United States Department of Agriculture

Central Contractor Registration Connector (CCRC)

Pegasys 7.8

User Guide

Contract: # HHSN316201200011W

Order # AG-3144-D-16-0278

Final Version 7.0

April 2021

Table of Contents

Table of Contents 1
Table of Figures 4
Table of Tables 5
Revision Log 6
1 CCRC Introduction 8
2 CCRC Overview 9
2.1 Central Contractor Registration Connector (CCRC) 9
2.2 Initial Load and Initial Vendor Selection 9
2.3 CCRC User Interface 10
2.4 CCRC Import Batch Job 10
2.4.1 New Vendors 10
2.4.2 Updated Vendor 10
2.4.3 Inactivated/Deleted Vendors 11
2.5 CCRC Publishing Agent 11
2.6 Subscribing Agent/Agency Applications 11
2.7 Security 12
3 Loading Data with SAM 13
3.1 SAM Data Load 13
3.1.1 Exporting SAM File 13
3.1.2 Processing the SAM File 14
3.1.3 Processing Options 15
3.1.4 Removing the SAM File from CCRC 16
3.2 Initial Vendor Selection 16
3.2.1 Select Vendors to Enable 16
3.2.2 Execute Initial File Creation Batch Process 19
3.2.3 Initial Vendor Selection Script and Synchronization 20
3.3 Daily Update Files 20
3.3.1 Daily CCRC Data Load 20
3.3.2 New Vendor 21
3.3.3 Existing Vendor 22
3.3.4 Deletion and Deactivation 22

4 Searching/Publishing Vendors 23
4.1 Searching for Vendors 23
4.1.1 Vendor Information Query 23
4.1.2 Search for Another Vendor 25
4.1.3 Case Insensitive Queries 25
4.2 Publishing Vendors 26
4.2.1 Publishing New Vendor Information 26
4.2.1.1 New Vendor Submissions 28
4.2.2 Publishing Updates 28
4.3 Integration 28
4.3.1 Audit 29
4.3.2 Cross References 29
5 System Administrator 31
5.1 CCRC Sign In 31
5.2 Data Loads 31
5.2.1 CCRC Holiday 31
5.3 Batch Execution 32
5.3.1 Batch Job Status 32
5.4 Security Policies 33
5.4.1 Adding, Deleting and Editing Policies 33
5.4.2 Passwords 36
5.4.2.1 Invalid Passwords 36
5.4.3 Reset a Locked User Account 37
5.4.4 System Locking 37
5.4.5 Secure Data 38
5.4.6 Dynamic Extensibility 38
5.5 Users and Groups 38
5.5.1 Users 38
5.5.1.1 Creating a New User 39
5.5.1.2 Deactivating a User 40
5.5.1.3 Reactivating a User 40
5.6 Security Log 41
5.7 Vendor Data 41

5.7.1 Audit 41
5.7.2 Cross Reference 42
5.8 Enhancements Included in 7.8 Upgrade 42
5.8.1 Link Address Codes 42
5.8.2 Cross Reference Enhancement 43
5.8.3 Vendor Mailing Address Requirement Accommodation 43
5.8.4 Display Updated Purpose of Registration Values 43
5.8.5 Security Assertion Markup Language 43
5.8.6 System for Award Management Phase 3 44
5.8.7 Vendor Update Support 44

Table of Figures

Figure 1: CCRC Cycle 9
Figure 2: File Maintenance Window 14
Figure 3: File Processing 15
Figure 4: SAM Vendor Maintenance Table 17
Figure 5: Available List of Vendors 19
Figure 6: SAM Vendor Maintenance Table 23
Figure 7: Case Insensitive Query in CCRC 26
Figure 8: CCRC Vendor Detail 27
Figure 9: WebMethods Error Screen 29
Figure 10: Auditing 29
Figure 11: Cross Reference Window 30
Figure 12: CCRC Sign In Page 31
Figure 13: CCRC Holiday Window 32
Figure 14: Batch Job Status Window 32
Figure 15: Security Maintenance Policy Window 33
Figure 16: Adding a Security Policy 34
Figure 17: Deleted Policy 36
Figure 18: Invalid Password Window 37
Figure 19: Reset Login 37
Figure 20: System Lock Window 38
Figure 21: Edit User Details Window 39
Figure 22: Security Log 41
Figure 23: Audit Window 42
Figure 24: Cross-Reference Window 42

Table of Tables

Table 1: Upload Parameters 14
Table 2: CCRC Data Maintenance Parameters 17
Table 3: Parameters 21
Table 4: SAM Extract Codes 21
Table 5: Search Parameters 24
Table 6: Batch Job Status Parameters 33
Table 7: Security Maintenance Information 34
Table 8: New User Fields 39

Revision Log

Date	Version No.	Description	Author	Reviewer	Review Date
2/11	Draft Version 1	Original Draft	Danielle Becker	Tegan Dinardo, Mike Wong	1/11
11/14	Draft Version 2	Draft- 7.1.2 Enhancements	Karin Keswani, Mathew Randall	Karin Keswani, Mathew Randall	11/14
1/15	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. In section 5.4.6, Figures 5-13 and Figure 5-14	Karin Keswani, Benjamin Bowden	Karin Keswani, Benjamin Bowden	1/15
10/17	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.	Kevin Hillman	Nick Longworth, Jenny Lewis, Marice Grissom	9/17 – 10/17
5/18	5.0	No additional changes.	Kevin Hillman	Jenny Lewis, Marice Grissom	5/18

Date	Version No.	Description	Author	Reviewer	Review Date
1/21	6.0	Revision 6.0 – updated to reflect the following changes for Pegasys 7.8: • Updated Figures 1-24 to reflect changes in 7.8. • Updated original Figures 4 and 10 by removing and changing them to Text (”Examples”.) • Updated text for Sections 2.2, 3, 3.2, 3.2.2, 3.3.2, 3.3.3, 3.3.4, 4.2.1, 4.3, 5.8.7 to include EFT Indicator and UEI. • Updated Table 2 and 5 to include UEI and EFT Indicator rows and description. • Updated Section 5.4.3 to include the new location to Reset a Locked User account with the breadcrumb steps to navigate there + Added a new Figure (Figure 19) to show the tab where the Administrator can reset a locked account.	Jad Youssef	Jun Kim Marice Grissom	1/21
4/21	7.0	Updated to reflect the following changes for the Pegasys 7.8 Upgrade: • Applied USDA/GSA comments dated 03/01/2021	Jad Youssef	Jun Kim Marice Grissom	3/21

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.

