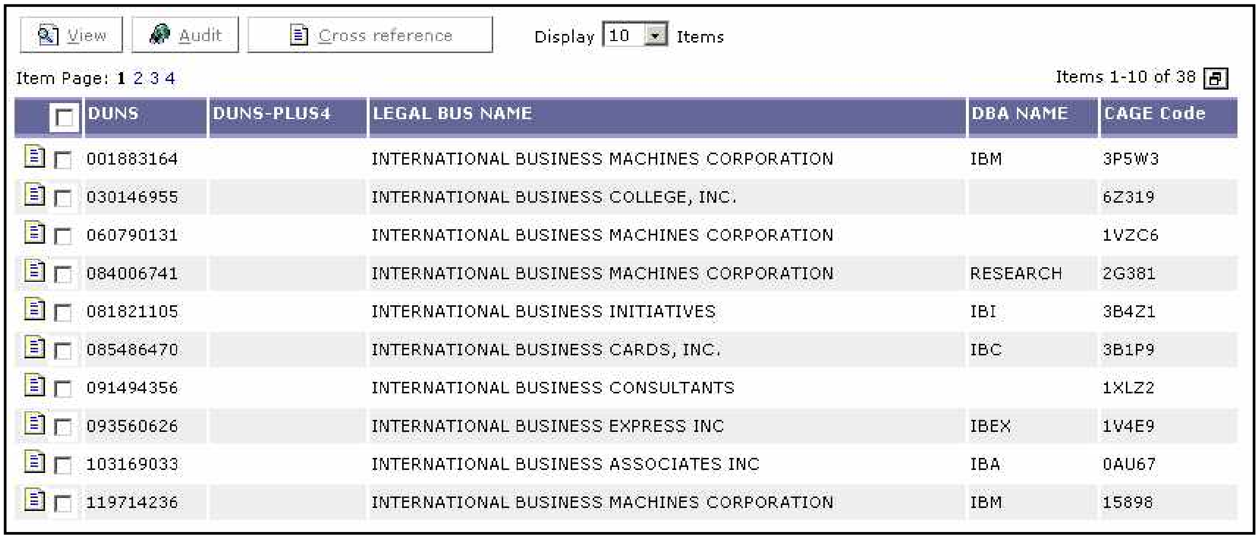
Through the CCRC Data Maintenance Table, the Administrator can enter desired search criteria in order to find the vendors the agency conducts business with. The system returns an “available” list of vendors that match the search criteria (see ***Figure 3-4: Available List of Vendors***).

3.2.1.1 CCRC Data Maintenance Partners

Parameter	Description
DUNS	(Data Universal Numbering System) A unique 9-digit numbering system that is used to identify a business.
DUNS-PLUS4	Used to identify vendors with more than one CCR record.
Legal Bus Name	The legal business name of the business.
DBA NAME	‘Doing Business As’ Name.
ST ADD 1	The street address of the business.
ST ADD 2	The alternate street address of the business.
City	The city of the business.

Parameter	Description
State or Province	The state or province of the business.
Postal Code	The postal code of the business.
Country Code	The country code of the business.
CAGE Code	(Commercial and Government Entity) Code that identifies contractors conducting business with the Government.
SIC Codes	(Standard Industrial Classification Codes) A 4-digit or 8-digit code used to identify products and services.
Tax Payer ID Number	The nine-digit number used for income tax purposes.
PSC Codes	(Product Service Codes) A 4-character, alpha-numeric code, used to identify services.
FSC Codes	(Federal Supply Classification Codes) A 4-digit code used to identify products.
Financial Status	Status of unpublished, submitted, accepted, or rejected.
Procurement Status	Status of unpublished, submitted, accepted, or rejected.
Travel Status	Status of unpublished, submitted, accepted, or rejected.
Status	The status of the vendor (pending, etc.)
8(a) Program Participant	Check box. The business is a participant in the 8(a) Program.
NAICS Code (group box)	Includes the NAICS Code, Small Business , and Emerging Small Business
HUB Zone Firm	Check box. The business is a participant in the HUB Zone.
Service Disabled Veteran Owned	Check box. The business is a participant in the Service Disabled Veteran Owned program.
Sheltered Workshop (AbilityOne Supplier)	Check box. The business is a participant in the Sheltered Workshop (JWOD Supplier) program.
Small Disadvantaged Business	Check box. The business is a participant in the Small Disadvantaged Business program.
Veteran Owned Business	Check box. The business is a participant in the Veteran Owned Business program.
Woman Owned Business	Check box. The business is a participant in the Woman Owned Business program.
Debarred	Indicates whether or not the vendor has been declared ineligible from receiving Federal contracts, as shown by records at the Excluded Parties Listing System (EPLS).

Figure 3-4: Available List of Vendors



☐	DUNS	DUNS-PLUS4	LEGAL BUS NAME	DBA NAME	CAGE Code
☐	001883164		INTERNATIONAL BUSINESS MACHINES CORPORATION	IBM	3P5W3
☐	030146955		INTERNATIONAL BUSINESS COLLEGE, INC.		6Z319
☐	060790131		INTERNATIONAL BUSINESS MACHINES CORPORATION		1VZC6
☐	084006741		INTERNATIONAL BUSINESS MACHINES CORPORATION	RESEARCH	2G381
☐	081821105		INTERNATIONAL BUSINESS INITIATIVES	IBI	3B4Z1
☐	085486470		INTERNATIONAL BUSINESS CARDS, INC.	IBC	3B1P9
☐	091494356		INTERNATIONAL BUSINESS CONSULTANTS		1XLZ2
☐	093560626		INTERNATIONAL BUSINESS EXPRESS INC	IBEX	1V4E9
☐	103169033		INTERNATIONAL BUSINESS ASSOCIATES INC	IBA	0AU67
☐	119714236		INTERNATIONAL BUSINESS MACHINES CORPORATION	IBM	15898

The Administrator can then “view” each vendor and either submit or approve the vendor to Pegasys. For more on submitting and approving vendors, see the *Publishing Vendors* section.

3.2.2 Execute Initial File Creation Batch Process

Within Pegasys, the Administrator executes the SAM Initial File Creation batch process (GSCCRI) to create the file to be sent to the CCRC. (The default output file name is ‘ccri’). The file contains the DUNS/DUNS + 4 for the vendors that will be enabled for the SAM file, so the SAM file information can be obtained for those vendors. The output file will be used in running the SQL script. See the *CCRC Batch Operation Guide* for parameters.

For each selected vendor address, the batch job performs the following steps:

- If the selected vendor address code has a DUNS/DUNS + 4 Number that has not yet been added to the file, the batch job writes the DUNS/DUNS + 4 of this vendor address code to an output file.
    - In the file, the batch job specifies that the vendor is to be published to Pegasys.
    - The batch job marks the vendor address as added to the Initial Download file.
- If the selected vendor address code does not have a DUNS/DUNS + 4 Number or has a DUNS/DUNS + 4 Number that already exists in a file, the batch job returns an informational message and does not add the vendor information for this address to the file.

After all vendor address records in the list are processed, the Batch Job saves the output file.

Note — The methods described assume that Pegasys is utilized. Other applications may need to employ a different mechanism for generating the output file described.

3.2.3 Initial Vendor Selection Script and Synchronization

The Administrator runs the initial vendor selection script (ccri.sql) that uses the output file created from the batch job in which the financials, procurement, and/or travel status for selected vendors is updated to ‘Accepted’. Once the script has been run, the vendors are then automatically marked for synchronization and published.

3.3 Daily Update Files

With vendor data constantly changing, it is necessary for an agency to complete either daily or monthly update loads. These loads can contain new vendor information as well as updates to existing vendors.

3.3.1 Daily CCRC Data Load

Daily update files can contain new vendors, changes to existing vendors, deactivations, and deletions. The vendor table in the CCRC contains additional fields to capture the timestamp when records are loaded or changed, the user last requesting a change or load, and the timestamp when the record was published to Pegasys.

The daily update load is done in much the same way as the initial SAM vendor load

The SAM File Upload can be accessed by the following path:

CCRC File Handler/Process CCR File/Document Management

Steps to Upload a SAM Extract File:

1. Click the CCRC subfolder, which will activate the **Upload** button.
2. Click the **Upload** button
3. Browse for the desired SAM Extract file and click the **Upload** button

Steps to Process a SAM Extract File:

1. Click the plus expansion button next to the CCRC subfolder
2. Select the file intended for processing
3. Click the **Process** button
4. Go to Batch Jobs/Batch Job Status to check the result of the processing or processed SAM Extract File

The Daily Data Load validates data-related SAM requirements in the following ways:

- It ensures that a Daily Data Load has not already been loaded for this date.

- It ensures that a Daily or Monthly Data Load has not already been loaded for a date greater than the date of this Daily Data Load.
- It also ensures that a preceding Daily Data Load has not been skipped.
- The CCRC Date Table contains an entry for every holiday. SAM files are expected to be received for every Tuesday—Saturday (except Holidays) throughout the year. Edits will be used to ensure that SAM Daily files are not loaded out of order (i.e., The Daily file from the 3rd is not loaded until the Daily file from the 2nd has been loaded).

3.3.1.1 Parameters

Field	Field Description
Description	The user has the ability to enter a description of the file for future reference.
Document	The filename/path of the extract file to be loaded. This parameter is required.

The daily load verifies the extract file layout by ensuring the SAM Extract Code of each record is set to ‘1’, ‘2’, ‘3’, or ‘4’ (see ***Figure 3-5: SAM Extract Codes***).

Figure 3-5: SAM Extract Codes

Extract Code	Extract Code Description
1	Deleted Record
2	New Record
3	Update Record
4	Deactivated Record
A	Record from the monthly file (treated the same as a 3)

3.3.2 New Vendor

If the record on the file is for a vendor that does not exist in the CCRC database, that vendor will be designated as new. Only records with a SAM Extract Code of 2 (new record) or 3 (update record) are eligible for consideration as a new vendor in the CCRC.

The data is loaded into the CCRC Vendor Table and the CCRC is populated with the timestamp of the load, the user running the load, the DUNS/DUNS + 4, and any other default information for each record.

Note — The record is not marked for publication at this stage.

3.3.3 Existing Vendor

If the record on the file is for a vendor that does exist in the CCRC database, that vendor will be designated as changed. Only records with a SAM Extract Code 2 (new record) or 3 (update record) will be eligible for consideration as a changed vendor in the CCRC.

Once the record is found in the CCRC, it is updated based on the data from SAM. The vendor record is marked as changed and the table is populated with the timestamp of the load, the user running the load, the DUNS/DUNS + 4, and any other default information for each record.

If the vendor has previously been published, i.e., the changed record has a status of ‘accepted’, the updated record is published and overwrites the previous information in Pegasys. If the vendor has not previously been published, the vendor will not be marked for publication.

3.3.4 Deletion and Deactivation

Only records with a SAM Extract Code 1 (deleted record) or 4 (deactivated record) will be eligible for consideration as a deleted or deactivated vendor in the CCRC.

Upon receiving a vendor with one of these extract codes, the record is then marked as deleted or inactive and the CCRC is populated with the timestamp of the load, the user running the load, the DUNS/DUNS + 4, and any other default information for each record.

If the vendor has previously been published, the record is marked as either inactive (for modules that don’t have a “prevent new spending” flag) or with a “prevent new spending flag” through the integration.

3.4 Supplemental Monthly Loads

In rare occasions, it may be necessary to load a supplemental monthly SAM file. Along with the Initial load and the Daily Load, the Supplemental load is done in very much the same way.

Example: ABD Agency did not perform Daily Data Loads during a given month and has determined that it would be advantageous to re-load from the Supplemental Monthly Data Load rather than executing each Daily Data Load in sequential order.

The SAM file upload can be accessed by the following path:

CCRC File Handler/Process CCR File/Document Management

3.4.1.1 Parameters

Field	Field Description
Description	The user has the ability to enter a description of the file for future reference.
Document	The filename/path of the extract file to be loaded. This parameter is required.

Steps to Upload a SAM Extract File:

1. Click the CCRC subfolder, which will activate the **Upload** button.
2. Click the **Upload** button
3. Browse for the desired SAM Extract file and click the **Upload** button

Steps to Process a SAM Extract File:

5. Click the plus expansion button next to the CCRC subfolder
6. Select the file intended for processing
7. Click the **Process** button
8. Go to Batch Jobs/Batch Job Status to check the result of the processing or processed SAM Extract File

The Monthly Data Load validates date-related SAM requirements.

The Monthly Data Load ensures that a Monthly Data Load has not already been loaded for this month. The CCRC is validated to ensure that a monthly file from this month has not already been processed.

The Monthly Data Load ensures that a Daily or Monthly Data Load has not already been loaded for a date greater than the date of this Monthly Data Load.

Refer to sections 3.3.2, 3.3.3, and 3.3.4 for information on New Vendors, Existing Vendors, and Deletion and Deactivation.

