Compensation Data Exchange

Summary of Changes

Contents

Introduction
This guide is for the carriers and third party administrators who use the CDX administrative application.

Compensation Data Exchange (CDX) has been developed as a secure Internet application with the goal of providing the ability to exchange data electronically between the carriers and CDX Members, or Data Collection Organizations (DCOs). Primarily, the product is used for the purpose of sending, receiving, and managing files. 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.

Information on the various products that are available can be found on the CDX website under the Products Overview page.

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.

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 Primary Administrator, and notifies affected DCOs that the Insurer Primary Administrator has been established.

Insurer UMG (User Management Group)
An Insurer User Management Group represents a group of carriers and users managed by a single Primary Administrator. Insurer Users are granted rights to send files and use applications within UMGs by the Primary Administrator.

Insurer Primary Administrator
There can be 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 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
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
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.

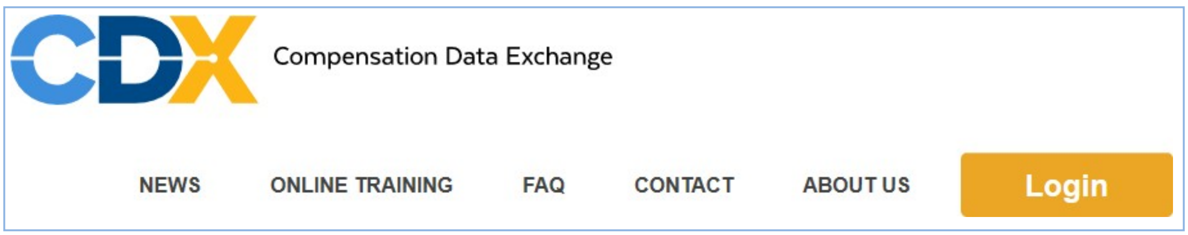
Signing Up with CDX

Request New UMG/Carrier Group

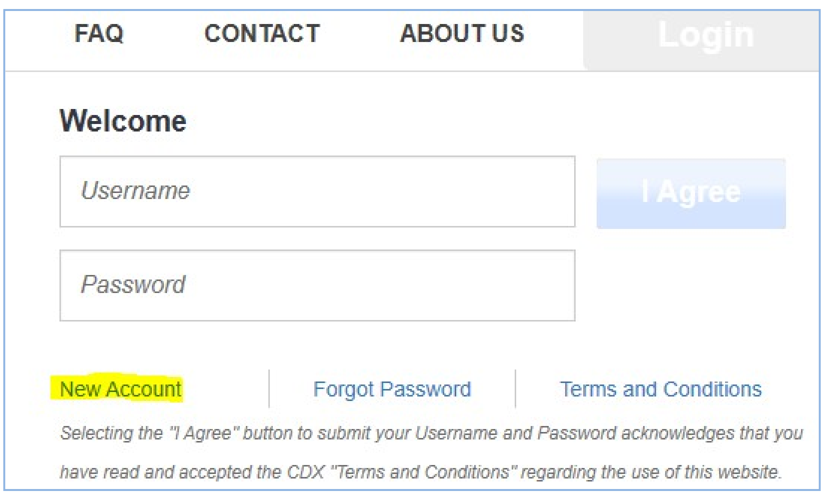
This process should be followed if your carrier is new to the CDX products. If your carrier group is already utilizing CDX and you need to request a new carrier to be added to your existing group, please follow the instructions under Carriers – Create a Carrier Request.

If you are new to CDX and do not have a primary administrator established, follow these instructions.

- 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 hard copy 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 ☑ New Carrier

Insurer UMG Primary Administrator Information

◉ *Request New Carrier UMG (User Management Group)*

NOTE: The ability to change the current Primary Administrator's contact information or assign a new Primary Administrator to an existing UMG is available to logged-in users via the Admin menu item.

Desired User ID:

☐ *New Carrier*

NOTE: Creating a new Carrier is not necessary if you are requesting a new UMG/Carrier Group in order to move an existing Carrier into it.

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

Applicant Information

Carrier Group Name:	**NCCI Number:**
First Name:	**Last Name:**
Address:	**Address 2:**
City:	**State** AK
ZIP:	
Phone Number:	**Ext.:**
Email Address:	**Fax Number:**

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

Carrier Information

Carrier Name:	**NCCI Number:**
Address:	**Address 2:**
City:	**State** AK
ZIP:	
Phone:	**Ext.:**
	Fax:

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.

Authorizing Officer

First Name:	**Last Name:**
Title:	**Email Address:**

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, or e-mailed to:

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

E-mail: support@cdxworkcomp.org

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.

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.

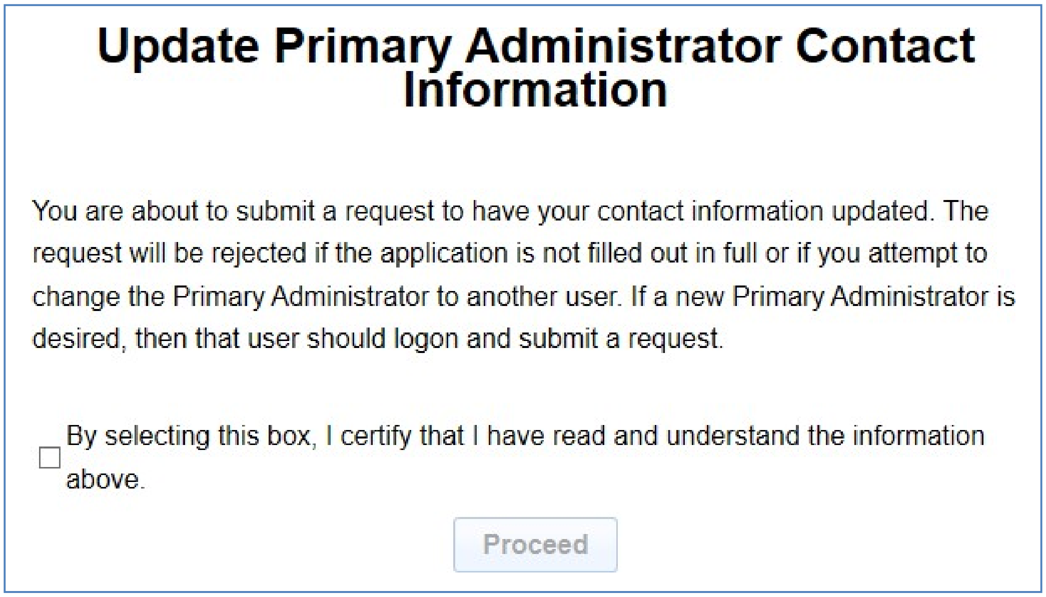
This printed application must be signed by the Primary Administrator and an Authorizing Officer of the Applicant who shall be fully authorized to bind the Applicant to the Terms and Conditions of Use at www.cdxworkcomp.org. The completed application with the signatures, along with a copy of the authorizing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

CDX Central Support
E-mail: support@cdxworkcomp.org

Replacing an Existing Primary Administrator

To replace an existing administrator, you will need to already have an account and will need to navigate to the Admin | Requests | Primary Admin menu and complete the steps.

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

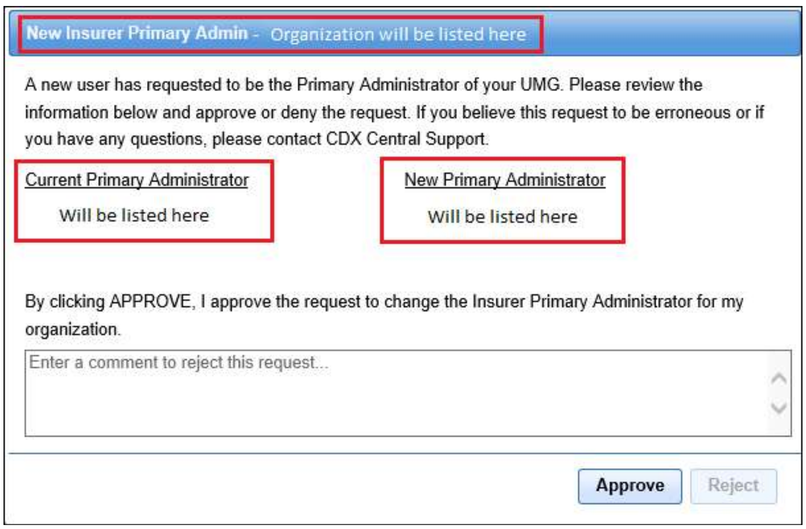


What's Next:
Central Support reviews the request:

- If Rejected - Requestor will receive an email notification with the reason for rejection
- If Approved - Outgoing Primary Admin and Authorizing officer receives email notification of request

The Outgoing Primary Admin reviews the request

- Logs on to CDX and the following popup is displayed.



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

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 approvethe 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

An Insurer UMG can only have on application request submitted at a time. To delete a pending application:

- 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

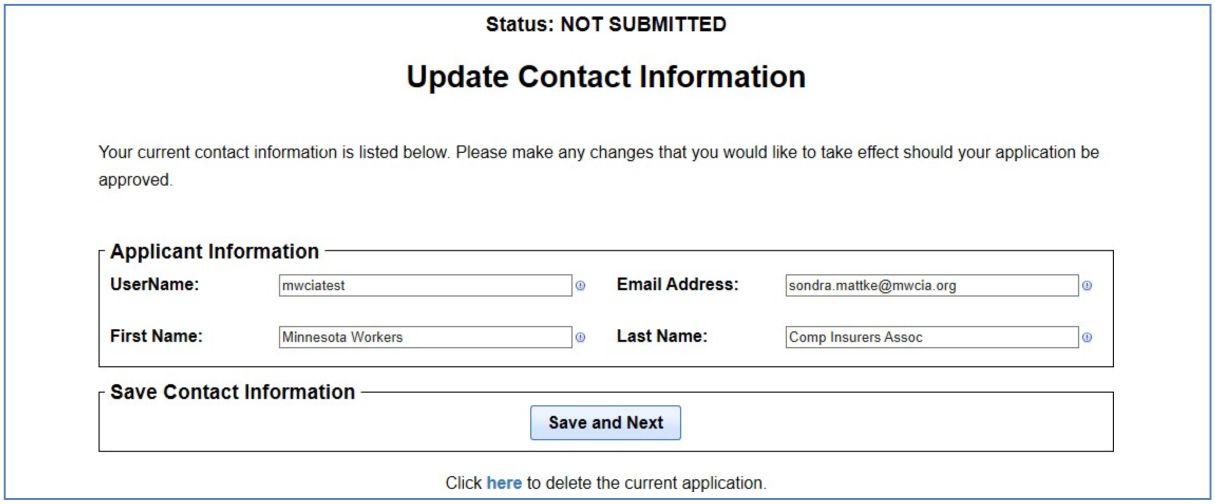
Primary Administrator – Updating Contact Information

Updates to the Primary Administrator information, such as name or email address, must be approved by CDX Central Support. To submit a request for change:

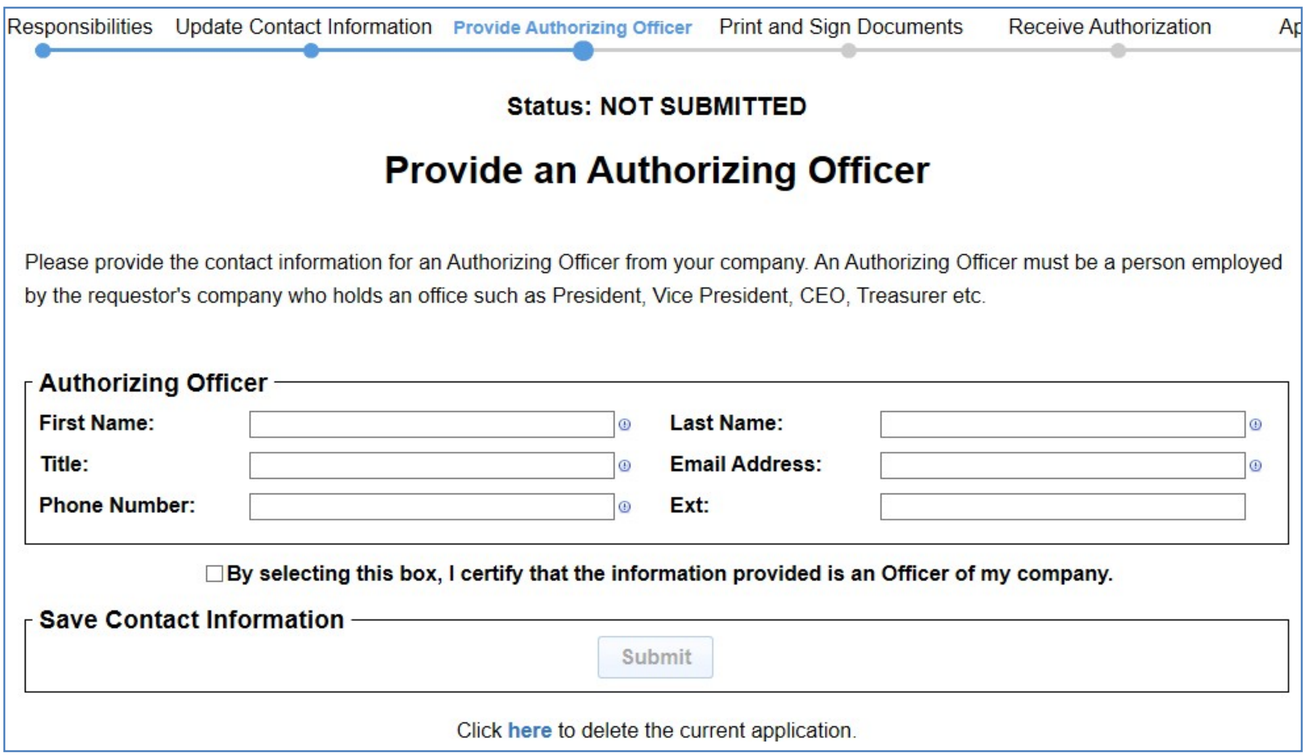
- Logon to CDX
- Select Admin | Requests | Primary Admin

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



- Select 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.

