# United States Department of Agriculture Central Contractor Registration Connector (CCRC) Pegasys 7.5.1 User Guide



Contract: # HHSN316201200011W

Order # AG-3144-D-16-0278

Version 5.00

May 2018

## Table of Contents

[Table of Contents 1](#_Toc511814706)

[Table of Figures 4](#_Toc511814707)

[Table of Tables 5](#_Toc511814708)

[Revision Log 6](#_Toc511814709)

[1 CCRC Introduction 7](#_Toc511814710)

[2 CCRC Overview 8](#_Toc511814711)

[2.1 Central Contractor Registration Connector (CCRC) 8](#_Toc511814712)

[2.2 Initial Load and Initial Vendor Selection 8](#_Toc511814713)

[2.3 CCRC User Interface 9](#_Toc511814714)

[2.4 CCRC Import Batch Job 9](#_Toc511814715)

[2.4.1 New Vendors 9](#_Toc511814716)

[2.4.2 Updated Vendor 9](#_Toc511814717)

[2.4.3 Inactivated/Deleted Vendors 10](#_Toc511814718)

[2.5 CCRC Publishing Agent 10](#_Toc511814719)

[2.6 Subscribing Agent/Agency Applications 10](#_Toc511814720)

[2.7 Security 11](#_Toc511814721)

[3 Loading Data with SAM 12](#_Toc511814722)

[3.1 SAM Data Load 12](#_Toc511814723)

[3.1.1 Exporting SAM File 12](#_Toc511814724)

[3.1.2 Processing the SAM File 13](#_Toc511814725)

[3.1.3 Processing Options 14](#_Toc511814726)

[3.1.4 Removing the SAM File from CCRC 15](#_Toc511814727)

[3.2 Initial Vendor Selection 15](#_Toc511814728)

[3.2.1 Select Vendors to Enable 15](#_Toc511814729)

[3.2.2 Execute Initial File Creation Batch Process 18](#_Toc511814730)

[3.2.3 Initial Vendor Selection Script and Synchronization 18](#_Toc511814731)

[3.3 Daily Update Files 19](#_Toc511814732)

[3.3.1 Daily CCRC Data Load 19](#_Toc511814733)

[3.3.2 New Vendor 20](#_Toc511814734)

[3.3.3 Existing Vendor 20](#_Toc511814735)

[3.3.4 Deletion and Deactivation 21](#_Toc511814736)

[4 Searching/Publishing Vendors 22](#_Toc511814737)

[4.1 Searching for Vendors 22](#_Toc511814738)

[4.1.1 Vendor Information Query 22](#_Toc511814739)

[4.1.2 Search for Another Vendor 24](#_Toc511814740)

[4.1.3 Case Insensitive Queries 24](#_Toc511814741)

[4.2 Publishing Vendors 25](#_Toc511814742)

[4.2.1 Publishing New Vendor Information 25](#_Toc511814743)

[4.2.1.1 New Vendor Submissions 27](#_Toc511814744)

[4.2.2 Publishing Updates 27](#_Toc511814745)

[4.3 Integration 27](#_Toc511814746)

[4.3.1 Audit 28](#_Toc511814747)

[4.3.2 Cross References 28](#_Toc511814748)

[5 System Administrator 30](#_Toc511814749)

[5.1 CCRC Sign In 30](#_Toc511814750)

[5.2 Data Loads 30](#_Toc511814751)

[5.2.1 CCRC Holiday 30](#_Toc511814752)

[5.3 Batch Execution 31](#_Toc511814753)

[5.3.1 Batch Job Status 31](#_Toc511814754)

[5.4 Security Policies 32](#_Toc511814755)

[5.4.1 Adding, Deleting and Editing Policies 33](#_Toc511814756)

[5.4.2 Passwords 35](#_Toc511814757)

[5.4.2.1 Invalid Passwords 36](#_Toc511814758)

[5.4.3 Reset a Locked User Account 36](#_Toc511814759)

[5.4.4 System Locking 36](#_Toc511814760)

[5.4.5 Secure Data 37](#_Toc511814761)

[5.4.6 Dynamic Extensibility 37](#_Toc511814762)

[5.5 Users and Groups 37](#_Toc511814763)

[5.5.1 Users 37](#_Toc511814764)

[5.5.1.1 Creating a New User 38](#_Toc511814765)

[5.5.1.2 Deactivating a User 39](#_Toc511814766)

[5.5.1.3 Reactivating a User 39](#_Toc511814767)

[5.6 Security Log 40](#_Toc511814768)

[5.7 Vendor Data 40](#_Toc511814769)

[5.7.1 Audit 40](#_Toc511814770)

[5.7.2 Cross Reference 41](#_Toc511814771)

[5.8 Enhancements Included in 7.5.1 Upgrade 41](#_Toc511814772)

[5.8.1 Link Address Codes 41](#_Toc511814773)

[5.8.2 Cross Reference Enhancement 42](#_Toc511814774)

[5.8.3 Vendor Mailing Address Requirement Accommodation 42](#_Toc511814775)

[5.8.4 Display Updated Purpose of Registration Values 42](#_Toc511814776)

[5.8.5 Security Assertion Markup Language 42](#_Toc511814777)

[5.8.6 System for Award Management Phase 3 42](#_Toc511814778)

[5.8.7 Vendor Update Support 43](#_Toc511814779)

## Table of Figures

[Figure 1: CCRC Cycle 8](#_Toc511814781)

[Figure 2: File Maintenance Window 13](#_Toc511814782)

[Figure 3: File Processing 14](#_Toc511814783)

[Figure 4: Initial Vendor Selection Example 15](#_Toc511814784)

[Figure 5: SAM Vendor Maintenance Table 16](#_Toc511814785)

[Figure 6: Available List of Vendors 18](#_Toc511814786)

[Figure 7: SAM Vendor Maintenance Table 22](#_Toc511814787)

[Figure 8: Case Insensitive Query in CCRC 25](#_Toc511814788)

[Figure 9: CCRC Vendor Detail 26](#_Toc511814789)

[Figure 10: Publishing Update Example 27](#_Toc511814790)

[Figure 11: WebMethods Error Screen 28](#_Toc511814791)

[Figure 12: Auditing 28](#_Toc511814792)

[Figure 13: Cross Reference Window 29](#_Toc511814793)

[Figure 14: CCRC Sign In Page 30](#_Toc511814794)

[Figure 15: CCRC Holiday Example 30](#_Toc511814795)

[Figure 16: CCRC Holiday Window 31](#_Toc511814796)

[Figure 17: Batch Job Status Window 31](#_Toc511814797)

[Figure 18: Security Maintenance Policy Window 32](#_Toc511814798)

[Figure 19: Adding a Security Policy 33](#_Toc511814799)

[Figure 20: Delete Policy 35](#_Toc511814800)

[Figure 21: Invalid Password Window 36](#_Toc511814801)

[Figure 22: System Lock Window 37](#_Toc511814802)

[Figure 23: Edit User Details Window 38](#_Toc511814803)

[Figure 24: Security Log 40](#_Toc511814804)

[Figure 25: Audit Window 40](#_Toc511814805)

[Figure 26: Cross Reference Window 41](#_Toc511814806)

## Table of Tables

[Table 1: Upload Parameters 13](#_Toc511814807)

[Table 2: CCRC Data Maintenance Partners 16](#_Toc511814808)

[Table 3: Parameters 20](#_Toc511814809)

[Table 4: SAM Extract Codes 20](#_Toc511814810)

[Table 5: Search Parameters 23](#_Toc511814811)

[Table 6: Batch Job Status Parameters 32](#_Toc511814812)

[Table 7: Security Maintenance Information 33](#_Toc511814813)

[Table 8: New User Fields 38](#_Toc511814814)

## Revision Log

| **Date** | **Version No.** | **Description** | **Author** | **Reviewer** | **Review** |
| --- | --- | --- | --- | --- | --- |
| 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 Mathew Randall | Karin Keswani and Mathew Randall | 11/2014 |
| 1/2015 | Final | Figures were updated to reflect correct sequential order: figure numbers have been corrected in paragraphis to reference correct figures. Updated BPN to SAM in applicable. In section 5.4.6, Figures 5-13 and Figure 5-14 | Karin Keswani, Benjamin Bowden | Karin Keswani, Benjamin Bowden | 1/2015 |
| 10/2017 | 4.0 | Revision 4.0 – updated to reflect the following changes for Pegasys 7.5.1 Upgrade:  Applied 508 standards.  Updated screen shots and provided Alternate Text.  Updated section 5.8 to reflect multiple enhancements included in the 7.5.1 Upgrade. | Kevin Hillman | Nick Longworth, Jenny Lewis, Marice Grissom | 9/2017 – 10/2017 |
| 5/2018 | 5.0 | No additional changes. | Kevin Hillman | Jenny Lewis, Marice Grissom | 5/2018 |

## 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

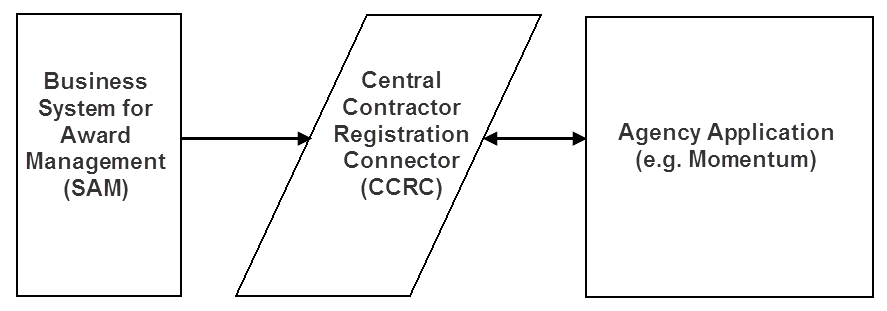
## CCRC Overview

### 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 1: CCRC Cycle



### 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).

### 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.

### 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.

#### 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.

#### 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.

#### 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).

### 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 USDA 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 USDA 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.