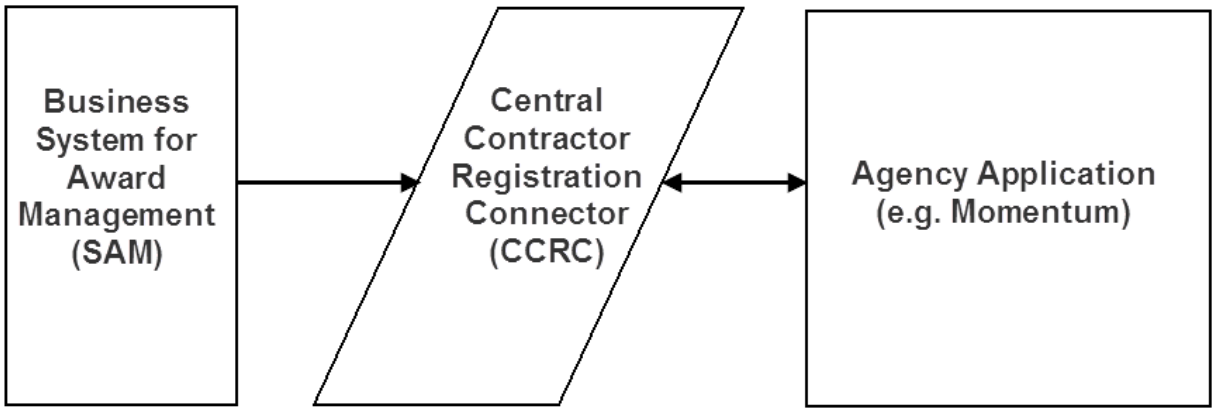
2 CCRC Overview

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. As shown in **Figure 1**, the CCRC is populated with SAM data, which is 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



2.2 Initial Load and Initial Vendor Selection

Vendors have created 700,000+ records within the government-wide SAM database; however not all agencies currently conduct, or are expected to conduct, business with each SAM vendor. 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 & 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). As a part of the Pegasys 7.8 upgrade Unique Entity Identifier (UEI) was introduced to comply with the

expansion of the Federal Acquisition Regulations (FAR), which affected more than 600,000 vendors that do business with the federal government. Along with the introduction of UEI, DUNS +4 was relabeled to EFT Indicator.

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 in the SAM Exclusion Records – Restricted. 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 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.

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 setup 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.

3 Loading Data with SAM

Vendors have created 700,000+ 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 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 & 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). As a part of the Pegasys 7.8 upgrade Unique Entity Identifier (UEI) was introduced to comply with the expansion of the Federal Acquisition Regulations (FAR), which affected more than 600,000 vendors that do business with the federal government. Along with the introduction of UEI, DUNS +4 has been relabeled to EFT Indicator.

3.1 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).

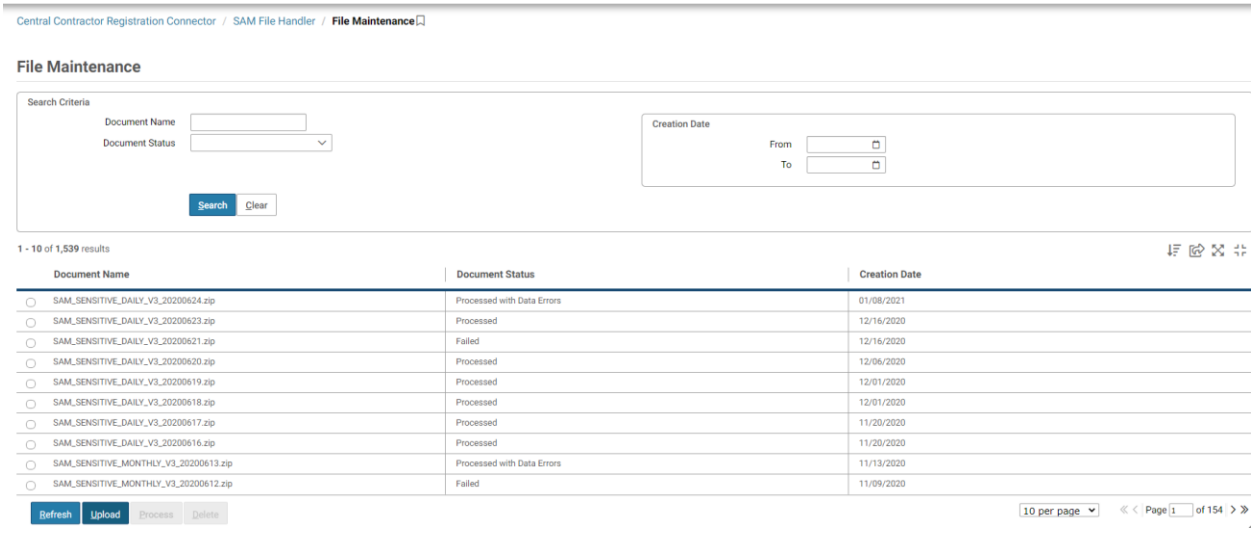
There are three types of files available:

- **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

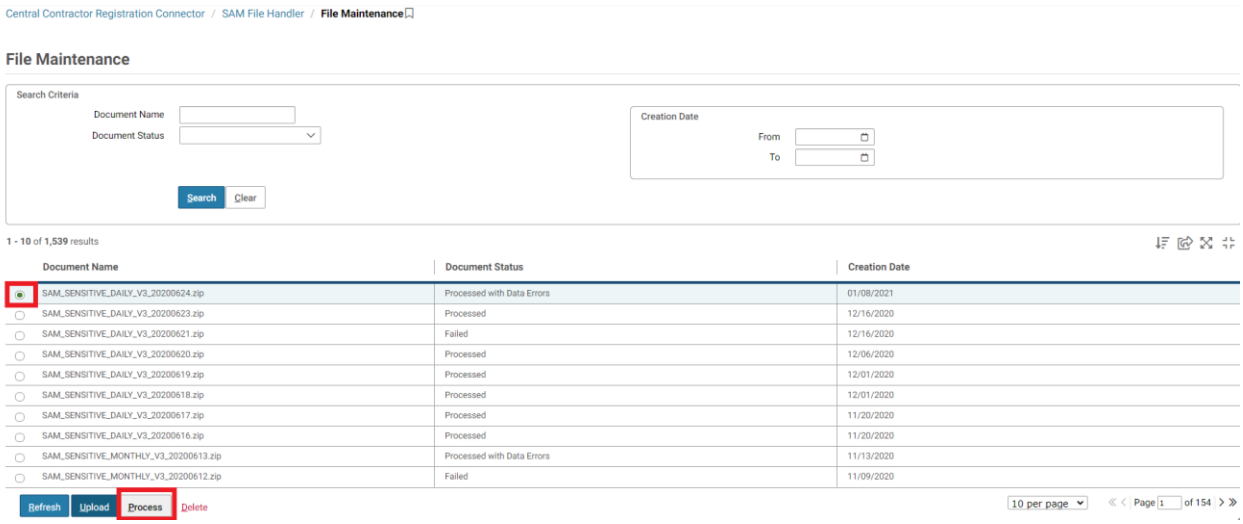
Field	Field Description
Description	The user has the ability to enter a description of the file for future reference.
Document	The filename/path of the extract file to be loaded. This parameter is required.

3.1.2 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.

3.1.3 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 file will override all of the data in the CCRC database (including any changes made through the dailies).

3.1.4 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.

