Summary of Changes
Introduction
This guide is for people who use or support the use of the CDX application. It describes the functions related to the program.

Compensation Data Exchange or CDX has been developed as a secure Internet application with the goal of providing the ability to exchange data electronically. Primarily, the product is used for the purpose of sending, receiving, and managing transactions. The transmitted data uses the WCIO standards such as WCPOLS, WCSTAT, etc. These standards are found in the *WCIO Workers Compensation Data Specifications Manual*. For additional information on the standards, visit [www.wcio.org](http://www.wcio.org).

Additionally, included in the product, is the ability to administer security and access the lookup of Experience Rating Worksheets. It also allows access to PEEP and BEEP applications.

Various access levels of user accounts exist within CDX and it is set up so that users can only see data with which they are associated. This guide describes the various access levels and detailed instructions for each type of user.

The access levels and instructions for DCO Users are not included in this guide; however, the roles and responsibilities of DCO Users are described in this guide. This section is intended to assist non DCO Users in understanding how accounts are established and managed by DCOs.

Definition of Roles and Responsibilities
Following are the various roles, definitions, and responsibilities: (Note: The term “Carrier” and “Insurer” are interchangeable in the CDX® User Guide and on the CDX® application.)

Data Collection Organizations (DCOs)
A DCO is an organization that collects workers compensation information. The DCO can be a bureau, jurisdiction, or statistical agent.

CDX Central Support
CDX Central Support receives the Insurer UMG Primary Administrator applications, establishes the Carrier’s Insurer Admin Primary, and notifies affected DCOs that the Insurer Admin Primary has been established.

DCO Primary Administrator
A DCO Primary Administrator is responsible for the setup and maintenance of the DCO Users. The DCO Primary Administrator is allowed to create DCO User accounts for that DCO. They provide their DCO Users with the privileges needed to properly function in the CDX environment. They also administer Product Setup for their specific DCO.
DCO Users
DCO Users have no administrative responsibilities. The role of the DCO User is to perform the actual functions of the application.

Insurer UMG (User Management Group)
An Insurer User Management Group represents a group of users managed by a single Primary Administrator. There can only be one Primary Administrator per UMG. Users can be in one and only one UMG. Insurer Users are granted rights to send files and use applications within UMG’s by the Primary Administrator.

Insurer Primary Administrator
There can be one and only one Primary Administrator within an Insurer UMG. The Primary Administrator has the ability to set up products, create and maintain Insurer Users, request additional carriers be included in their UMG, grant application access and setup transfer permissions. They also request Third Party Administrators (TPAs) to be set up for their UMG and administer TPA rights for their UMG. The Primary Administrator also will be contacted periodically with a reminder e-mail to review their Users and to remove any Users that are no longer active.

Insurer User
The role of the User is to perform the actual functions of the application. Any User can have Admin permissions if this is granted by the Insurer Primary Administrator.

TPA Primary Administrator (Third Party Administrator)
The TPA Primary Administrator has the ability to create and maintain TPA Users including setting up transfer permissions for CDX products and application access. TPA organizations must be approved by the Insurer Primary Administrators for application access and transfer permissions.

TPA User (Third Party Administrator)
The role of the TPA User is to perform the actual functions of the application. Any TPA user can have Admin permissions if this is granted by the TPA Primary Administrator.
Signing Up with CDX

Request New UMG/Carrier Group

- Navigate to www.cdxworkcomp.org
- Click on “Login”
- Click on “New Account”:
- This will navigate to the Insurer UMG Primary Administrator Application.
Fill out the form completely, submit it online, print a copy, sign it, and follow the instructions to submit the hardcopy version.
Choose a username for the Primary Administrator. If the username is already taken, you will be instructed to choose another.

If you are entering a new carrier – click on **New Carrier** then enter the appropriate Carrier information below.

Enter the contact information for the Primary Administrator, the person who will administer your Users and carriers in CDX.

The Carrier information section will only appear if this is a new carrier.

Enter the contact information for the corporate officer authorized to approve this request on behalf of your company.

CDX Central Support will contact this person prior to processing your request.
Click the hyperlink ‘Terms and Conditions’ to view the CDX Terms and Conditions as a PDF in a separate window or tab.

**Agreement**

By submitting this form, you agree to abide by all Terms and Conditions (PDF download).

When you have finished filling out the application, click the Submit button

| Submit Form | Submit |

Errors on the form will be highlighted in red and displayed at the top of the screen. Fix any errors and click Submit again.

Example of errors on Insurer UMG Primary Administrator Application

- You must enter a User ID.
- You must enter an Email address.
- You must enter the authorizing officer’s first name.
- You must enter the authorizing officer’s last name.
- You must enter the authorizing officer’s title.
- You must enter the authorizing officer’s email address.

Once you have successfully submitted the application, you will see notification that the application has been sent:

**Application Submitted**

Your application has been submitted. Please click the link below to print a copy of the application. This printed form must be signed by the UMG Primary Administrator and an Authorizing Officer of the Applicant who shall be fully authorized to bind the Applicant to the Terms and Conditions of Use at www.CDXWorkComp.org. The completed form with the signatures, along with a copy of the authorizing officer’s business card or letter head, must be mailed, faxed, or e-mailed to:

CDX Central Support  
c/o Ferragut Systems  
2775 Meridian Pkwy  
Durham, NC 27713

E-mail: cdxinfo@wrbmca.org  
Fax: 919-572-0783

If a method other than mailing is used, a signed original must also be mailed to CDX Central Support. Once your account has been created, the Applicant’s Insurer UMG Primary Administrator will receive an e-mail notifying the UMG Primary Administrator that an account has been established and informing the Applicant’s Insurer Primary Administrator of its temporary password. A copy of this e-mail, without the password, will be sent to the Applicant’s Authorizing Officer.

For a printed version of the application click the hyperlink labeled ‘Click here to print this application for submission’ to launch a printable version.

| Print This Application | Click here to print this application for submission. |
• You will receive an e-mail titled “Insurer UMG Primary Administrator Application Received”, which also includes a link to print the application.

• The printable copy will include instructions on how to complete the application process.

• This printed application must be signed by the Primary Administrator and an Authorizing Officer of the Applicant who shall be fully authorized to bind the Applicant to the Terms and Conditions of Use at www.cdxworkcomp.org. The completed application with the signatures, along with a copy of the authorizing officer's business card or letterhead, must be mailed, faxed, or e-mailed to:

  CDX Central Support  
c/o Farragut  
2775 Meridian Parkway  
Durham, NC 27713  
E-mail: cdxinfo@wcribma.org  
Fax: 919-572-0783

**Replacing an Existing Primary Administrator**

To replace an existing administrator, use the same application process for setting up a new administrator described above.

The current administrator is not allowed to just simply change the name.

---

**Update Primary Administrator Contact Information**

You are about to submit a request to have your contact information updated. The request will be rejected if the application is not filled out in full or if you attempt to change the Primary Administrator to another user. If a new Primary Administrator is desired, then that user should logon and submit a request.

☐ By selecting this box, I certify that I have read and understand the information above.