4 Searching/Publishing Vendors

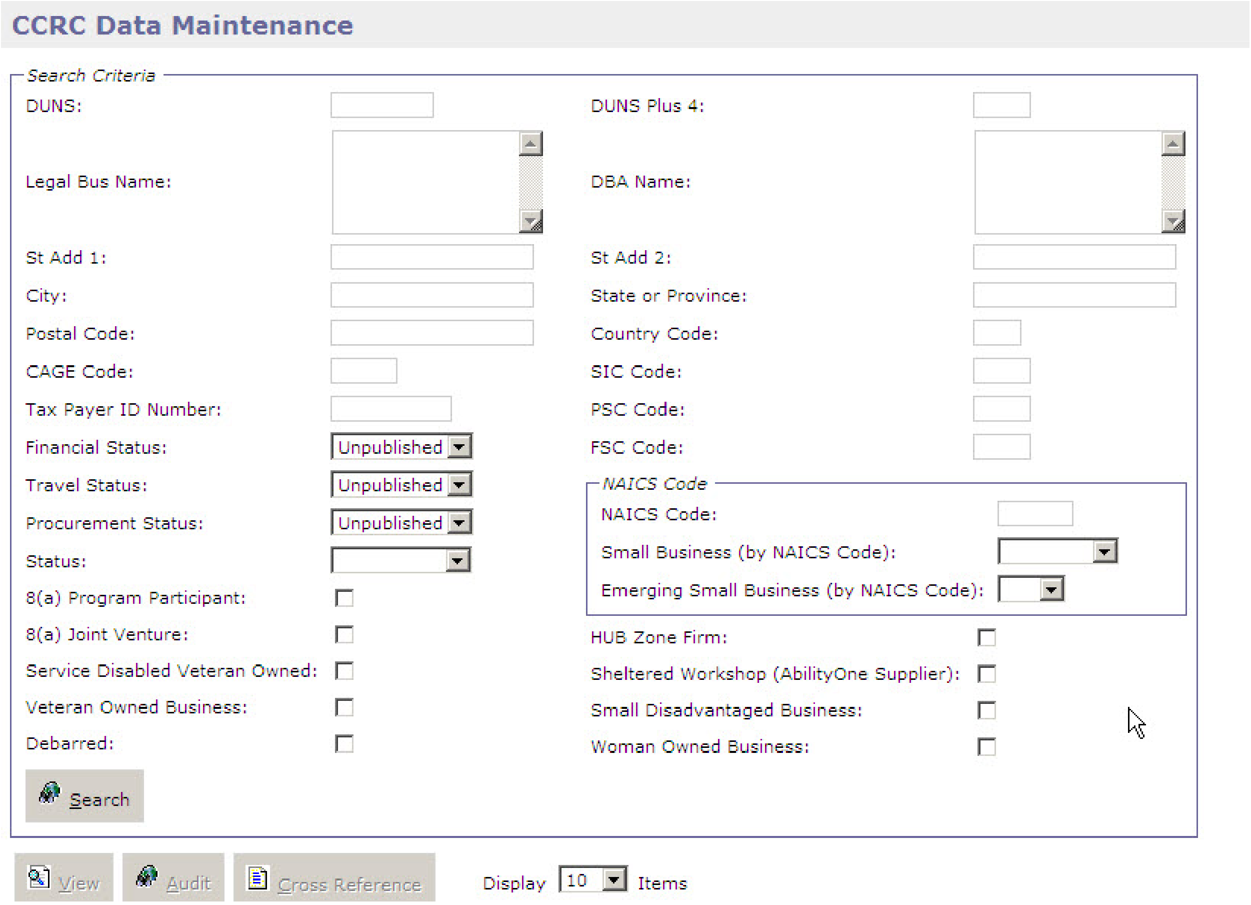
4.1 Searching for Vendors

Users are able to login to the CCRC to query vendor information and select a new vendor for publication and publish that vendor. Vendors will only be published to the set of Agency Applications designated for that vendor. Only a user with “Approver” access or “Requestor” access will have the ability to publish vendors.

4.1.1 Vendor Information Query

Users may search for vendor using a variety of search criteria, including any combination of the following parameters (Wildcards are allowed in the beginning, middle, or end. * is for multiple characters, ? is for single characters) (see ***Figure 4-1: CCRC Data Maintenance Table***).

Figure 4-1: CCRC Data Maintenance Table



CCRC Data Maintenance

Search Criteria

DUNS:		DUNS Plus 4:	
Legal Bus Name:		DBA Name:	
St Add 1:		St Add 2:	
City:		State or Province:	
Postal Code:		Country Code:	
CAGE Code:		SIC Code:	
Tax Payer ID Number:		PSC Code:	
Financial Status:	Unpublished	FSC Code:	
Travel Status:	Unpublished		
Procurement Status:	Unpublished		
Status:			
8(a) Program Participant:	□	HUB Zone Firm:	□
8(a) Joint Venture:	□	Sheltered Workshop (AbilityOne Supplier):	□
Service Disabled Veteran Owned:	□	Small Disadvantaged Business:	□
Veteran Owned Business:	□	Woman Owned Business:	□
Debarred:	□		

NAICS Code

NAICS Code:	
Small Business (by NAICS Code):	
Emerging Small Business (by NAICS Code):	

Display 10 Items

4.1.2 Search Parameters

Parameter	Description
DUNS	(Data Universal Numbering System) A unique 9-digit numbering system that is used to identify a business.

Parameter	Description
DUNS-PLUS4	Used to identify vendors with more than one CCR record.
Legal Bus Name	The legal business name of the business.
DBA NAME	'Doing Business As' Name.
ST ADD 1	The street address of the business.
ST ADD 2	The alternate street address of the business.
City	The city of the business.
State or Province	The state or province of the business.
Postal Code	The postal code of the business.
Country Code	The country code of the business.
CAGE Code	(Commercial and Government Entity) Code that identifies contractors conducting business with the Government.
SIC Codes	(Standard Industrial Classification Codes) A 4-digit or 8-digit code used to identify products and services.
Tax Payer ID Number	The nine-digit number used for income tax purposes.
PSC Codes	(Product Service Codes) A 4-character, alpha-numeric code, used to identify services.
FSC Codes	(Federal Supply Classification Codes) A 4-digit code used to identify products.
Financial Status	Status of unpublished, submitted, accepted, or rejected.
Procurement Status	Status of unpublished, submitted, accepted, or rejected.
Travel Status	Status of unpublished, submitted, accepted, or rejected.
Status	The status of the vendor (pending, etc.)
8(a) Program Participant	Check box. The business is a participant in the 8(a) Program.
NAICS Code (group box)	Includes the NAICS Code, Small Business , and Emerging Small Business
HUB Zone Firm	Check box. The business is a participant in the HUB Zone.
Service Disabled Veteran Owned	Check box. The business is a participant in the Service Disabled Veteran Owned program.
Sheltered Workshop (AbilityOne Supplier)	Check box. The business is a participant in the Sheltered Workshop (JWOD Supplier) program.
Small Disadvantaged Business	Check box. The business is a participant in the Small Disadvantaged Business program.
Veteran Owned Business	Check box. The business is a participant in the Veteran Owned Business program.
Woman Owned Business	Check box. The business is a participant in the Woman Owned Business program.
Debarred	Indicates whether or not the vendor has been declared ineligible from receiving Federal contracts, as shown by records at the Excluded Parties Listing System (EPLS).

The user has several options once the search for a particular vendor has been completed. They are able to search for another vendor, publish a new vendor, or publish updates to an existing vendor.

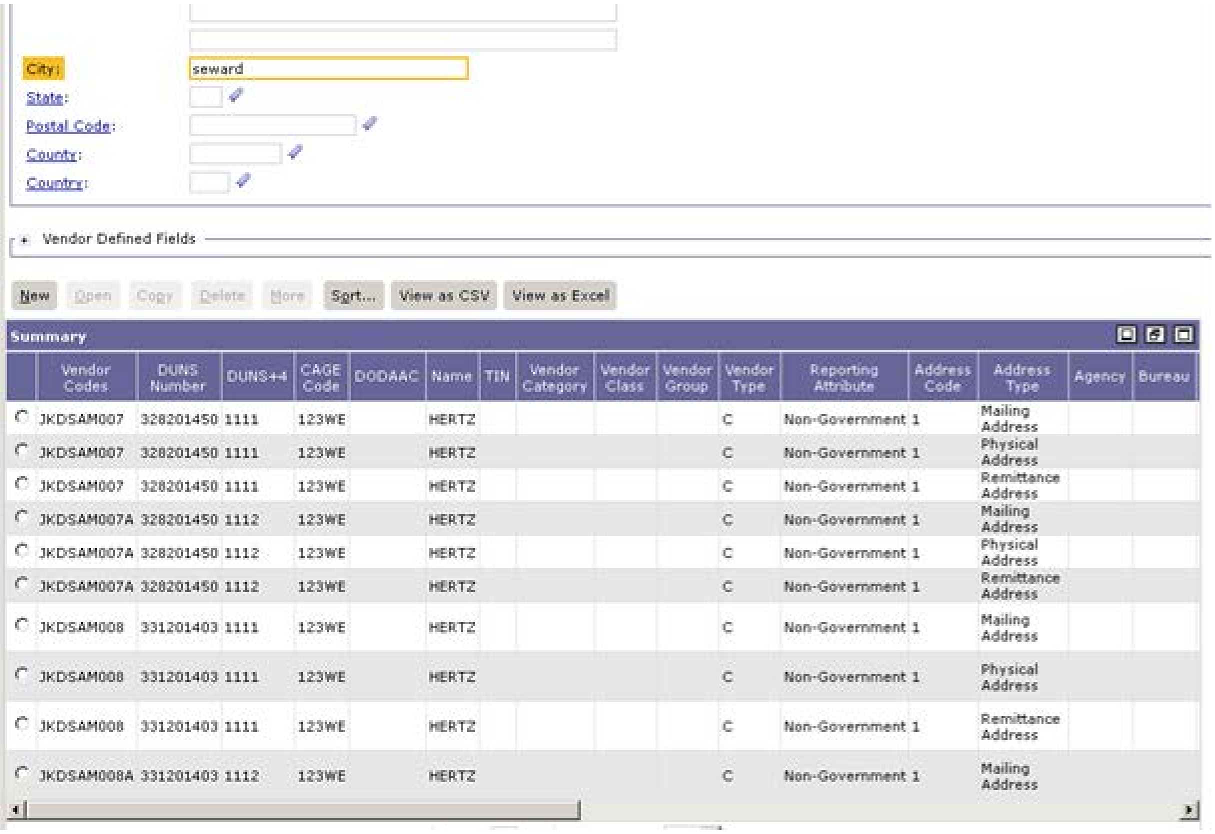
4.1.3 Search for Another Vendor

If the user chooses to search for another vendor, he/she will return to the initial search screen. The user is then prompted to retain the original search criteria or may opt to refresh the criteria. With either option, the user can change the search criteria before executing the next search

4.1.4 Case Insensitive Queries

Certain text fields on CCRC queries support case insensitive searches. This allows the user to enter search criteria in either upper or lowercase, and have all matching results returned, regardless of the case of the results. An example is shown in [Exhibit 4-2] below.

Figure 4-2: Case Insensitive Query in CCRC



City: seward
State:
Postal Code:
County:
Country:

	Vendor Codes	DUNS Number	DUNS+4	CAGE Code	DODAAC	Name	TIN	Vendor Category	Vendor Class	Vendor Group	Vendor Type	Reporting Attribute	Address Code	Address Type	Agency	Bureau
○	JKDSAM007	328201450	1111	123WE		HERTZ					C	Non-Government	1	Mailing Address		
○	JKDSAM007	328201450	1111	123WE		HERTZ					C	Non-Government	1	Physical Address		
○	JKDSAM007	328201450	1111	123WE		HERTZ					C	Non-Government	1	Remittance Address		
○	JKDSAM007A	328201450	1112	123WE		HERTZ					C	Non-Government	1	Mailing Address		
○	JKDSAM007A	328201450	1112	123WE		HERTZ					C	Non-Government	1	Physical Address		
○	JKDSAM007A	328201450	1112	123WE		HERTZ					C	Non-Government	1	Remittance Address		
○	JKDSAM008	331201403	1111	123WE		HERTZ					C	Non-Government	1	Mailing Address		
○	JKDSAM008	331201403	1111	123WE		HERTZ					C	Non-Government	1	Physical Address		
○	JKDSAM008	331201403	1111	123WE		HERTZ					C	Non-Government	1	Remittance Address		
○	JKDSAM008A	331201403	1112	123WE		HERTZ					C	Non-Government	1	Mailing Address		

The following CCRC fields on the following queries support case insensitive searches:

- **Vendor Search:** Address Line 1 - Address Line 4, Agency Location Code, CAGE Code, City, Country, DBA Name, DODAAC, Legal Business Name, Postal Code, PSC Code, St Add 1 - St Add 2, State or Province
- **Holiday Maintenance Table:** Description
- **Document Management:** Document Name
- **WebMethods Maintenance:** Server Id, Service Name
- **WebMethods Error:** Server Id, Service Name
- **Cross Reference:** Application Id, Native Id, Object Name
- **Batch process Status:** Job Definition, Step Name

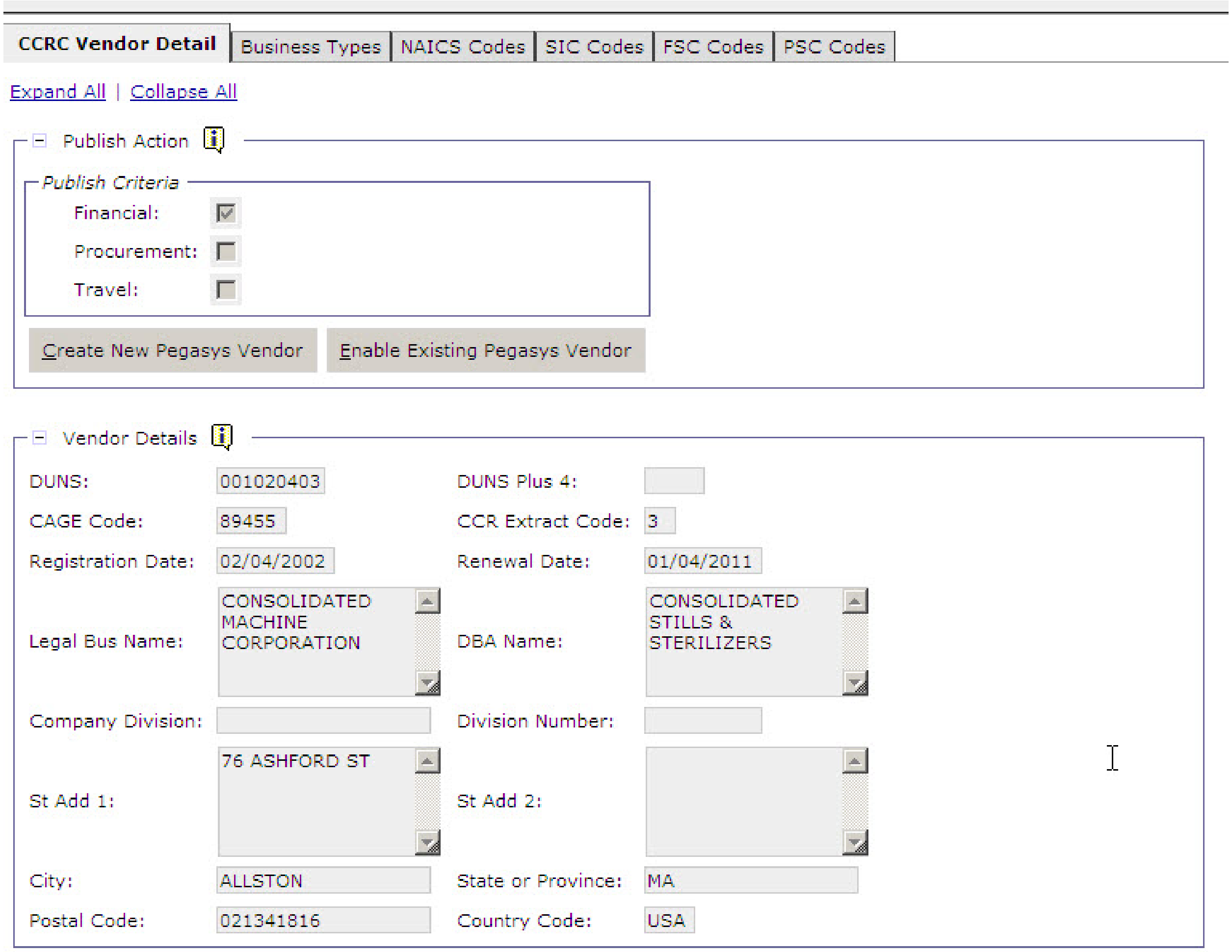
4.2 Publishing Vendors

A vendor's information is sent to Pegasys when it is 'published'.