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:

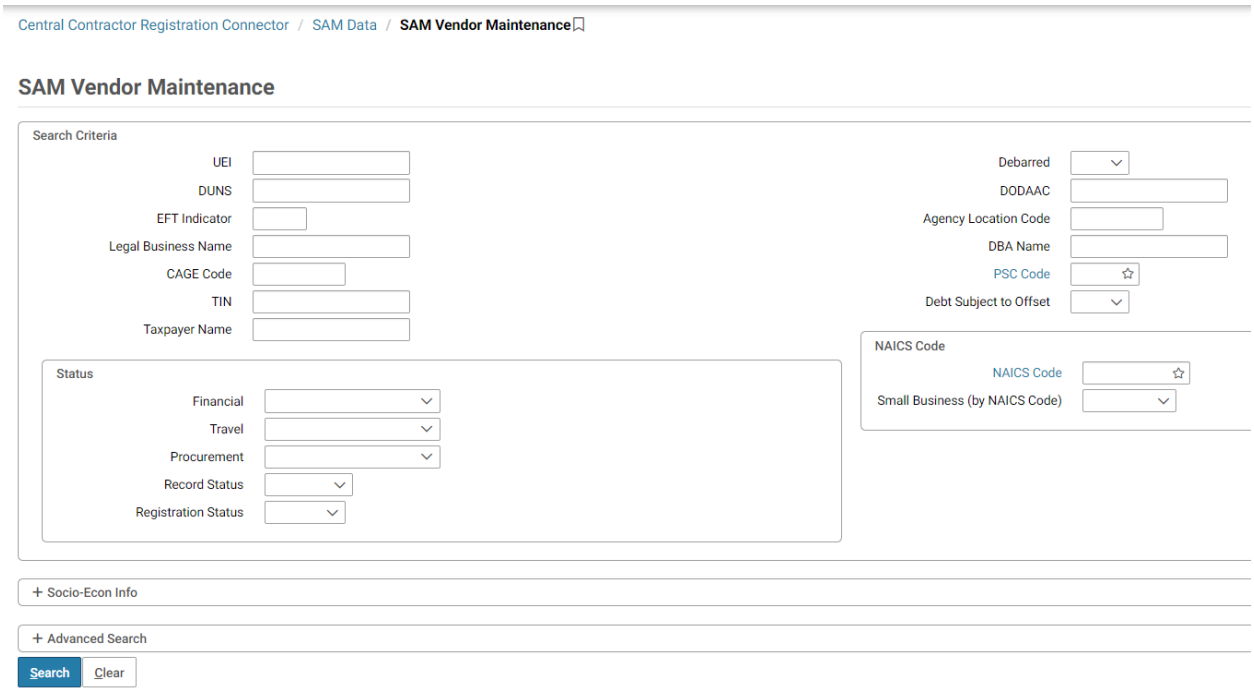
- Select Vendors to Enable from Pegasys
- Execute Batch Process (GSCCRI)
- Run Initial Vendor Selection script

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/EFT Indicator and UEI. 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 SAM Vendor Maintenance Table (see **Figure 4**).

Figure 4: SAM Vendor Maintenance Table



Through the SAM Vendor Maintenance Table, the Administrator can enter desired search criteria in order to find the vendors with whom the agency conducts business. The system returns an "available" list of vendors that match the search criteria (see **Figure 5**).

Table 2: CCRC Data Maintenance Parameters

Parameter	**Description**
DUNS	(Data Universal Numbering System) A unique 9-digit numbering system that is used to identify a business.
UEI	Unique Entity Identifier - An identifier used to identify a specific commercial, non-profit, or Government Entity.
EFT Indicator	Unique code used to identify additional bank accounts associated to a single UEI. DUNS +4 relabeled to EFT Indicator.
Legal Business Name	The legal business name of the business.
DBA NAME	'Doing Business As' (DBA) Name.
DODAAC	The Department of Defense Activity Address Code (DODAAC) used for interagency transfers. It is an alphanumeric field that uniquely identifies a unit, activity, or organization. The field size is nine characters.
Agency Location Code	A symbol used to identify an agency accounting location or regional financial office. Field length is ten characters.

Parameter	Description
Delinquent Federal Debt	Indicates whether a vendor/entity has a past due debt with the federal government.
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 (CAGE) Code that identifies contractors conducting business with the Government.
TIN	A nine-character field that contains the Taxpayer ID number associated with a record.
Taxpayer Name	The name of the taxpayer.
PSCCodes	Product Service Codes (PSC) A 4-character, alphanumeric code, used to identify 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.
Record Status	Specifies whether the record in CCRC is a new record or has been changed by an extract file.
Registration Status	This field indicates the registration status of a vendor in the System for Award Management (SAM) system.
8(a) Program Participant	Check box. The business is a participant in the 8(a) Program.
NAICS Code (group box)	Includes the NAICS Code and 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.

Parameter	Description
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 the vendor has been declared ineligible from receiving Federal contracts, as shown by records in the SAM Exclusion Records - Restricted.

Figure 5: Available List of Vendors

1 - 10 of 115,254 results

UEI	DUNS	EFT Indicator	DODAAC	Agency Location Code	Legal Business Name	DBA Name	Debt Subject to Offset	CAGE Code
ELQBEXN821Y7	112920647				LMJ & ASSOCIATES, LLC		False	8NHX6
UDFMKGJNDJN9	111296274				AIMCO PARTNERS, LLC		False	8Q7P0
HHDNL21D9B38	001003748				STERLINGWEAR OF BOSTON, INC.		False	1CT45
P5NJQDN75C54	001004332				UNION MACHINE COMPANY OF LYNN, INC.		False	51992
	001007918				E J F CONSULTING INC		False	308U9
LAJRBMGGFKN6	001009851				NEPTUNE GARMENT COMPANY		False	0NJB7
UF1GNHC86DN5	001013796				AMERICAN INK & OIL CORPORATION		False	82956
E7Y6BE2RU2M5	001015429				RUSSELECTRIC INC.		False	23312
M3Q6CBYHM8J4	001016906				UNITED PROSTHETICS, INC.		False	0VLB6
U4TVWNEK81K4	001018535				GOLDEN, WEISE AND ASSOCIATES, LLC	GWA	False	1S3F2

View

10 per page Page 1 of 11,526

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**.

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/EFT Indicator and UEI 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/EFT Indicator and UEI that has not yet been added to the file, the batch job writes the DUNS/EFT Indicator and UEI 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/EFT Indicator UEI or has a DUNS/EFT Indicator and UEI 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.

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)

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/EFT Indicator and UEI, 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/EFT Indicator and UEI, 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 marked as deleted or inactive and the CCRC is populated with the following information: load timestamp, user running the load, DUNS/EFT Indicator and UEI, 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 do not have a "prevent new spending" flag or with a "prevent new spending flag" through the integration) or deleted.

4 Searching/Publishing Vendors

4.1 Searching for Vendors

Users are able to login to the CCRC to query vendor information and to select a new vendor for publication and publish that vendor. Vendors only will 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

As shown in **Figure 6**, 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.