### Subscribing Agent/Agency Applications

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

### Security

The CCRC allows the Administrator to create and edit user accounts, including the set up of user ids and passwords. 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.

## Loading Data with 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).

### SAM Data Load

#### 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).

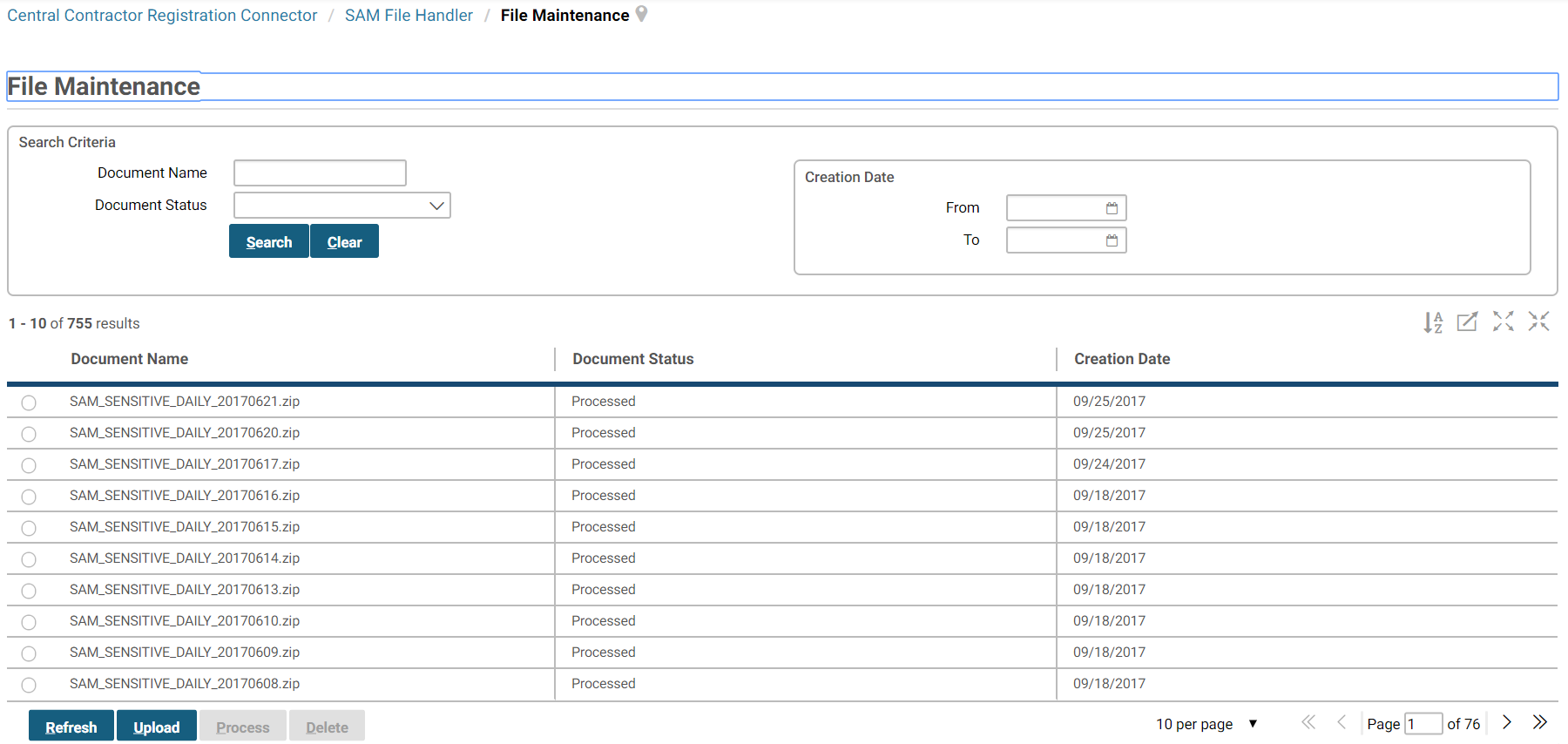
There are three types of files available:

* **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.

**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.

**NOTE:** File Upload and Processing can be accessed on the File Maintenance window (see **Figure 2**) by selecting **SAM File Handler → File Maintenance**.

Figure 2: File Maintenance Window



Steps to Upload a SAM Extract File:

1. Select the **Upload** button.
2. Browse for the desired SAM Extract file and select the **Upload** button.

Table 1: Upload Parameters

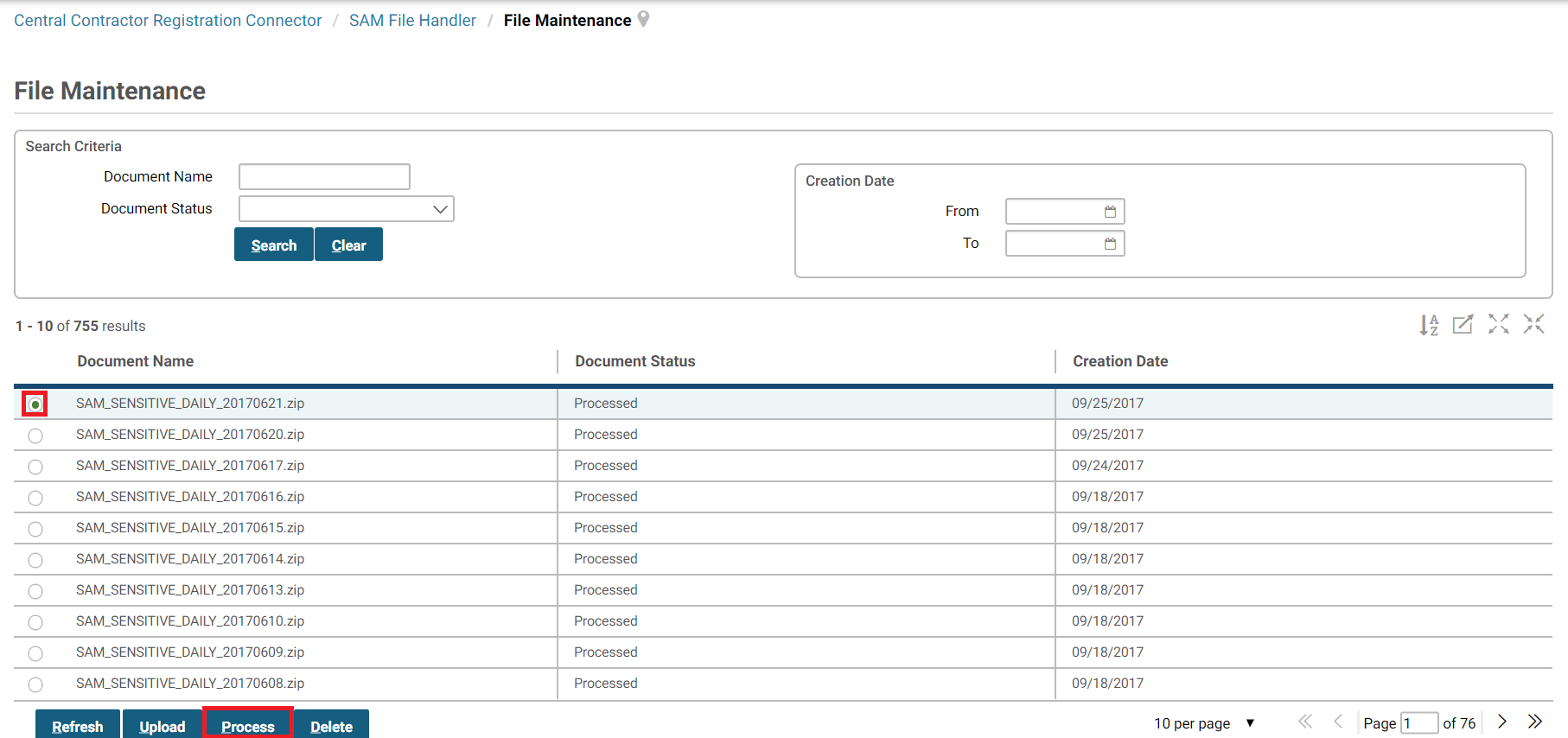
| **Field** | **Field Description** |
| --- | --- |
| Description | The user has the ability to enter a description of the file for future reference. |
| Document | The filename/path of the extract file to be loaded. This parameter is required. |

#### Processing the SAM File

Although a user 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.

**Figure 3** displays the File Maintenance window, where SAM files can be processed.

Figure 3: File Processing



Steps to Process a SAM Extract File:

1. Select the file intended for processing
2. Select the **Process** button
3. 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.