4.2.1 Publishing New Vendor Information

By selecting a vendor, the user is given several options (see ***Figure 4-3: CCRC Vendor Detail***).

Figure 4-3: CCRC Vendor Detail



Publish Criteria

Financial: ☑
Procurement: □
Travel: □

DUNS:	001020403	DUNS Plus 4:	
CAGE Code:	89455	CCR Extract Code:	3
Registration Date:	02/04/2002	Renewal Date:	01/04/2011
Legal Bus Name:	CONSOLIDATED MACHINE CORPORATION	DBA Name:	CONSOLIDATED STILLS & STERILIZERS
Company Division:		Division Number:	
St Add 1:	76 ASHFORD ST	St Add 2:	
City:	ALLSTON	State or Province:	MA
Postal Code:	021341816	Country Code:	USA

Through the CCRC Vendor Detail window, the user is able to publish the vendor by clicking either the Create New Pegasys Vendor button or the Enable Existing Pegasys Vendor button. GSA users will always have the Financial box checked in the Publish Action group box.

- **Create New Pegasys Vendor -**If the vendor is new, the ‘Create New Pegasys Vendor’ button should be chosen. If Pegasys is being used, a vendor form is created (pre-populated with the SAM data) and routed to Pegasys where a user is able to populate any additional needed data. The user can then process the Pegasys vendor form. At that point the financial status in CCRC is updated to ‘Accepted.’
- **Enable Existing Pegasys Vendor** -If the vendor already exists within Pegasys, a user with Approve permission can bypass the need to separately process a form within the agency’s application by clicking ‘Enable Existing Pegasys Vendor’ in the CCRC Vendor Detail window. The vendor’s status is changed to ‘Published’ and all information is published to the CCRC and the agency’s application.

The user is also able to view the following, depending on the user’s access (see Users for more information):

- **Vendor Details**-Provides public information related to that vendor (i.e., DUNS/DUNS + 4 number, address information, registration date).
- **Status Information**-Provides the status information related to that vendor (i.e., Published status, Time-stamp, Record status)
- **Business Details**-Provides business information related to that vendor (i.e., SIC codes, Business type, URL).
- **POC Mailing Address Details**-Provides multiple mailing addresses related to that vendor.
- **Proprietary Information**-Provides proprietary information related to that vendor (e.g., Tax Payer number, Annual Revenue, Average number of Employees)
- **Sensitive Information**-Provides sensitive information related to that vendor (i.e., Bank Account number, Lockbox number, Remittance information)

4.2.1.1 New Vendor Submissions

When vendors are being published for the first time, new vendor forms are created in Pegasys pre-populated with SAM data. The vendor forms may then be corrected by individual(s) responsible for populating Non-SAM data. Using the vendor form created, the user will be able to thus create a new vendor or overwrite an existing vendor with the SAM data received.

Note —SAM vendor information always takes precedence over Pegasys vendor information.

4.2.2 Publishing Updates

Following the daily/monthly load, updates for previously published vendors will be automatically published to Pegasys. The CCRC screen for the DUNS shall display a publication status of “accepted” for successfully published updates if there are no errors of a functional or technical nature that prevent the data from updating Pegasys.

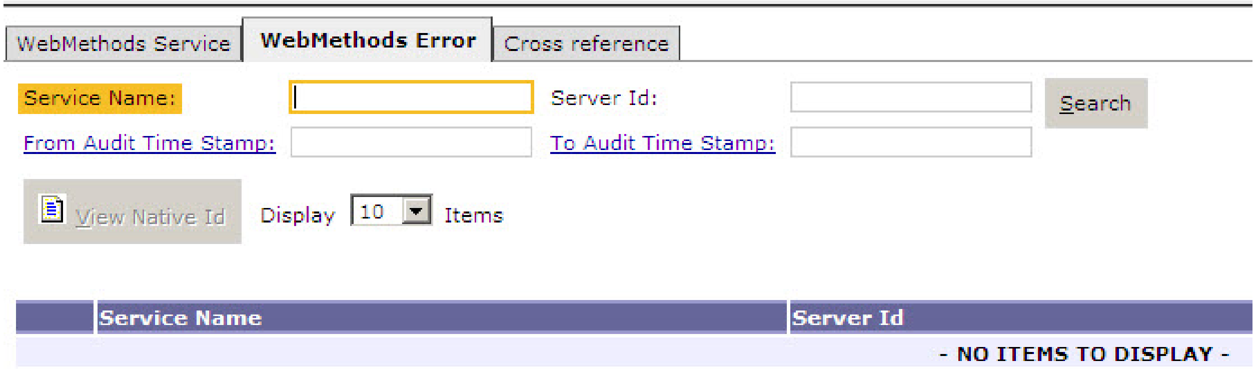
> **Example:** Vendor XYZ was originally published in March to Momentum and the vendor changes address information in April via SAM. The changes to the address information in April will automatically be published to Momentum with no user intervention.

Pegasys will confirm successful posting of the published data to its system and the CCRC will update the Posted date and time information within CCRC for this record.

4.3 Integration

Integration contains errors about vendors that were not accepted by Pegasys. The screens provide the Administrator with the tools to research and identify errors in publishing data via webMethods to Agency Applications. The user is able to search based on multiple criteria and link to DUNS/DUNS + 4 defined vendors that are impacted by the errors. You can view the Webmethods Error screen by navigating to Integration > Webmethods Maintenance > Webmethods Error (See ***Figure 4-4: Webmethods Error Screen***.)

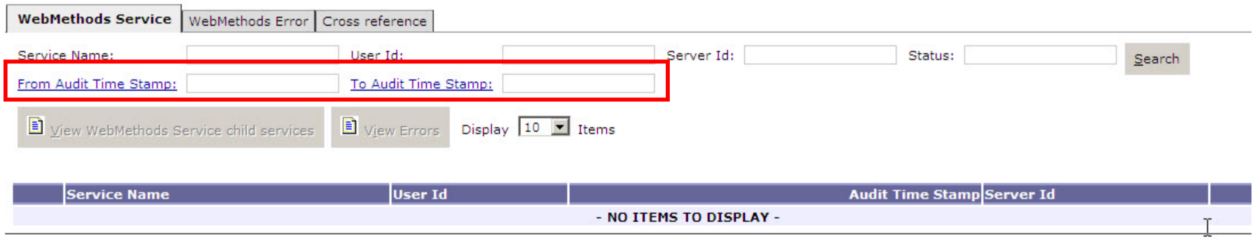
Figure 4-4: Webmethods Error Screen



4.3.1 Audit

The Administrator has the ability to look at an Audit log for a given vendor (see ***Figure 4-5: Auditing***). The Audit log is accessed by selecting a vendor from the CCRC Data Maintenance Page and clicking the audit button. From this screen it is possible to see the integration history for a particular vendor in CCRC. For example, an administrator can determine what if any errors might have resulted in attempting to publish a particular vendor. Other information accessible through this page would include the Service Name, User ID associated with publication, Server ID, and status.

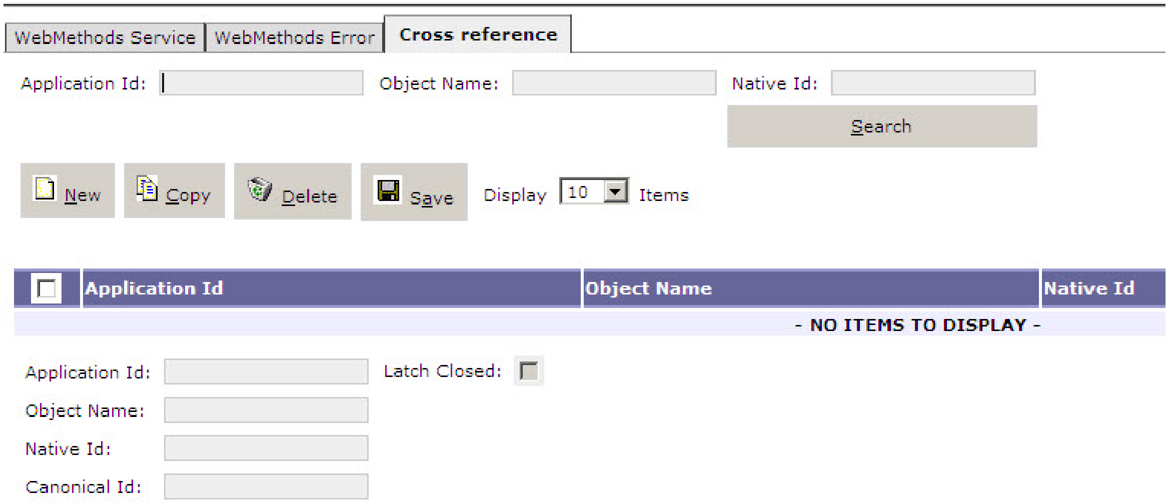
Figure 4-5: Auditing



4.3.2 Cross References

In addition to being able to assess the history of a particular vendor through the audit button, the Cross Reference functionality provides valuable insight to an administrator (see ***Figure 4-6: Cross-Reference Window***). The Cross Reference page is accessed by selecting a vendor from the CCRC Data Maintenance screen and clicking the Cross Reference button. The Cross Reference screen allows the administrator to link between applications that are connected via webMethods. This means that the administrator is able to link a given vendor in CCRC to a given vendor entity stored in Pegasys. For example, after selecting the cross reference screen for a given vendor, the administrator can change the application ID in the search section at the top of the form to “Pegasys” and find out what vendor is getting updated in Pegasys e.g. Vendor Code = ABC, Address Code= 1. This identification of the vendor entity will be found in the Native ID field. For the example previously mentioned, the Native ID would be displayed as ABC/1. If the application ID were changed back to CCRC, the Native ID would return to the DUNS/DUNS +4 since this is the identity within CCRC. Object Name and Canonical ID are also displayed as information for the administrator.

Figure 4-6: Cross-Reference Window

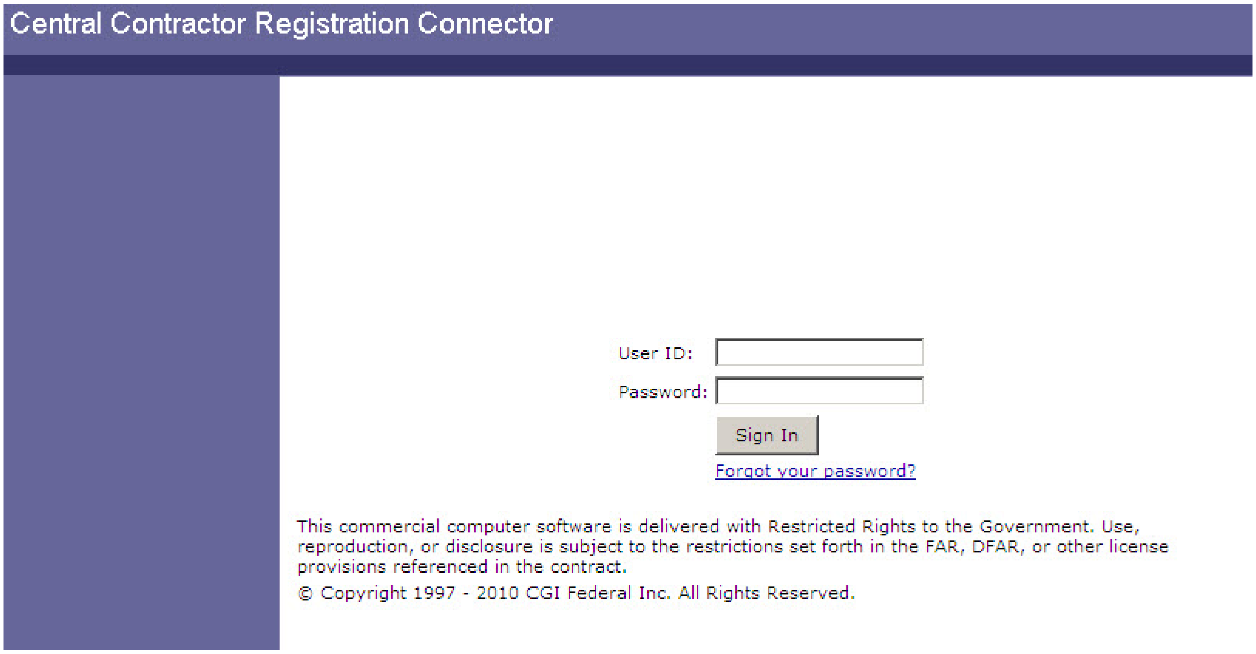


5 System Administrator

5.1 CCRC Sign In

In order to use the system, a user must login to the CCRC. This application can be accessed through the CCRC Login Page (see ***Figure 5-1: CCRC Sign In Page***).