Figure 6: SAM Vendor Maintenance Table

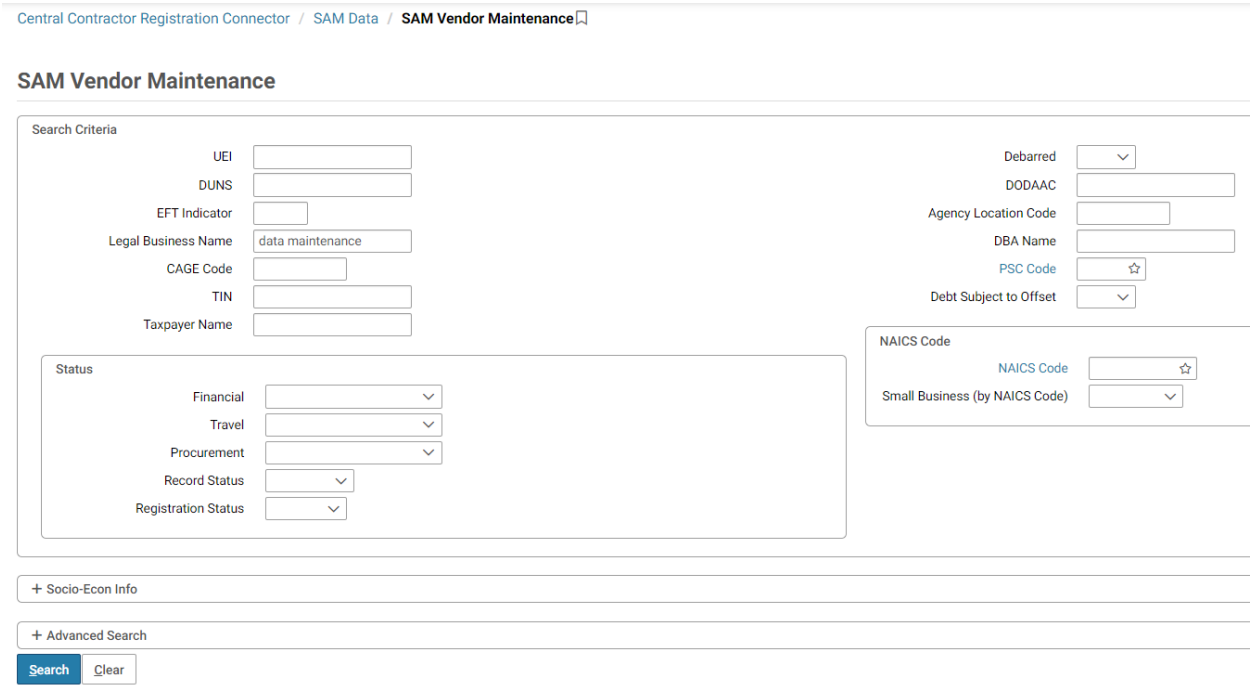


Table 5: Search Parameters

Parameter	Description
DUNS	(Data Universal Numbering System) A unique 9-digit numbering system that is used to identify a business.
UEI	Unique Entity Identifier assigned to all entities.
EFT Indicator	Unique code used to identify additional bank accounts associated to a single UEI. DUNS +4 relabeled to EFT Indicator.
Legal Business Name	The legal business name of the business.
DBA NAME	'Doing Business As' Name.
DODAAC	The Department of Defense Activity Address Code DODAAC used for interagency transfers. It is an alphanumeric field that uniquely identifies a unit, activity, or organization. The field size is nine characters.
Agency Location Code	A symbol used to identify an agency accounting location or regional financial office. Field length is ten characters.
Delinquent Federal Debt	Indicates whether a vendor/entity has a past due debt with the federal government.
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.
PSC Codes	(Product Service Codes) A 4-character, alphanumeric code, used to identify 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.
Record Status	Specifies whether the CCRC record is a new record or has been changed by an extract file.

Parameter	Description
Registration Status	This field indicates the registration status of a vendor in the System for Award Management (SAM) system.
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 the vendor has been declared ineligible from receiving Federal contracts, as shown by records in the SAM Exclusion Records - Restricted.

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.

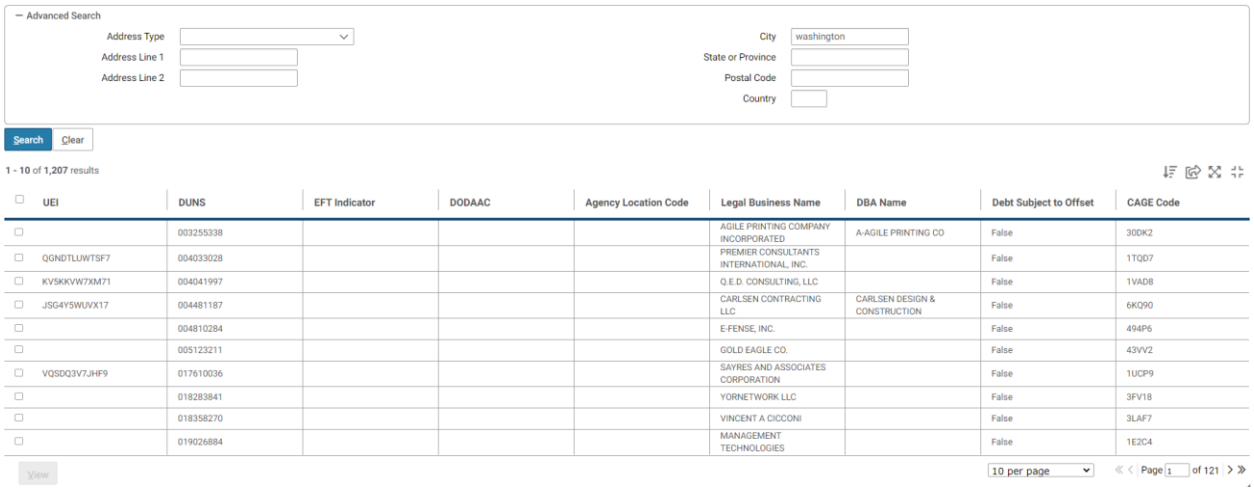
4.1.2 Search for Another Vendor

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.

4.1.3 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 7** below.

Figure 7: Case Insensitive Query in CCRC



UEI	DUNS	EFT Indicator	DODAAC	Agency Location Code	Legal Business Name	DBA Name	Debt Subject to Offset	CAGE Code
	003255338				AGILE PRINTING COMPANY INCORPORATED	A-AGILE PRINTING CO	False	30DK2
QGNDTLUWTSF7	004033028				PREMIER CONSULTANTS INTERNATIONAL, INC.		False	1TQD7
KV5KKVW7XM71	004041997				Q.E.D. CONSULTING, LLC		False	1VAD8
JSG4Y5WUVX17	004481187				CARLSEN CONTRACTING LLC	CARLSEN DESIGN & CONSTRUCTION	False	6KQ90
	004810284				E-FENSE, INC.		False	494P6
	005123211				GOLD EAGLE CO.		False	43VV2
VQSDQ3V7JHF9	017610036				SAYRES AND ASSOCIATES CORPORATION		False	1UCP9
	018283841				YORNETWORK LLC		False	3FV18
	018358270				VINCENT A CICCONI		False	3LAF7
	019026884				MANAGEMENT TECHNOLOGIES		False	1E2C4

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

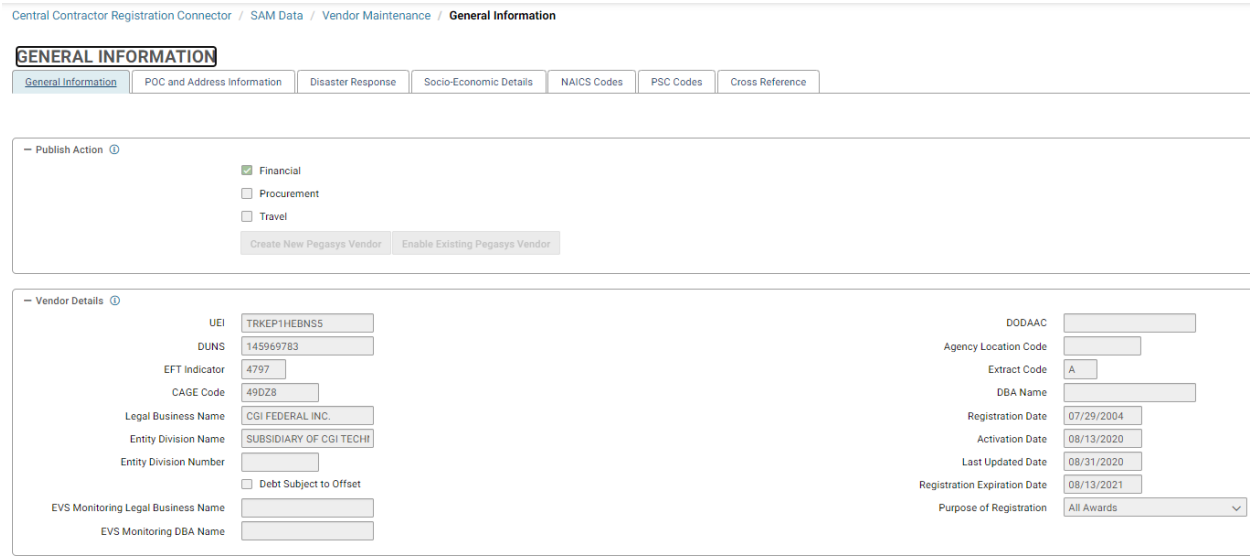
4.2 Publishing Vendors

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 8**). On 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 always will have the Financial box checked in the Publish Action group box.