[Proceed]
What’s Next:

- Central Support reviews the request
  - Rejecting
    - Requestor will receive an email notification with the reason for rejection
  - Approving
    - Outgoing Primary Admin and Authorizing officer receives email notification of request

- Outgoing Primary Admin reviews the request
  - Logs on to CDX
  - The following popup is displayed.

  ![Popup Image]

  - Rejecting
    - Enter a comment (reason) and select Reject
    - Requestor will receive an email notification with the reason for rejection
  - Approving
    - Select approve
    - Requestor will receive an email notification stating request was approved

- Authorizing Officer reviews the request (Required ONLY if the outgoing Primary Admin is no longer available)
  - Selects secure link in email
  - The following pop-up is displayed.
  - Rejecting
    - Enter a comment (reason) and select Reject
    - Requestor will receive an email notification with the reason for rejection
  - Approving
    - Select approve
    - Requestor will receive an email notification stating request was approved

Note: Once the outgoing Primary Administrator or Authorizing Officer approves/rejects the request, this popup will no longer appear.
**View Application Status**
- Log into CDX
- Select Admin->Requests->Primary Admin
- The Application Review and Authorization page will be in the view with current status information at the top of the page
- Status types include:
  - NOT SUBMITTED – the request was started but has not been submitted.
  - IN PROCESS – the request has been submitted, but not all required documents have been provided and reviewed by Central Support
  - PENDING APPROVAL – all attached documents meet the specified requirements, and additional parties have been asked to approve the request.
  - PENDING RESPONSE – one or more documents do not meet the specified requirements, and Central Support has requested a replacement.
  - APPROVED – the request has been approved by all required parties.
  - COMPLETED – Central Support has completed account setup.
  - REJECTED – the required approving parties have rejected the request or requirements were not met when the application was submitted. CDX will automatically set the application to rejected if all requirements are not met with in two weeks of the application submission

**Delete Application Request**
- Log into CDX
- Select Admin->Requests->Primary Admin
- The Application Review and Authorization page will be in the view
- Select the link provided in the "Click here to delete the current application" message at the bottom of the page.
- A pop up Delete Application message appears
- Select the Delete button to delete the application.
  - WARNING: Once selected, this action cannot be undone.
- Select Cancel if you do not want to delete the application.
Primary Administrator – Updating Contact Information

- Logon to CDX
- Select Admin ➔ Requests ➔ Primary Admin

- Select the “By selecting this box, I certify…” checkbox
- Select proceed

Update Primary Administrator Contact Information

You are about to submit a request to have your contact information updated. The request will be rejected if the application is not filled out in full or if you attempt to change the Primary Administrator to another user. If a new Primary Administrator is desired, then that user should logon and submit a request.

- By selecting this box, I certify that I have read and understand the information above.

- Proceed

- Verify contact information and make any changes necessary
- Changes will be applied only if the application is accepted
- Select Save and Next
• Fill out Authorizing Officer information
• Select the “By selecting this box, I certify…” checkbox
• Select Submit

![Status: NOT SUBMITTED](image)

Provide an Authorizing Officer

Please provide the contact information for an Authorizing Officer from your company. An Authorizing Officer must be a person employed by the requestor’s company who holds an office such as President, Vice President, CEO, Treasurer etc.

<table>
<thead>
<tr>
<th>Authorizing Officer</th>
</tr>
</thead>
<tbody>
<tr>
<td>First Name:</td>
</tr>
<tr>
<td>Last Name:</td>
</tr>
<tr>
<td>Title:</td>
</tr>
<tr>
<td>Email Address:</td>
</tr>
<tr>
<td>Phone Number:</td>
</tr>
<tr>
<td>Ext:</td>
</tr>
</tbody>
</table>

☐ By selecting this box, I certify that the information provided is an Officer of my company.

Save Contact Information

Submit

Click [here](link) to delete the current application.

• Select Print Application

![Status: IN PROCESS](image)

Print, Sign, and Upload Required Documents

You must now print the application, sign it, and upload a copy of the signed application on this page. Additionally, you must supply ONE of the following in .pdf format:

- A scanned copy of your Authorizing Officer's business card.
- A signed letter from your Authorizing Officer on company letterhead.

These documents may be uploaded using the fields below. You may submit files containing one or more of the required documents. Please check the box for all documents included in the uploaded file. Uploaded documents may be replaced at your discretion prior to being submitted to Central Support.

Print Application

• Scan the fully signed application and any supporting documents back onto your device.
**Steps to Upload Documents:**
- Select browse to locate the signed application and corresponding documents
- Select the appropriate check box for the documents that are being uploaded
- Select Upload File
- Repeat upload steps for each attachment

Reminder: You must upload the application with either the business card or signed letter to have the ability to submit your request

- Select submit

This completes the initial application submission steps.

**What's Next:**
- Central Support reviews the request
- Rejecting
  - Requestor will receive an email notification with the reason for rejection
- Approving
  - Outgoing Primary Admin and Authorizing officer receives email notification of request
• Authorizing Officer reviews the request
  • Selects secure link in email
  • The following popup is displayed.

![Application Review and Authorization popup](image)

- **Rejecting**
  - Enter a comment (reason) and select Reject
  - Requestor will receive an email notification with the reason for rejection

- **Approving**
  - Select approve
  - Requestor will receive an email notification stating request was approved

**Note:** Once the Authorizing Officer approves/rejects the request, this popup will no longer appear.

**View Application Status**

• Log into CDX
• Select Admin->Requests->Primary Admin
• The Application Review and Authorization page will be in the view with current status information at the top of the page
• Status types include:
  • NOT SUBMITTED – the request was started but has not been submitted.
  • IN PROCESS – the request has been submitted, but not all required documents have been provided and reviewed by Central Support
  • PENDING APPROVAL – all attached documents meet the specified
requirements, and additional parties have been asked to approve the request.

- **PENDING RESPONSE** – one or more documents do not meet the specified requirements, and Central Support has requested a replacement.
- **APPROVED** – the request has been approved by all required parties.
- **COMPLETED** – Central Support has completed account setup.
- **REJECTED** – the required approving parties have rejected the request or requirements were not met when the application was submitted. CDX will automatically set the application to rejected if all requirements are not met within two weeks of the application submission.

### Delete Application Request

- Log into CDX
- Select Admin->Requests->Primary Admin
- The Application Review and Authorization page will be in the view
- Select the link provided in the “Click here to delete the current application” message at the bottom of the page.
- A pop-up Delete Application message appears
- Select the Delete button to delete the application.
- Select Cancel if you do not want to delete the application.
Create a New Insurer User

Before Users can log into CDX, BEEP, PEEP, or EXR they must be set up as a user within their Insurer UMG. The Primary Administrator or a User with Admin permissions can create and set up users. This section covers how to create or edit the User login record and their privilege level. Once these tasks are completed, Application Access and Transfer Permissions need to be added or reviewed. Section Setup Application Access has instructions.

- Log in to your Insurer UMG.

- The screen with the Notifications information will appear. Choose Profile then MyUMG.
- The screen labeled Insurer UMG’s will appear.
My Account
The My Account menu will allow a user to view or change their profile by clicking on Edit Profile. The user can also click on Change Password to change their password.