#### 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)

#### Removing the SAM File from CCRC

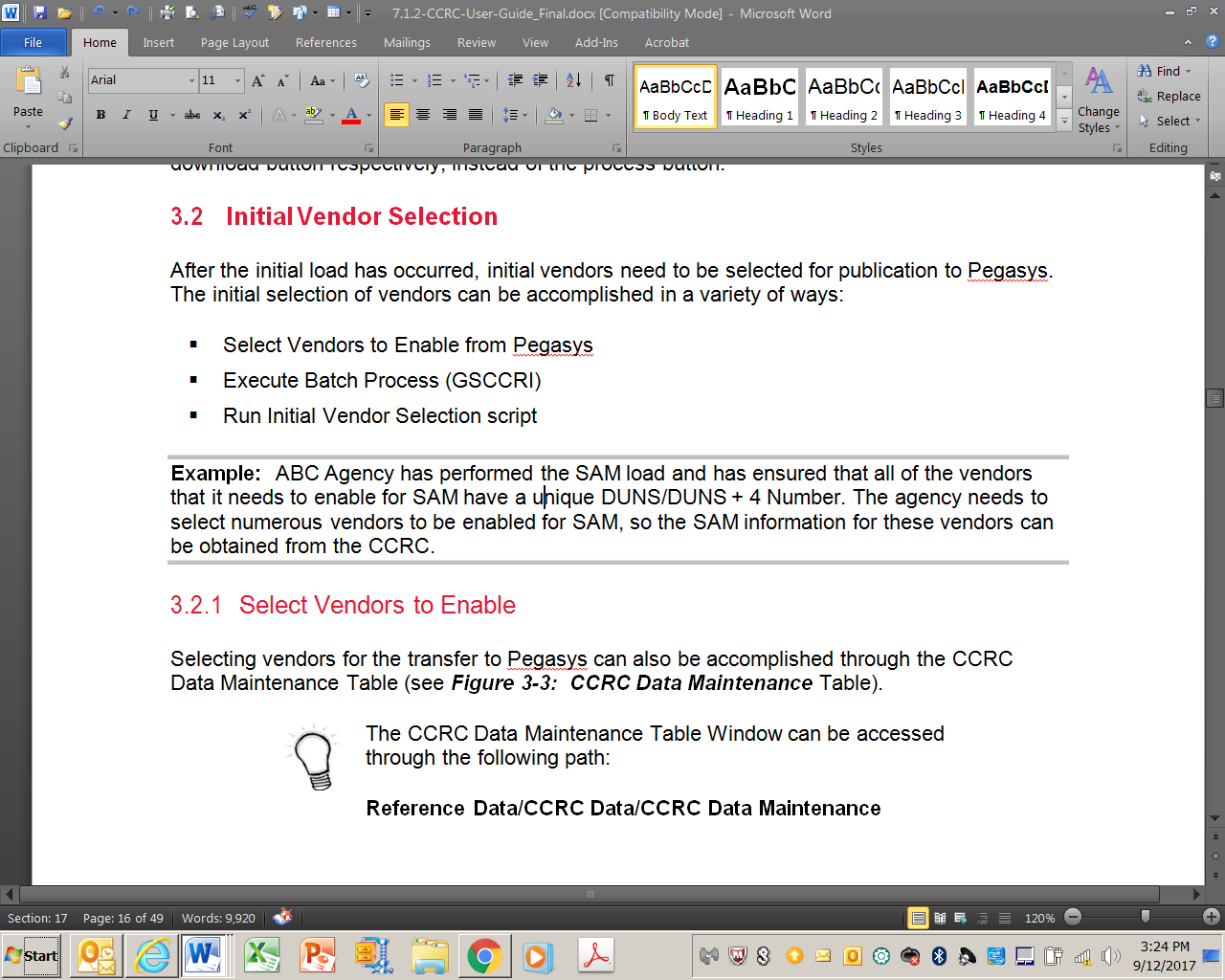
This is not advised, but a user with required permissions can remove a file from the file list or entirely remove the file from the system. To delete a file entry from the file list or remove the file from the system, select the desired file by following the same steps when processing the file, then select the Delete button instead of the Process button.

### 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

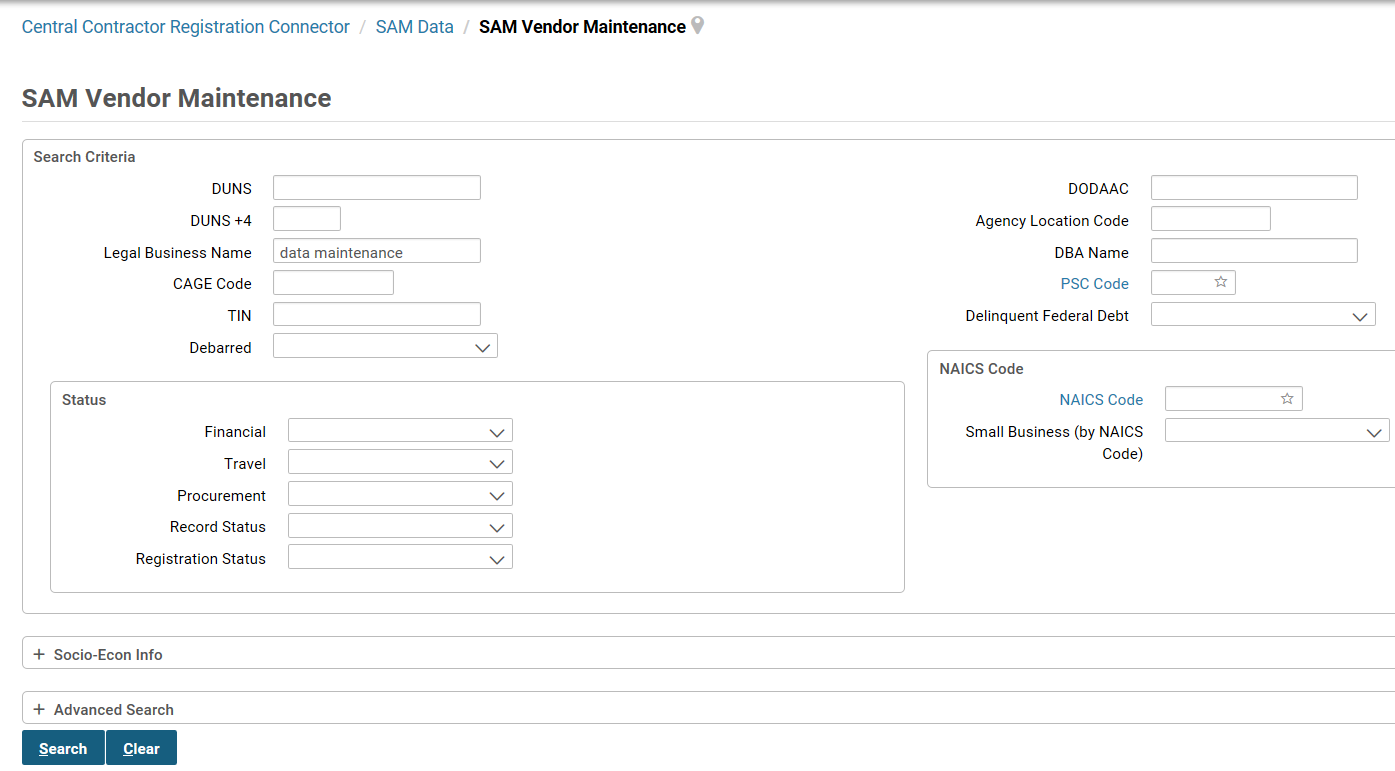
Figure 4: Initial Vendor Selection Example



#### Select Vendors to Enable

Selecting vendors for the transfer to Pegasys can also be accomplished through the SAM Vendor Maintenance Table (see **Figure 5**).

Figure 5: SAM Vendor Maintenance Table



Through the SAM Vendor 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 6**).

Table 2: 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 Business 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. |
| 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 6: Available List of Vendors



The Administrator can then “view” each vendor and either submit or approve the vendor to Pegasys. For more on submitting and approving vendors, see **Section 4.2**.

#### 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 Guidefor 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.

#### 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.

### 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.

#### 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.

**NOTE:** The SAM File Upload can be accessed by selecting **SAM File Handler → File Maintenance**.

Steps to Upload a SAM Extract File:

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

Steps to Process a SAM Extract File:

1. Select the plus expansion button next to the CCRC subfolder
2. Select the file intended for processing
3. Select 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).

Table 3: 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 **Table 4**).

Table 4: 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) |

#### 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.

#### 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.

#### 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.

## Searching/Publishing Vendors

### 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.

#### Vendor Information Query

Users may search for vendors using a variety of search criteria, including any combination of the following parameters (Wildcards are allowed in the beginning, middle, or end. An asterisk (\*) is for multiple characters, a question mark (?) is for single characters. See **Figure 7**.