Figure 8: CCRC Vendor Detail



- **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. Then 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/EFT Indicator and UEI, address information, registration date).
- **Status Information** - Provides the status information related to that vendor (i.e., Published status, Timestamp, Record status).
- **Business Details** - Provides business information related to that vendor (i.e., Company Security Level, 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.

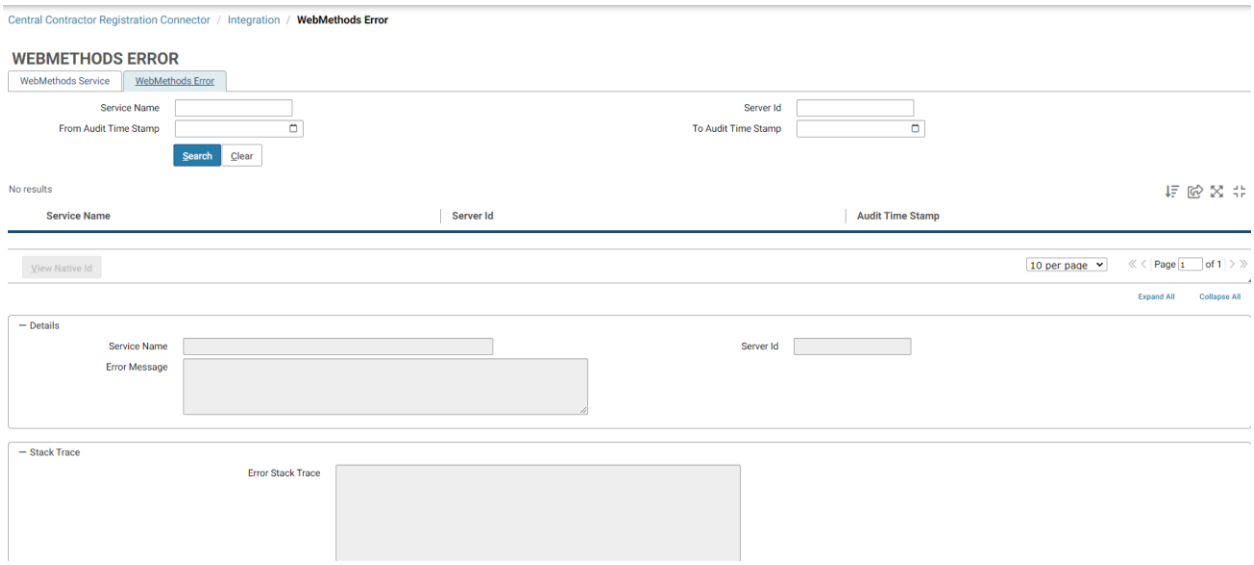
Example: Vendor XYZ was originally published in March to Pegasys and the vendor changes address information in April via SAM. The changes to the address information in April will automatically be published to Pegasys with no user intervention.

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/EFT Indicator and UEI 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 9**).

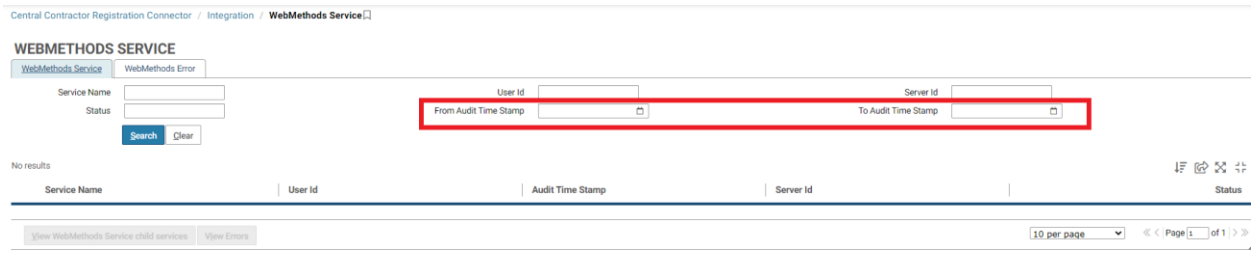
Figure 9: WebMethods Error Screen



4.3.1 Audit

The Administrator has the ability to look at an Audit log for a given vendor (see **Figure 10**). The Audit log is accessed by selecting WebMethods 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 10: Auditing



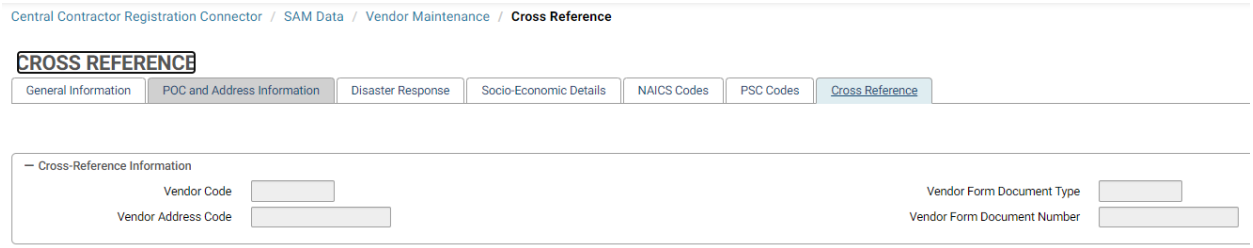
4.3.2 Cross References

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 11**). 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 only will be available for Vendors added after implementation.

Figure 11: Cross Reference Window

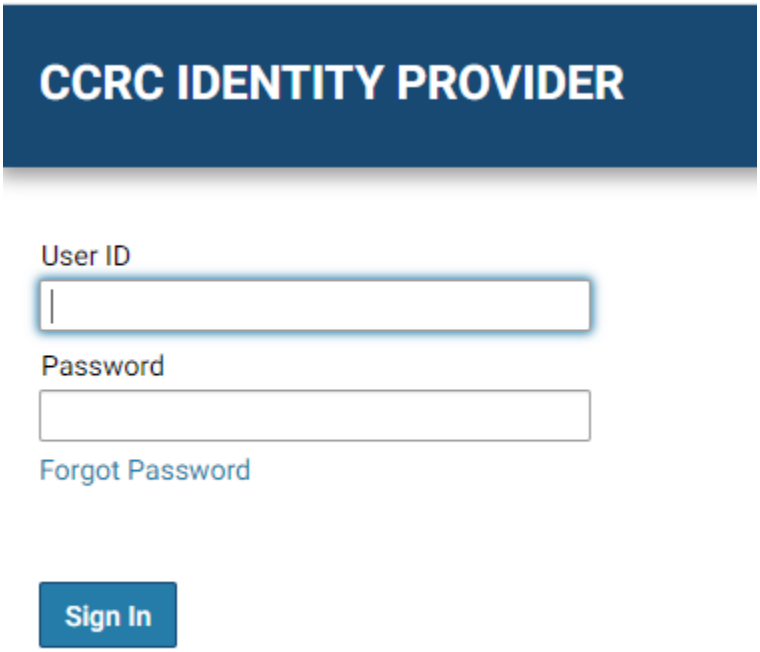


5 System Administrator

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 12**).