The User Profile will be displayed with the ability to edit and reset the password. The changes can be saved by clicking the save button.
Change Password
A user can change their password by entering the Current Password and then entering a new password.

**Reset Password**

Current Password: 
Enter new password: 
Retype new password: 

Reset

**Password Requirements:**
- Password must be at least 8 characters long
- Password must contain at least 1 numeric characters
- Password must contain at least 1 lowercase characters
- Password must contain at least 1 uppercase characters
- Password must contain at least 1 characters from this list: @#$%^&+=
- Password cannot contain Username
- New Passwords cannot match any of the previous 3 passwords.

To cancel password reset, navigate away from this page using top dropdown menus.

Forgot Password
If a user forgets their password the option to receive a new password is located on the logon page. The user would need to click the 'Forgot Password' hyperlink.
This will open the Forgot Password screen where the user will be prompted to enter their username and text from a security image. Once entered the user will click submit to receive an e-mail that contains a link to initiate the password reset process. The link contained within the e-mail is only good for 10 minutes. Clicking on the link within the e-mail will route the user to the CDX reset password page.

If this screen was navigated to in error the user can select the ‘Click here to return to login page’ to exit the ‘Forgot Password’ screen.

**Password Attempts**

If a user fails to provide the correct login credentials within 3 attempts the user will be locked out of the application. If this happens, contact your Primary Administrator for resolution. The Primary Administrator will need to send a reset password for the user. The Primary Administrator navigates to the user under My UMG and clicks the edit icon and the ‘Reset Password’ button. The user will then receive an e-mail with the reset password.

Once the password has been reset, the user will receive an e-mail with the subject ‘Password reset by administrator’. Upon login the user will be prompted to reset their password following the password requirements.

Once the password has been reset, the user will receive an e-mail with the subject ‘Password Reset’.

**Password Expiration**

Passwords will expire every three months and users will be forced to create new passwords based on the password requirements.
CDX Notifications or Announcements

The screen shown upon log in is called either the Notifications or Announcements screen. This screen will display any changes or upcoming updates to the CDX Products.

Help

This menu item will allow the user to navigate to Online Training, CDX Admin User Guide, BEEP, PEEP and EXR User Guides, FAQ, and Contact List

Online Training

This link will open the Computer Based Training (CBT) page.

CDX Admin User Guide

This link will open a PDF of the CDX Admin User Guide document.

CDX BEEP, PEEP and EXR User Guides

These links will open a PDF of the individual BEEP, PEEP or EXR User Guides.
FAQs
This link navigates to a list of administration questions.

You also have the option to click on one of the specific products or you can scroll down.

Contact
This screen displays a listing of all the contact names and contact information by product.

Note: View the website page for the most current contact information.
At the bottom of the CDX screen are the following options:

Terms and Conditions
This link will open a PDF of the CDX Terms and Conditions document.

**CDX® TERMS AND CONDITIONS OF USE**

**INTRODUCTION**
Welcome to the Web site of Compensation Data Exchange, LLC (the “CDX® Site”). Please review the following terms and conditions concerning your use of this site.

**COMPENSATION DATA EXCHANGE**
**Compensation Data Exchange** is a service of Compensation Data Exchange, LLC (“CDX®”), which is owned by the following data collection organizations:

- Workers’ Compensation Insurance Rating Bureau of California
- Delaware Compensation Rating Bureau, Inc.
- Workers’ Compensation Rating and Inspection Bureau of Massachusetts
- Compensation Advisory Organization of Michigan
- Minnesota Workers’ Compensation Insurers Association, Inc.
- New Jersey Compensation Rating and Inspection Bureau
- New York Compensation Insurance Rating Board
- North Carolina Rate Bureau
- Pennsylvania Compensation Rating Bureau
- Wisconsin Compensation Rating Bureau
**CDX Security Overview**
This menu will open a PDF of the CDX Security Overview document.

---

**CDX Information Security and Protection Overview**

The Compensation Data Exchange system (CDX) is a secure Internet facility for the electronic exchange of workers compensation insurance data between carriers and Data Collection Organizations (DCOs). Primarily, CDX is used to send, receive, and manage transactions. The transmitted data uses the WCIO format standards such as WCPOLS and WCSTAT. Additionally, CDX allows access to CDX’s Web-based PEEP and BEEP systems for entering WCPOLS and WCSTAT data and can allow lookup of Rating Worksheets.

The purpose of this document is to provide a general overview for all participants of how CDX protects the system and the data. The accessibility, security and integrity of member company data are of the utmost importance to CDX. All CDX systems that hold member data run on a proven infrastructure designed to provide maximum security, performance, and reliability.

---

**CDX Retention Policy**

**Record Retention and Deletion Policy:**

Records deleted on a daily basis:

- EXRs that have an expiration date older than 2 years and an issue date older than 2 years
- Policies that have an expiration date older than 2 years and an entry date older than 2 years
- Delete any USRs that meet the following criteria:
  - Have a most recent submission date that is older than 3 years or
  - Have not been submitted and have an entry date older than 3 years

See the PEEP and BEEP User Guides for additional archive information.

---

Also, at the bottom of the screen are FAQ and Contacts which were presented in the Help section.
About Us

Overview:
Compensation Data Exchange, LLC (CDX) was formed in 2003 to provide a common platform for insurance carriers and data collection organizations (DCOs) to exchange data that conforms to the industry approved WClO format. CDX benefits its customers by providing a single location for SFTP/FTPS configuration and their fully redundant file transmission architecture ensures secure delivery of data to the recipient. In addition to file transmissions, CDX offers its customers products to satisfy DCO policy and unit statistical data reporting requirements as well as products to distribute experience rating information. While many of the DCOs offer data reporting tools on their respective, secured websites, CDX is committed to providing additional options for customers to meet statutory reporting obligations for policy and unit statistical data.

Mission Statement:
CDX enables the secure exchange of transactional workers’ compensation data by providing insurers and their data reporters a common platform for submitting data to and accessing data from DCOs. Specifically, CDX will:
- Provide insurers the tools and interfaces necessary for the timely and complete exchange of data with the DCOs that comprise the CDX membership.
- Facilitate data reporting in accordance with the WCIO’s national reporting standards.
- Seek continuous improvement to optimize the efficiency of the data exchange process and to respond to the evolving needs of insurers.

CDX Members
- Workers’ Compensation Insurance Rating Bureau of California
- Delaware Compensation Rating Bureau, Inc.
- Workers’ Compensation Rating and Inspection Bureau of Massachusetts
- Compensation Advisory Organization of Michigan
- Minnesota Workers’ Compensation Insurers Association, Inc.
- New Jersey Compensation Rating & Inspection Bureau
- New York Compensation Insurance Rating Board
- North Carolina Rate Bureau
- Pennsylvania Compensation Rating Bureau
- Wisconsin Compensation Rating Bureau
ADMIN menu

My UMG
The My UMG option is only available to the Primary Administrator and Users who have Admin permissions. My UMG will take a user to the User Management Group. The tabs will be accessible depending on the user’s security.

Base: Name of the Insurer UMG
**Users**: A listing of all users in this Insurer UMG. Add new users and edit users from this screen.