Figure 5-1: CCRC Sign In Page



This commercial computer software is delivered with Restricted Rights to the Government. Use, reproduction, or disclosure is subject to the restrictions set forth in the FAR, DFAR, or other license provisions referenced in the contract.

© Copyright 1997 - 2010 CGI Federal Inc. All Rights Reserved.

Once logged in, the Administrator may customize the system to GSA’s needs. The Administrator has the ability to create/edit/delete security policies and passwords for users as well as the ability to view the security log.

5.2 Data Loads

5.2.1 CCRC Holiday

The Administrator can designate Holidays that can be used for date-related edits. Refer to Daily CCRC Data Load for more information.

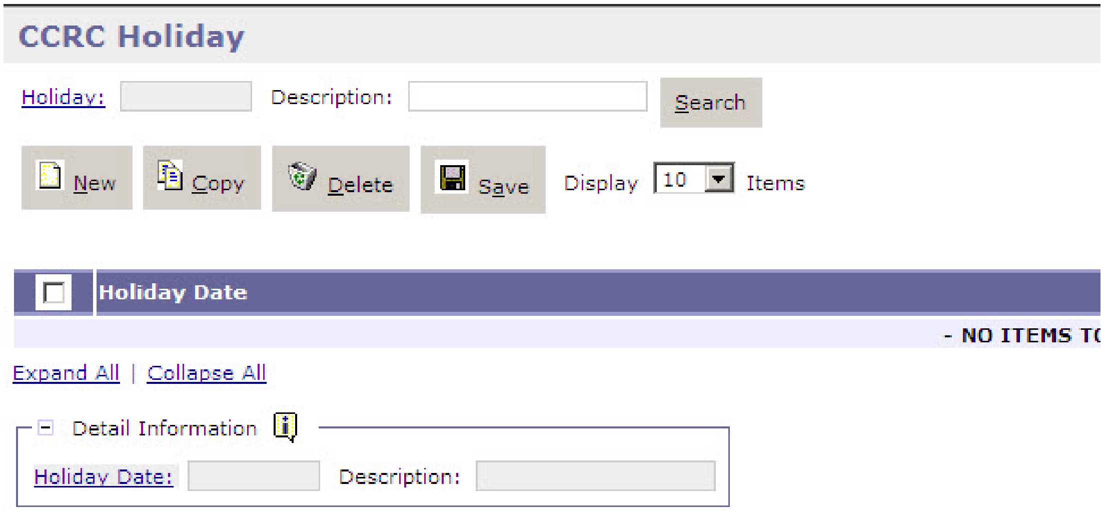
Example: ABC Agency will be closed on July 4th for Independence Day holiday. Therefore, there will be no SAM data expected because this is a Federal Holiday.

The CCRC Holiday window can be accessed by the following path:

Reference Data/Holidays/CCRC Holiday Maintenance View/CCRC Holiday

Figure 5-2: CCRC Holiday Window displays the CCRC Holiday window.

Figure 5-2: CCRC Holiday Window

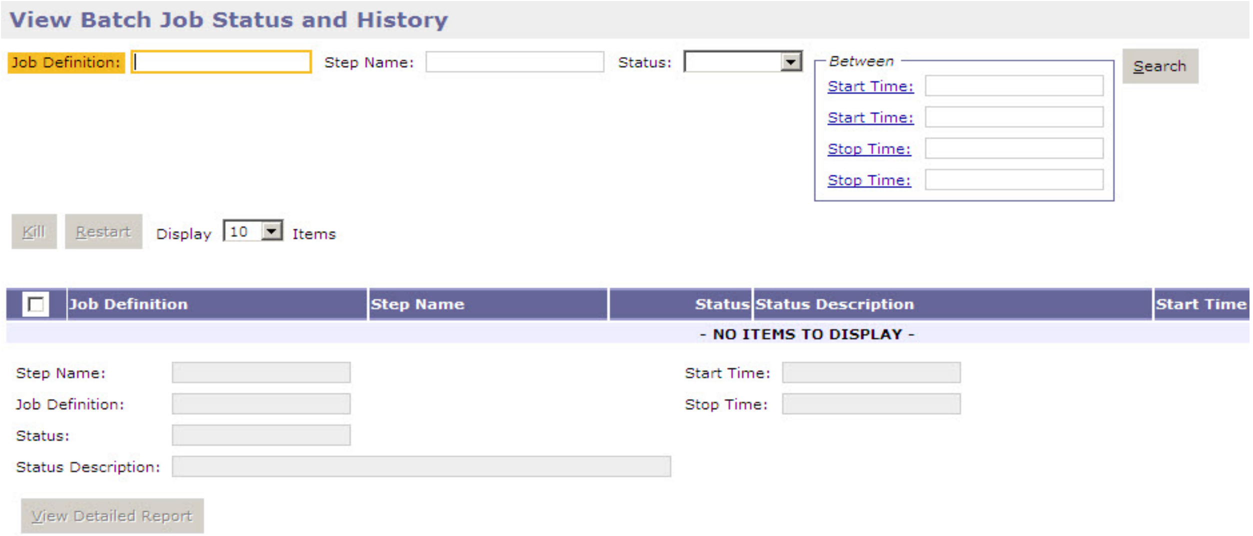


5.3 Batch Execution

5.3.1 Batch Job Status

The Batch Job Status provides a means for the administrator to assess the status of batch job executions (see ***Figure 5-3: Batch Job Status Window***). The administrator can enter various search criteria including batch job name, process, status, and start/completion time range to evaluate the progress of executions. The screen also provides the ability to view a detailed report on the execution, or restart or kill a batch job.

Figure 5-3: Batch Job Status Window



5.3.1.1 Batch Job Status Parameters

Parameters	Description
Batch Job Name	The name of the batch job.
Batch Job Definition	A definition of the batch job.
Batch Job Status	The status of the batch job (running, completed, killed, failed).
Batch Start Time	The time the batch job started.
Batch Completion Time	The time the batch job completed.

5.4 Security Policies

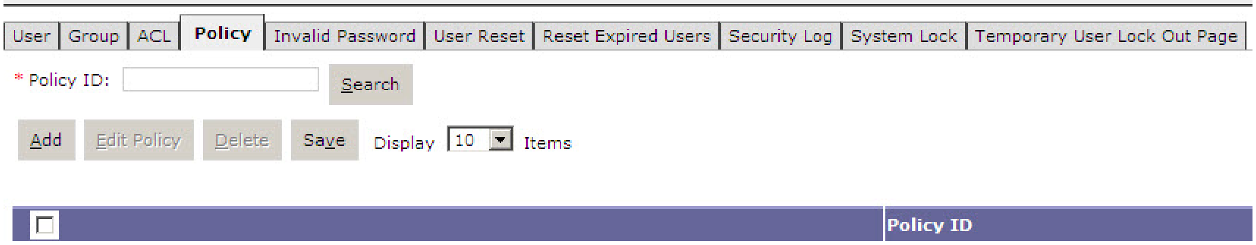
GSA has the option to customize security policies to fit their needs (e.g., number of failed login attempts before deactivating a UserID, length of grace periods, etc). Each Group/User is associated with a security policy. These policies can be accessed in the Security Maintenance window.

The Security Maintenance Window can be accessed by the following path:

Security/Security Maintenance

Figure 5-4 Security Maintenance Policy Window displays the Security Maintenance Policy Window.

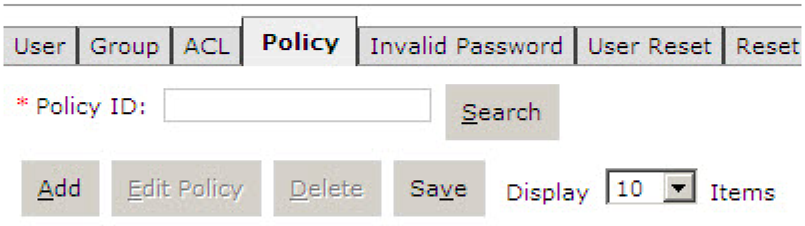
Figure 5-4: Security Maintenance Policy Window



5.4.1.1 Adding, Deleting and Editing Policies

By choosing the “Policy” tab, the Administrator has the ability to add a new policy, edit an existing policy, save a policy, or delete a policy (see ***Figure 5-4: Security Maintenance Policy Window).*** In order to add a new security policy, the Administrator must create a unique Policy Id (see ***Figure 5-5: Adding a Security Policy***.)

Figure 5-5: Adding a Security Policy



It may be necessary to edit security policies to reflect recent changes in security rules. If the Policy ID is known, then the Administrator can search for that specific Policy ID and edit by checking the box next to the appropriate Policy ID, clicking the Edit Policy button, and clicking the Edit RDBMS Policy Details tab. ***Figure 5-6: Security Maintenance Information*** describes the security maintenance information.

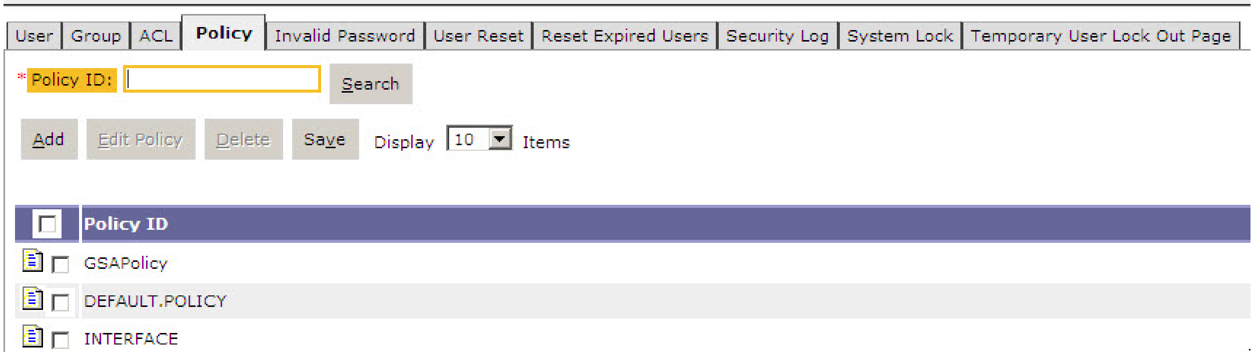
Figure 5-6: Security Maintenance Information

Field	Description
Password Reset	
Allow Password Reset Link	Allow the password reset link to be used.
Allow Generated Password Reset	Allow the generated password reset.
Enable Password Email	Enable the password email.
Allow Administrative Manual Password Reset	Allow a manual password reset.
Use Security Questions	Use the security questions.
Display Previous Login Details	Display the previous login details.
Number of Secret Questions to Answer	Number of Questions a principal assigned to this policy will answer
Number of Guesses Before the User is Locked Out	Number of Guesses a principal assigned to this policy will have
Minimum length of answers(0 is for no restrictions)	The minimum length of answers the principal must have
Verification	
Number of Consecutive Failed Logins	The Number of consecutive failed logins.
Max Number of Concurrent Sessions	The maximum number of concurrent sessions.
Password Criteria	
Password is Valid for (Days)	The number of days that must transpire before the principal must change their password.
Minimum Password Length	The minimum number of characters that a principal’s password must contain.
Maintain Password for (Days)	The number of days for which a previously used password is maintained by the system. The principal will not be able to re-use the previously used password.
Minimum Number of Passwords Maintained	The number of previously used passwords that the system will track. Cannot be more than 12.
Password Salt Size	The password salt size.
Enforce password expiration warning	Enforce the password expiration warning. Checkbox.
Unique characters	Number of unique characters.
Minimum Password Length	Minimum password length.

Field	Description
Maximum Password Length	Maximum password length.
Generated Password Length	Generated password length
Password Expiration Warning	
Strong Password Criteria	
Upper Case Alphabetic	Minimum Upper Case Characters, Maximum Upper Case Characters, and Maximum Upper Case Repeated Characters.
Lower Case Alphabetic	Minimum Lower Case Characters, Maximum Lower Case Characters, and Maximum Lower Case Repeated Characters.
Generic Alphabetic	Minimum Generic Alphabetic Characters, Maximum Generic Alphabetic Characters, and Maximum Generic Alphabetic Repeated Characters.
Numeric	Minimum Numeric Characters, Maximum Numeric Characters, and Maximum Numeric Repeated Characters.
Special	Minimum Special Characters, Maximum Special Characters, and Maximum Special Repeated Characters.

If a policy becomes invalid, the Administrator has the ability to delete that policy. If the Policy Id is known, then the Administrator can search for that Policy Id. Once the policy has been found, it can be deleted by checking the box next to the appropriate Policy and clicking on the Delete button (see ***Figure 5-7: Delete Policy***).

Figure 5-7: Delete Policy



*Policy ID:

Display 10 Items

□	Policy ID
□	GSAPolicy
□	DEFAULT.POLICY
□	INTERFACE

The new or edited security policy is viewable as soon as the Administrator clicks the “Save” button and can be associated with user accounts. If the policy has been deleted, it will no longer be seen in the Policy window.