Figure 12: 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.

5.2 Data Loads

5.2.1 CCRC Holiday

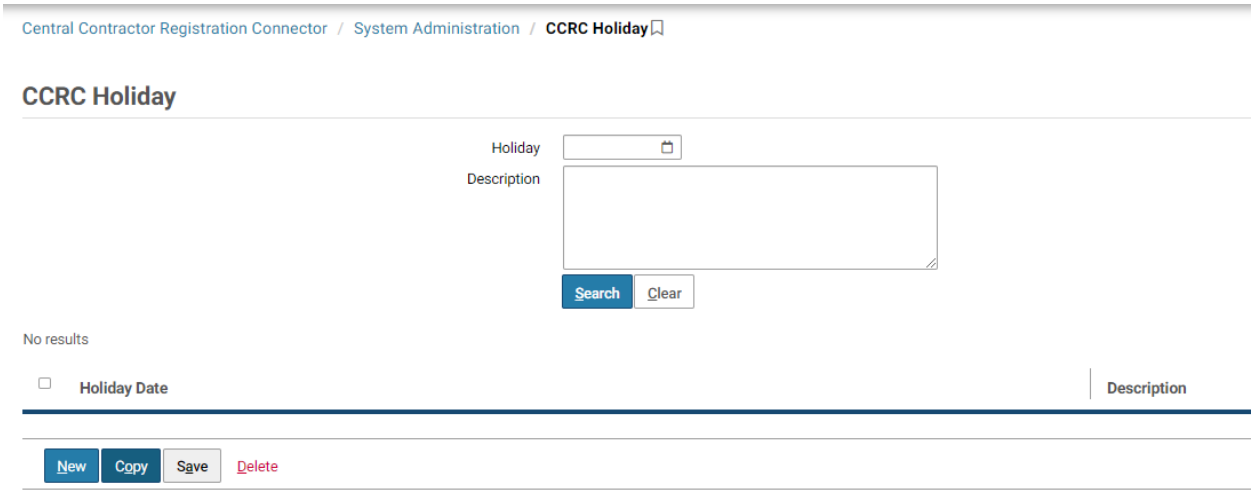
The Administrator can designate Holidays that can be used for date-related edits. Refer to Daily CCRC Data Load for more information.

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.

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

Figure 13 displays the CCRC Holiday window.

Figure 13: 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 14**). 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 14: Batch Job Status Window

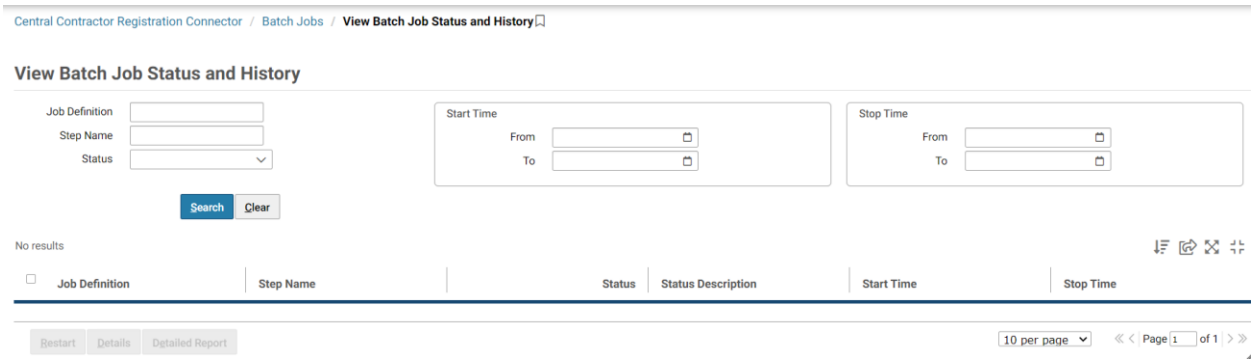


Table 6: Batch Job Status Parameters

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.

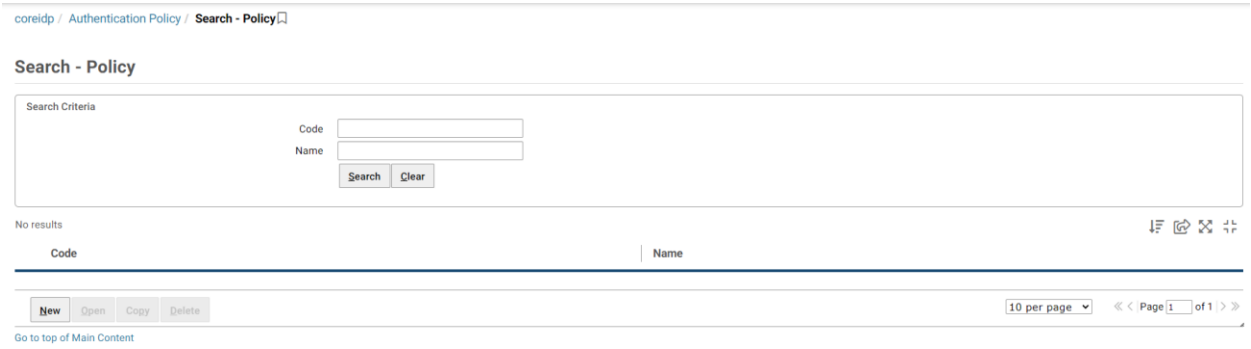
5.4 Security Policies

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). 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 15 displays the Security Maintenance Policy Window.

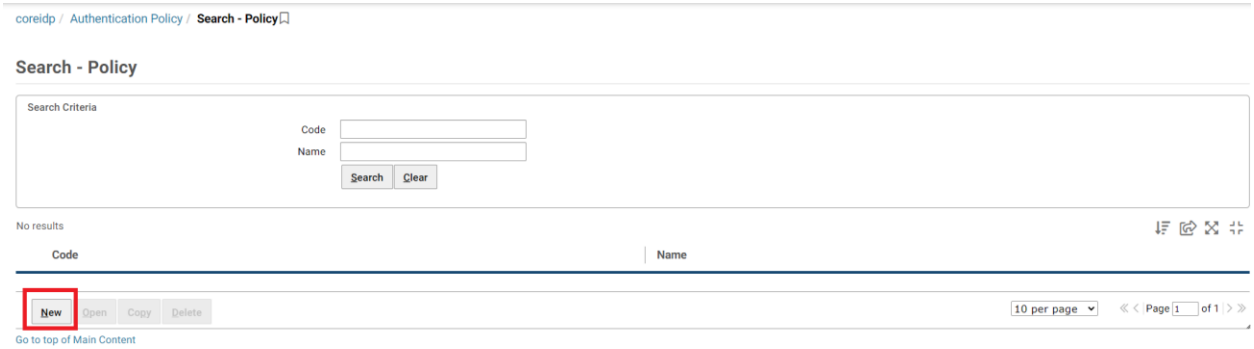
Figure 15: Security Maintenance Policy Window



5.4.1 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 15**). In order to add a new security policy, the Administrator must create a unique Policy Code (see **Figure 16**).

Figure 16: 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.