- To setup a new user, choose the tab labeled Users.
- Click the Add User button.

The Create User screen will appear.

- Create a user login name (must be unique in CDX®, no spaces allowed). The only special characters allowed will be: $ _ -
- Check the active box to make this user active immediately.
- Fill in the users first and last name and the basic contact information (e-mail, phone, address). Fields with a little icon to the right are required fields.
- When finished click the Create button.

- A “Success” box will appear with the message “User successfully created”
- The new User will show up in the users list.
- The new User will receive an e-mail with their temporary password.
- Upon login, they will be prompted to change their password.
Edit User

- Select ADMIN then My UMG.
- Click the Users tab.
- To edit a user click the pencil icon at the end of the user information or the hyperlink of the users name. The Edit User screen will appear where the user’s information can be edited.

To cancel the edit, click the Users hyperlink to navigate back to the Insurer UMG’s screen.
• To save the edit click the Save button. A “Success” box will appear with the message “User successfully saved”
Inactivating a User account

- Uncheck the Active box
- Click Save
- Click OK on the “Success” box
Deleting a User account

- Click on the Delete User button
- Confirm deletion by clicking OK
- Click OK on the “Success” box
Reset User Password

- Select ADMIN then My UMG.
- Click the Users Tab.
- Click the hyperlink for the user or the pencil icon at the end of the user information; this will navigate you to the Edit User screen.

Password Requirements:
- Password must be at least 8 characters long
- Password must contain at least 1 numeric character
- Password must contain at least 1 lowercase character
- Password must contain at least 1 uppercase character
- Password must contain at least 1 character from this list @#$%^&*+=!
- Password cannot contain Username
- New Passwords cannot match any of the previous 3 passwords.
- To exit, select the 'Users' hyperlink to navigate back to the Insurer UMG's screen.
Upon the Users next login, they will be prompted for the Current Password (the reset password received via e-mail). They must enter a new password that meets the password requirements.

Once complete the user will receive an e-mail that the reset password was completed successfully.

Reset Password

Current Password: 

Enter new password: 

Retype new password: 

Password Requirements :
- Password must be at least 8 characters long
- Password must contain at least 1 numeric character
- Password must contain at least 1 lowercase character
- Password must contain at least 1 uppercase character
- Password must contain at least 1 character from this list @#$%^&+=!
- Password cannot contain Username
- New Passwords cannot match any of the previous 3 passwords.
Setup Permissions for Users

- Click ADMIN then My UMG.
- Click the Permissions tab.

The screen will list all users within your Insurer UMG.

The columns listed on the right side of the screen are the functions available for users to perform. Grant or deny a User access by changing the blank circle to a green check mark (for granting the permission) or red x (for denying the permission) by clicking the circle.

- To save the changes to this screen click Save.
- To undo the changes to this screen click Reset.
- If the User setting up permissions is not the Primary Administrator, they may not be able to change permissions. Users also cannot change their own permissions.

The following describes the Permission Columns:

**Manage Users and Permissions for this UMG**
Granting this permission will allow the user the ability to add, edit and delete users for this UMG.

**Manage Carriers and Carrier Groups**
Granting this permission will allow the user the ability to request a new carrier for the UMG.
Manage Locations for this UMG
Granting this permission will allow the user to add, edit and delete Locations for the UMG. Locations are where and how the carriers will receive files.

Manage FTP Credentials
Granting this permission will allow the user to add, edit and delete FTP credential. FTP credentials are setup for the secure FTP of files.

Manage File Transfer Configuration
Granting this permission will allow the user to setup for users to send files by product type, such as WCPOLS, WCSTAT, and WCMED.

Basic Insurer Access Rights
This permission is defaulted and gives the user basic access rights to the web application.

Basic Application Access Rights
This permission is defaulted and gives the user basic application access rights to the web application.

Warning: New Insurer User setup is not complete without Application Access and Transfer Permissions. Section Setup Application Access has instructions to configure these permissions.
Carriers
This tab contains a list of the carriers in this Insurer UMG. Each column can be sorted and the user may enter data in the blank fields at the top of each column to filter the list.

Once a carrier is approved on the Carrier Request tab they are moved to this list.

Selecting a carrier link will display the carrier profile information that can be edited and will provide the ability to edit the Global Product Setup, the ETR Response Setup, and Registrations.

Carrier Profile Information
The carrier profile fields can be updated by changing the data and clicking the save button. There is also an alternate method (path) of modifying the application access and transfer permissions for a User by changing the carrier drop down list.

Application Access and Transfer Permissions are explained later in the Guide.
Global Product Setup

The locations for the products being received by the Carrier are assigned here.

ETR Response Setup

The e-mail that will receive delivery status notification and due days by product are assigned here.
Registrations

The Carrier DCO registration status list includes the ability to view carrier profile information by selecting the pencil icon for a given DCO.

To view the Associated DCO Product Setup screen and set up receiving files from a specific DCO, click on the icon farthest to the right.

Mark the checkbox to enable a Location for a product and select from the drop down list. For instructions on how to configure Locations, view section Setup Locations.
Carrier Groups
Listing of the carrier group(s) in the Insurer UMG.

Carrier and TPA Requests
The Primary Administrator or a User with Admin permissions will have an Admin menu where they can create Carrier Request and TPA Requests.

Create a Carrier Request
- Choose the Admin menu, then Requests, then Carrier.
- This will navigate to the Carrier Requests screen.
- The Carrier Request screen will list the current carrier requests for your UMG and their Status.
- To request a new carrier, click the ‘Request a New Carrier’ button.

- The Request a New Carrier screen will appear.
- Fill out the Carrier Name, NCCI Number, Phone and Address information. Required fields are marked with the exclamation point in circle icon.
- Click the Submit Request button. To cancel click the Back button.
A pop-up message displays indicating the request has been submitted for review.

You will also receive an e-mail titled ‘New Carrier Request’ indicating that your request has been submitted for review.

The request will appear in the Carrier Requests list.

The Carrier Request screen can also be accessed by choosing My UMG.

Select the Carrier Requests tab.

Select the Request a New Carrier button. This will navigate to the Carrier Requests screen.
Request TPAs

- Choose the Admin menu, then Requests, then TPA. This will navigate to the TPA Requests screen.
- Click the Create Request button.
- Enter the TPA Name and TPA Number, if known.

- The requesting Primary Administrator is pulled from the logged in user.
- Complete the Initial Administrative User information.
- To process the request, select the ‘Send To System Admin’ button.
- To cancel the request, choose the ‘Cancel’ button.
- The new request will appear in the TPA requests page with an “Open” status.
- An e-mail will be sent to you with the title “New TPA Request” stating that your request has been submitted for review.
- To view the approved TPA’s, select Profile, then My UMG. Click the TPAs tab and you will receive a list of TPAs linked to your UMG.
- If the Active checkbox is not checked, then this TPA is not active.

Once a TPA is linked to your UMG, you will need to give the TPA, Application Access and Transfer Permissions. Follow the same process used to give permissions to Users (see Setup Application Access). The TPA will appear in
Application Access as a User with User Type TPA and in Transfer Permissions as a Sender with Sender Type TPA:
Disassociate TPAs

- Choose the Admin menu, then My UMG, then the TPA tab. This will navigate to the TPA screen.