Figure 7: SAM Vendor Maintenance Table

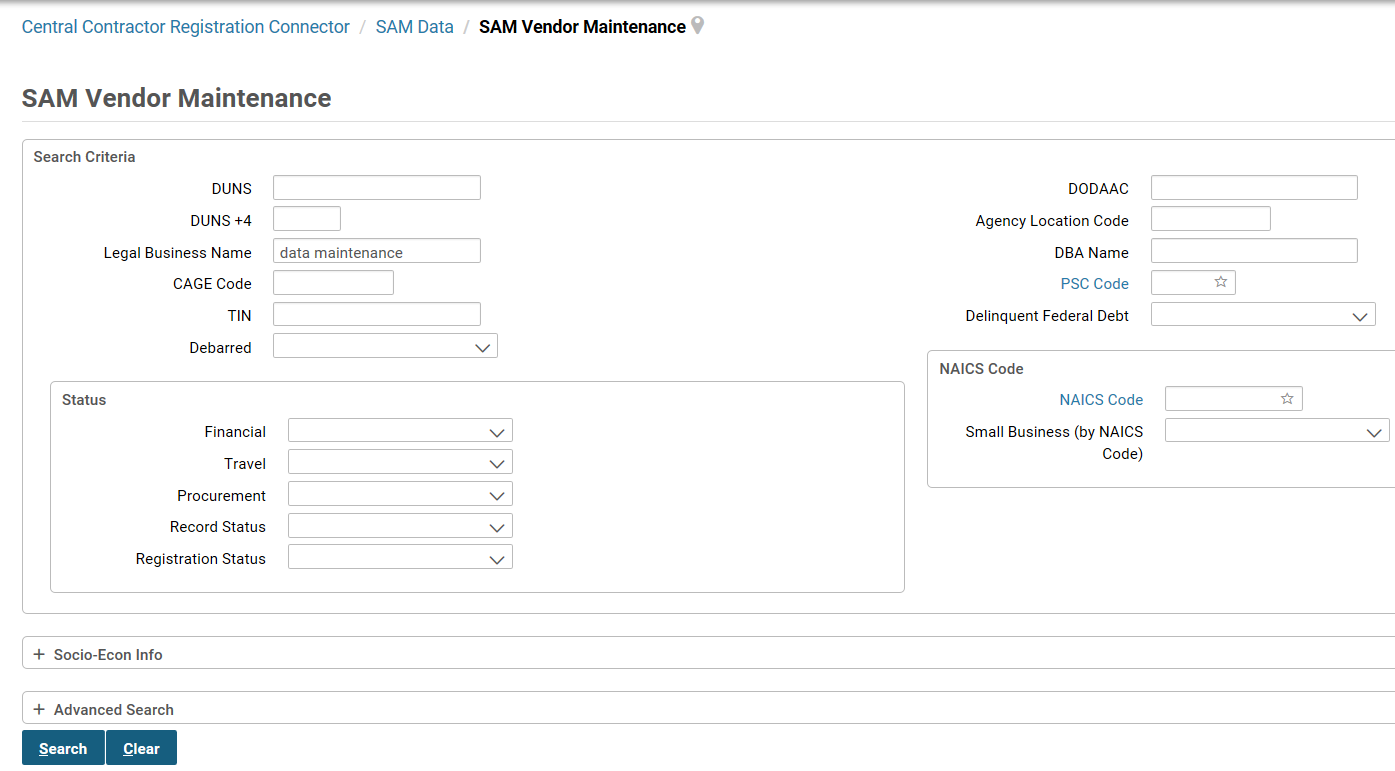


Table 5: Search Parameters

| **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 Business 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.

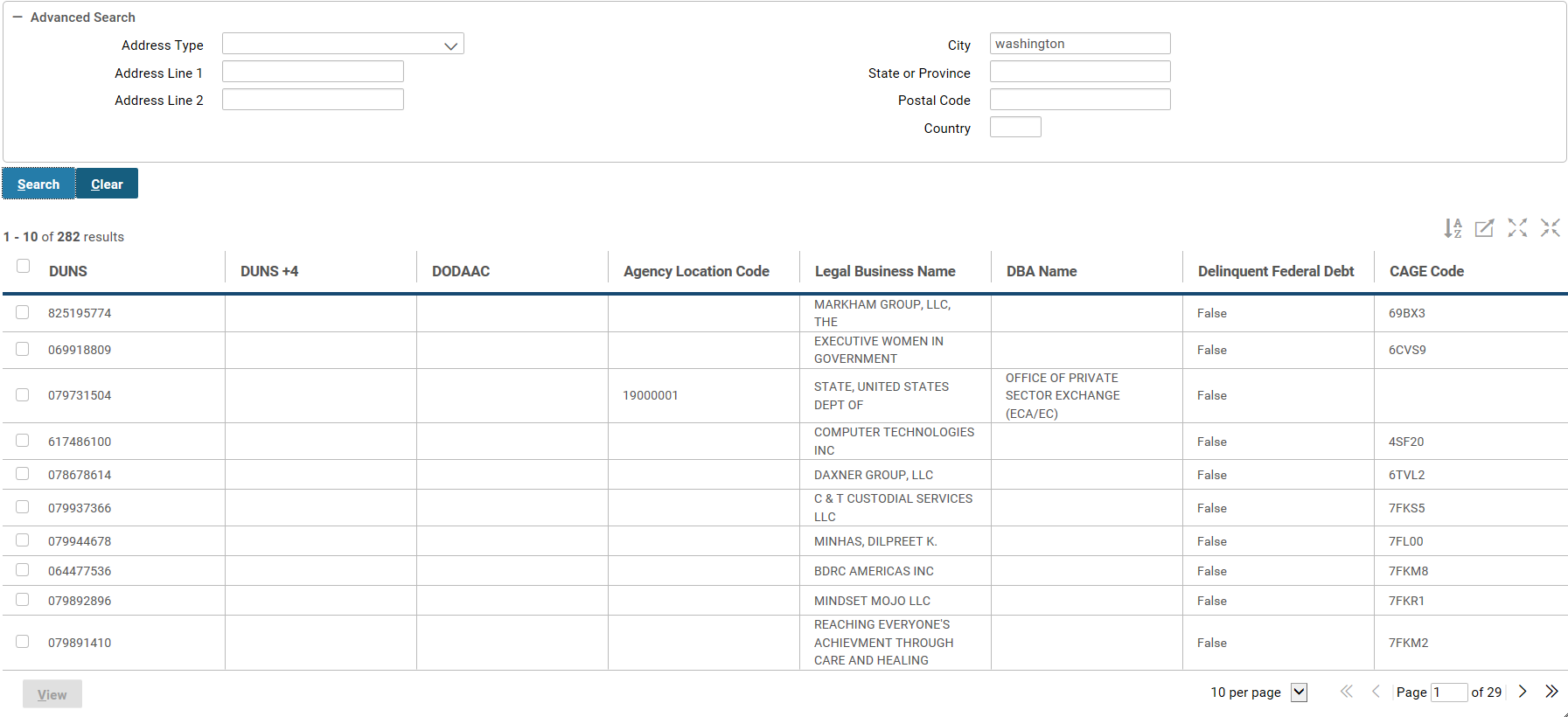
#### Search for Another Vendor

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.

#### 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 **Figure 8** below.

Figure 8: Case Insensitive Query in CCRC



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

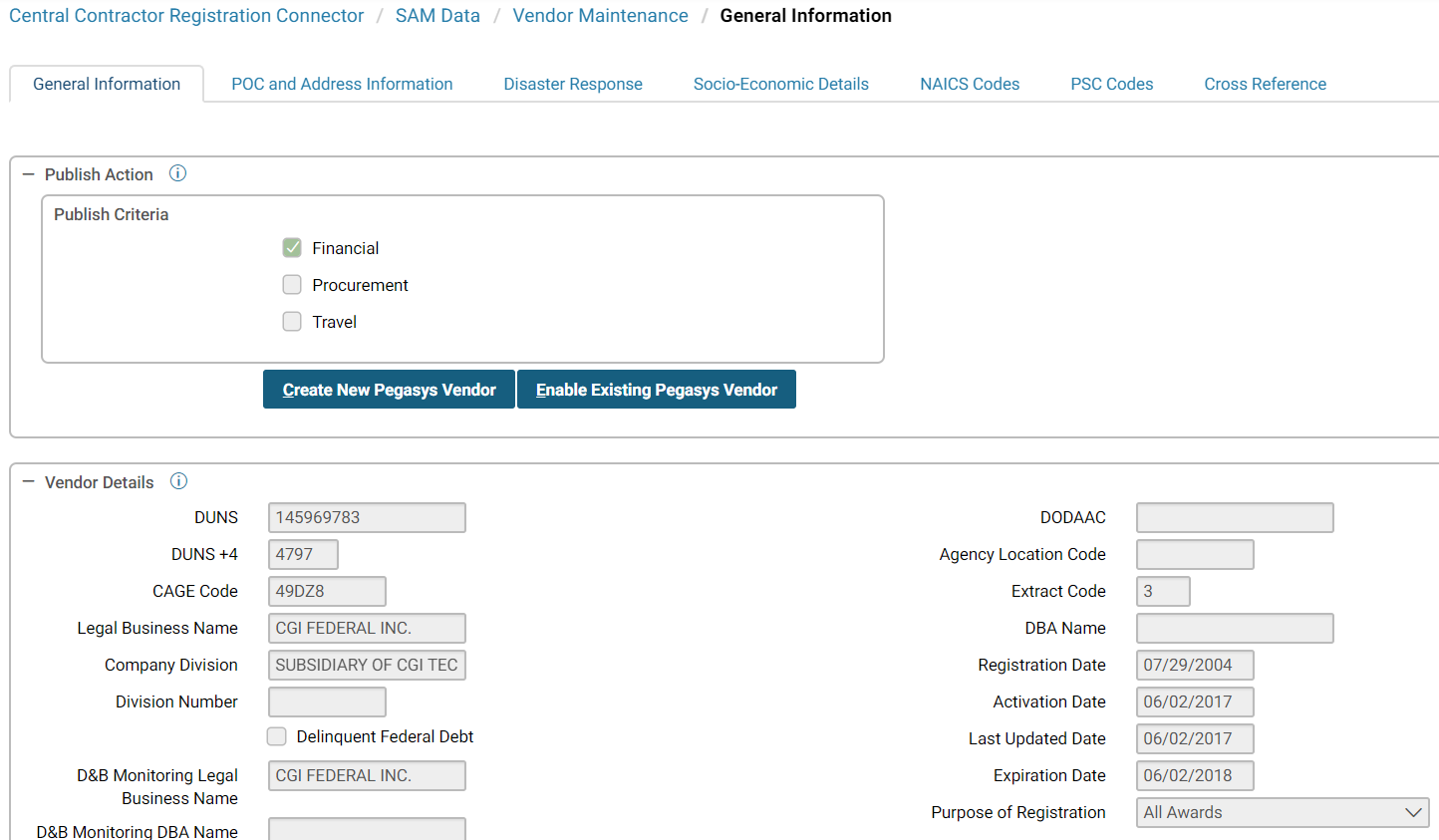
### Publishing Vendors

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

#### Publishing New Vendor Information

By selecting a vendor, the user is given several options (see **Figure 9**).