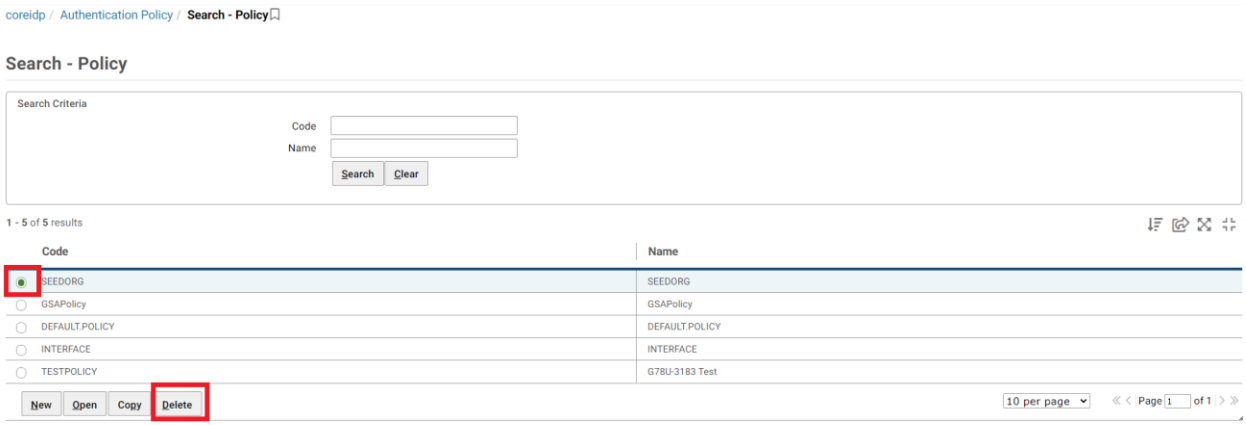
Table 7: Security Maintenance Information

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

Field	Description
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 17**).

Figure 17: Deleted 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.

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 15**).

5.4.2.1 Invalid Passwords

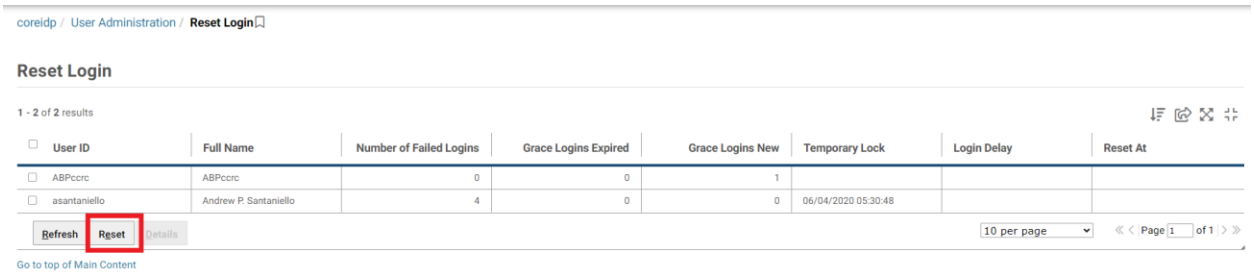
The Administrator can create invalid passwords to prevent them from being used in the CCRC. This may be done from the Invalid Password window, which is located under **Account Maintenance → Authentication Policy → Invalid Passwords**. In the Invalid Password window, the Administrator can add and delete passwords that the agency determines should be invalid (see **Figure 18**).

Figure 18: 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, which is located under **Account Maintenance → User Administration → Reset Login**. This may be done by selecting the User and selecting the button **Reset** under the list of Users (see **Figure 19**). Once the password has been reset, the user is able to login to the CCRC.

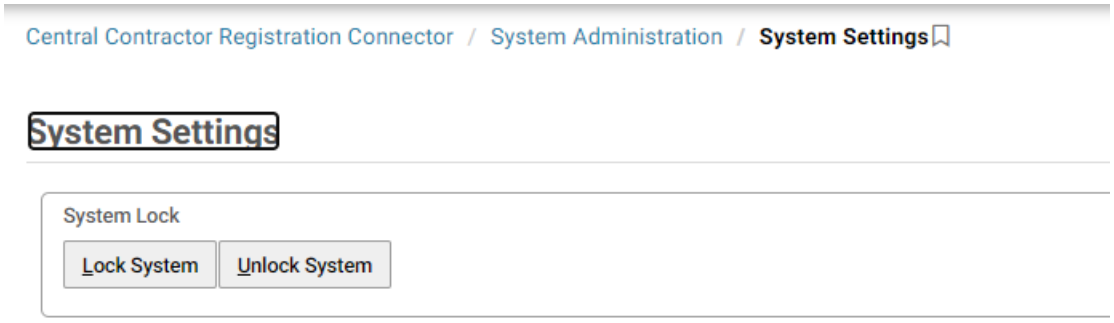
Figure 19: Reset Login



5.4.4 System Locking

The Administrator is able to lock and unlock the system from **CCRC → System Administration → System Settings** (see **Figure 20**). When the system is locked, only users with access during a system lock 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 20**).

Figure 20: System Lock Window



5.4.5 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.

5.4.6 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.

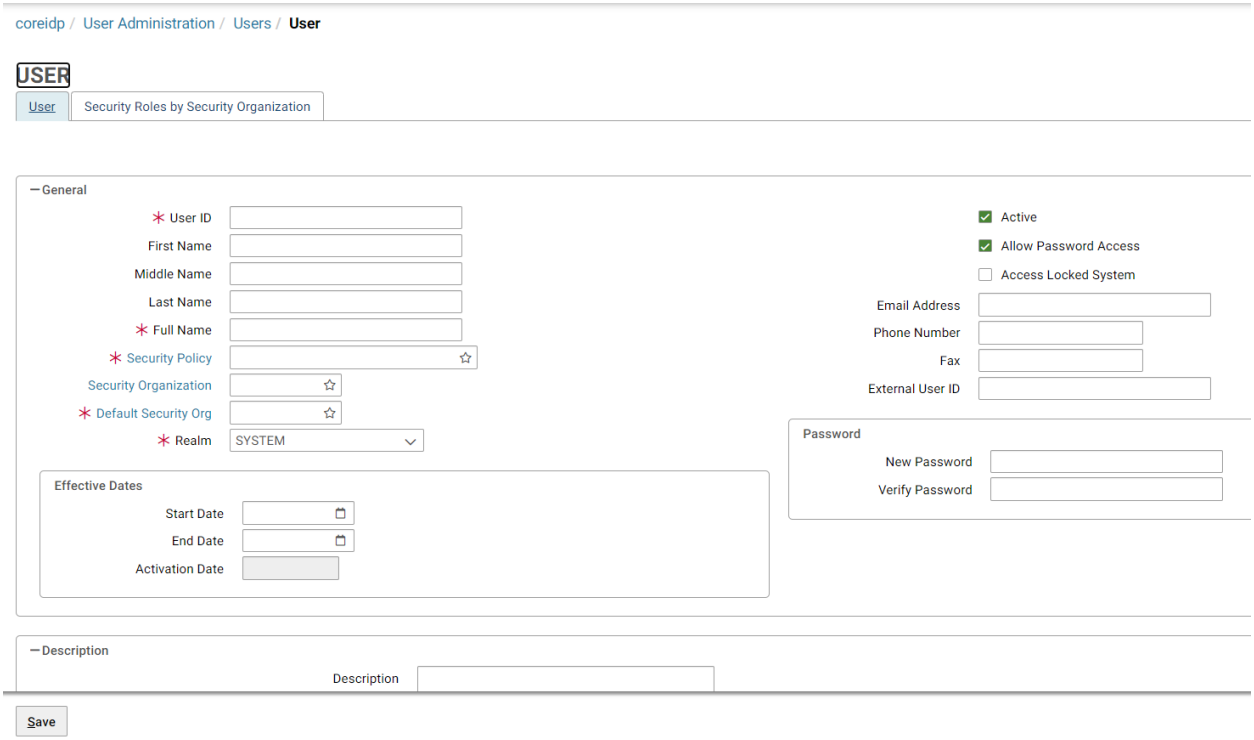
Additionally, dynamic extensibility provides the ability to populate transactions using pre-defined dynamic variables that set the value of a field based on the current date or user's principal data. Examples include a system administrator setting a global level dynamic extension to populate with a current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

5.5 Users and Groups

5.5.1 Users

An Administrator has the ability to search for, add, edit, and deactivate users, which is located under **Account Maintenance → User Administration → Users → User** (see **Figure 21**).