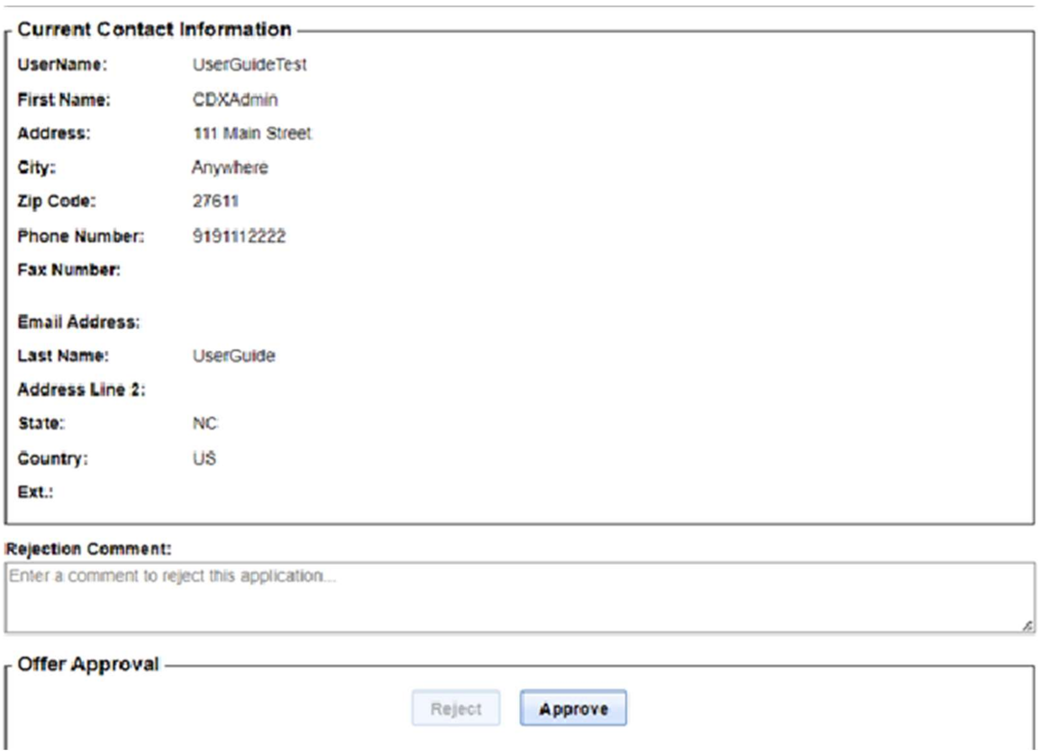
What's Next:

Central Support reviews the request:

- If Rejected - Requestor will receive an email notification with the reason for rejection
- If Approved – An email is sent to the Authorizing Officer.

The Authorizing Officer will complete the process by clicking the link within the email, reviewing the details and either Rejecting or Approving

Upon logging into the CDX site, the Primary Administrator

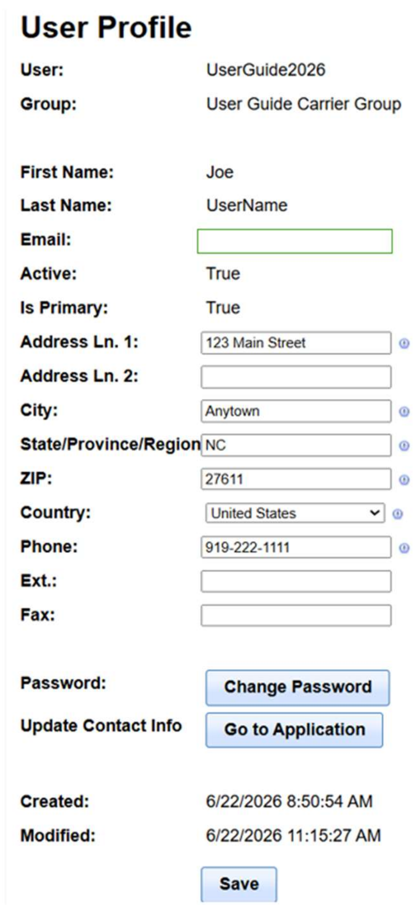


My Account

The My Account menu on the upper right 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.

When Edit Profile is chosen, the User Profile will be displayed with modifiable fields in boxes; this screen also includes the ability to edit and reset the password using a button below the fields. The changes can be saved by clicking the Save button at the bottom of the screen.

NOTE: Primary Administrators cannot change their own information. Please see the Updating Primary Administrator Contact Information section of this guide.



User Profile

User:	UserGuide2026
Group:	User Guide Carrier Group
First Name:	Joe
Last Name:	UserName
Email:	
Active:	True
Is Primary:	True
Address Ln. 1:	123 Main Street
Address Ln. 2:	
City:	Anytown
State/Province/Region	NC
ZIP:	27611
Country:	United States
Phone:	919-222-1111
Ext.:	
Fax:	
Password:	Change Password
Update Contact Info	Go to Application
Created:	6/22/2026 8:50:54 AM
Modified:	6/22/2026 11:15:27 AM
	Save

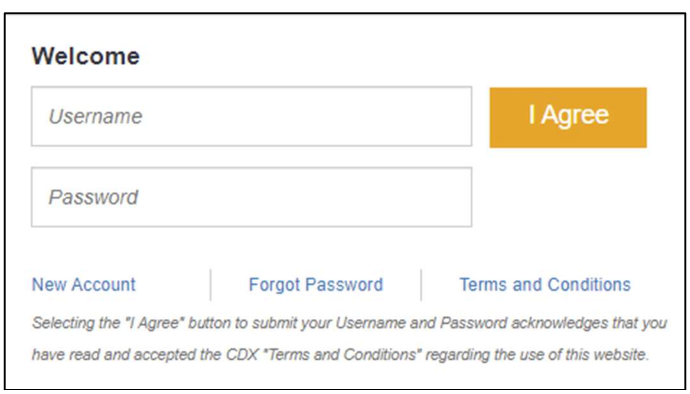
Change Password

This screen can be accessed by selecting Change Password from the My Account drop-down menu, or by clicking the Change Password button in the Edit Profile screen. A user can change their password by entering the Current Password and entering and retyping a new password.

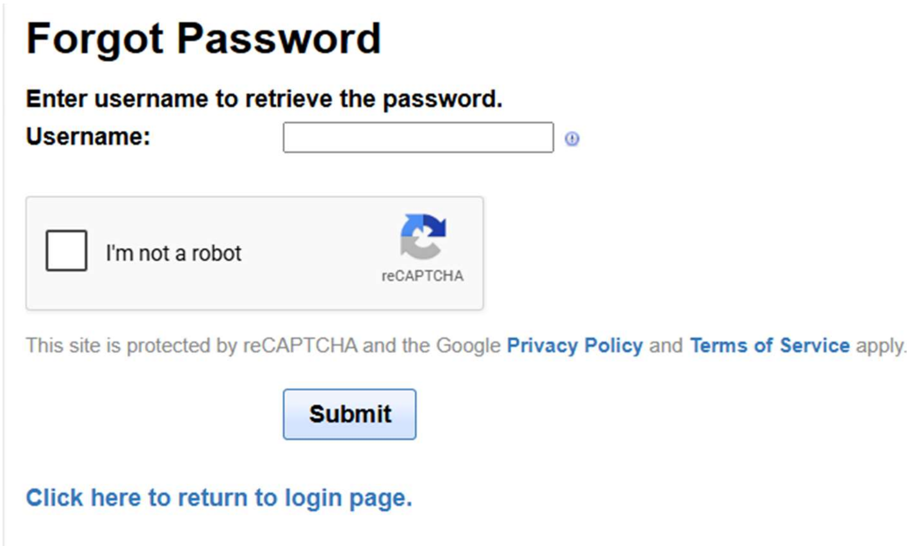
To cancel password reset, navigate away from this page using top dropdown menus.

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 confirm reCAPTCHA. Once entered the user will click the Submit button 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.

Locked Accounts

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, the account can be unlocked by resetting the password via "Forgot Password", contacting your Primary Administrator, or by contacting Central Support. The Primary Administrator can 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 a link to initiate the password reset process.

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

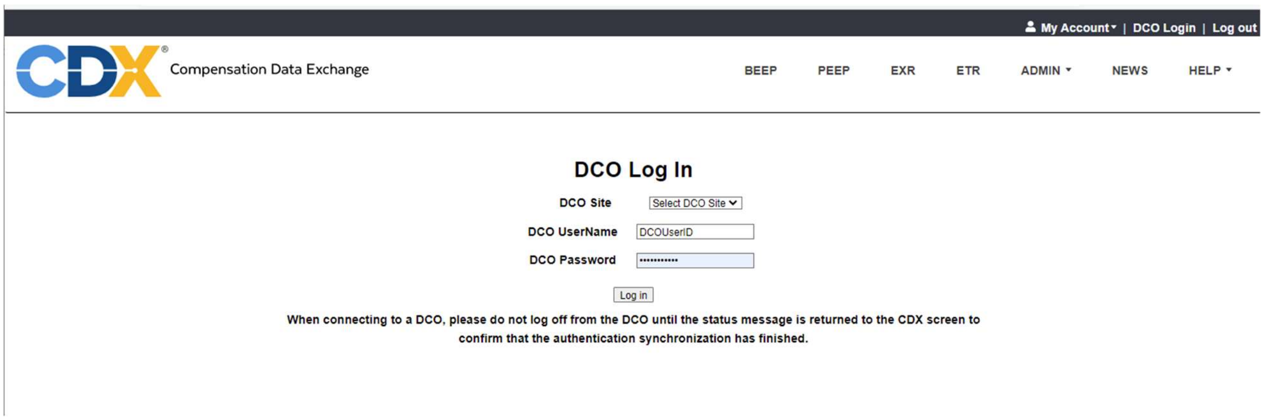
Password Expiration

Passwords will expire every three months and users will be forced to create new passwords.

DCO Login

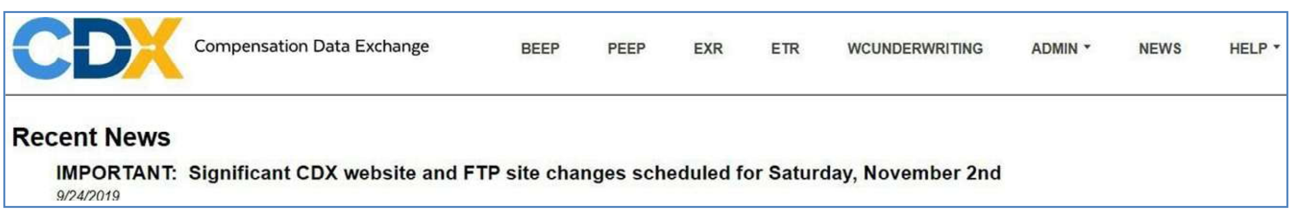
The DCO Log In page allows a CDX user to connect to participating DCO sites utilizing your CDX credentials. Please see the Single Sign On (SSO) section of this guide for configuration of this feature.

NOTE: As of July 2026, the only DCO Site supporting SSO is NCRB.