Figure 9: CCRC Vendor Detail



Through the CCRC Vendor Detail window, the user is able to publish the vendor by selecting either the Create New Pegasys Vendor button or the Enable Existing Pegasys Vendor button. USDA 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 selecting ‘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)

##### New Vendor Submissions

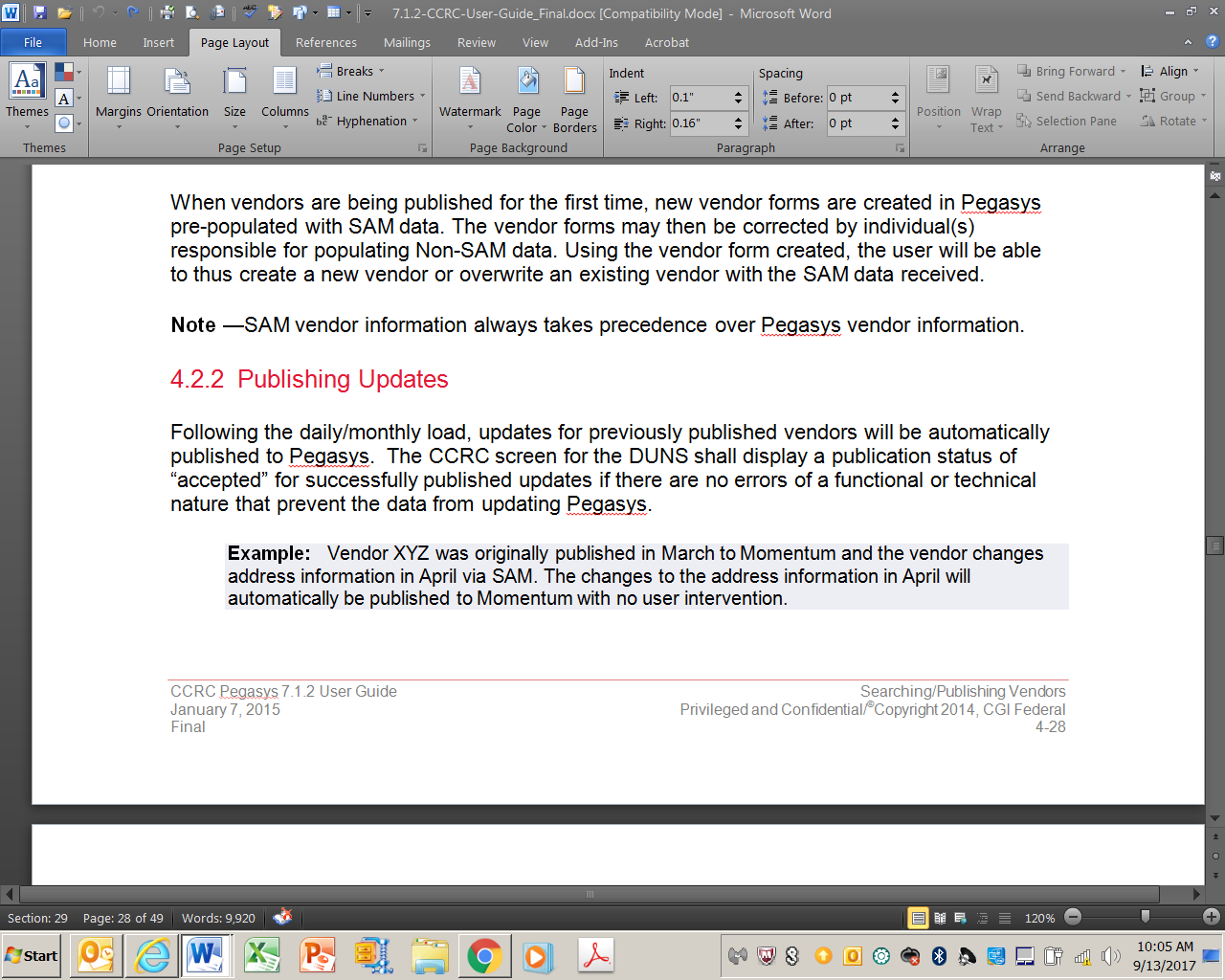
When vendors are being published for the first time, new vendor forms are created in Pegasys pre-populated with SAM data. The vendor forms may then be corrected by individual(s) responsible for populating Non-SAM data. Using the vendor form created, the user will be able to thus create a new vendor or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

**NOTE:** SAM vendor information always takes precedence over Pegasys vendor information.

#### 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.

Figure 10: Publishing Update Example



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.

### 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 11**).

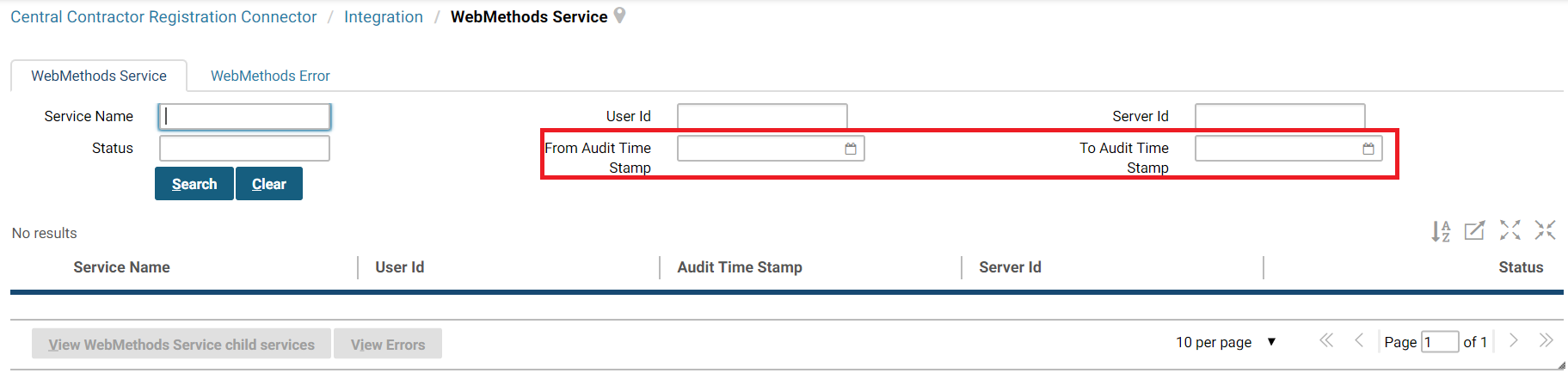
Figure 11: WebMethods Error Screen

Description: Description: The Webmethods error screen is where you can search for Webmethods errors using search criteria. Available search criteria includes Service Name, Server Id, From Audit Time Stamp, and To Audit Time Stamp. Once results are displayed the View Native ID button below the search results can be selected.


#### Audit

The Administrator has the ability to look at an Audit log for a given vendor (see **Figure 12**). The Audit log is accessed by selecting MebMethods Service from the Integration menu. 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 12: Auditing

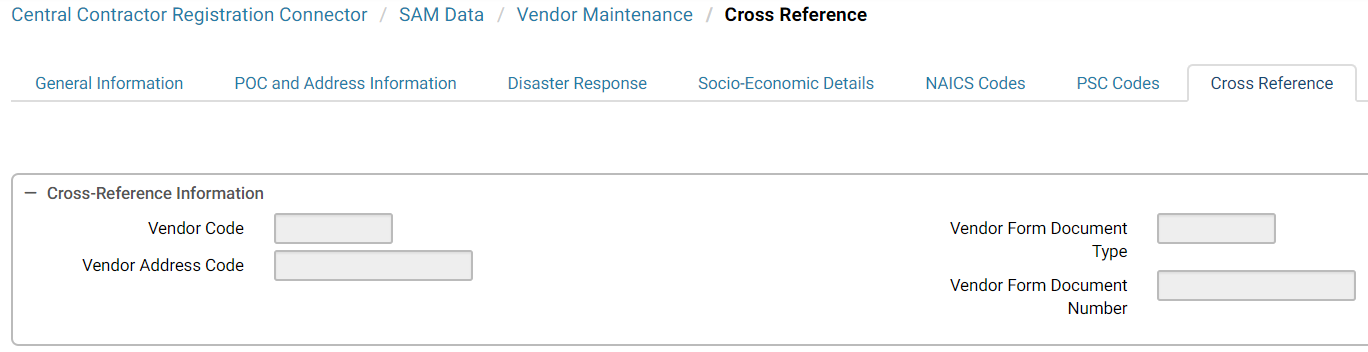


#### Cross References

In addition to being able to assess the history of a particular vendor, the Cross Reference functionality provides valuable insight to an administrator (see **Figure 13**). The Cross Reference page is accessed by selecting and viewing a vendor from the SAM Vendor Maintenance screen and selecting 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.