Figure 21: Edit User Details Window



5.5.1.1 Creating a New User

A new user account can be created on the Edit User Details tab (see **Figure 21**). 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 User ID that the user will use to access the system.	Required
New Password/Verify Password	The password that the user will use to access the system.	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

Field	Description	Required/Optional
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.

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 selects 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.

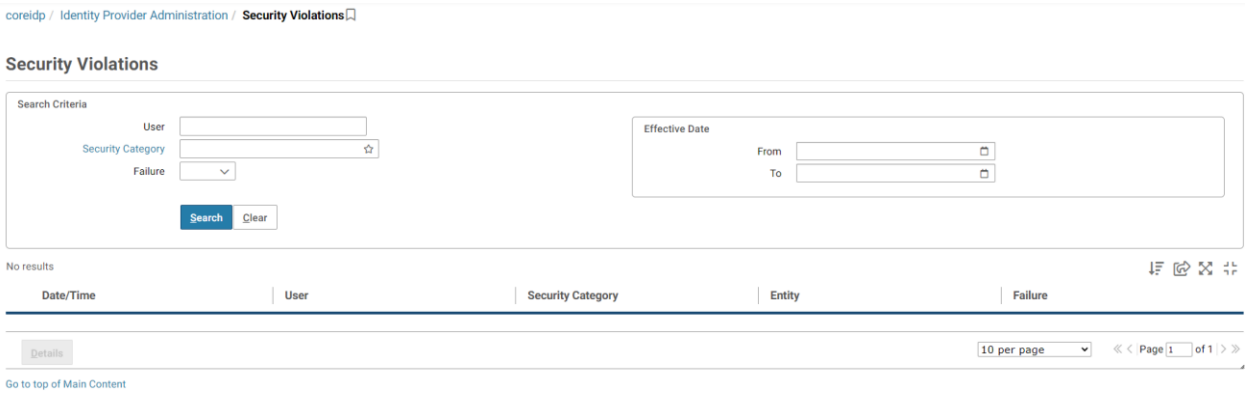
To reactivate the user, the Administrator must select the "Active" checkbox so that the checkbox is checked. Once the Administrator selects the "Save" button, the user account has been reactivated successfully and the user is now able to access the system.

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 22**).

The Administrator can search for all security violations committed in the system or for the security violations committed by a specific user (see **Figure 22**).

Figure 22: Security Log

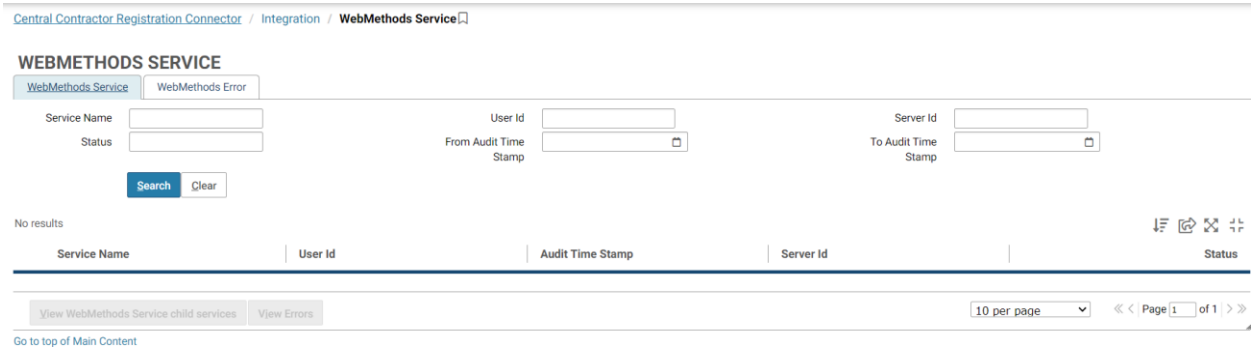


5.7 Vendor Data

5.7.1 Audit

The Administrator has the ability to look at an Audit log for a given vendor (see **Figure 23**). 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.

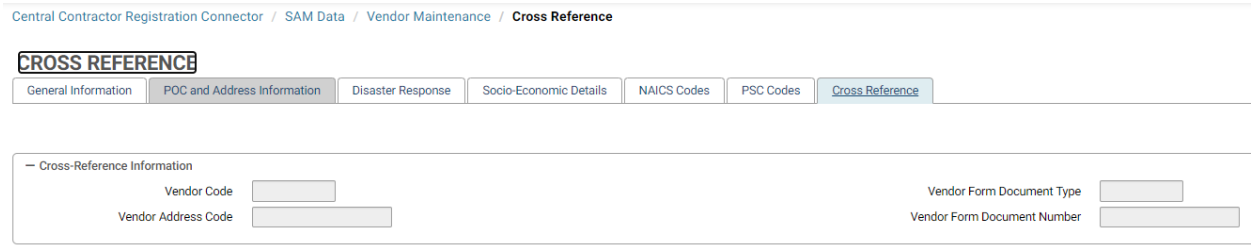
Figure 23: Audit Window



5.7.2 Cross Reference

In addition to being able to access the history of a particular vendor, the Cross Reference functionality provides valuable insight to an administrator (see **Figure 24**). 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 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.

Figure 24: Cross-Reference Window



5.8 Enhancements Included in 7.8 Upgrade

5.8.1 Link Address Codes

Currently, users are able to record a DODAAC on Pegasys 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 Pegasys, this field is reference-backed and utilizes the AAC/DODAAC import file to load AAC/DODAAC values into Pegasys 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.

5.8.2 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.

5.8.3 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 Pegasys required a mailing address for all vendors. When attempting to synchronize or submit one of these vendors through CCRC to Pegasys, they received a system error stating that a mailing address was required.

5.8.4 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 Pegasys Vendor record.

5.8.5 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 Pegasys 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).

5.8.6 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 Pegasys through MOMAPI.
- Concurrent with existing functionality, any changes made to records that are synchronized between CCRC and Pegasys via a SAM extract file will automatically be published to Pegasys. This will verify that the agency's financial application continues to store the most current data available for SAM entity records.
- From Pegasys, agencies will continue to have the possibility of transmitting this entity data to Vendor Self Service (VSS) and Maximo.

5.8.7 Vendor Update Support

This change allows the user to update vendors that do not have a DODAAC in Pegasys but that do have a matching DODAAC\DUNS\EFT Indicator\UEI 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 Pegasys 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 Pegasys 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.