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

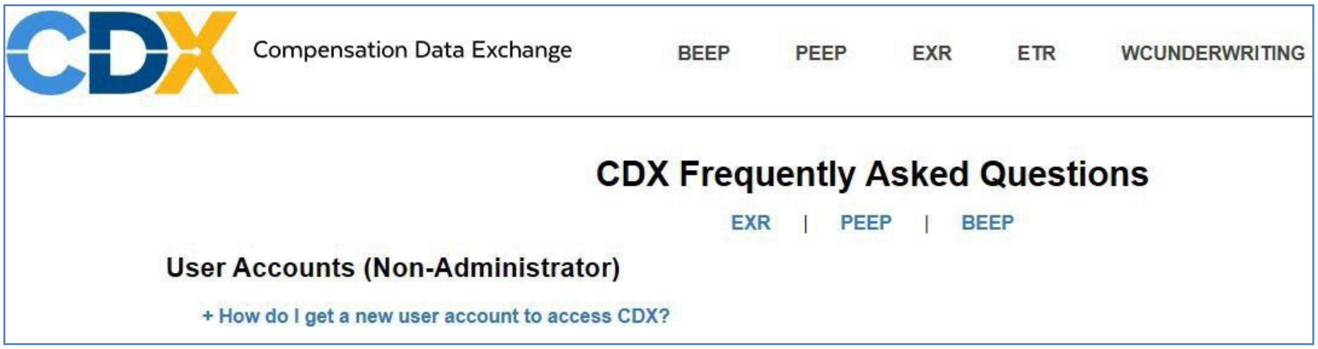
This menu item will allow the user to navigate to Online Training, CDX Admin User Guide, BEEP, PEEP and EXR User Guides, FAQ, and Contact Us

Online Training
This link will open the Online Training Videos page.

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

BEEP, PEEP and EXR User Guides
These links will open a PDF of the individual BEEP, PEEP or EXR User Guides.

FAQ
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.

To return to the top of the FAQ page, you can click the Return to FAQ Home button under each section.

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

Note: View the CDX website page for the most current contact information.

Contact Us

For technical support or user account setup, contact:

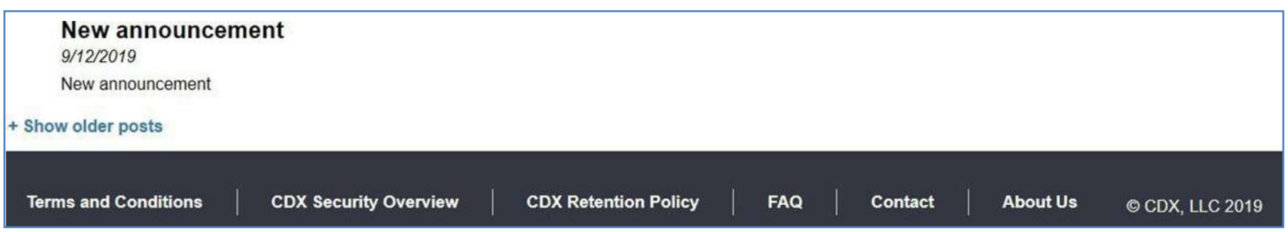
CDX Central Support
919-595-1890
support@cdxworkcomp.org

For questions relating to the Indemnity Data Call or the Medical Data Call, please contact the individual DCO.

For assistance with data reporting requirements, missing experience modifications, edits and submission files, contact:

ORGANIZATION MEMBERS	DCO #	PEEP CONTACT INFO	BEEP CONTACT INFO	EXR CONTACT INFO	FOR ALL OTHER INQUIRIES
Workers' Compensation Insurance Rating Bureau of **California**	00004	Customer Service 888-229-2472 **customerservice@wcirb.com**	Customer Service 888-229-2472 **customerservice@wcirb.com**	Customer Service 888-229-2472 **customerservice@wcirb.com**	Customer Service 888-229-2472 **customerservice@wcirb.com**
Delaware Compensation Rating Bureau, Inc.	00007	DCRB Central Support 215-320-4933 **centralsupport@dcrb.com**	Diane Weldon 215-320-4461 **centralsupport@dcrb.com**	Alex Pagan 215-320-4429 **centralsupport@dcrb.com**	DCRB Central Support 215-320-4933 **centralsupport@dcrb.com**
Workers' Compensation Rating and Inspection Bureau of **Massachusetts**	00020	Data Operations 617-646-7566 **dataoperations@wcribma.org**	Data Operations 617-646-7566 **dataoperations@wcribma.org**	WCRIBMA Tech Support 617-646-7546 **wcribma-techsupport@wcribma.org**	WCRIBMA Tech Support 617-646-7546 **wcribma-techsupport@wcribma.org**
Compensation Advisory Organization of **Michigan**	00021	Tammy Gluth 734-462-9600 Ext. 275 **tgluth@caom.com**	Data Services 734-462-9600 **cdxbac@caom.com**	Data Services 734-462-9600 **cdxbac@caom.com**	Data Services 734-462-9600 **cdxbac@caom.com**
Minnesota Workers' Compensation Insurers Association, Inc.	00022	Data Services 952-897-1737 **cdxmn@mwcia.org**	Data Services 952-897-1737 **cdxmn@mwcia.org**	Data Services 952-897-1737 **cdxmn@mwcia.org**	Data Services 952-897-1737 **cdxmn@mwcia.org**
New Jersey Compensation Rating & Inspection Bureau	00029	Frank Furnari 973-622-6014 Ext. 247 **cdx_notifications@njcrib.com**	Frank Furnari 973-622-6014 Ext. 247 **cdx_notifications@njcrib.com**		Frank Furnari 973-622-6014 Ext. 247 **cdx_notifications@njcrib.com**
New York Compensation Insurance Rating Board	00031	Lennora Snipes 929-436-2988 **peepsupport@nycirb.org**	Lennora Snipes 929-436-2988 **beepsupport@nycirb.org**	Lennora Snipes 929-436-2988 **exrsupport@nycirb.org**	Lennora Snipes 929-436-2988 **cdxsupport@nycirb.org**

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.

1 of 10

CDX Services Terms and Conditions of Use

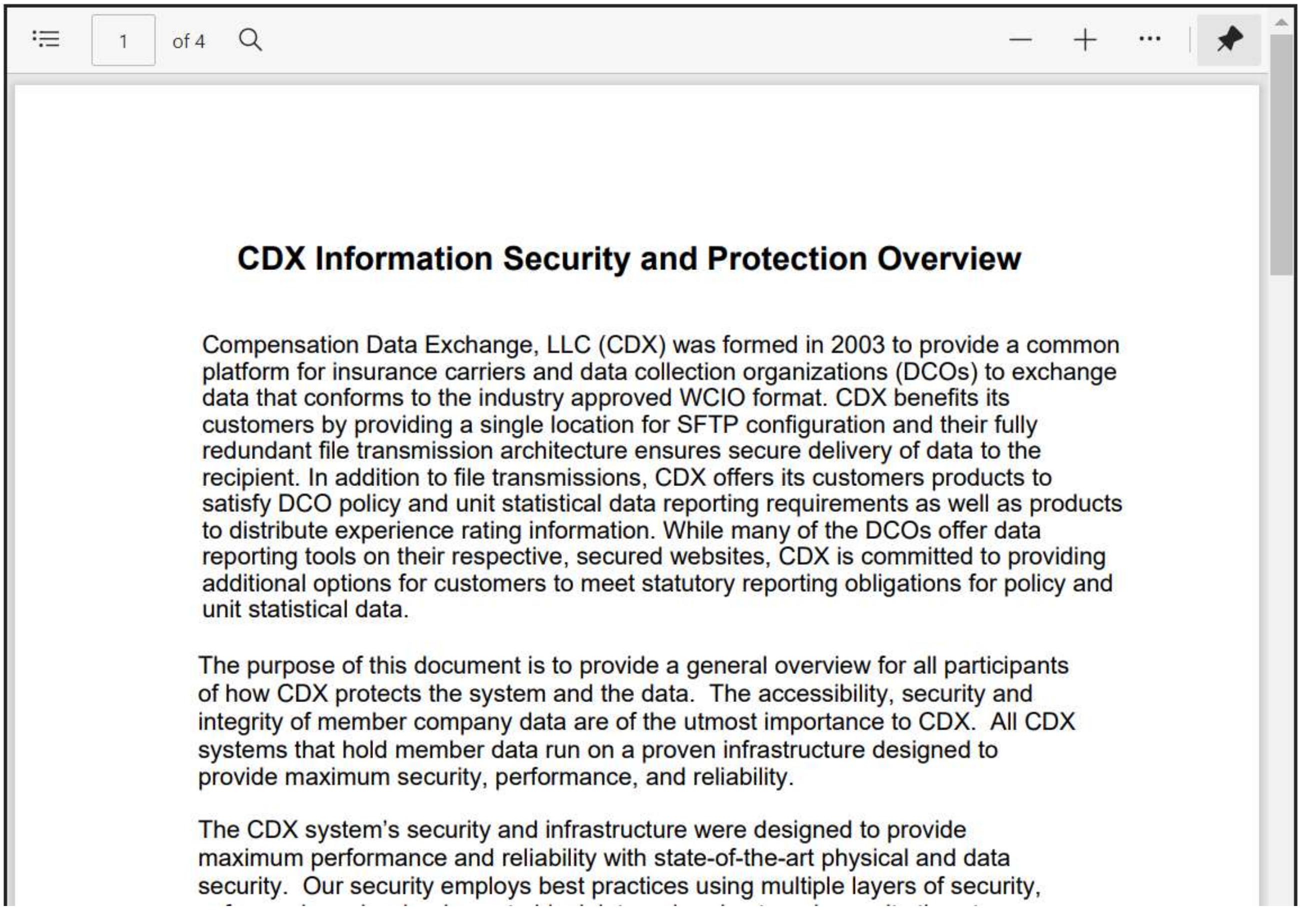
This CDX Services Terms and Conditions of Use agreement ("Agreement") is made by and between Compensation Data Exchange, LLC ("CDX," "Us, "We" or "Our"), and you ("you" or "your,"). For the avoidance of doubt, you includes each Authorized User (as defined herein). This Agreement contains the terms and conditions that govern your use of the CDX website and the compensation data exchange services offered by CDX including without limitation any FTP services (collectively and independently, the website and the compensation data exchange services being the "Services"). CDX is owned by participating state independent rating and data collection organizations ("Participating DCOs"). This Agreement does not govern the use of the Services by the Participating DCOs.

BY ACCESSING, VISITING, BROWSING, USING, DOWNLOADING OR ATTEMPTING TO INTERACT WITH ANY PART OF THE SERVICES, INCLUDING WITHOUT LIMITATION THE SERVICE'S FORMS OR OTHERWISE, YOU AGREE, ON BEHALF OF YOURSELF AND ANY ENTITY FOR WHICH YOU ARE AN AGENT OR YOU APPEAR TO REPRESENT (SUCH ENTITY ALSO BEING INCLUDED IN THE TERMS "YOU," OR "YOUR" REFERRED TO ABOVE) THAT YOU HAVE READ, UNDERSTAND, AND AGREE TO BE BOUND BY THIS AGREEMENT. IF YOU DO NOT AGREE TO BE BOUND BY THIS AGREEMENT, DO NOT ACCESS OR USE ANY PART OF THE SERVICES.

WITHIN THE SERVICES YOU MAY BE PRESENTED WITH ADDITIONAL TERMS AND CONDITIONS THAT YOU MUST ACCEPT TO USE CERTAIN FEATURES OR

CDX Security Overview

This menu will open a PDF of the CDX Security Overview document.



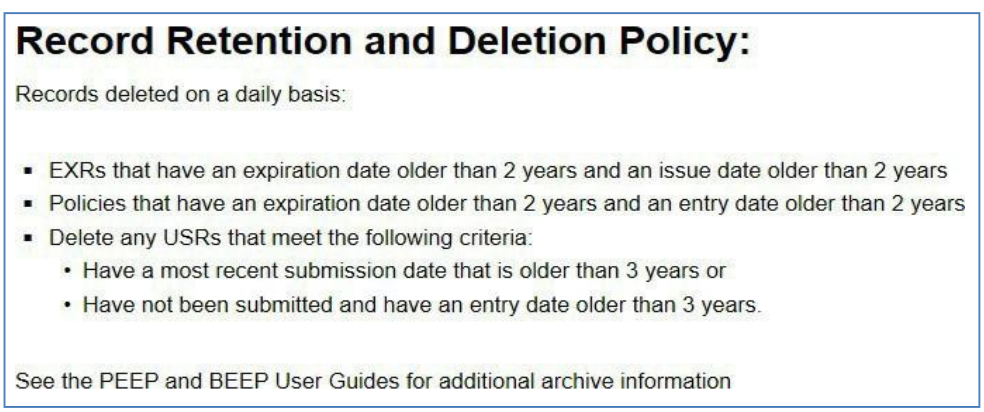
CDX Information Security and Protection Overview

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 WCIO format. CDX benefits its customers by providing a single location for SFTP 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.

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.

The CDX system's security and infrastructure were designed to provide maximum performance and reliability with state-of-the-art physical and data security. Our security employs best practices using multiple layers of security,

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 Contact which were presented in the Help section.

About Us

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 **WCIO** 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.