**NOTE:** Cross Reference data will only be available for Vendors added after implementation.

Figure 13: Cross Reference Window

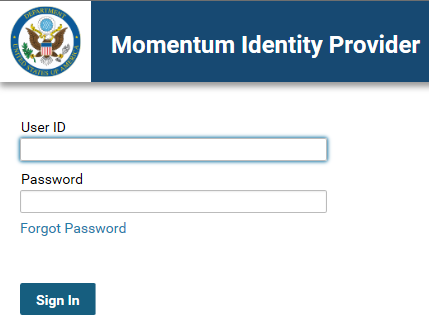


## System Administrator

### 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 14**).

Figure 14: CCRC Sign In Page



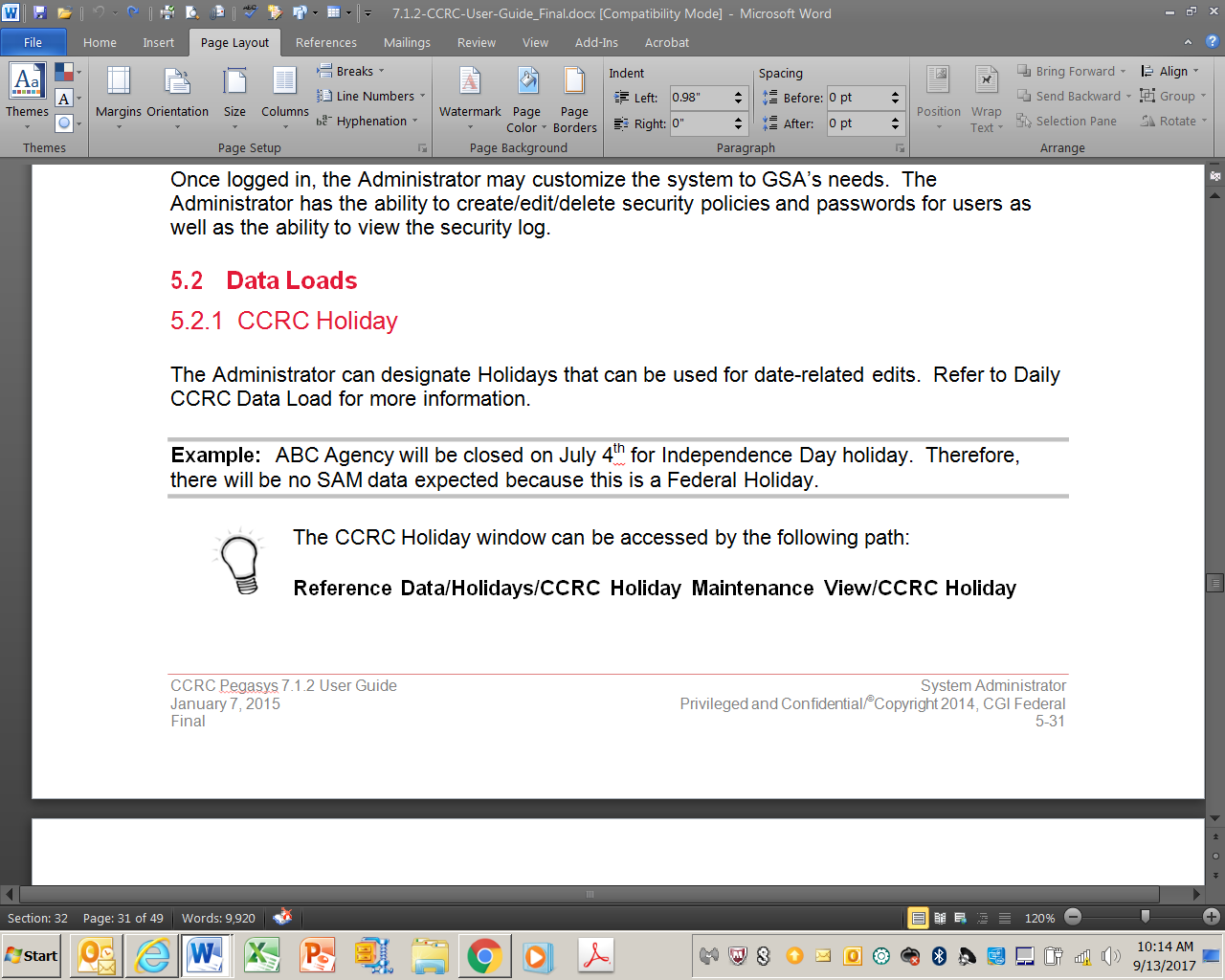
Once logged in, the Administrator may customize the system to USDA’s needs. The Administrator has the ability to create/edit/delete security policies and passwords for users as well as the ability to view the security log.

### Data Loads

#### CCRC Holiday

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

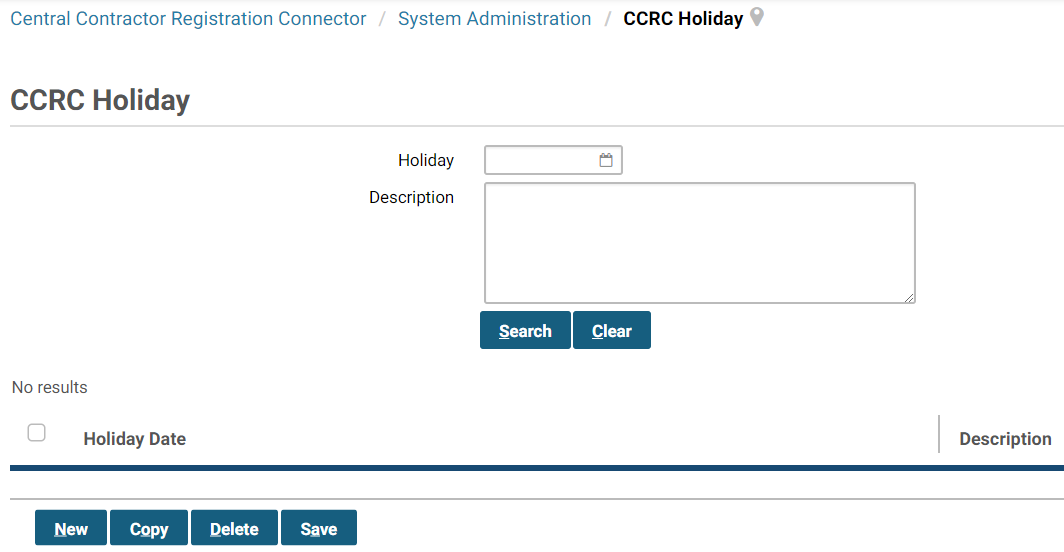
Figure 15: CCRC Holiday Example



**NOTE:** The CCRC Holiday Window can be accessed by selecting **System Administration → Holiday Maintenance**.

[**Figure 16**](#_bookmark10)displays the CCRC Holiday window.

Figure 16: CCRC Holiday Window



### Batch Execution

#### Batch Job Status

The Batch Job Status provides a means for the administrator to assess the status of batch job executions (see **Figure 17**). 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 17: Batch Job Status Window

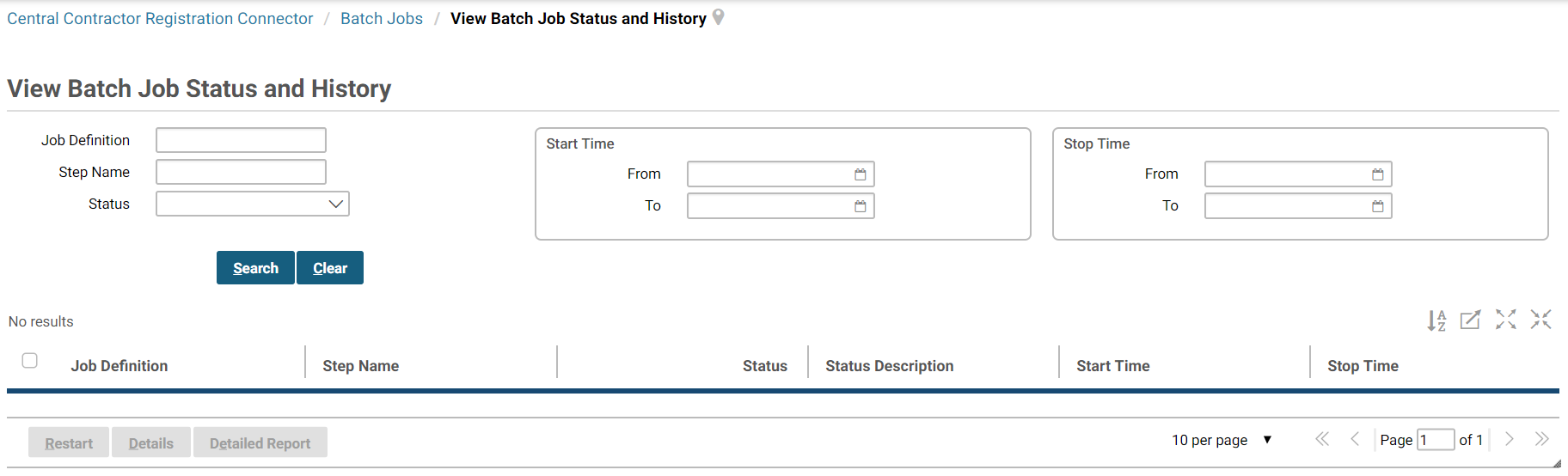


Table 6: Batch Job Status Parameters

| **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. |

### Security Policies

USDA 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.

**NOTE:** The Security Maintenance Policy Window can be accessed by selecting **Account Maintenance → Authentication Policy → Policies**.

[**Figure 18**](#_bookmark12)displays the Security Maintenance Policy Window.