5.4.2 Passwords

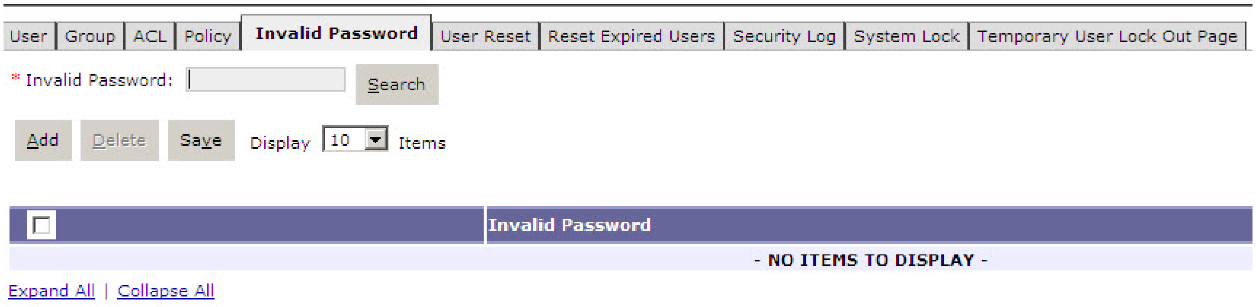
The Administrator has the option to create policy control password requirements for guest users. This policy can be created in the Security Maintenance window (see ***Figure 5 4: Security Maintenance Window***).

5.4.2.1 Invalid Passwords

The Administrator can create invalid passwords to prevent them from being used in the CCRC. This may be done by choosing “Invalid Passwords” tab. In the Invalid Password window, the

Administrator can add and delete passwords that the agency determines should be invalid (see ***Figure 5-8: Invalid Password Window***).

Figure 5-8: Invalid Password Window



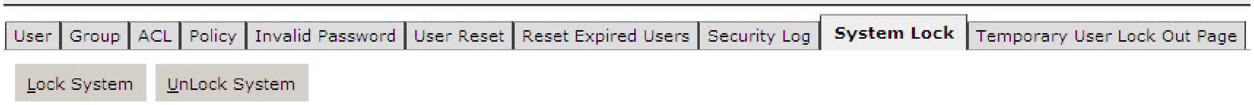
5.4.3 Reset a Locked User Account

A user account can become locked in the case of an expired password or too many failed login attempts. The Administrator has the ability to reset the user account once it has become locked. This may be done by choosing “User Reset” tab (see ***Figure 5-4: Security Maintenance Window***). Once the password has been reset, the user is able to login to the CCRC.

5.4.4 System Locking

The Administrator is able to lock and unlock the system (see ***Figure 5-9: System Lock Window***). When the system is locked, only users with access during a system locked will be able to login. The flag is set on all Edit User Screens. When the system is unlocked all other users will be able to login again. The Administrator can access the System Lock tab (see ***Figure 5-4: Security Maintenance Window***).

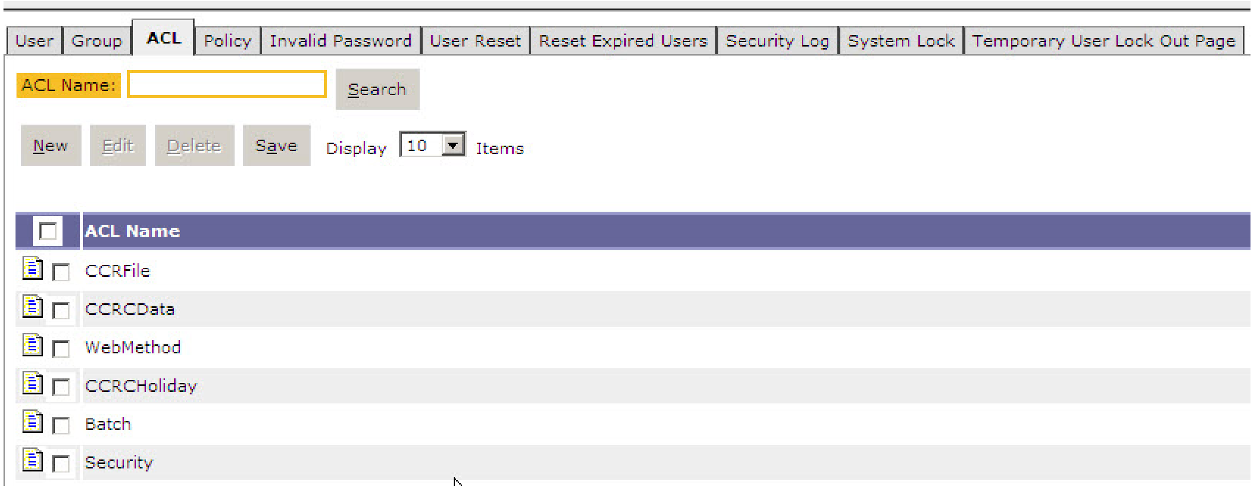
Figure 5-9: System Lock Window



5.4.5 Access Control List

The Access Control List (ACL) allows the administrator to give specific group permissions to perform certain tasks (see ***Figure 5-10: ACL Window***). Within the five groups, users have the permission to perform none or any of the following: Edit, Delete, Query, Upload, Publish, or Process.

Figure 5-10: ACL Window



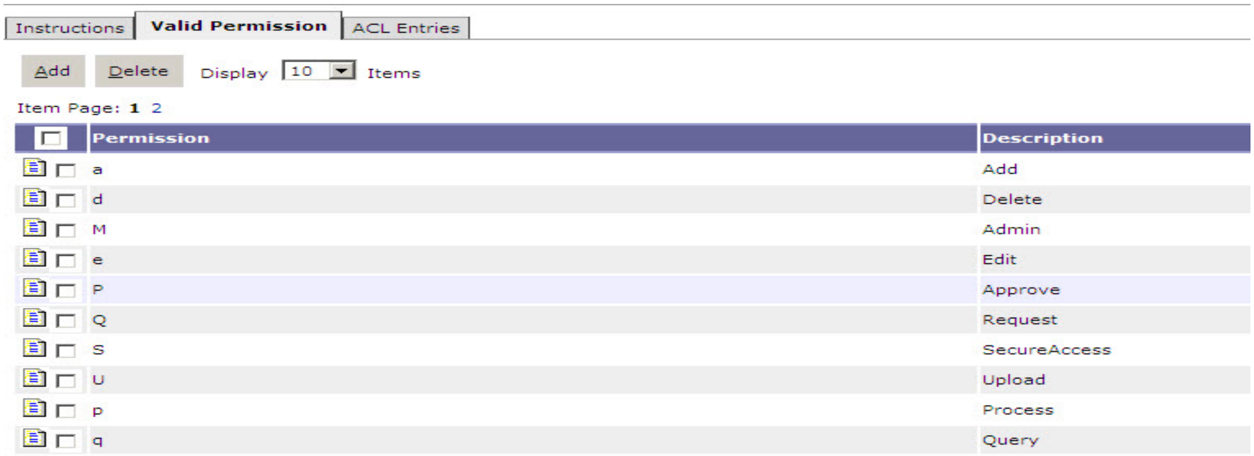
	ACL Name
□	CCRFile
□	CCRCData
□	WebMethod
□	CCRCHoliday
□	Batch
□	Security

5.4.5.1 ACL Descriptions

Field	Description
CCRFile	Used to control access to a CCR File.
CCRCData	Used to control access to a CCRC Data object
WebMethod	Used to control access to WebMethod data.
CCRCHoliday	Used to control access to CCRC Holiday data.
Batch	Used to control access to all objects in the batch framework.
Security	Used to control access to security maintenance.

Figure 5-11: Valid Permissions Window displays the valid permissions associated with the CCL name “CCRFile”. To display this window, navigate to the ACL tab, choose an ACL, and click Edit.

Figure 5-11: Valid Permissions Window



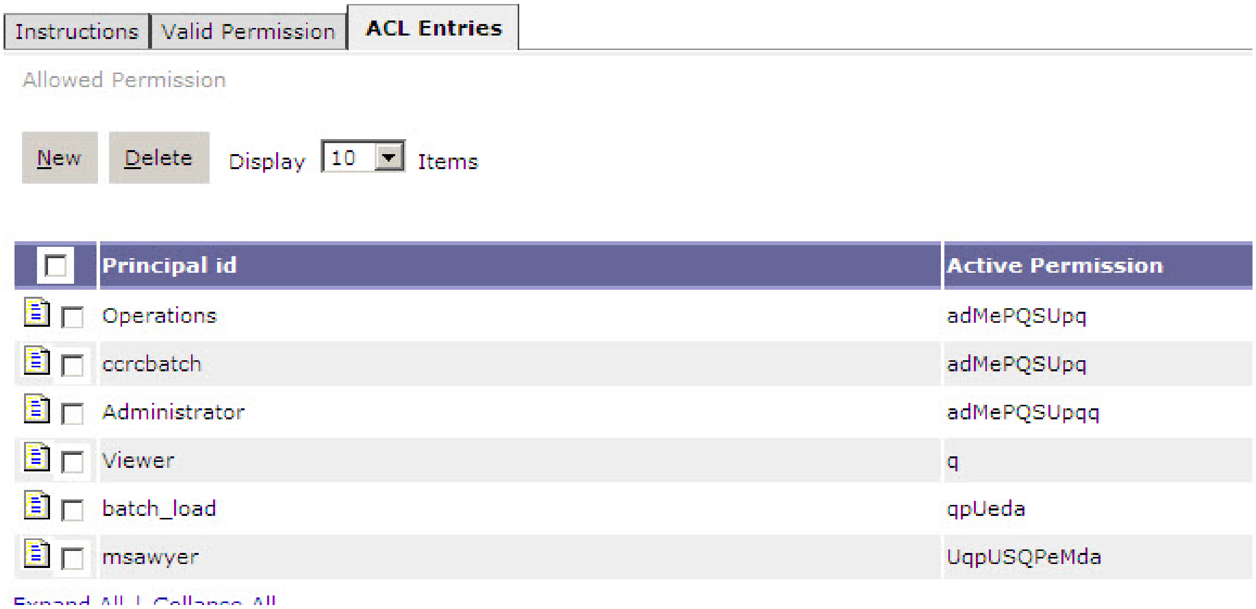
	Permission	Description
□	a	Add
□	d	Delete
□	M	Admin
□	e	Edit
□	P	Approve
□	Q	Request
□	S	SecureAccess
□	U	Upload
□	p	Process
□	q	Query

5.4.5.2 ACL Permissions

Permission	Description
a	Add
d	Delete
e	Edit
U	Upload
p	Process
q	Query

Click the 'Add' icon to add additional entries to this ACL. An entry consists of a set of a 'Principal' (a User or Group) and the active Permission set for that Principal (a subset of the complete Permission list available to the ACL (see ***Figure 5-12: ACL Entries***).

Figure 5-12: ACL Entries



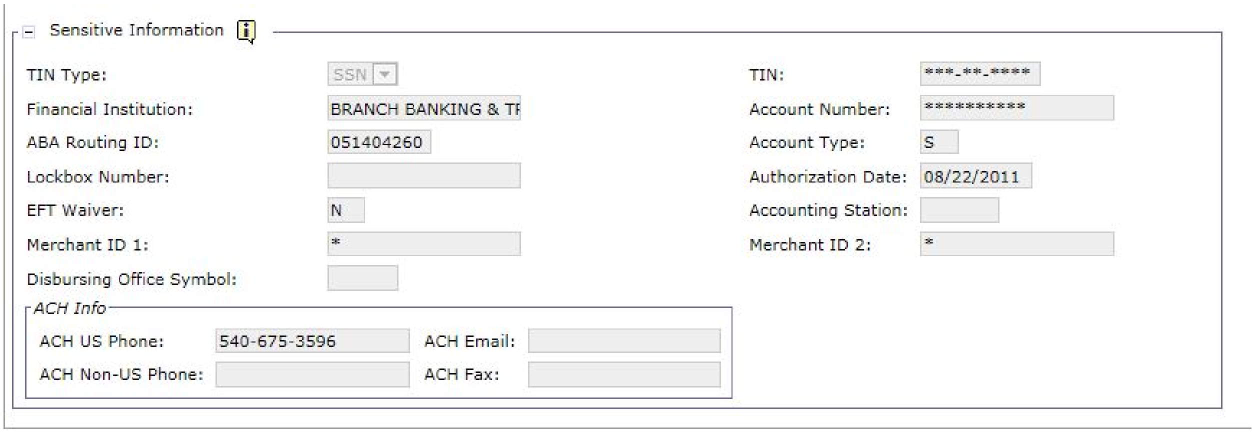
☐	Principal id	Active Permission
☐	Operations	adMePQSUpq
☐	ccrcbatch	adMePQSUpq
☐	Administrator	adMePQSUpqq
☐	Viewer	q
☐	batch_load	qpUeda
☐	msawyer	UqpUSQPeMda

5.4.6 Secure Data

Bank Account information, TIN, and Lockbox are all secure data within the CCRC database. The only users able to see this information are those with ‘Secure Accessor’ and ‘Administrator’ rights.

The Tax ID Number Field allows GSA to apply the Confidential Data Policy to the Tax ID Number and Social Security Number fields in CCRC (shown in [Figure 5-13] and [Figure 5-14] below). Fields are masked from a user without proper permissions (i.e., a user who does not have the relevant security group associated with it). On the other hand, if a user has proper permissions, then he or she will see the relevant data.   This only deals with viewing data in fields that are masked from a user without proper permissions, not searching by data.