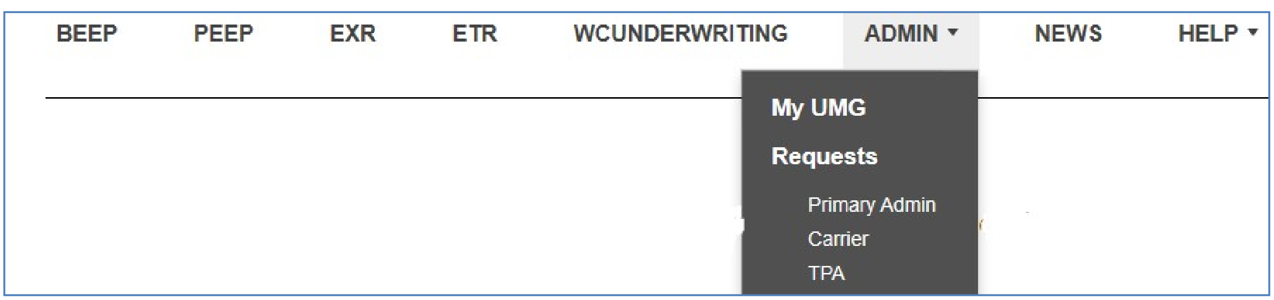
CDX Members

- 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

My UMG

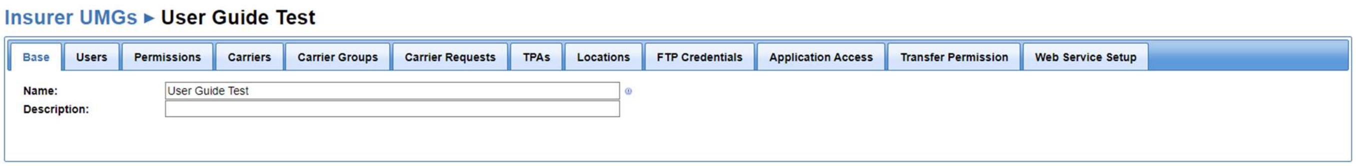
The My UMG menu option is only available to the Primary Administrator and Users who have Admin permissions (Manage Users and Permissions For This UMG, Manage Carriers and Carrier Groups, and/or Manage Locations for this UMG checked green for user). Selecting My UMG will take a user to the User Management Group.



The tabs will be accessible depending on the user's permissions.

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.

Add User

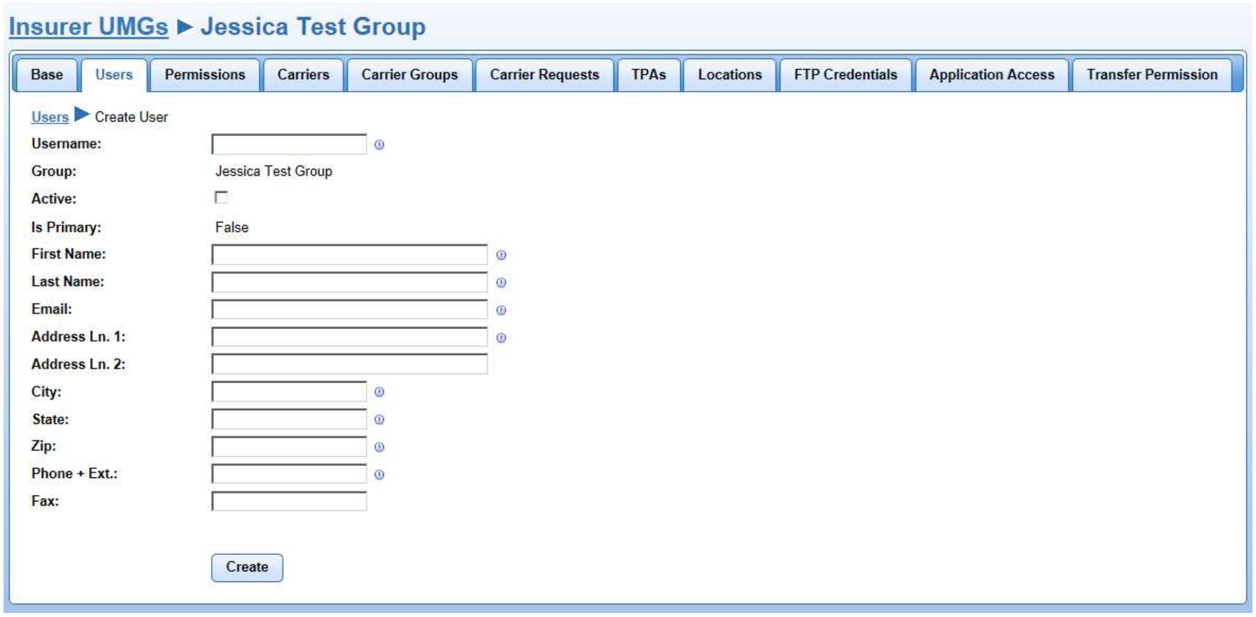
- To setup a new user, choose the tab labeled Users.

- Click the Add User button at the bottom of the screen.

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.
- Most permissions (with exception of the Manage Permission value can be copied from an already existing user.
- 

- 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 a link to create their password.

Edit User

- Select Admin | My UMG.
- Click the Users tab.

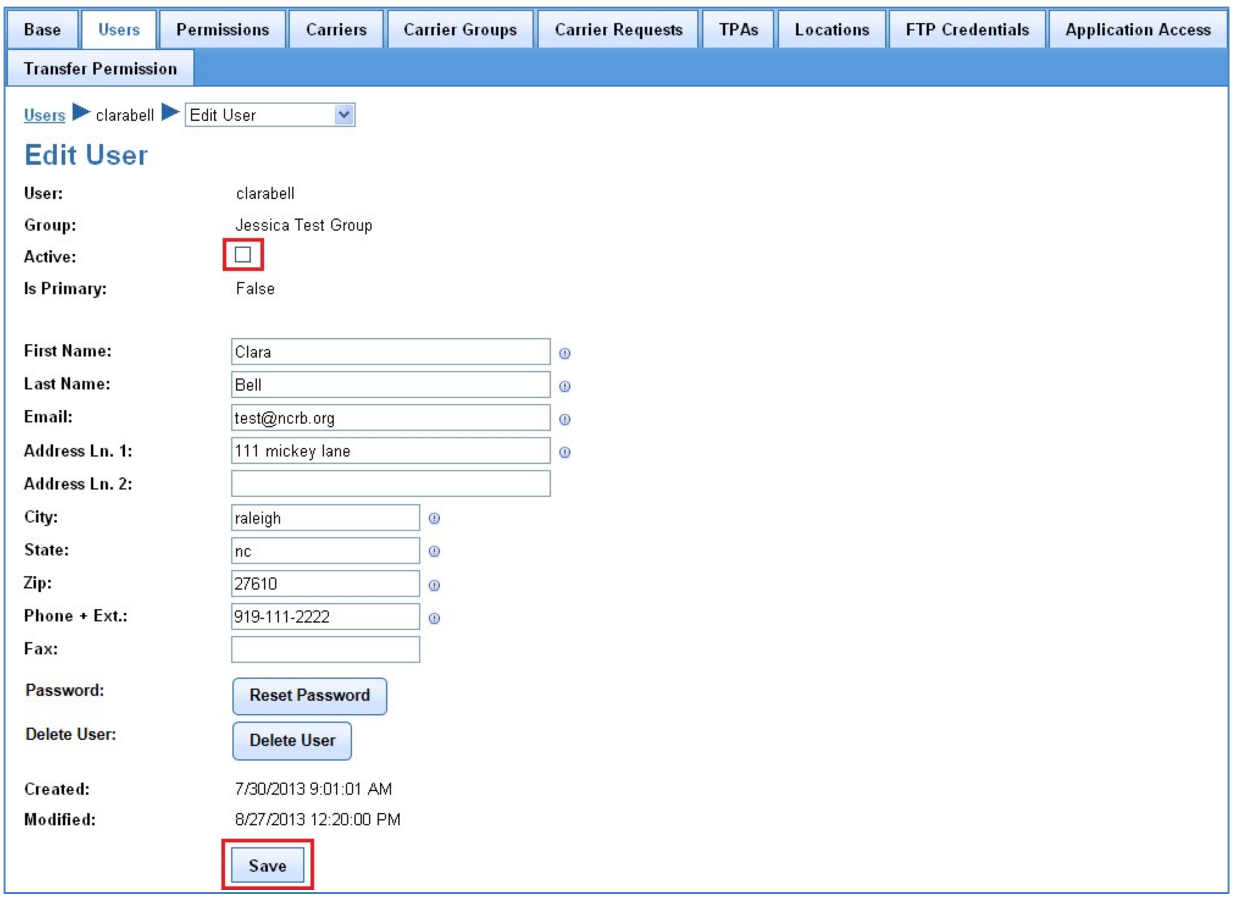
- To edit a user, click the hyperlink for the user or the pencil icon at the end of the user information. The Edit User screen will appear where the user's information can be edited.

- To cancel the edit, click the blue 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"

Inactivate User

To inactivate a user:

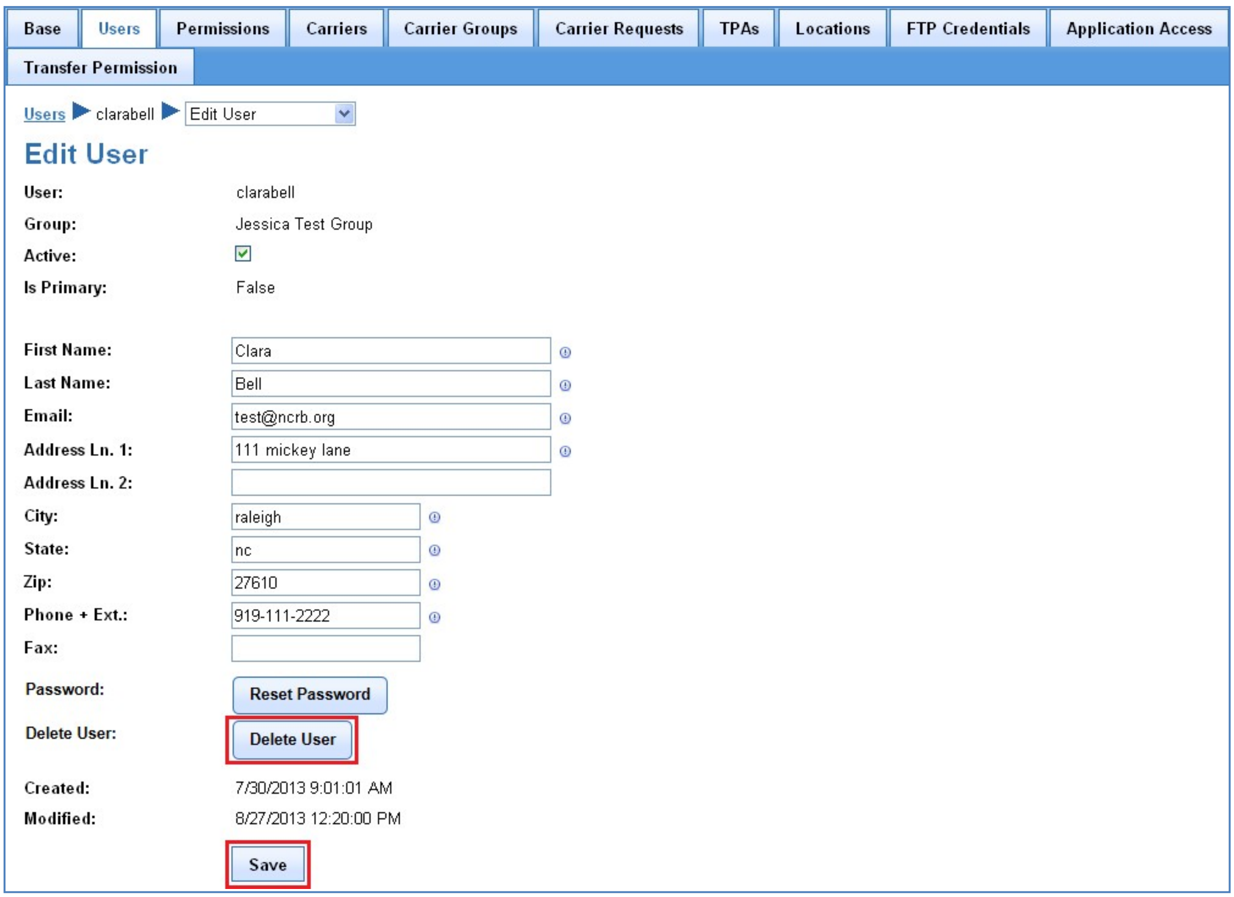
- Select Admin | My UMG.
- Click the Users Tab.
- Click the User hyperlink for the user or the pencil icon at the end of the user information; this will navigate you to the Edit Userscreen.
- Uncheck the Active box.
- Click Save.