- Click on the TPA name you wish to disassociate.
- Then click on the Dissociate button.

- An “Are you sure…” confirmation box will pop up. Select OK.
- A “Successfully disassociated…” confirmation box will pop up. Select OK.

- The TPA will no longer appear in the list of TPAs for the UMG and the TPA will no longer be able to report or view data for the carrier(s) in the UMG.
Setup Locations
Locations are where and how carriers will receive files that are sent from the DCOs. On the ADMIN tab, select My UMG, and then Locations.

The Location screen will display the UMG and the current Location setups. Locations are setup as to where files can be sent, whether it is SFTP, e-mail, etc. Once Locations are setup, the Primary Administrator or User with Admin permissions will be able to setup the Global Product Setup for each product type with the Location.

Add Location
- Select ADMIN, My UMG, then the Locations tab.
- Select the ‘Add Location’ button.

- The ‘Create Location’ screen will appear.
- In the Location Name field, enter the product type; ex. WCRATING or WCNOA.
- The location you set up will be the default location where this file will be received.
- Fields to complete
  - Check the box for Global
  - Check the box for Active
  - Compression: Choose either Zip or None
  - Encoding: Choose either ASCII or EBCIDIC
  - Line Terminator: Choose either None, CR or CRLF
  - Failure Notification E-mail: Input a valid e-mail address for the failure notification
  - Type: Choose how you would like to receive the file: either FTP, SFTP, E-mail, or Web.
For FTP
Please note that only secure FTP (SFTP) connections are permitted to connect to the CDX FTP Server.

- Address: FTP server address
- Username: Input your username (as listed in the FTP Credentials page).
- Password: Input your password (as listed in the FTP Credentials page).
- Directory Tree: input the directory tree
- Append: check the box if you want this to apply.
- SSL: check the box if you want this to apply.

For SFTP

- SFTP Address: SFTP server address
- Username: Input your username (as listed in the FTP Credentials page).
- Password: Input your password (as listed in the FTP Credentials page).
- Directory Tree: input the directory tree
- Append: check the box if you want this to apply.

For E-mail

- Recipient E-mail: Valid e-mail address for the recipient of the file.

For Web

- Nothing additional.

- Click the ‘Create’ button to save the location.
- Click the ‘Back’ button to cancel out of creating a location.
Edit Location

- Click ADMIN, then My UMG.
- Click the Locations Tab.
- Click the pencil icon located at near the end of the row.

- The ‘Edit Location’ screen will appear, and you can change any of the fields. Click the ‘Save’ button to save the changes.
- Click the UMG Locations Listing hyperlink to cancel out of making any changes.
Delete Location

- Click ADMIN, then My UMG.
- Click the Locations Tab.
- Click the trash can located at the end of the row.
- A popup will appear asking “Are you sure you want to delete this Location?”
- Click OK to delete the location. You will receive a popup “Location Deleted successfully”
- Click Cancel to terminate the deletion. You will be navigated back to the Locations screen.

Setup FTP Credentials

Setup, edit and delete FTP credentials.

Create FTP Credentials

- Click ADMIN, then My UMG.
- Click the FTP Credentials tab.
- Click the ‘Create’ button.
- The Create FTP Credentials screen will appear.
- Make sure the enabled check box is checked.
- Enter a unique username for the FTP Credentials.
- Enter a password following the password requirements or click the Generate Password button to generate a random password.
- Enter a description for the FTP Credentials (not required).
- Click the ‘Create’ button to save the FTP Credentials.
- Click the ‘Back’ button to cancel out of creating the FTP Credentials.

Technical Contact Information

If one does not exist for your organization, a pop up will be displayed asking for the Technical Contact information. This person is normally an IT staff member that is responsible or familiar with your organizations FTP setup/process.

- Enter the name (first & last)
- Enter the Email address
- Enter the Phone number
- Click Save.
- Click Close.
The Technical Contact information will be displayed on the FTP Credential Tab

To edit the Technical Contact Information

- Make any necessary changes
- Click Save.

Edit FTP Credentials

- Click ADMIN, then My UMG.
- Click the FTP Credentials tab. Edit Credential is selected by default.
- Click the pencil icon located at near the end of the row.

- The Edit Credentials screen will appear, and you can change any of the fields.
- Click the ‘Save’ button to save the changes.
- Click the ‘Back’ button to cancel out of the changes.
- To edit the FTP Transfer Permissions, click on the down arrow next to Edit Credential to select TransferPermission.
- Click Save to save changes or Reset to undo changes. For further details on this type of permission, see the Setup Transfer Permission section of this document.
Delete FTP Credentials

- Click ADMIN, then My UMG.
- Click the FTP Credentials Tab
- Click the trash can located at the end of the row.
- A pop-up will appear asking “Are you sure you want to delete this FTP credential?”
- Click OK to delete the FTP Credential. You will receive a pop-up “Successfully deleted FTP credentials.”
- Click Cancel to terminate the deletion. You will be navigated back to the FTP Credentials screen.
Successfully deleted FTP credentials

OK
Setup Application Access

The Primary Administrator or User with Admin permissions has the ability to set up application access by Users and by Carrier.

- Select ADMIN, then My UMG.

- Click the Application Access tab.

  - The default view is Group by Carrier and all the users will be shown under each carrier name when expanded.
  - The Expand All button will expand all collapsed listings. You can also click the + icon next to the name to expand one at a time.
  - The Collapse all button will collapse all expanded columns. You can also click the – icon next to the name to collapse one at a time.
  - Click Expand All button to see all users by carrier Id.
  - Click Collapse All button to see only CarrierNames.
To group the screen by users, choose ‘Group by User’ in the dropdown box and the screen will show the User name and all the carriers this user has access to when expanded.

**Example of Group by Carrier**

The Group by Carrier screen displays a listing of all carriers and the users per carrier. It also indicates the Applications that each user is allowed to access.

### Insurer UMGs  ▶  Jessica Test Group

<table>
<thead>
<tr>
<th>Carrier Name</th>
<th>Carrier RCC</th>
<th>User Name</th>
<th>First Name</th>
<th>Last Name</th>
<th>User Type</th>
<th>Access UCEP</th>
<th>Access PTEP</th>
<th>Access ETR</th>
<th>Access ECR</th>
</tr>
</thead>
<tbody>
<tr>
<td>Daisy Duck Carrier</td>
<td>75999</td>
<td>Donald Duck</td>
<td>Donald</td>
<td>Duck</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>goofygoof</td>
<td>Goofy</td>
<td>Goof</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mickeymouse</td>
<td>Mickey</td>
<td>Mouse</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>minnie mouse</td>
<td>Minnie</td>
<td>Mouse</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pluto</td>
<td>Pluto</td>
<td>the dog</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Geofy Carrier</td>
<td>59999</td>
<td>Donald Duck</td>
<td>Donald</td>
<td>Duck</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>goofygoof</td>
<td>Goofy</td>
<td>Goof</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mickeymouse</td>
<td>Mickey</td>
<td>Mouse</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>minnie mouse</td>
<td>Minnie</td>
<td>Mouse</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pluto</td>
<td>Pluto</td>
<td>the dog</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td>Pluto Carrier</td>
<td>33333</td>
<td>Donald Duck</td>
<td>Donald</td>
<td>Duck</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>goofygoof</td>
<td>Goofy</td>
<td>Goof</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>mickeymouse</td>
<td>Mickey</td>
<td>Mouse</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>minnie mouse</td>
<td>Minnie</td>
<td>Mouse</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
<tr>
<td></td>
<td></td>
<td>Pluto</td>
<td>Pluto</td>
<td>the dog</td>
<td>User</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
</tr>
</tbody>
</table>
Example of Group by User
The Group by User screen displays each user the Carriers are associated with and the Application they are allowed to access for the Carrier.