Figure 5-13: Social Security Masked from User



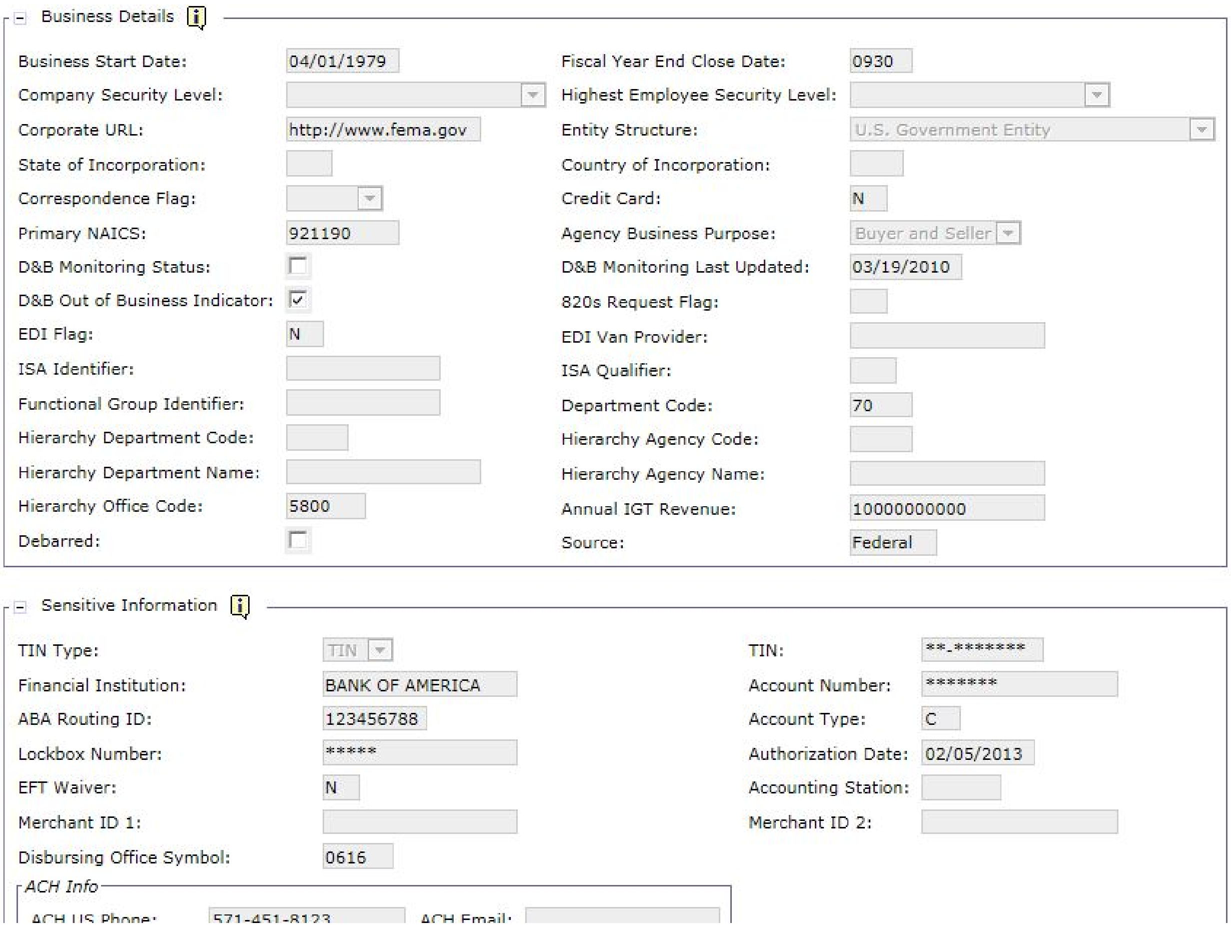
Sensitive Information

TIN Type:	SSN	TIN:	***_**_*****
Financial Institution:	BRANCH BANKING & TF	Account Number:	**********
ABA Routing ID:	051404260	Account Type:	S
Lockbox Number:		Authorization Date:	08/22/2011
EFT Waiver:	N	Accounting Station:	
Merchant ID 1:	*	Merchant ID 2:	*
Disbursing Office Symbol:			

ACH Info

ACH US Phone:	540-675-3596	ACH Email:	
ACH Non-US Phone:		ACH Fax:	

Figure 5-124: Tax Payer ID Masked from User



Business Details

Business Start Date:	04/01/1979	Fiscal Year End Close Date:	0930
Company Security Level:		Highest Employee Security Level:	
Corporate URL:	http://www.fema.gov	Entity Structure:	U.S. Government Entity
State of Incorporation:		Country of Incorporation:	
Correspondence Flag:		Credit Card:	N
Primary NAICS:	921190	Agency Business Purpose:	Buyer and Seller
D&B Monitoring Status:	☐	D&B Monitoring Last Updated:	03/19/2010
D&B Out of Business Indicator:	☑	820s Request Flag:	
EDI Flag:	N	EDI Van Provider:	
ISA Identifier:		ISA Qualifier:	
Functional Group Identifier:		Department Code:	70
Hierarchy Department Code:		Hierarchy Agency Code:	
Hierarchy Department Name:		Hierarchy Agency Name:	
Hierarchy Office Code:	5800	Annual IGT Revenue:	10000000000
Debarred:	☐	Source:	Federal

Sensitive Information

TIN Type:	TIN	TIN:	**_*******
Financial Institution:	BANK OF AMERICA	Account Number:	********
ABA Routing ID:	123456788	Account Type:	C
Lockbox Number:	*****	Authorization Date:	02/05/2013
EFT Waiver:	N	Accounting Station:	
Merchant ID 1:		Merchant ID 2:	
Disbursing Office Symbol:	0616		

ACH Info

ACH US Phone:	571-451-8123	ACH Email:	

5.4.7 Dynamic Extensibility

Through extensibility, GSA can modify existing and add new application components, control the visibility and location of fields in screens, indicate whether a field is required or not, and change virtually any label within the application.

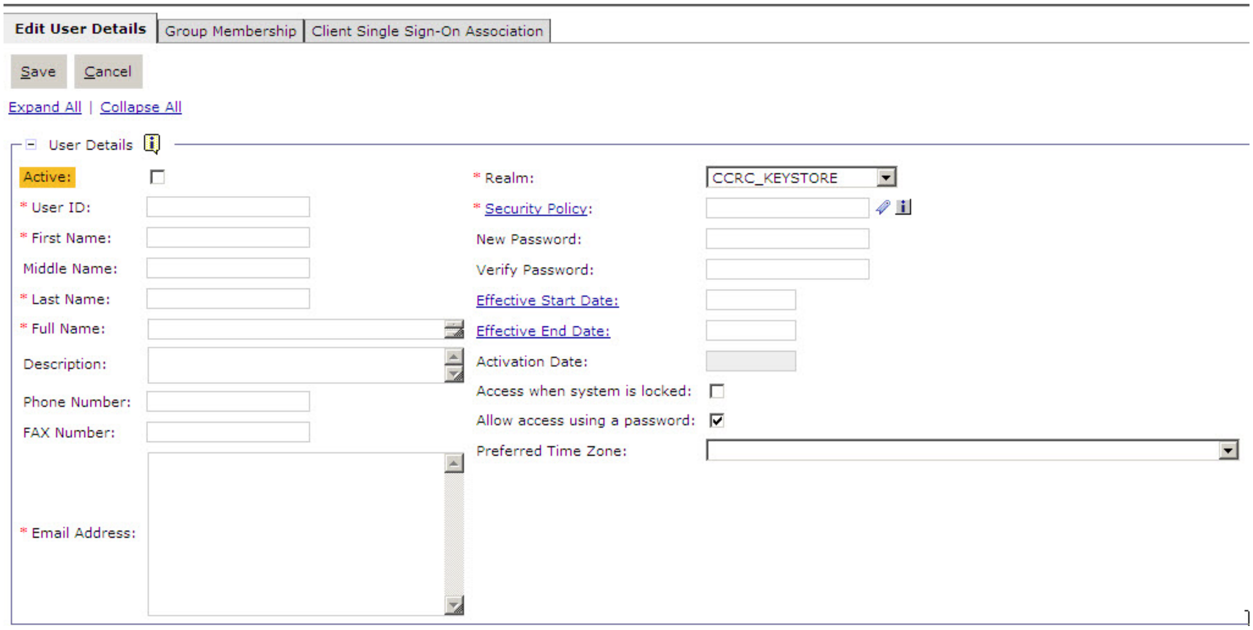
Additionally, dynamic extensibility provides the ability to populate transactions using pre-defined dynamic variables that set the value of a field based on the current date or user's principal data. Examples include a system administrator setting a global level dynamic extension to populate with a current user's name or setting a date field to populate with the current date, as well as an individual user setting a user level dynamic extension to populate with his/her name.

5.5 Users and Groups

5.5.1 Users

An Administrator has the ability to search for, add, edit, and deactivate users (see ***Figure 5-15: Edit User Details Window***).

Figure 5-135: Edit User Details Window



Active:	□	* Realm:	CCRC_KEYSTORE
* User ID:		* Security Policy:	
* First Name:		New Password:	
Middle Name:		Verify Password:	
* Last Name:		Effective Start Date:	
* Full Name:		Effective End Date:	
Description:		Activation Date:	
Phone Number:		Access when system is locked:	□
FAX Number:		Allow access using a password:	☑
* Email Address:		Preferred Time Zone:	

5.5.1.1 Creating a New User

A new user account can be created on the Edit User Details tab (see ***Figure 5-15: Edit User Details Window***). Here, the Administrator has the ability to add information about the user as well as security policies that may be applied to the user.

When creating a new user, certain fields are required and must be populated (see ***Figure 5-16: New User Fields***). Other fields are optional and can be populated at the discretion of the Agency.

Figure 5-146: New User Fields

Field	Description
Required	
User ID	The UserId that the user will access the system with.
New Password/Verify Password	The password that the user will access the system with.
First Name	The first name of the user.
Last Name	The last name of the user.
Full Name	Full name of the user.
Email Address	The email address for the user.
Security Policy	The security policies that will apply to user.
Optional	
Active Checkbox	The box is checked if the user is Active in the system.
Middle Name	The middle name of the user.
Access when System is Locked Checkbox	If box is checked, the user is able to access a locked system.
Description	Description/notes for the user.
Phone Number	The phone number of the user.
Fax Number	The fax number of the user.
Effective Start Date	The effective start date that the user will have access.
Effective End Date	The effective end date that the user will have access.
Email Address	The email address of the user.

Once all necessary and optional information is entered, the Administrator saves the information in the system and the new user is now able to access the system. If the password is listed as an invalid password, it will be rejected and another password will have to be used.

Note — The Active box must be checked for the user to be Active in the system.

5.5.1.2 Deactivating a User

An Administrator has the ability to deactivate a user so that he/she will no longer be able to access the CCRC. A user is deactivated when the Active box is unchecked on the Edit User Details tab.

Once the Administrator clicks the “Save” button, the user account has been deactivated successfully and the user no longer has access to the CCRC system.

5.5.1.3 Reactivating a User

This is done in much the same way as deactivating a user. If a user has been previously deactivated but now needs access to the system, the Administrator has the ability to reactivate that user’s account.

To reactivate the user, the Administrator must click the “Active” checkbox so that the checkbox is checked. Once the Administrator clicks the “Save” button, the user account has been reactivated successfully and the user is now able to access the system.

5.5.2 Groups

There are five groups of users that come preconfigured and are able to navigate through the CCRC system. These five groups are listed below:

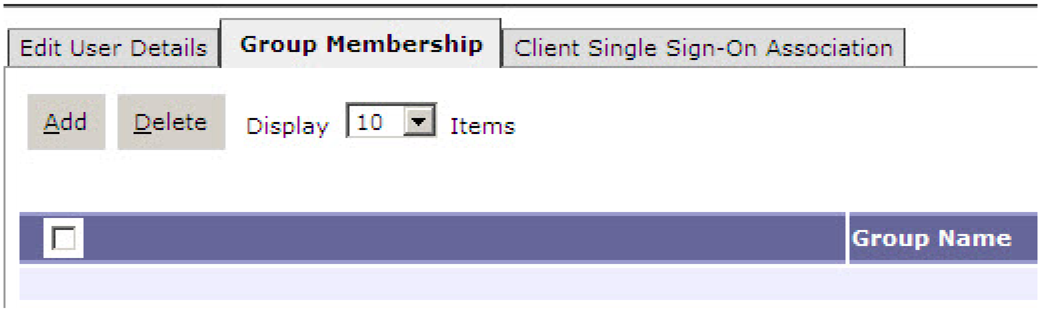
- **Administrators** have the ability to load SAM extract files, administer user accounts, and configure the system.
- **Everybody** has the ability to query non-sensitive vendor information.
- **Secure Assessors** have the ability to view sensitive vendor information (i.e., Lockbox number, Bank account and TIN).
- **Requesters** have the ability to use the ‘Submit’ button for new vendor submissions to subscribing agency applications.
- **Approvers** have the ability to use both the ‘Submit’ button for new vendor submissions as well as the ‘Accept’ button to initiate synchronization with vendors that already exist within subscribing agency applications.

By associating a user to a certain group, the Administrator is essentially applying certain permissions to that user. There is the possibility within CCRC to add groups, although it is not encouraged.

Note—All users should be assigned to the “Everybody” group at a minimum.

(See ***Figure 5-17: Group Window***)

Figure 5-157: Group Window



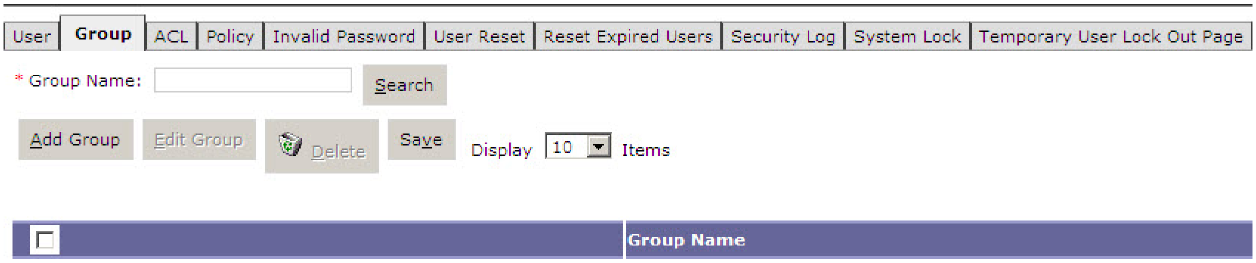
An Administrator has the ability to view, edit and delete users in a specific group.