Delete User

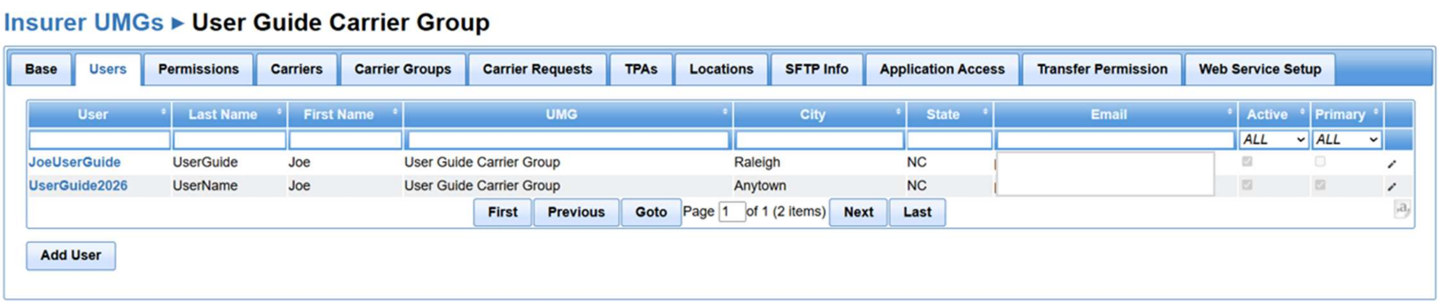
To delete a user account:

- Select Admin | My UMG.
- Click the Users Tab.
- Click the User hyperlink for the user or the pencil icon at the end of the user information; this will navigate you to the Edit Userscreen.
- Click on the Delete User button
- Confirm deletion by clicking OK



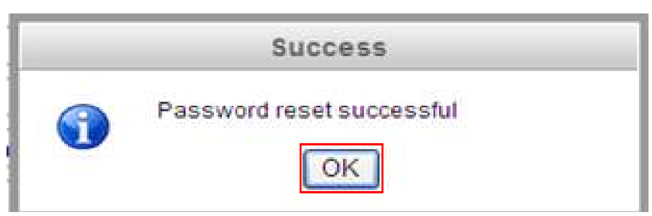
Reset User Password
To reset a user’s password:

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



Click the Reset Password button.

Click OK.

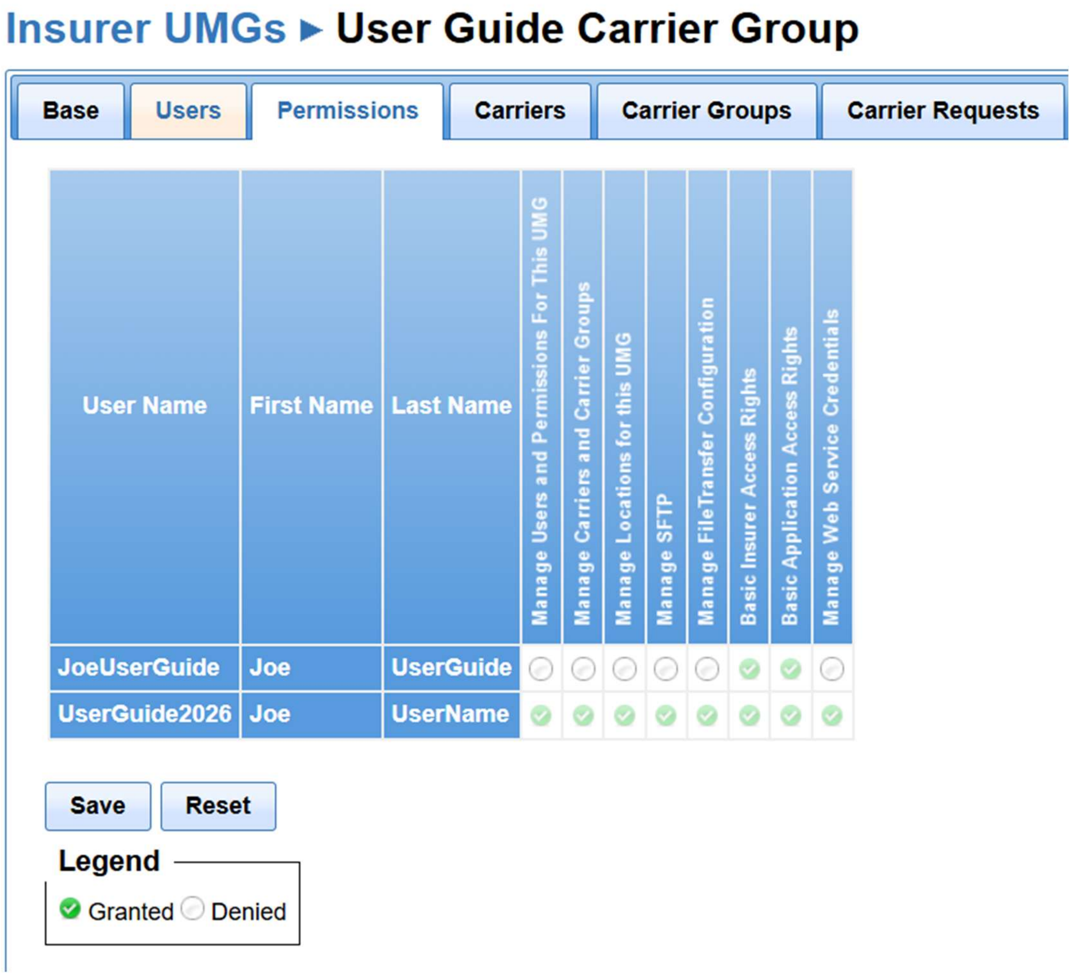


The user will receive an email that allows them to reset their own password.

Permissions

The Permissions page is used to configure the permissions for the users within the UMG.

- Click Admin | 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 leave blank (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 instead of Save.
- 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 that are available:

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 SFTP
Granting this permission will allow the user to:

- Add, edit and delete SFTP credentials. SFTP credentials are setup for the secure FTP transfer of files.
- Add, edit and delete SFTP Whitelist IP addresses. These are required in order to have access to submit files to the CDX SFTP server.
- Enter Technical Contact Information to receive CDX communications related to SFTP

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.

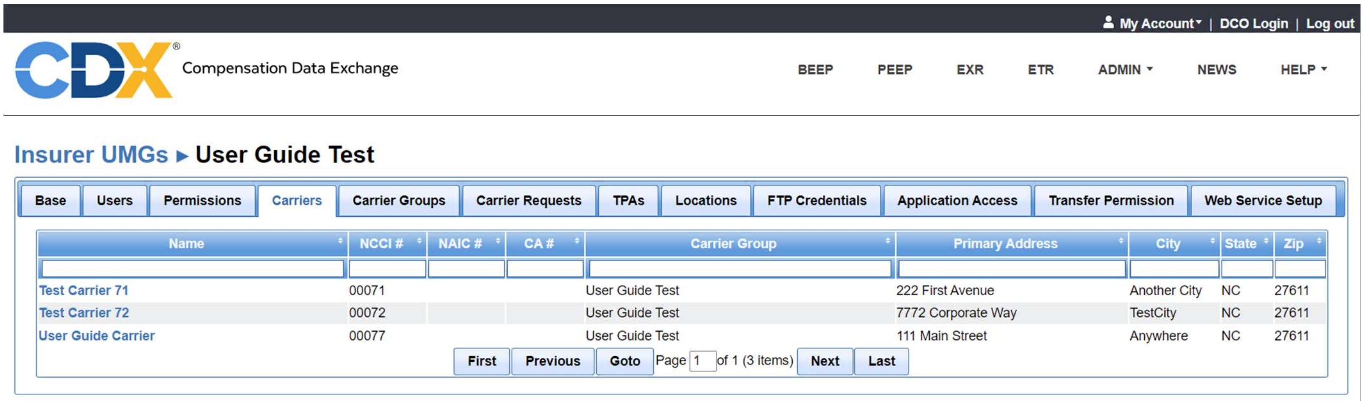
Manage Web Service Credentials
This permission is defaulted and gives the user access to the Web Service Setup tabs where you can obtain approval to use the WCUnderwriting web services.

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 the list of carriers in the 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.

New carrier requests will appear on this tab once they are approved by CDX.

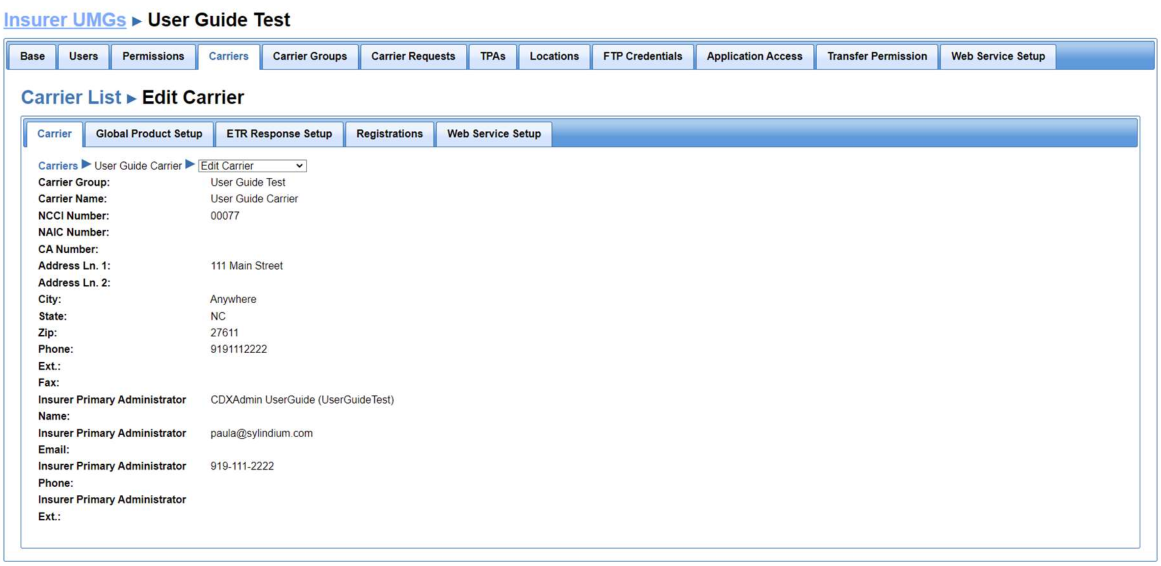


Selecting the name link will display the Edit Carrier section for that carrier. The Edit Carrier section includes tabs for

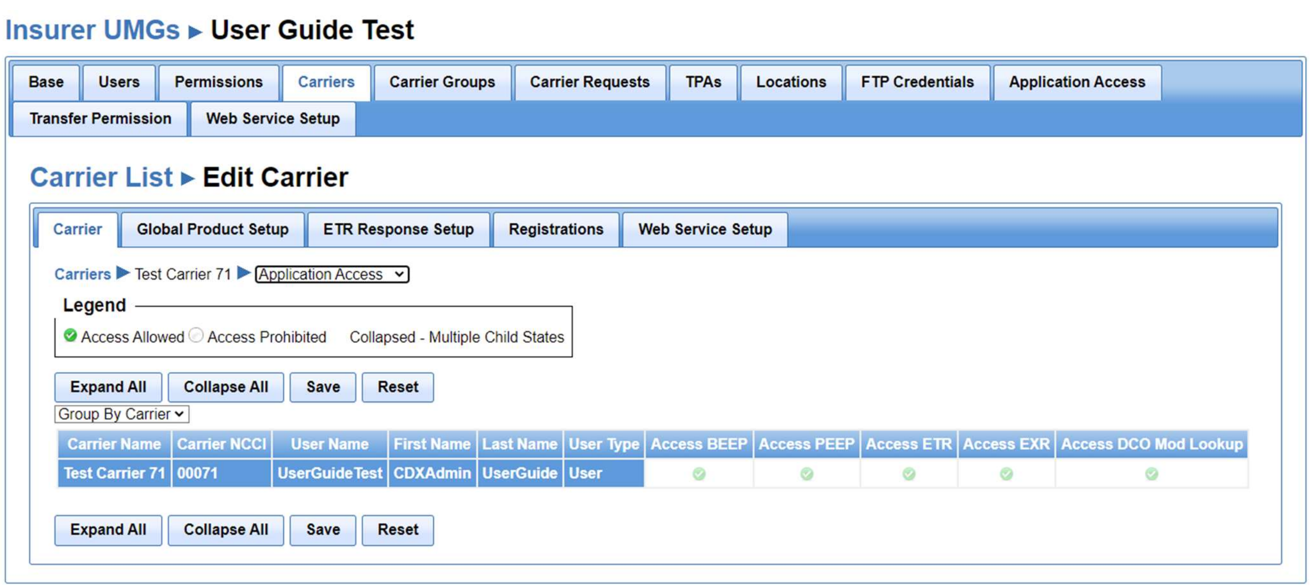
- **Carrier** – Modify carrier demographics
- **Global Product Setup** – Specify the Location for receipt of DCO data files
- **ETR Response Setup** – Configure
- **Registrations** – View the status of approval to submit/receive data with the DCOs
- **Web Service Setup** – Request approval and obtain API key for WCUnderwriting

Carrier

The **Carrier** tab displays basic carrier information, including the Insurer Group Primary Administrator. To request updates to this information, please contact CDX Central Support.