Insurer UMGs ➤ Jessica Test Group

- Setup access to BEEP®, PEEP®, ETR and EXR by clicking the circle under each for each user or carrier.
- To allow access, the box should have a green checkmark.
- To deny access, the box should have a red “X”.
- If nothing has been done, the box will have a blank circle. This essentially is the same as access denied.
- To save the changes to the Application Access, click the Save button.
- After saving changes, you will get a Success pop-up that says “Permissions successfully saved”.
- To reset the screen and remove any changes that have been made, click the Reset button.
- The Primary Administrator cannot make changes to their own Application Access, but they will have the default access to all.
Setup Transfer Permission

Ability to setup and edit Transfer access to DCOs by Product.

- Click ADMIN, then My UMG.
- Click the Transfer Permission tab.
- The Expand All button will expand all collapsed listings. You can also click the + icon next to the name to expand one at a time.
- The Collapse all button will collapse all expanded columns. You can also click the – icon next to the name to collapse one at a time.
- Filter By, Group Columns By, and Group RowsBy:
  - Destination: Filter by the DCO
  - Source: Filter by Carrier
  - Sender: Filter by User
  - Product: Filter by Product Type

Note: When filtering the screen all 3 cannot be the same filter or you will receive an error.

- However the screen is filtered, the actions used will be the same.
- To allow access, the box should have a green checkmark.
• To deny access, the box should have a red ‘X’.
• If nothing has been done, the box will have a blank circle. This, essentially, is the same as access denied.
• To save the changes to the Transfer Permissions, click the Save button.
• After saving changes, you will get a Success pop-up stating “Permissions successfully saved.”
• To reset the screen and remove any changes that have been made, click the Reset button.

ETR (Electronic Transmittal Record)
Within this menu a user has access to the ETR Search, ETR Log and ETR Web Upload.

ETR Search
ETR Search allows users to search for submissions sent or received for all carriers in the UMG or a specific carrier. ETR Log is a complete listing of all submissions for a UMG.

• Click the ETR menu
• Choose ETR Search
  • When conducting a search, the search can consist of a single-search criteria, or a combination of criteria.
  • Search by dates: enter a date range in mm/dd/yyyy format or click the hyperlink to search for today’s date, a week date range, month date range, or a year’s date range. The dates will be prefilled if you choose the hyperlink. You can also click in the blank box to bring up a calendar to select a date from.
  • Search by Statuses/Grouping which consist of:
    o ETR Processing Status: the processing status of the file (see glossary for status explanations). Choose one from the dropdown list
    o Product: All CDX products; choose one from the dropdown list.
    o Submission Type Code: Type of file; choose one from the dropdown list.
    o File Picked Up Status: either true or false; Choose one.
  • Search by DCO or Carrier.
  • Search by File Name.
  • Search by ETR ID.
Once you have entered your search criteria, select the Search button or press the Enter key on your computer.

To clear entered or chosen search criteria, click the Clear button.
- The ETR Search Results will display with the search criteria shown at the top of the applicable column.
- The First button will bring you to the first page of the list.
- The Previous button will take you to the previous page in the list.
- The Goto button will take the user to a specified page. In the Page box enter the page number to go to. If the user keys a number greater than the total of pages the system will take the user to the last page.
- The Next button will take you to the next page in the list.
- The Last button will take you to the last page of the list.
- The icon located at the end of the row will take you to a screen which displays the details of the file. See ETR Log section for further description of this screen.
- The down arrow icon at the end of the row allows you to download the file by opening or saving the file. This is limited to the last month of results.
- To refine the search or to change the search completely, click the Refine Search button at the bottom of the screen. This will re-direct you to the ETR Search screen with your current search criteria pre-filled.
ETR Log
The ETR Log will display all files without a specific search.

- Click the ETR menu.
- Choose ETR Log.
- The First button will bring you to the first page of the list.
- The Previous button will take you to the previous page in the list.
- The Goto button will jump you to a specified page. In the Page box enter a number and this number cannot be larger than the total of pages.
- The Next button will take you to the next page in the list.
- The Last button will take you to the last page of the list.
- The pencil icon located near the end of the row will take you to a screen which displays the details of the file. See below for further description of this screen.
- The down arrow icon at the end of the row allows you to download the file by opening or saving the file. This is limited to the last month of results.
- To refine the search even further or to change your search completely, click the Refine Search button at the bottom of the screen will direct you to the ETR Search screen with your current search criteria.
- Another option for refining your search from the results screen is by entering values into one or more of the blank boxes under each column description, such as File Name, Sender, etc.
- For example, to see all files with a record count of 72 you would enter the number 72 in the record Count box and click enter. The list would be filtered to only show files that have a record count of 72.
- You can also refine by selecting a dropdown value from certain columns such as Product or ETR status, for example. The search results will immediately change. For example, selecting WCPOLS will show only WCPOLS files after selecting the value.

<table>
<thead>
<tr>
<th>File Name</th>
<th>Product</th>
<th>Count</th>
<th>Date</th>
<th>Sender</th>
<th>Receiver</th>
<th>Status</th>
<th>Due</th>
<th>Response</th>
</tr>
</thead>
<tbody>
<tr>
<td>551041032000651.psd</td>
<td>WCPOLS</td>
<td>72</td>
<td>11/01/2006 12:12:12</td>
<td>55104</td>
<td>00022</td>
<td>Sent</td>
<td>2009</td>
<td>Accepted</td>
</tr>
<tr>
<td>551041032000652.psd</td>
<td>WCPOLS</td>
<td>72</td>
<td>11/01/2006 12:12:12</td>
<td>55104</td>
<td>00022</td>
<td>Sent</td>
<td>2009</td>
<td>Accepted</td>
</tr>
<tr>
<td>551041032000653.psd</td>
<td>WCPOLS</td>
<td>72</td>
<td>11/01/2006 12:12:12</td>
<td>55104</td>
<td>00022</td>
<td>Sent</td>
<td>2009</td>
<td>Accepted</td>
</tr>
</tbody>
</table>
• The Refine Search button at the bottom of the screen will direct you to the ETR Search screen where the list can be filtered.

• The pencil icon (says Edit when hovered over with cursor) located near the end of the row will take you to a screen which displays the details of the submission.

• The down arrow icon at the end of the row (says Download when hovered over with cursor) allows you to download the file by opening or saving the file. This is limited to the last month of results.