The Group Members Window can be accessed by the following path:

Security/Security Maintenance/Group

Figure 5-18: Group Members Window displays the Group Members window.

Figure 5-168: Group Members Window

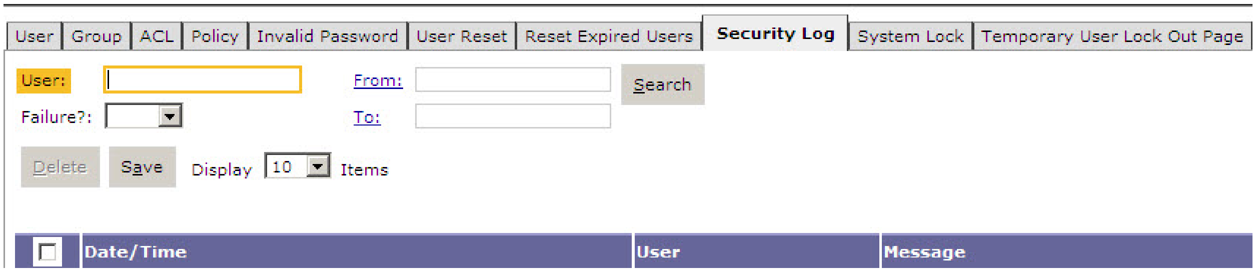


5.6 Security Log

Security logs are created when users attempt to login to the CCRC. The Administrator is able to view these logs to monitor security violations committed in the system. The Security Log can be accessed through the Security Maintenance Window (see ***Figure 5-4: Security Maintenance Window***).

The Administrator can search for all security violations committed in the system or for the security violations committed by a specific user (see ***Figure 5-19: Security Log).***

Figure 5-179: Security Log

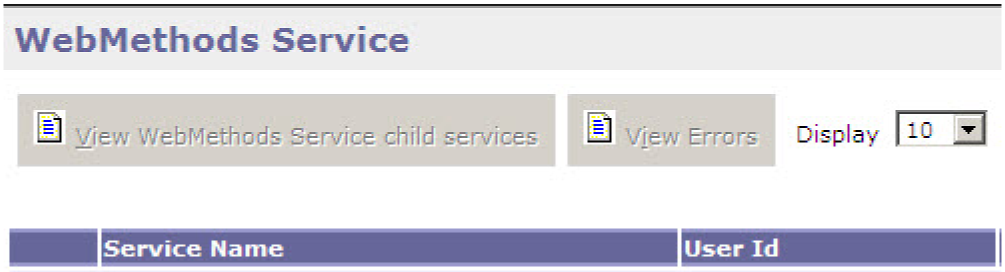


5.7 Vendor Data

5.7.1 Audit

The Administrator has the ability to look at an Audit log for a given vendor (see ***Figure 5-20: Audit Window***). The Audit log is accessed by selecting a vendor from the CCRC Data Maintenance Page and clicking the audit button. From this screen it is possible to see the integration history for a particular vendor in CCRC. For example, an administrator can determine what if any errors might have resulted in attempting to publish a particular vendor. Other information accessible through this page would include the Service Name, User ID associated with publication, Server ID, and status.

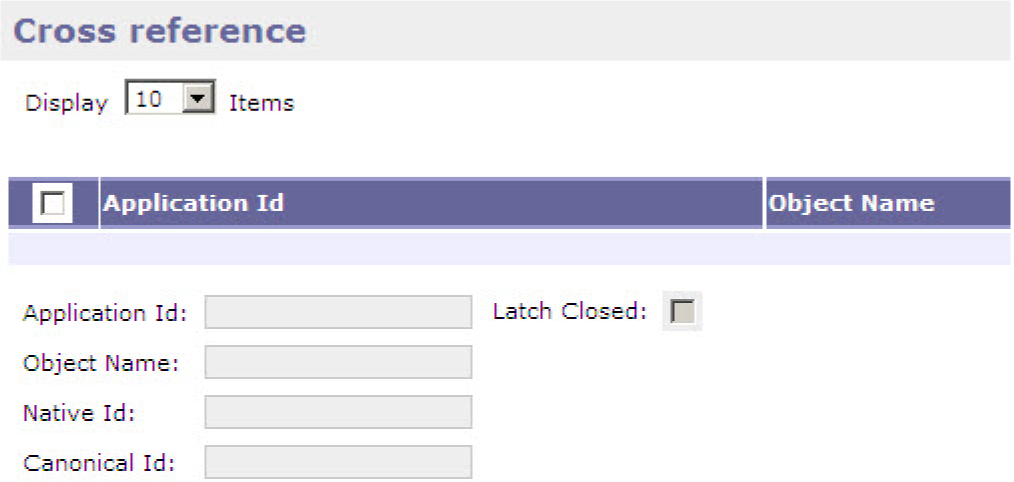
Figure 5-20: Audit Window



5.7.2 Cross References

In addition to being able to assess the history of a particular vendor through the audit button, the Cross Reference functionality provides valuable insight to an administrator (see ***Figure 5-21: Cross-Reference Window***). The Cross Reference page is accessed by selecting a vendor from the CCRC Data Maintenance screen and clicking the Cross Reference button. The Cross Reference screen allows the administrator to link between applications that are connected via webMethods. This means that the administrator is able to link a given vendor in CCRC to a given vendor entity stored in Pegasys. For example, after selecting the cross reference screen for a given vendor, the administrator can change the application ID in the search section at top to Pegasys and find out what vendor is getting updated in Pegasys e.g. Vendor Code = ABC, Address Code= 1. This identification of the vendor entity will be found in the Native ID field. For the example previously mentioned, the Native ID would be displayed as ABC/1. If the application ID were changed back to CCRC, the Native ID would return to the DUNS/DUNS +4 since this is the identity within CCRC. Object Name and Canonical ID are also displayed as information for the administrator.

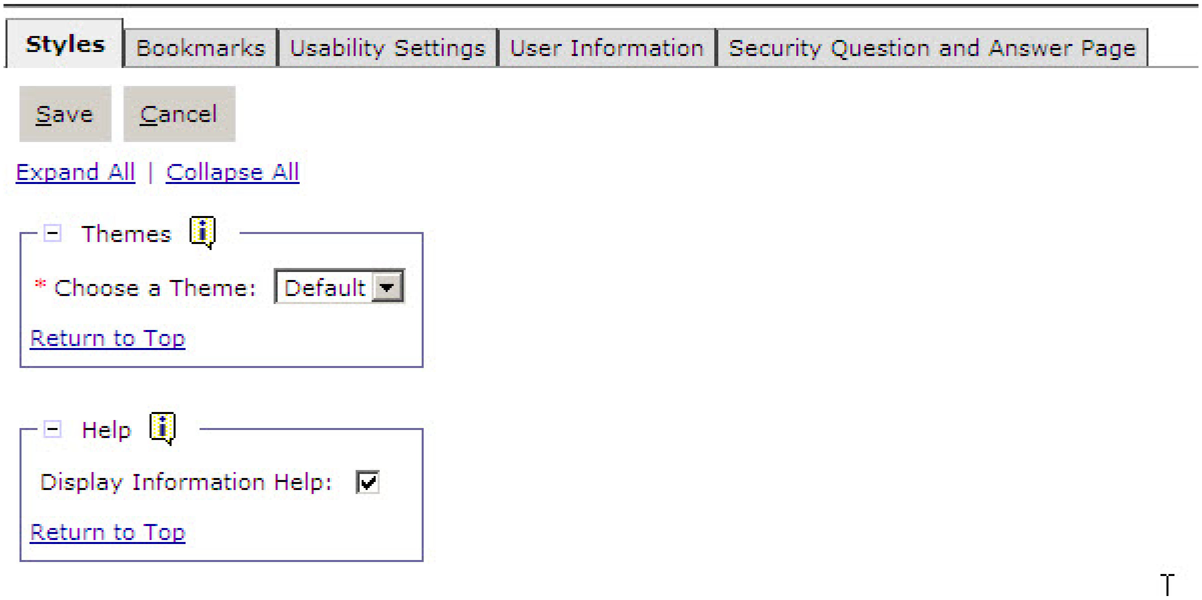
Figure 5-21: Cross-Reference Window



5.8 CCRC Preferences

The CCRC allows for users to change the theme of the CCRC system, see ***Figure 5-22: Preferences***.

Figure 5-22: Preferences



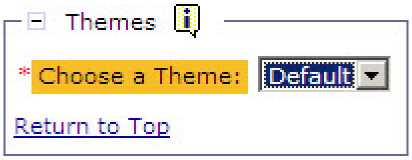
* Choose a Theme: Default

Display Information Help: ☑

5.8.1 Themes

The user has the option to change the overall look and feel, based on two pre-set Themes Default and Simple (see ***Figure 5-23: Themes***).

Figure 5-183: Themes

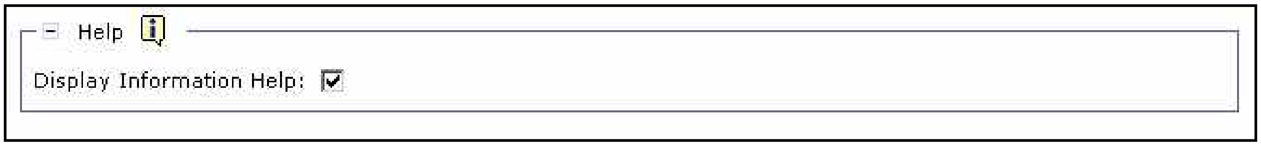


* Choose a Theme: Default

5.8.2 Help

The user has the option to display the help information on the page (see ***Figure 5-24: Help***).

Figure 5-194: Help



Display Information Help: ☑

5.9 Vendor Management/CCRC: SAM Entity Management Enhancements in 7.1.2 Upgrade

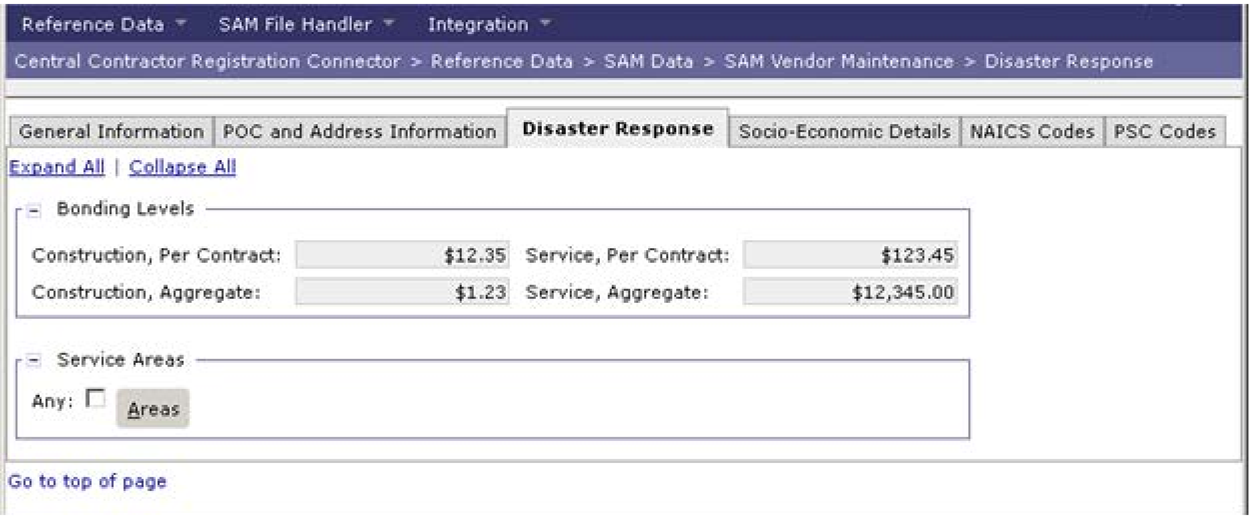
5.9.1 Capture Additional Data

This enhancement introduces changes to both Pegasys and the Central Contractor Registration Connector (CCRC) module. For Pegasys, the updates include terminology changes throughout the system to align with the new SAM initiative. The SAM initiative also captures more data elements than were previously recorded by the SAM predecessor, CCR. The additional data elements, changed data elements, and new capabilities that are supported for these elements include:

- The optional ability to record a Bureau for an Agency Location Code
- A new overrideable warning that alerts you of a vendor's Delinquent Federal Debt
- The addition of a reference-backed County maintenance table in order to validate counties entered on vendor records
- The addition of Disaster Response information to the vendor record ***[Figure 5-25]***
- Increasing the database length of vendor names and postal codes throughout the system

The addition of a fourth address line to the "Standard" address format ***[Figure 5-26]***