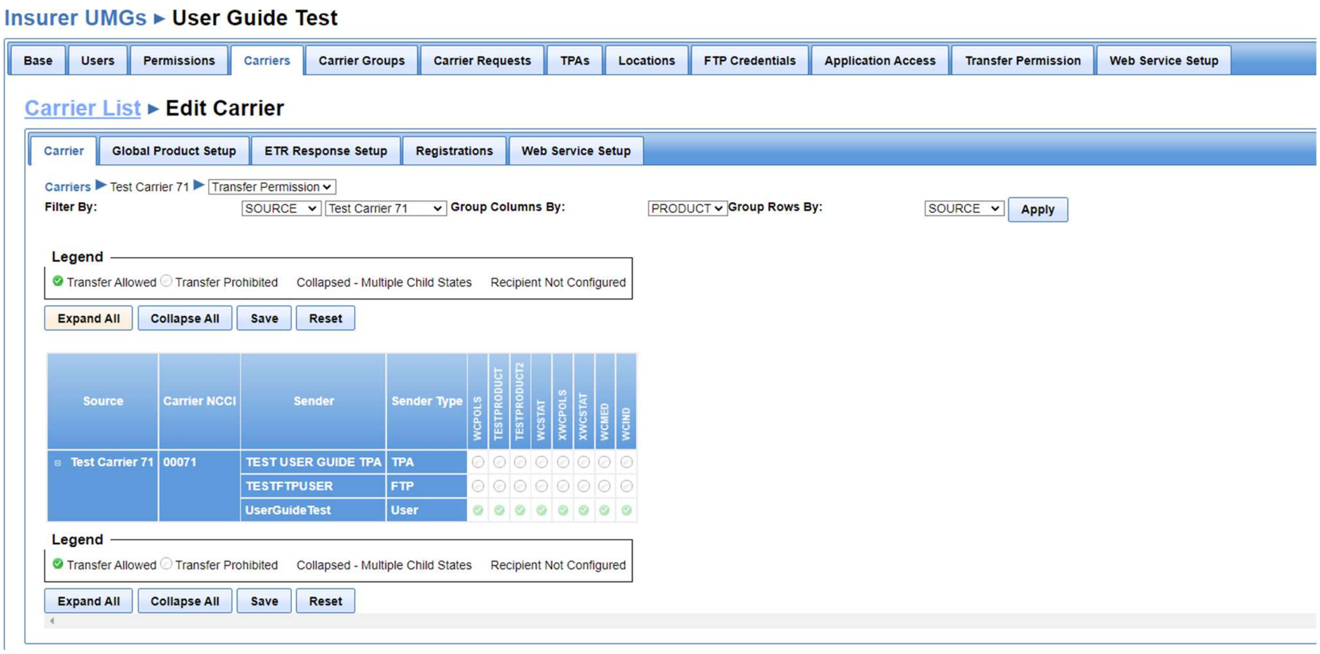


Selecting **Application Access** from the dropdown will display a list of users that are associated with the selected carrier and their product access. Administrators can select/deselect access privileges and Save to update.



Selecting **Transfer** Permissions from the dropdown will display the list of Transfer Permissions that are set up for the selected carrier and user id. Each user account, including the FTP account, that will be sending files through CDX will be required to have the transfer permissions selected here for the required product(s).

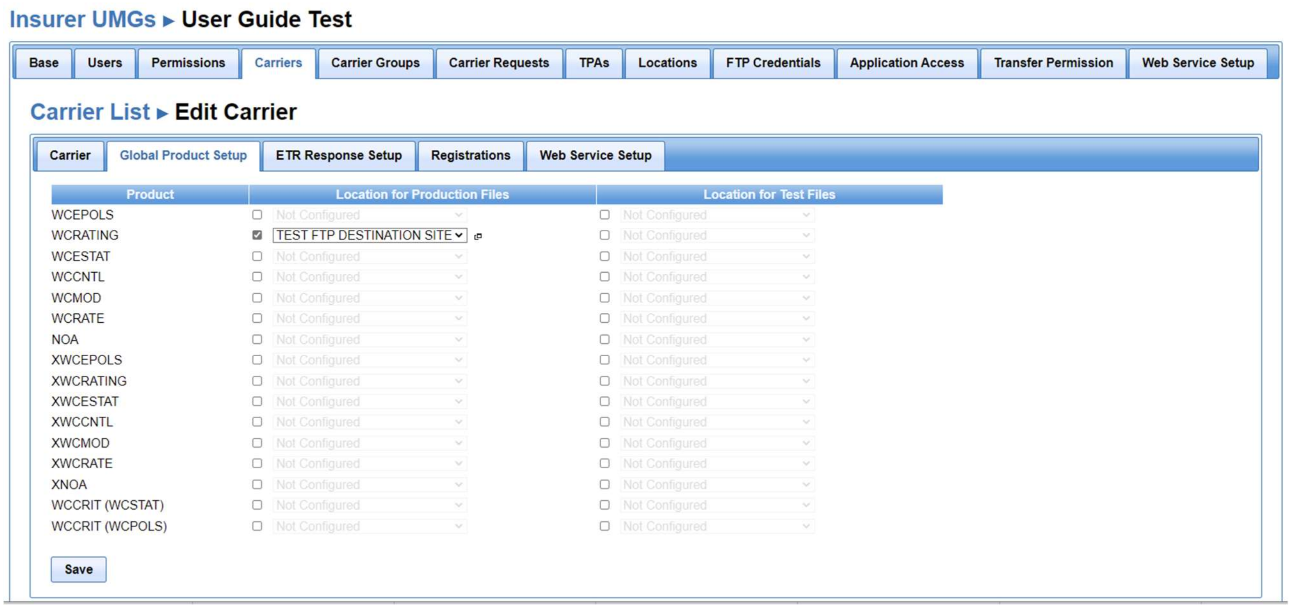
Administrators can select/deselect access privileges and Save to update.



Global Product Setup

The **Global Product Setup** tab lists the products that can be sent from DCOs to carriers. Each product has an associated checkbox and dropdown field. The dropdown lists available locations where product files may be sent. Note that there are separate columns to specify locations for Production files and for Test files. (Location details are in the Locations tab, which is addressed in another section of this guide.)

For each product that is to be received, click the associated checkbox and select the appropriate location from the dropdown. After all selections have been made, click Save.



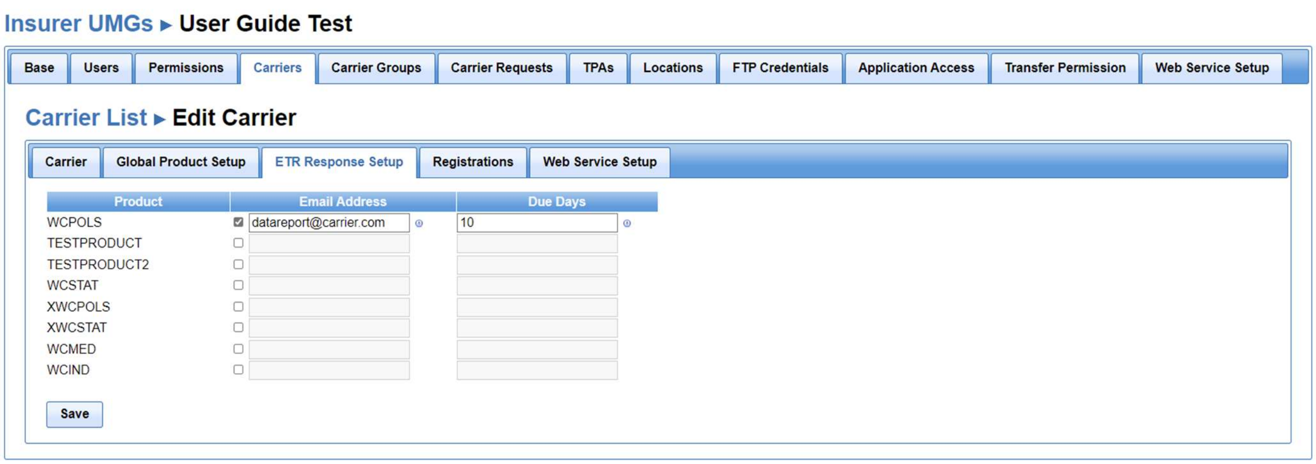
ETR Response Setup

The **ETR Response Setup** tab lists products that can be sent from carriers to DCOs.

The **Email Address** is the address to which CDX will send delivery status notifications.

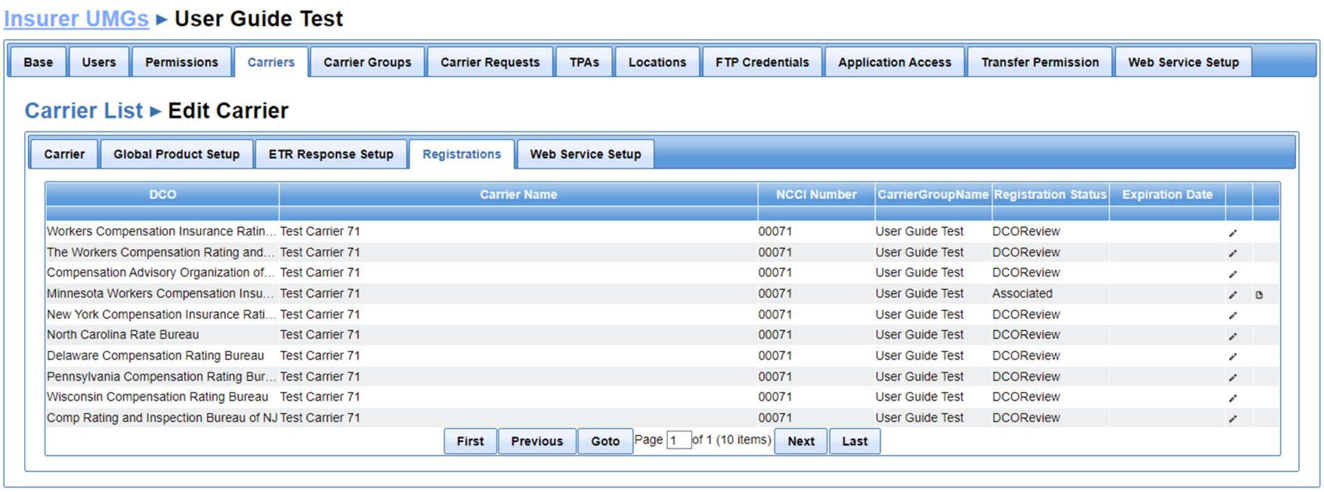
The **Due Days** field is used to calculate the Due Date when viewing the results in the ETR product. It is a simple calculation of the Received Date + the # of days entered. This can be used to help a carrier identify when they should follow-up with a DCO for file processing status. For example, if you submit a file to a DCO on 1/1/2022 and the Due Days is set to 10, then the ETR Due column will display 1/11/2022 as the date you would expect a DCO to have processed your file.

For each product that will be sent to a DCO, click the checkbox, enter the e-mail address that is to receive delivery status notification, from CDX, and if desired, enter the number of due days. After all data has been entered, click Save.



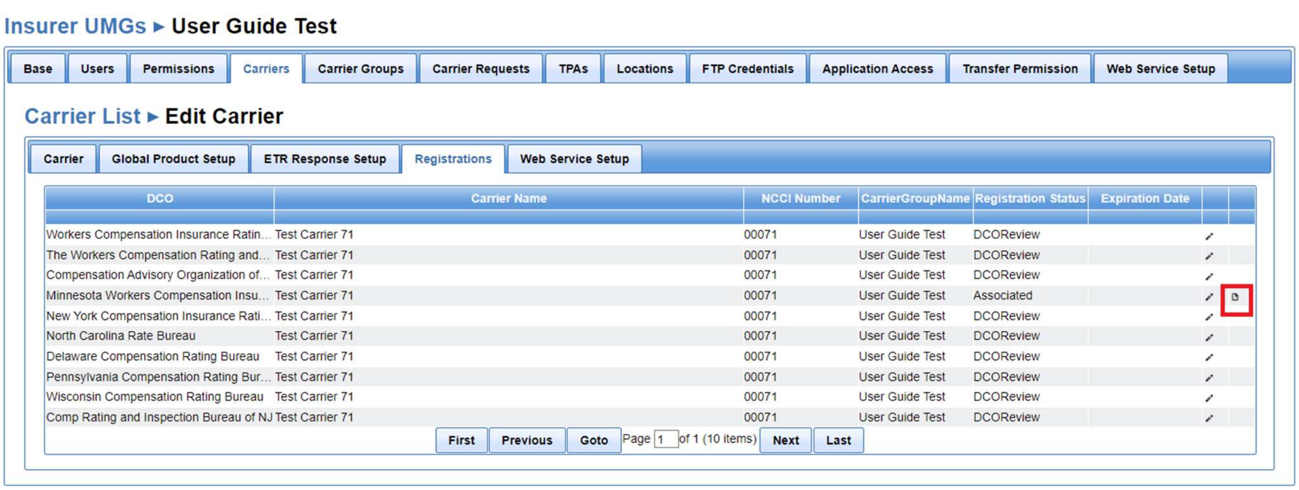
Registrations

The Registrations tab lists the CDX Members (DCOs) and the carrier's registration status for each DCO. One a DCO approves a carrier for data submissions, the Registration Status will reflect 'Associated'.