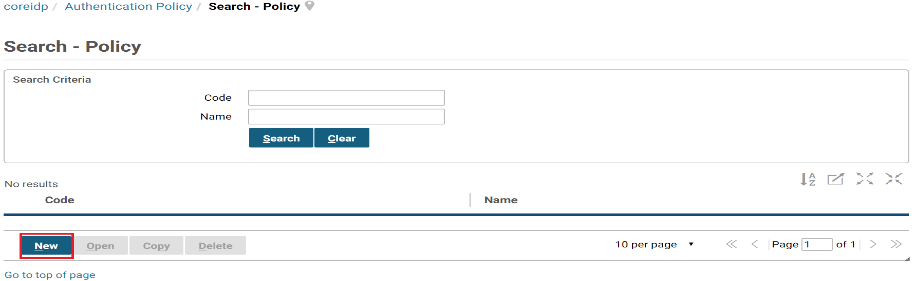
Figure 18: Security Maintenance Policy Window



#### Adding, Deleting and Editing Policies

By selecting 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 18**).In order to add a new security policy, the Administrator must create a unique Policy Code (see **Figure 19**).

Figure 19: Adding a Security Policy



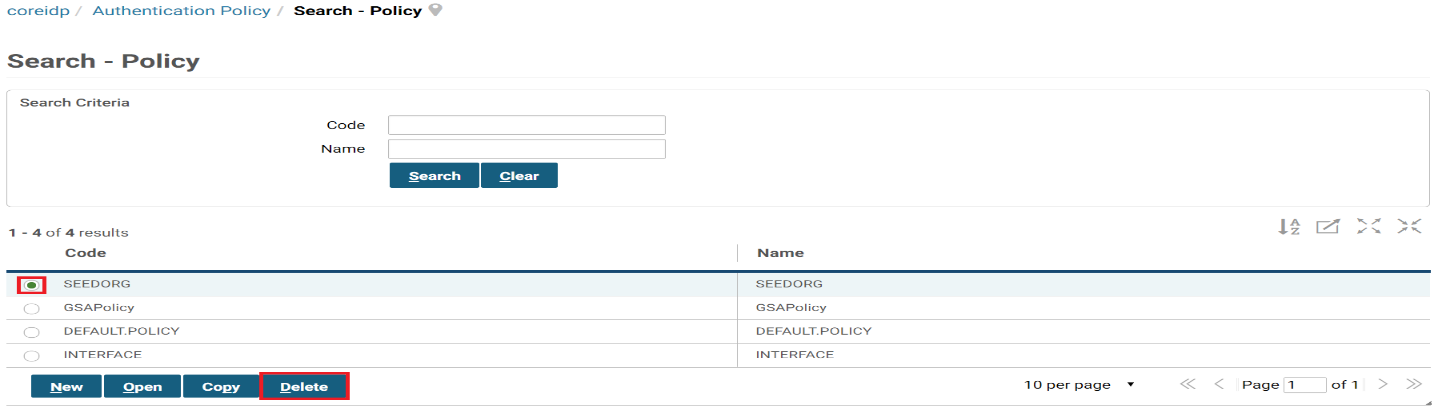
It may be necessary to edit security policies to reflect recent changes in security rules. If the Policy Code is known, then the Administrator can search for that specific Policy Code and edit by checking the box next to the appropriate Policy Code, selecting the Open button, then editing as necessary. **Table 7** describes the security maintenance information.

Table 7: Security Maintenance Information

| **Field** | **Description** |
| --- | --- |
| Password Reset Section | N/A |
| 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 |
| Password Criteria Section | N/A |
| Maximum Password Age (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. |
| Maximum Password Length | Maximum password length. |
| Generated Password Length | Generated password length |
| Enforce Password Expiration Warning | Enforces the password expiration warning policy. |
| Strong Password Section | N/A |
| 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 Code is known, then the Administrator can search for that Policy Code. Once the policy has been found, it can be deleted by checking the box next to the appropriate Policy and selecting the Delete button (see **Figure 20**).

Figure 20: Delete Policy



The new or edited security policy is viewable as soon as the Administrator selects 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.

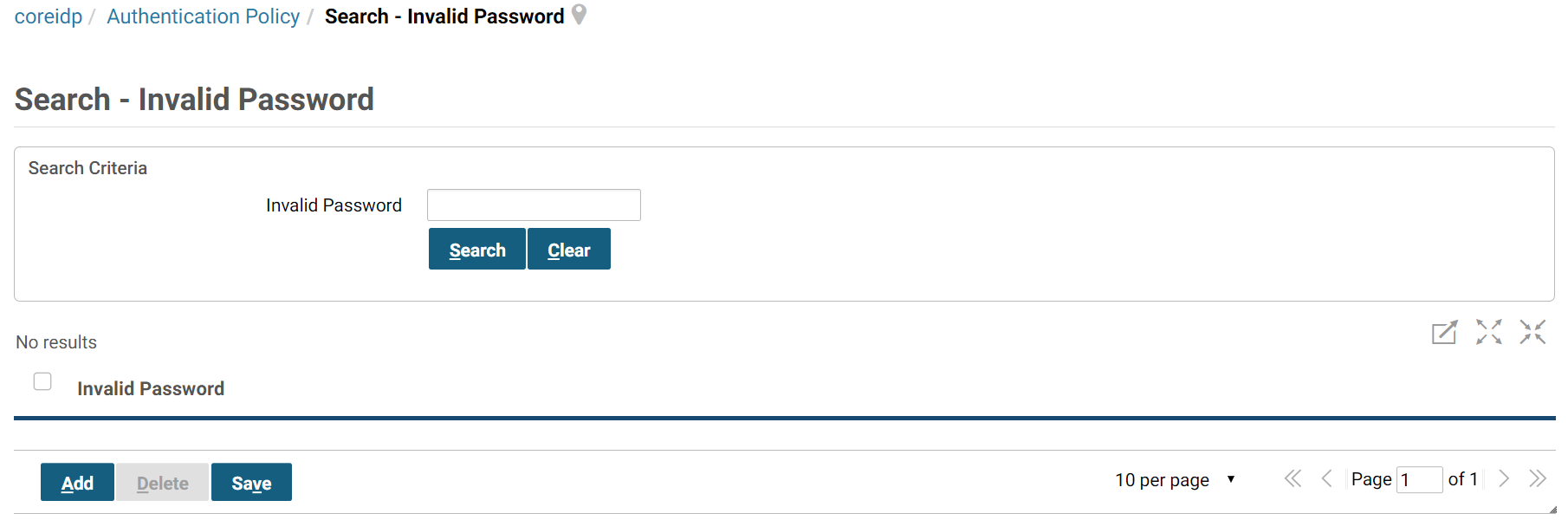
#### Passwords

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 18**).

##### Invalid Passwords

The Administrator can create invalid passwords to prevent them from being used in the CCRC. This may be done from the Invalid Password window, which is located under **Account Maintenance → Authentication Policy → Invalid Passwords**. In the Invalid Password window, the Administrator can add and delete passwords that the agency determines should be invalid (see **Figure 21**).

Figure 21: Invalid Password Window



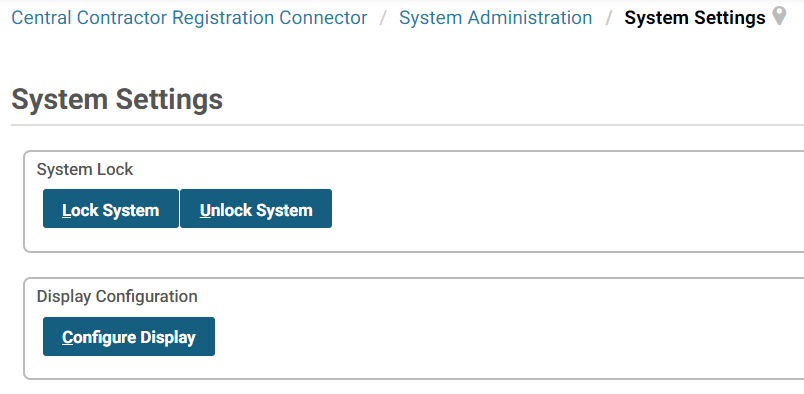
#### Reset a Locked User Account

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 18**). Once the password has been reset, the user is able to login to the CCRC.

#### System Locking

The Administrator is able to lock and unlock the system (see **Figure 22**). 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 under System Settings (see **Figure 18**).

Figure 22: System Lock Window



#### 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 USDA to apply the Confidential Data Policy to the Tax ID Number and Social Security Number fields in CCRC. 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.

#### Dynamic Extensibility

Through extensibility, USDA 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.