Figure 5-205: Vendor Record Contains Disaster Response Information

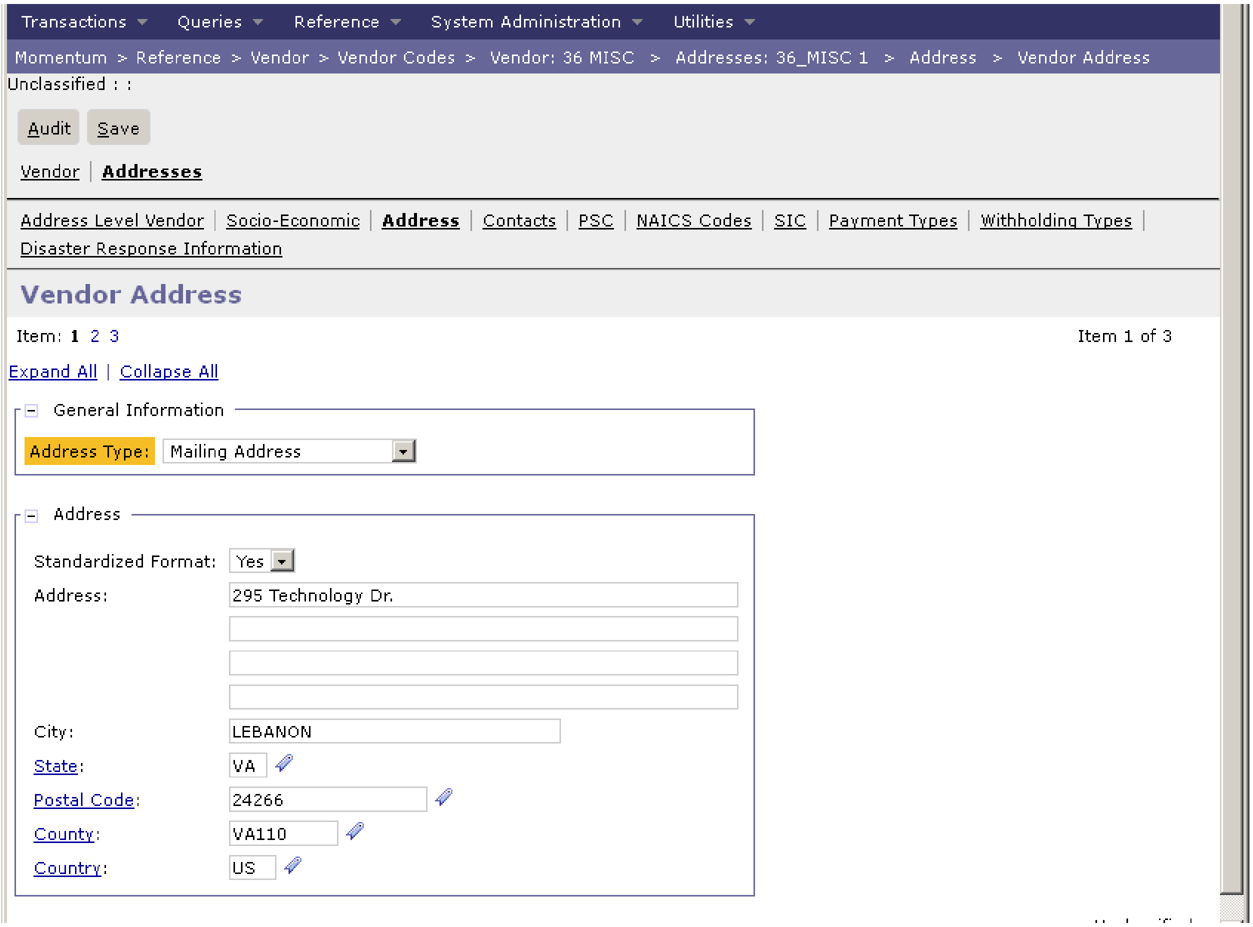


Construction, Per Contract: $12.35 Service, Per Contract: $123.45

Construction, Aggregate: $1.23 Service, Aggregate: $12,345.00

Any: □

Figure 5-216: Fourth Address Line Added to the “Standard” Address Format


Transactions
Queries
Reference
System Administration
Utilities
Momentum > Reference > Vendor > Vendor Codes > Vendor: 36 MISC > Addresses: 36_MISC 1 > Address > Vendor Address
Unclassified : :
Audit
Save
Vendor | Addresses
Address Level Vendor | Socio-Economic | Address | Contacts | PSC | NAICS Codes | SIC | Payment Types | Withholding Types | Disaster Response Information
Item: 1 2 3
Item 1 of 3
Expand All | Collapse All

Vendor Address

General Information

Address Type: Mailing Address

Address

Standardized Format: Yes

Address: 295 Technology Dr.

City: LEBANON

State: VA

Postal Code: 24266

County: VA110

Country: US

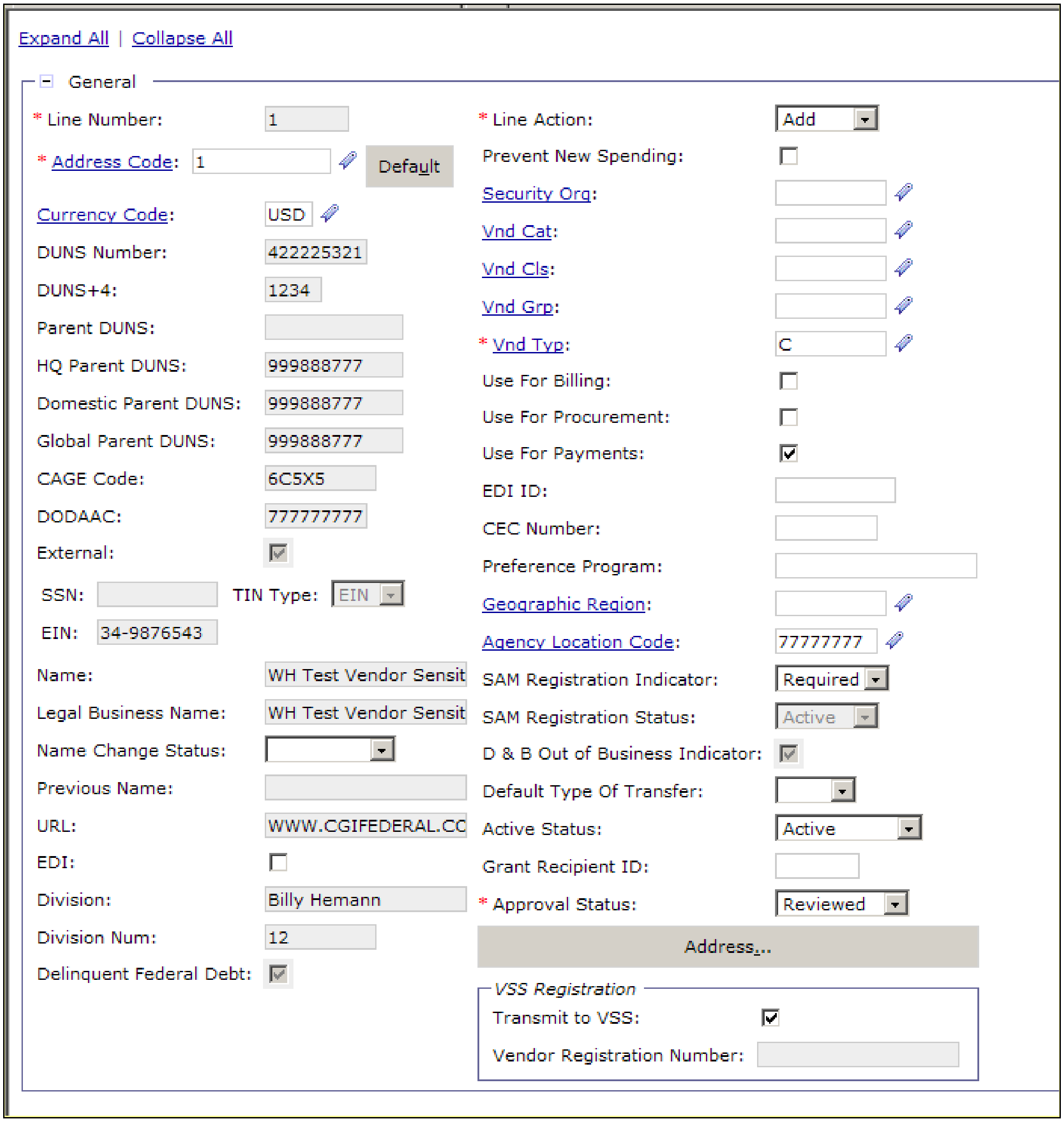
5.9.2 Data Import Capabilities

As part of the Integrated Acquisition Environment (IAE) SAM initiative, new file formats were established for the extraction of vendor data from SAM, to eventually replace the legacy SAM file formats used by CCR. SAM introduces new data elements, such as delinquent debt and disaster response indicators, that were not previously available in CCR. The CCRC 7.1.2 release includes configuration options in CCRC and the integrations to allow CCRC to process either the legacy (SAM) extract file format or the new SAM extract file format. This enhancement adds no extra steps to GSA’s current business process.

5.9.3 Display and Search by DODAAC

Allows the ability to register vendors by DODAAC in VCSS (for those vendors previously registered in FedReg who might have a DODAAC in place of a DUNS) [Figure 5-27], and display and search the information in VCSS and Pegasys [Figure 5-28]. A user will be able to search for vendors by DODAAC on the vendor reference tables.

Figure 5-227: VCSS Ability to Register Vendors by DODAAC



Expand All | Collapse All

⊟ General

* Line Number: 1

* Address Code: 1 Default

Currency Code: USD

DUNS Number: 422225321

DUNS+4: 1234

Parent DUNS:

HQ Parent DUNS: 999888777

Domestic Parent DUNS: 999888777

Global Parent DUNS: 999888777

CAGE Code: 6C5X5

DODAAC: 777777777

External: ☑

SSN: TIN Type: EIN

EIN: 34-9876543

Name: WH Test Vendor Sensit

Legal Business Name: WH Test Vendor Sensit

Name Change Status:

Previous Name:

URL: WWW.CGIFEDERAL.CC

EDI: □

Division: Billy Hemann

Division Num: 12

Delinquent Federal Debt: ☑

* Line Action: Add

Prevent New Spending: □

Security Org:

Vnd Cat:

Vnd Cls:

Vnd Grp:

* Vnd Typ: C

Use For Billing: □

Use For Procurement: □

Use For Payments: ☑

EDI ID:

CEC Number:

Preference Program:

Geographic Region:

Agency Location Code: 77777777

SAM Registration Indicator: Required

SAM Registration Status: Active

D & B Out of Business Indicator: ☑

Default Type Of Transfer:

Active Status: Active

Grant Recipient ID:

* Approval Status: Reviewed

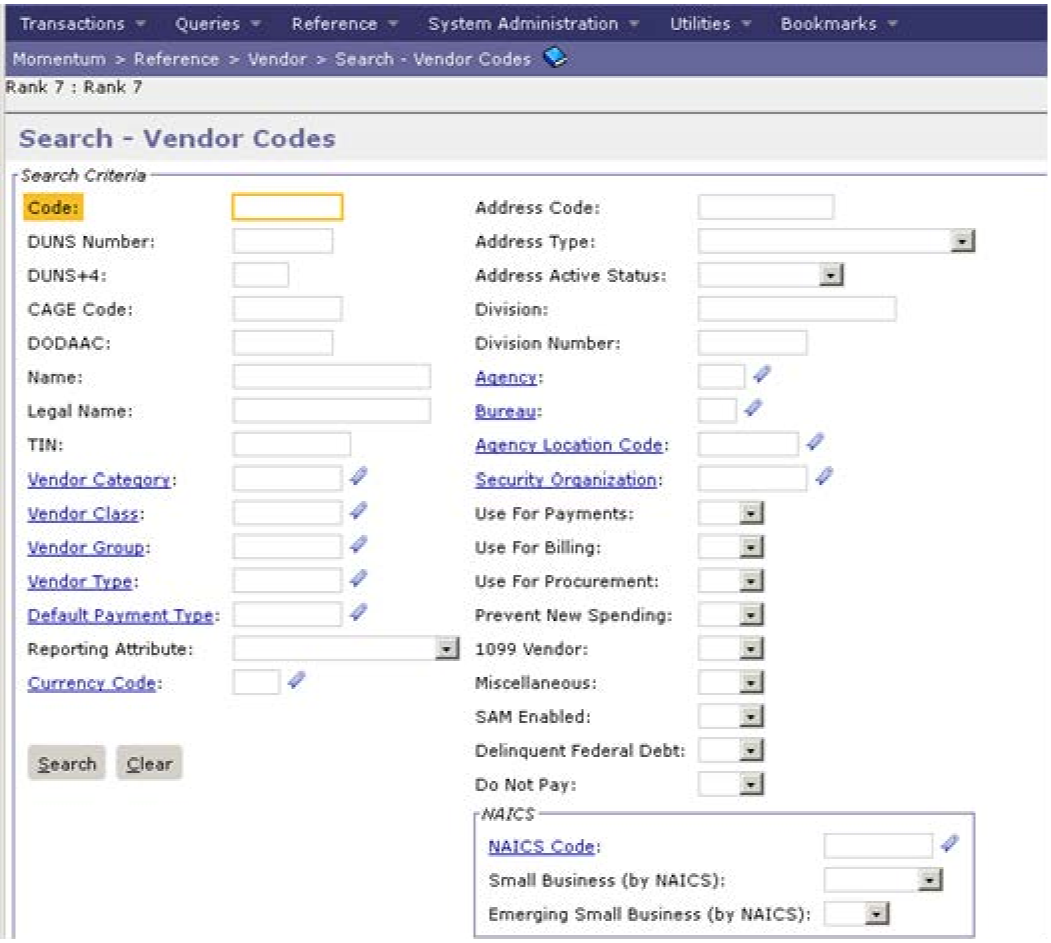
Address...

VSS Registration

Transmit to VSS: ☑

Vendor Registration Number:

Figure 5-238: Ability to Display and Search by DODAAC


Transactions
Queries
Reference
System Administration
Utilities
Bookmarks
Momentum > Reference > Vendor > Search - Vendor Codes
Rank 7 : Rank 7
Search - Vendor Codes
Search Criteria
Code:
DUNS Number:
DUNS+4:
CAGE Code:
DODAAC:
Name:
Legal Name:
TIN:
Vendor Category:
Vendor Class:
Vendor Group:
Vendor Type:
Default Payment Type:
Reporting Attribute:
Currency Code:
Search
Clear
Address Code:
Address Type:
Address Active Status:
Division:
Division Number:
Agency:
Bureau:
Agency Location Code:
Security Organization:
Use For Payments:
Use For Billing:
Use For Procurement:
Prevent New Spending:
1099 Vendor:
Miscellaneous:
SAM Enabled:
Delinquent Federal Debt:
Do Not Pay:
NAICS
NAICS Code:
Small Business (by NAICS):
Emerging Small Business (by NAICS):