• Base tab displays the ETR Record base, the ETR record details and the Contact information from the submission.
ETR Record Base

Sender: 33333
Receiver: 00032
Product: WCSTAT
Original FileName: UBER_33333_C_00032_201308190931.TXT
New FileName: 52754b37-ac07-46f6-ac6e-c0e6956b392c/UBER_33333_C_00032_201308190931.TXT.20130819093124
Submission Type Code: S
Record Count: 6
Date Received: 8/19/2013 9:31:24 AM

ETR Record Details

Data Provider Type Code: WCS
Data Provider Code: 33333
Data Receiver Code: 00032
Data Type Code: E
Electronic or Paper Receipt Code: E
Record Type Code: Submission Replacement
Submission Replacement Identifier:
Transmission Version: 13231V01
Identifier:
Processed Date: 8/19/2013 12:00:00 AM
Error Reporting Code: FEIR:

Contact Information

Data Provider Contact: minnie mouse
Email: jill@nerb.org
Street: 2010 Summer Blvd
City: Raleigh
State: NC
Zip: 27616
Phone: 9196106933
Phone Extension:
Fax: 0000000000
ETR Response tab displays the ETR Response Status, Rejection Reason and Response Date for this file (if file is rejected). See glossary for Response explanations.

The Errors tab displays the errors that were generated from the file if there were any. Files with an ETR Status of “Invalid” in the ETR Log or ETR Search will have an error displayed in this tab. See glossary for status explanations.

The Back to ETR Log button will direct you back to the ETR Listscreen.
ETR Web Upload
This will allow a user to upload a file directly to CDX® to submit to a DCO.

- Click the ETR menu.
- Choose ETR—Web Upload.

ETR - Web Upload
Select File for Import:  

Browse...  

Import
BEEP®

The BEEP application is used to enter or modify Unit Statistical Reports. Please see the BEEP User Guide for more information.

PEEP®

The PEEP application is used to enter or modify policy transactions. Please see the PEEP User Guide for more information.

EXR®

The EXR application is used to retrieve rating worksheets from participating DCOs. Please see the EXR User Guide for more information.
**Single Sign On (SSO)**

The Single Sign On (SSO) environment allows CDX users to log in to the CDX website and to securely gain access to participating DCO websites without being prompted to log in again at each of the independent DCO websites.

To access Single Sign On:

1. Log in to the CDX website with your CDX UserName and password.
2. Click on the “DCO Login” link located in the top right-hand corner. The SSO environment is displayed.

When connecting to a DCO, please do not log off from the DCO until the status message is returned to the CDX screen to confirm that the authentication synchronization has finished.
**Initial DCO Log In**
CDX Users must have an active account on the DCO’s website to establish a trusted relationship between CDX and the DCO website.

Note: The browser pop-up blocker must be turned off for SSO to work properly.

To access a DCO’s website for the first time:
1. Select a DCO from the DCO Site dropdown menu.
2. Type the DCO UserName and password.
3. Click the Log in button. If the connection is successful, the DCO’s website is displayed and the user will be logged in.

**Unsuccessful DCO Log In**
The DCO Log In may fail due to the following. Contact the DCO for each scenario below:

a. If the login is not successful because the DCO UserName and/or Password are invalid, the error message “Login to DCO site was unsuccessful. Please contact the DCO to resolve the issue” is displayed.

b. If the login is not successful because the DCO UserName is already in use by another CDX User, the error message “This DCO user is already in use. Please contact the DCO to resolve the issue” is displayed.

**Subsequent DCO Log In**
When the initial DCO Log In set up is successfully completed, it is not necessary to enter the DCO User name and password again to connect to the DCO.

Note: The browser pop-up blocker must be turned off for SSO to work properly.

To access a DCO’s website:
1. Select a DCO from the DCO Site dropdown menu.
2. Click the Log in button. If the connection is successful, the DCO’s website is displayed and the user will be logged in.

**WCUnderwriting**
The WCUnderwriting Search provides immediate access to experience modification factors, merit rating factors and related rating information retrieved from the individual DCO systems, by means of the WCUnderwriting web service, for which the user has authentication.
Note that only DE, MA and PA have implemented the WCUnderwriting service at this time. Requirements:

- The user must be set up for Single Sign On connection to the individual DCO sites. Refer to the Single Sign On (SSO) section of this user guide for information.
- The user must be granted the WCUnderwriting permission. Contact your Primary Administrator for access.

How to perform a search:

1. Select WCUnderwriting from the menu options. You will be directed to the WCUnderwriting Search screen.

2. Select the checkbox for each DCO to be included in the search. Multiple DCOs can be selected.

   The checkbox is disabled for DCOs that have not implemented the WCUnderwriting service and for DCOs that the user does not have a Single Sign On connection set up.

   Each DCO’s search criteria will display separately. Field applicability varies by jurisdiction. Contact individual DCO for state specific implementation guidelines.

3. Enter values for the search criteria.
   
   a. Enter a value for either the Risk ID or the FEIN.
   
   b. Optional - Enter a value for Start Date and End Date (Format: MM/DD/YYYY). Field applicability varies by jurisdiction.

   If multiple DCOs were selected in the previous step, the values entered for the FEIN, Start Date and End Date fields are copied across the DCOs, if applicable.
4. Click on the **Search** button. The search results are displayed below the search criteria.

Badges are displayed at the top of the search results to indicate status of the query.

<table>
<thead>
<tr>
<th>Badge</th>
<th>Definition</th>
</tr>
</thead>
<tbody>
<tr>
<td>ST:</td>
<td>No data found for the Risk ID or FEIN entered. Hover mouse pointer over the badge to view the error message.</td>
</tr>
<tr>
<td>ST:</td>
<td>Results returned for the Risk ID or FEIN entered.</td>
</tr>
<tr>
<td>ST:</td>
<td>No results returned due to invalid search parameters entered. Hover mouse pointer over the badge to view the error message.</td>
</tr>
<tr>
<td>ST:</td>
<td>Connection to the DCO’s WCUnderwriting service was not established due to invalid credentials (account is inactive or disabled).</td>
</tr>
</tbody>
</table>

“ST” denotes DCO.

Below are sample error messages:
- No data found.
- Invalid Risk ID (This is a numeric field).
- FEIN must be numeric.
- Status Code 401: Credentials are not valid, or account is inactive.
5. Select the link within the Name of Insured column to view detailed rating information.