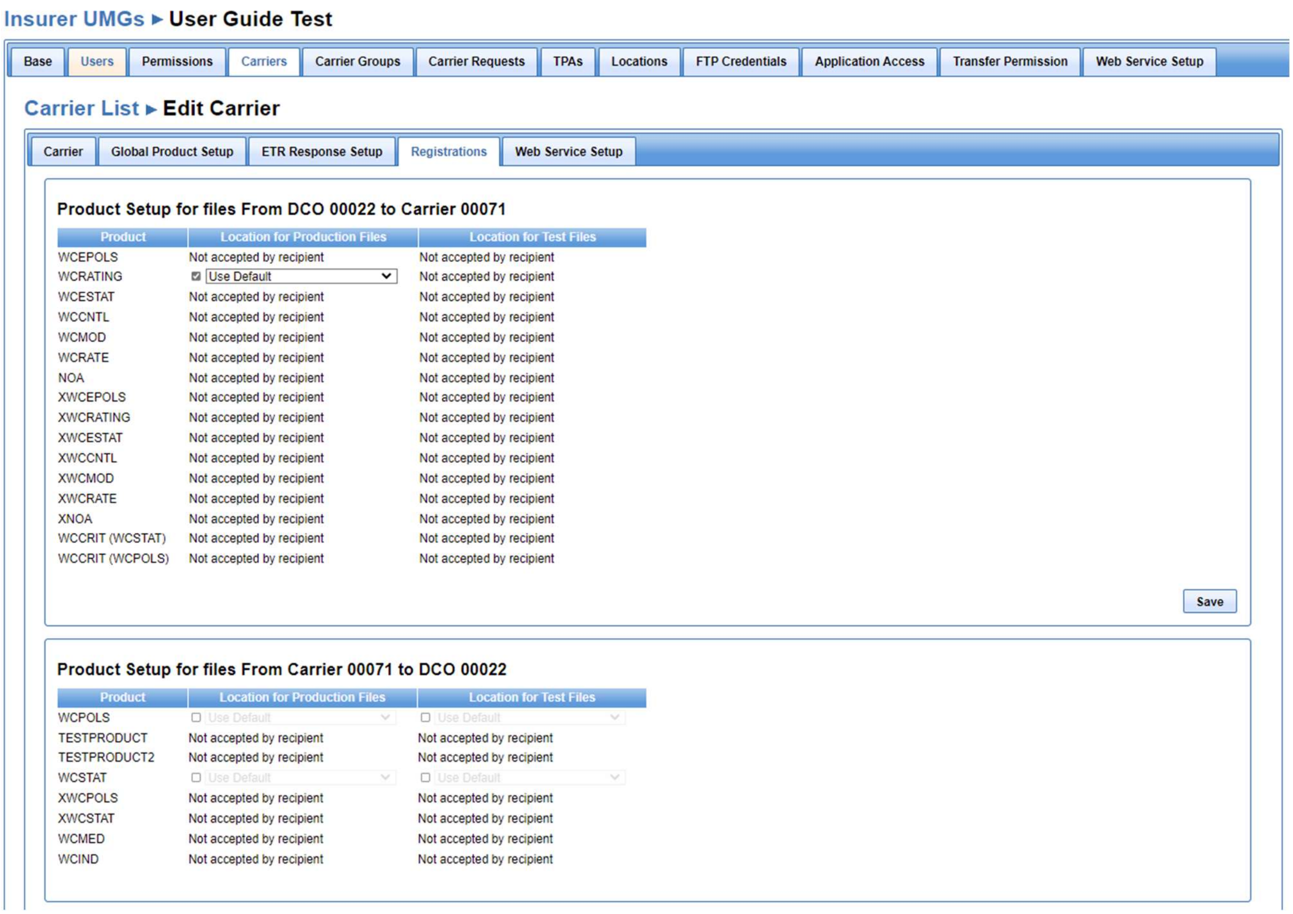


DCO	Carrier Name	NCCI Number	CarrierGroupName	Registration Status	Expiration Date
Workers Compensation Insurance Ratin…	Test Carrier 71	00071	User Guide Test	DCOReview	
The Workers Compensation Rating and…	Test Carrier 71	00071	User Guide Test	DCOReview	
Compensation Advisory Organization of…	Test Carrier 71	00071	User Guide Test	DCOReview	
Minnesota Workers Compensation Insu…	Test Carrier 71	00071	User Guide Test	Associated	
New York Compensation Insurance Rati…	Test Carrier 71	00071	User Guide Test	DCOReview	
North Carolina Rate Bureau	Test Carrier 71	00071	User Guide Test	DCOReview	
Delaware Compensation Rating Bureau	Test Carrier 71	00071	User Guide Test	DCOReview	
Pennsylvania Compensation Rating Bur…	Test Carrier 71	00071	User Guide Test	DCOReview	
Wisconsin Compensation Rating Bureau	Test Carrier 71	00071	User Guide Test	DCOReview	
Comp Rating and Inspection Bureau of NJ	Test Carrier 71	00071	User Guide Test	DCOReview	

For Associated DCOs, the Registrations status list includes the ability to view the associated DCO Product Setup screen, by selecting the document icon on the far right.



DCO	Carrier Name	NCCI Number	CarrierGroupName	Registration Status	Expiration Date
Workers Compensation Insurance Ratin…	Test Carrier 71	00071	User Guide Test	DCOReview	
The Workers Compensation Rating and…	Test Carrier 71	00071	User Guide Test	DCOReview	
Compensation Advisory Organization of…	Test Carrier 71	00071	User Guide Test	DCOReview	
Minnesota Workers Compensation Insu…	Test Carrier 71	00071	User Guide Test	Associated	
New York Compensation Insurance Rati…	Test Carrier 71	00071	User Guide Test	DCOReview	
North Carolina Rate Bureau	Test Carrier 71	00071	User Guide Test	DCOReview	
Delaware Compensation Rating Bureau	Test Carrier 71	00071	User Guide Test	DCOReview	
Pennsylvania Compensation Rating Bur…	Test Carrier 71	00071	User Guide Test	DCOReview	
Wisconsin Compensation Rating Bureau	Test Carrier 71	00071	User Guide Test	DCOReview	
Comp Rating and Inspection Bureau of NJ	Test Carrier 71	00071	User Guide Test	DCOReview	



The section Product Setup for files From DCO X to Carrier Y, lists all products that may be sent from a DCO to a carrier. Products must first be configured in the Global Product Setup tab before they can be configured on the DCO Registration page. Once a product is enabled on Global Product Setup, a checkbox will appear on this page with a corresponding dropdown to specify the destination location of the files. The default setting on the dropdown field is Use Default, which is the location specified in Global Product Setup.

If the location that was specified in Global Product Setup is appropriate, no action is needed on this screen. If a location other than the location in Global Product Setup is needed, for a given product and DCO, then check the associated box and select the location from the dropdown.

The section Product Setup for files From Carrier Y to DCO X lists all products that may be sent from a carrier to a DCO. Products that have been set up, in Global Product Setup, will have a corresponding checkbox and dropdown field. This section may be edited by the DCO.

Web Service Setup

The Web Service Setup page is used to request approval from participating DCOs to utilize the WCUnderwriting web service. This service enables a carrier to electronically receive ratings factors from participating DCOs. In order to use this service, each DCO must approve the carrier. After approved, the carrier utilizes this screen to obtain an API Authorization Key.

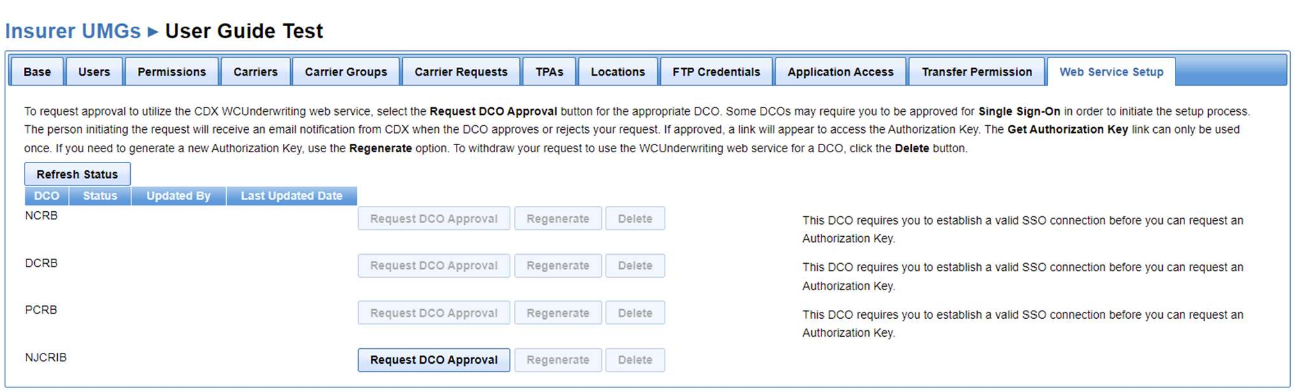
NOTES:
TPAs must obtain API Authorization Keys from their carriers. Please reach out to your carrier to initiate the process.

Some DCOs require the carrier to have established a Single Sign On (SSO) account first. Please see the Single Sign On (SSO) section of this guide for further instructions.

Depending on what configuration the DCOs support, Authorization Keys can be established at either the Group Level or the individual Carrier Level.

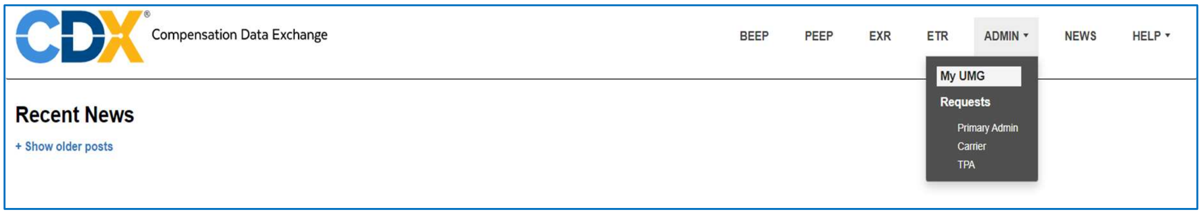
To access the Group Level, select Admin, then MyUMG and then the Web Services Setup tab.

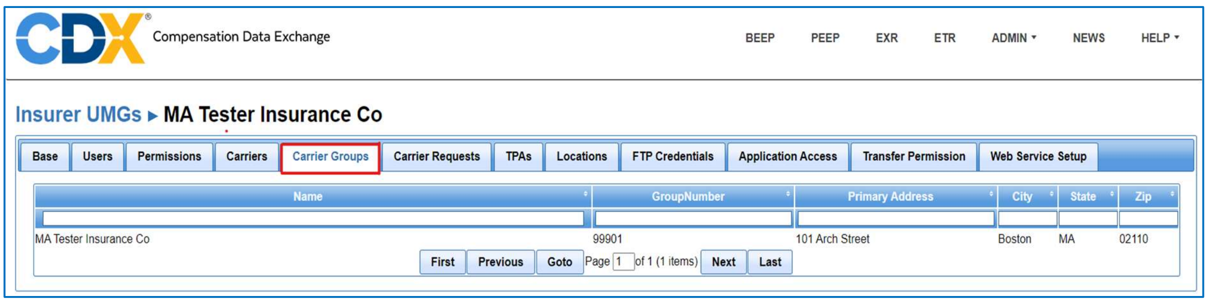
To access the Carrier Level, select Admin, then MyUMG, then the Carrier tab. Select the carrier id link and then click the Web Services Setup tab.



Carrier Groups

The Carrier Groups tab lists the carrier group(s) in the Insurer UMG. It is accessible to the Primary Administrator and users who have security to manage Carriers and Carrier Groups. For such users, the Carriers tab and Carrier Requests tab are also accessible. Select the Admin menu, then My UMG.





Carrier and TPA Requests

The Primary Administrator or a User with Admin permissions to Manage Carriers and Carrier Groups will have an Admin menu where they can create Carrier Requests.