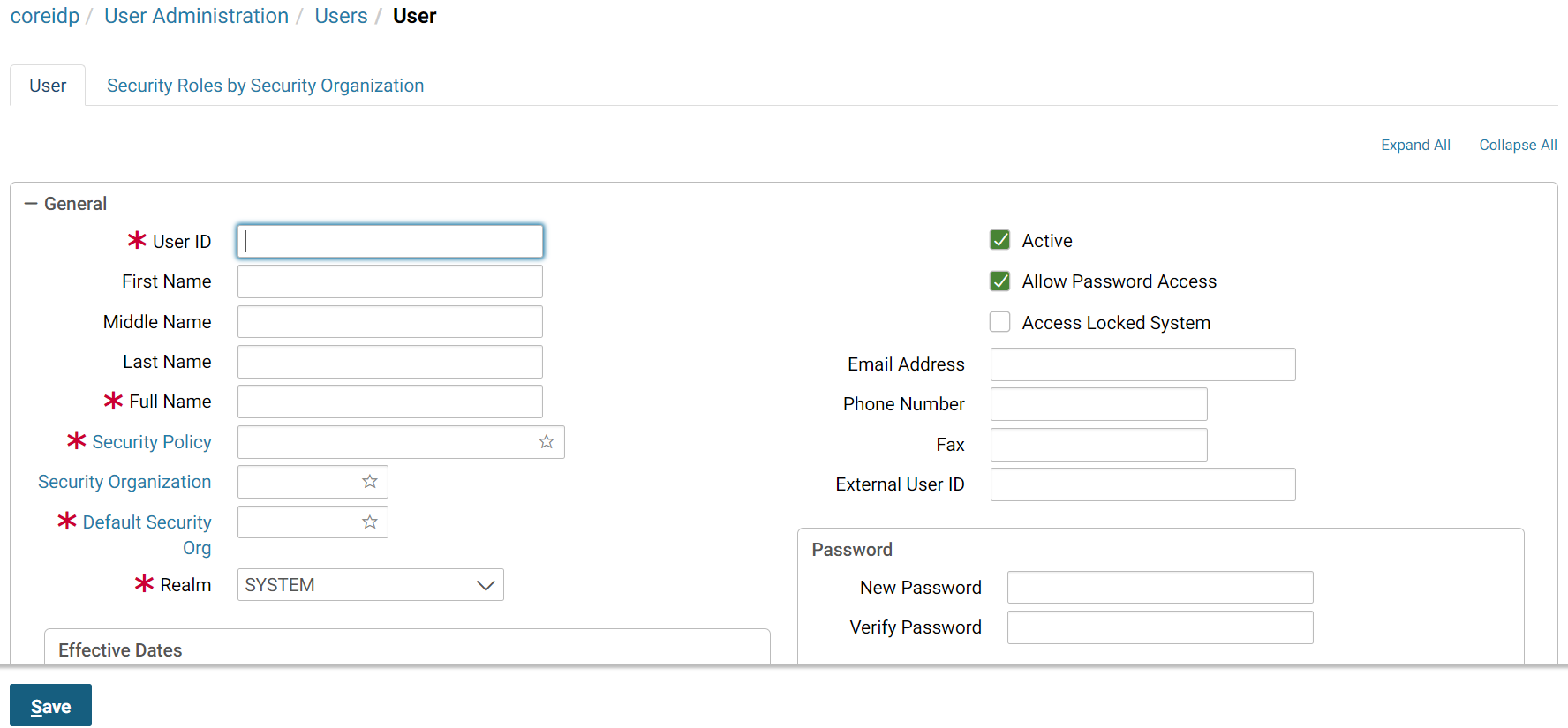
Additionally, dynamic extensibility provides the ability to populate transactions using pre-defined dynamic variables that set the value of a field based on the current date or user's principal data. Examples include a system administrator setting a global level dynamic extension to populate with a current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

### Users and Groups

#### Users

An Administrator has the ability to search for, add, edit, and deactivate users (see **Figure 23**).

Figure 23: Edit User Details Window



##### Creating a New User

A new user account can be created on the Edit User Details tab (see **Figure 23**). 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 **Table 8**). Other fields are optional and can be populated at the discretion of the Agency.

Table 8: New User Fields

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

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.

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

##### 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.

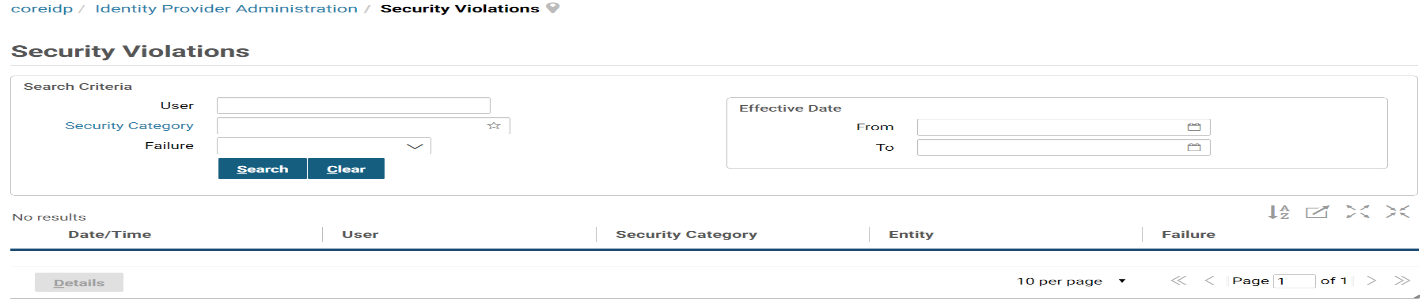
To reactivate the user, the Administrator must select the “Active” checkbox so that the checkbox is checked. Once the Administrator selects the “Save” button, the user account has been reactivated successfully and the user is now able to access the system.

### 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 18**).

The Administrator can search for all security violations committed in the system or for the security violations committed by a specific user (see **Figure 24**).

Figure 24: Security Log



### Vendor Data

#### Audit

The Administrator has the ability to look at an Audit log for a given vendor (see **Figure 25**). The Audit log is accessed by selecting **Integration → WebMethods Service**. 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 25: Audit Window

Description: Description: The Audit window, where you can search the integration history for a vendor. 
The Audit window allows for searches based on the Service Name, Status, User ID, Server ID, From Audit Time Start Up and To Audit Time Start Up. After the results are displayed the view webmethods service child services and the view errors button should become enabled so users are able to select them.

#### Cross Reference

In addition to being able to access the history of a particular vendor, the Cross Reference functionality provides valuable insight to a user (see **Figure 26**). The Cross Reference page is accessed by selecting and viewing a vendor from the SAM Vendor Maintenance screen and selecting the Cross Reference tab. The Cross Reference screen allows the user to link between applications that are connected via webMethods. This means that the user 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 user can change the application ID in the search section at to Pegasys and find out what vendor is getting updated in Pegasys e.g. Vendor Code = ABC, Address Code= 1.

Figure 26: Cross Reference Window

Description: Description: The cross reference window where you can view any available cross reference information for a selected vendor. Under the Cross-Refrence tab there is the vendor code, vendor Address code, the vendor form Document type, and the vendor Form Document number are all displayed.


### Enhancements Included in 7.5.1 Upgrade

#### Link Address Codes

Currently, users are able to record a DODAAC on Momentum vendors. This enhancement supports the ability to link an AAC/DODAAC to a vendor record and office address record, in addition to recording on IPAC transactions as in previous releases.

* The AAC/DODAAC uniquely identifies a unit, activity, or organization that has the authority to requisition and/or receive material.
* In Momentum, this field is reference-backed and utilizes the AAC/DODAAC import file to load AAC/DODAAC values into Momentum from the AAC/DODAAC file provided by the Defense Logistics Agency (DLA).
* This field is now available as search criteria when searching for vendors and office addresses. It allows the user to locate vendors and offices by the AAC/DODAAC reference value.
* This enhancement adds the ability to record Agency Location Code (ALC) from SAM extract files via CCRC, including the ability to derive Agency and Bureau on vendors from this ALC.

#### Cross Reference Enhancement

* Modifies Central Contractor Registration Connector (CCRC) by moving the Cross Reference page from Momentum Integration platform (WebMethods Integration Server) to the SAM Vendor Detail Cross Reference tab.
* The release updates the Cross Reference page to include the Vendor Code, Vendor Address Code, Vendor Form Document Type, and Vendor Form Document Number fields.

#### Vendor Mailing Address Requirement Accommodation

* This Requirement Change implemented multiple improvements in order to accommodate vendors that are not required to have mailing addresses.
* Previously, SAM Vendors with an 'IGT-Only' SAM registration did not require a mailing address while Momentum required a mailing address for all vendors. When attempting to sync or submit one of these vendors through CCRC to Momentum, they received a system error stating that a mailing address was required.

#### Display Updated Purpose of Registration Values

* November 3, 2015 SAM began including the Purpose of Registration value for SAM Extract code 1 (Deleted/Deactivated Record) and 4 (Expired Record).
* The CCRC Integration has been modified to support the ability to display the updated Purpose of Registration value for the SAM Extract codes on the Momentum Vendor record.

#### Security Assertion Markup Language

* System for Award Management (SAM) is the official US Federal Government system that provides extract files containing vendor data.
* This enhancement will allow CCRC to upload and process vendor data using the latest release of SAM extract file.
* Legacy extract files were de-supported in August 2014.
* This enhancement added functionality to the SAML 2.0 enhancement that was in the Momentum 7.1 release.
* This enhancement, which has reduced the workload on administrators and reduced the likelihood of transcription errors and stale data, introduced functionality that allows synchronization of user records from a Service Provider (SP) to its associated Identity Provider (IdP).

#### System for Award Management Phase 3

* The SAM Phase 3 enhancement will provide the capability to import data from SAM into CCRC using the v1.0 extract files provided by SAM.
* Remaining consistent with current functionality, agencies will have the capability to publish new records from CCRC to Momentum through the use of MOMAPI.
* Concurrent with existing functionality, any changes made to records that are synchronized between CCRC and Momentum via a SAM extract file will automatically be published to Momentum. This will verify that the agency's financial application continues to store the most current data available for SAM entity records.
* From Momentum, agencies will continue to have the possibility of transmitting this entity data to Vendor Self Service (VSS) and Maximo.

#### Vendor Update Support

This change allows the user to update vendors that do not have a DODAAC in Momentum but that do have a matching DODAAC\DUNS\DUNS+4 in CCRC. The system will follow the following logic for accepted vendors:

* If the vendor has a DODAAC value, the system will retrieve any matching vendors from Momentum with the DODAAC key.
* If no vendors are retrieved and a DUNS/DUNS+4 key also exists on the record, the system will retrieve any matching vendors from Momentum with the DUNS/DUNS+4 key.
* If no vendors are retrieved by either of the previous methods, the transaction will end in the integration with no errors as before.
* If a vendor only has a DUNS/DUNS+4, the logic will work as before.