6. Select the **Close** button on the Rating Information window to return to the WCUnderwriting Search screen.

7. Select the **Clear** button on WCUnderwriting Search to reset the screen.
File Naming Convention for CDX

AAEP_SSSSSC_RRRRR_CCYYMMDDHHMM.FFF

Where:

**AA = Type of Data**
PP = WCPOLS - Policy data in PEEP format (ASCII)
PD = WCPOLS - Policy data in WCIO tape format *
UB = WCSTAT - Unit Stat data in BEEP format (ASCII)
UD = WCSTAT - Unit Stat data in WCIO tape format*
RG = WCRATING - Experience Modification Adjustment *
PE = WCEPOLs - Policy Errors *
UE = WCESTAT - Unit Stat Errors *
MD = WCMOD - Experience Modification *
RT = WCRATE - Classes and Rates *
CT = WCCNTL - Unit Report Control Listing *
NA = WCNOA - Notice of Assignment *
ID = WICSTAT - ICR Data *
EC = WCCRIT - Workers Compensation Criticism Information
MC = WCMED - Medical Data Call
IC = WCIND - Indemnity Data Call**

**Note:** * WCIO tape format (EBCDIC)

** For NY, please refer to the Indemnity Data Call Guide and Manual on NYCIRB’s website.

**E = Source**
E = CDX
D = Direct FTP
M = E-mail

**P = Data Type**
P = Production
T = Test

_ = 1 underscore delimiter for readability

**SSSSS = Sender Carrier/State Code (preceded by ZEROS if code is less than 5)**

**C = Sender Type**
C = Carrier
T = TPA
D = DCO

_ = 1 underscore delimiter for readability

**RRRRR = Receiver Carrier/State Code (preceded by ZEROS if code is less than 5)**

_ = 1 underscore delimiter for readability
CCYYMMDDHHMM = Submission Date/Time
CC = Century (i.e. 20)
YY = Year (i.e. 03)
MM = Month (i.e. 01 thru 12)
DD = Day (i.e. 01 thru 31)
HH = Hour (on a 24-hour clock [i.e. 01 thru 24])
MM = Minute (on 60 minute hour [i.e. 01 thru 60])

FFF = File Extension
BIN = Binary
TXT = Text
<table>
<thead>
<tr>
<th>GLOSSARY OF TERMS</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ASCII</strong></td>
</tr>
<tr>
<td><strong>ASWG</strong></td>
</tr>
<tr>
<td><strong>Batch Number</strong></td>
</tr>
<tr>
<td><strong>BEEP®</strong></td>
</tr>
<tr>
<td><strong>Breadcrumbs</strong></td>
</tr>
<tr>
<td><strong>Bureau Version Identifier (Edition Number)</strong></td>
</tr>
<tr>
<td><strong>Carrier Version Identifier</strong></td>
</tr>
<tr>
<td><strong>CDX®</strong></td>
</tr>
<tr>
<td><strong>Correction Report</strong></td>
</tr>
<tr>
<td><strong>DCO</strong></td>
</tr>
<tr>
<td><strong>Date Entered</strong></td>
</tr>
<tr>
<td><strong>EBCDIC</strong></td>
</tr>
<tr>
<td><strong>Edit Status</strong></td>
</tr>
<tr>
<td>----------------</td>
</tr>
<tr>
<td><strong>Employee Leasing Policy Type Code</strong></td>
</tr>
<tr>
<td><strong>Endorsement Number</strong></td>
</tr>
<tr>
<td><strong>Endorsements with Variable Data</strong></td>
</tr>
<tr>
<td><strong>ETR</strong></td>
</tr>
<tr>
<td><strong>Exposure Period Code</strong></td>
</tr>
<tr>
<td><strong>EXR</strong></td>
</tr>
<tr>
<td><strong>First Report</strong></td>
</tr>
<tr>
<td><strong>IAIABC</strong></td>
</tr>
<tr>
<td><strong>Import</strong></td>
</tr>
<tr>
<td><strong>Legal Nature of Entity Code</strong></td>
</tr>
<tr>
<td><strong>Legal Nature of Insured Code</strong></td>
</tr>
<tr>
<td><strong>Link Data</strong></td>
</tr>
<tr>
<td><strong>Name Link Identifier</strong></td>
</tr>
<tr>
<td>Term</td>
</tr>
<tr>
<td>---------------------------</td>
</tr>
<tr>
<td>PEEP</td>
</tr>
<tr>
<td>POC</td>
</tr>
<tr>
<td>Policy Change Effective Date</td>
</tr>
<tr>
<td>Policy Change Expiration Date</td>
</tr>
<tr>
<td>Primary Administrator</td>
</tr>
<tr>
<td>Replacement Report Code</td>
</tr>
<tr>
<td>Retrospective Rating Code</td>
</tr>
<tr>
<td>Secondary Administrator</td>
</tr>
<tr>
<td>SFTP</td>
</tr>
<tr>
<td>SSL</td>
</tr>
<tr>
<td>State Unemployment Number</td>
</tr>
<tr>
<td>Submission File</td>
</tr>
<tr>
<td>Subsequent Report</td>
</tr>
<tr>
<td>TPA/TPE</td>
</tr>
<tr>
<td>Transaction Issue Date</td>
</tr>
<tr>
<td>Transaction Type Code</td>
</tr>
<tr>
<td>UMG</td>
</tr>
<tr>
<td>Validate</td>
</tr>
</tbody>
</table>
## Summary of Changes

<table>
<thead>
<tr>
<th>Page, Section, etc.</th>
<th>Date of Change</th>
<th>Change/Update</th>
</tr>
</thead>
<tbody>
<tr>
<td>Page 71</td>
<td>11/18/19</td>
<td>Indemnity Data Call File Naming Convention</td>
</tr>
<tr>
<td>Entire User Guide</td>
<td>10/10/19</td>
<td>Updates to new CDX website design.</td>
</tr>
<tr>
<td>Pages 8-13, 74-77</td>
<td>09/17/18</td>
<td>IPA Request New UMG Primary Admin User for Existing UMG, Update Contact Info for Existing UMG Primary Admin User, &amp; WCUNDERWRITING Search User Guide Information</td>
</tr>
<tr>
<td>Pages 54-55</td>
<td>03/19/18</td>
<td>Update for Member Verification Technical Contact Information</td>
</tr>
<tr>
<td>Pages 20-22</td>
<td>11/09/17</td>
<td>Updates to Password Reset Functionality</td>
</tr>
<tr>
<td>Pages 41-42</td>
<td>02/16/17</td>
<td>Add Disassociate TPA Section</td>
</tr>
<tr>
<td>Pages 26-27</td>
<td>12/10/2015</td>
<td>Added Inactivating a User Account and Deleting a User Account</td>
</tr>
<tr>
<td>Pages 68-70</td>
<td>06/05/2015</td>
<td>Updated Glossary; replaced date with link to Summary of Changes on cover page</td>
</tr>
<tr>
<td>Page 64 and 65</td>
<td>06/03/2015</td>
<td>Added Note to SSO section regarding pop-up blockers</td>
</tr>
<tr>
<td>Page 66</td>
<td>05/29/2015</td>
<td>Updated the ACCCTs File Naming Convention for CDX®; Source from E=ACCCT’s EDI to E=CDX</td>
</tr>
<tr>
<td>Pages 23, 33, 41</td>
<td>05/13/2015</td>
<td>Included information on TPA Edits</td>
</tr>
<tr>
<td>Pages 64, 65</td>
<td>04/15/2015</td>
<td>Added Single Sign On (SSO) Information</td>
</tr>
<tr>
<td>Pages 52, 57</td>
<td>06/23/2014</td>
<td>Inserted references to Glossary in ETR Section</td>
</tr>
<tr>
<td>Pages 60, 61</td>
<td>06/23/2014</td>
<td>Added Glossary</td>
</tr>
<tr>
<td>Page 61</td>
<td>06/23/2014</td>
<td>Added Summary of Changes</td>
</tr>
</tbody>
</table>