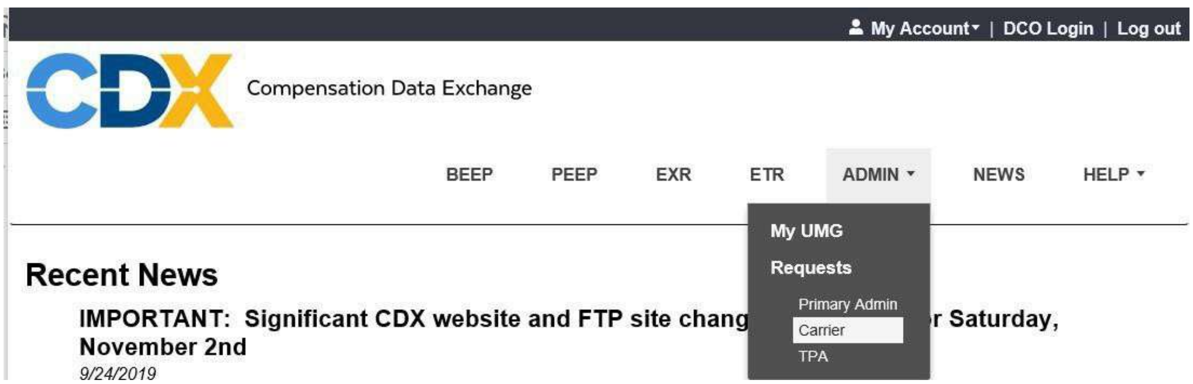
The Primary Administrator or a User with Admin permissions to Manage Users and Permissions will have an Admin menu where they can create TPA Requests.

Create a Carrier Request

A Carrier Request is a request sent to CDX Central Support to add a new carrier to the UMG. There are two options, for navigating to the Carrier Request screen.

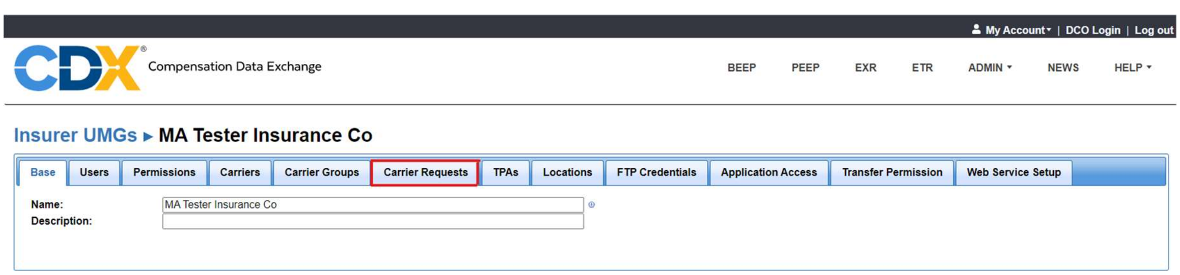
Option 1

- Choose the Admin menu, then Requests, then Carrier.

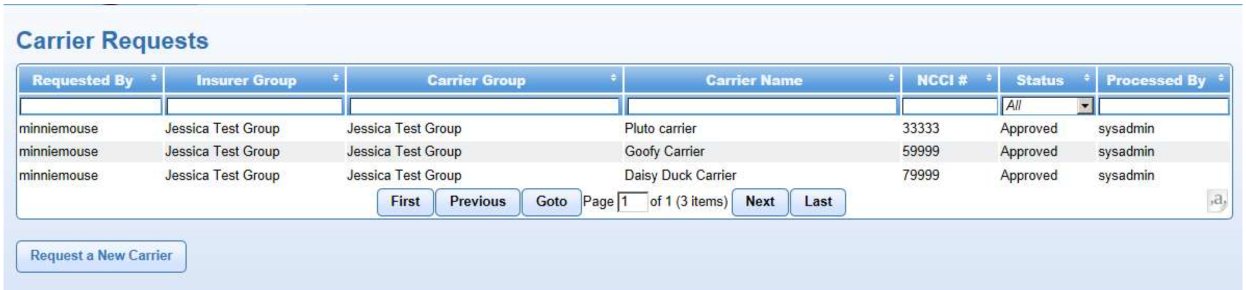


Option 2

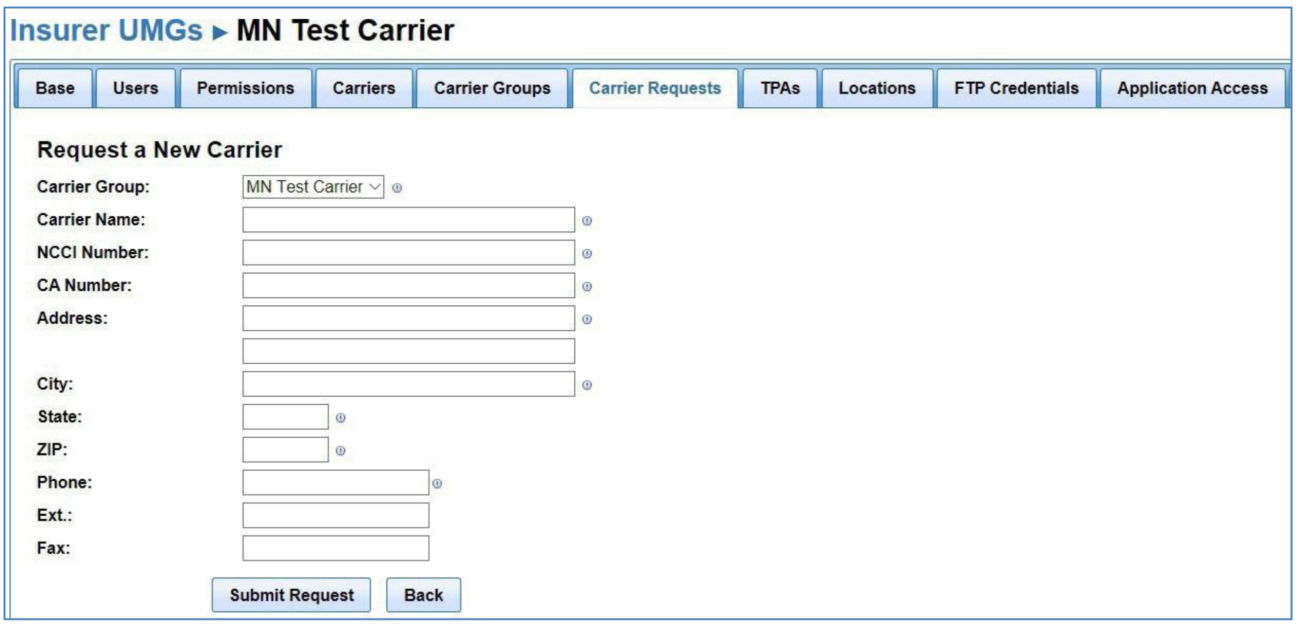
- Choose the Admin menu, then My UMG.
- Select the Carrier Requests tab.



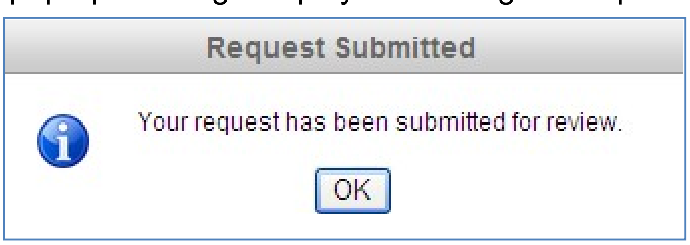
- The Carrier Request screen will list the current carrier requests for your UMG and their Status.
- To request a new carrier, click the 'Request a New Carrier' button.



- The Request a New Carrier screen will appear.
- Fill out the Carrier Name, NCCI Number, Phone and Address information.
- 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.

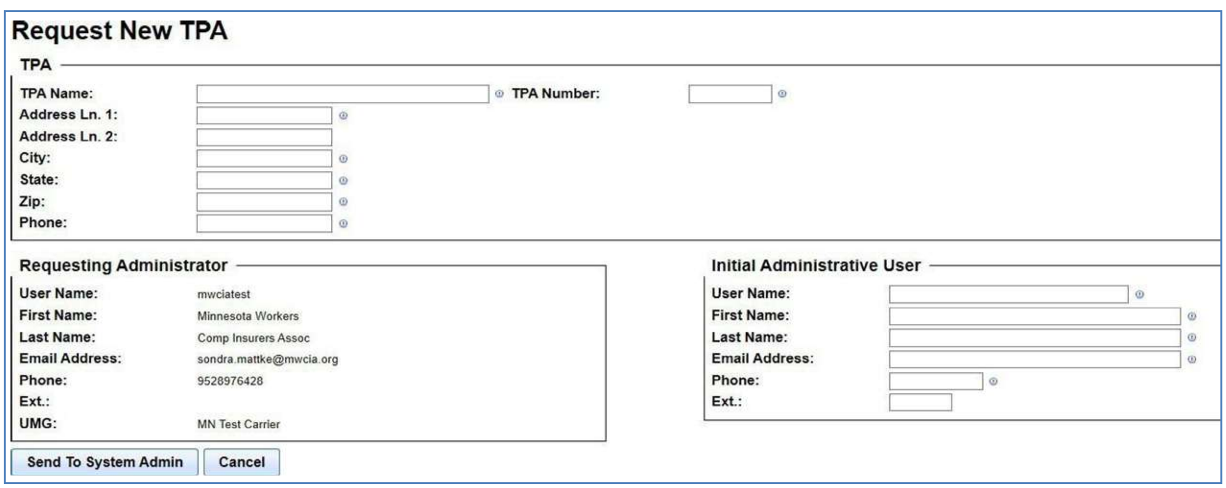
Create a TPA Request

A TPA Request is a request sent to **CDX Central Support** to add a new TPA to CDX.

- Choose the Admin menu, then Requests, then TPA. This will navigate to the TPA Requests screen.

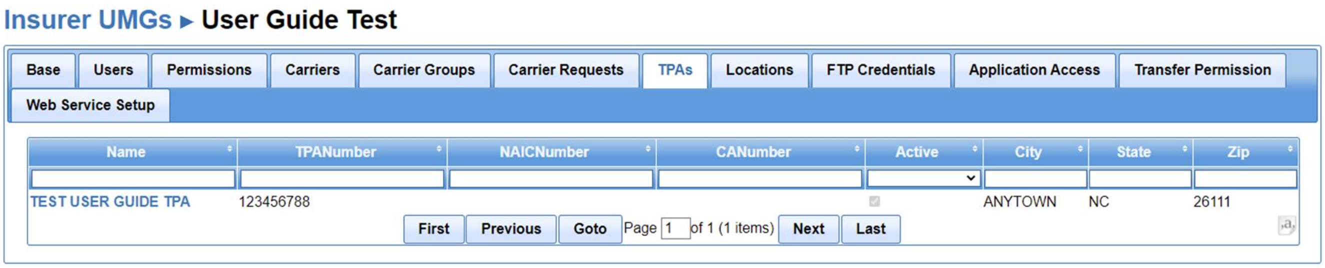
- Click the ‘Create Request’ button.

- Enter the TPA Name and TPA Number, if known. Typically, the TPA Number will be the FEIN # of the TPA.



- The requesting Primary Administrator is pulled from the logged in user.
- Complete the Initial Administrative User information. This information would contain the user that will become the primary administrator for the TPA.
- 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 TPAs, select Admin, 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 isnot approved and cannot access carrier data or transfer files.

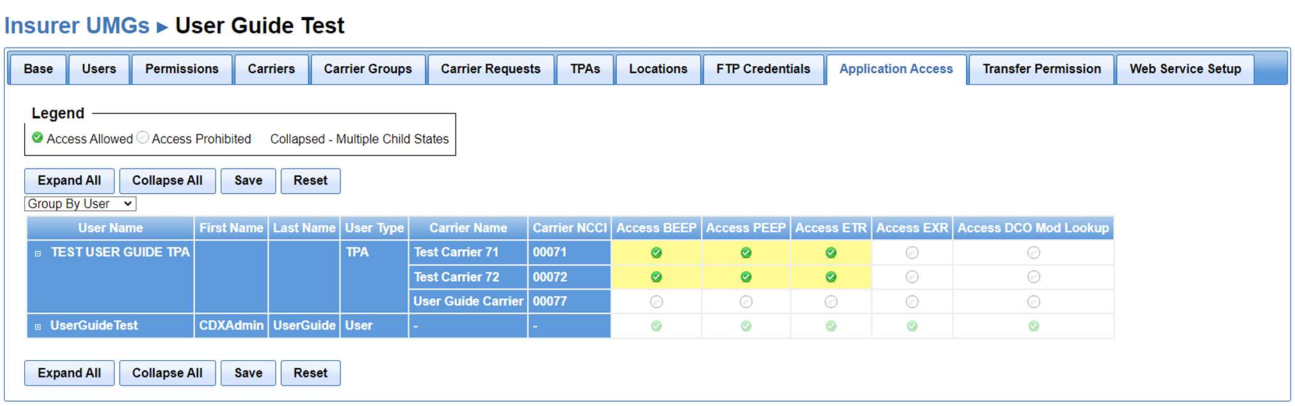


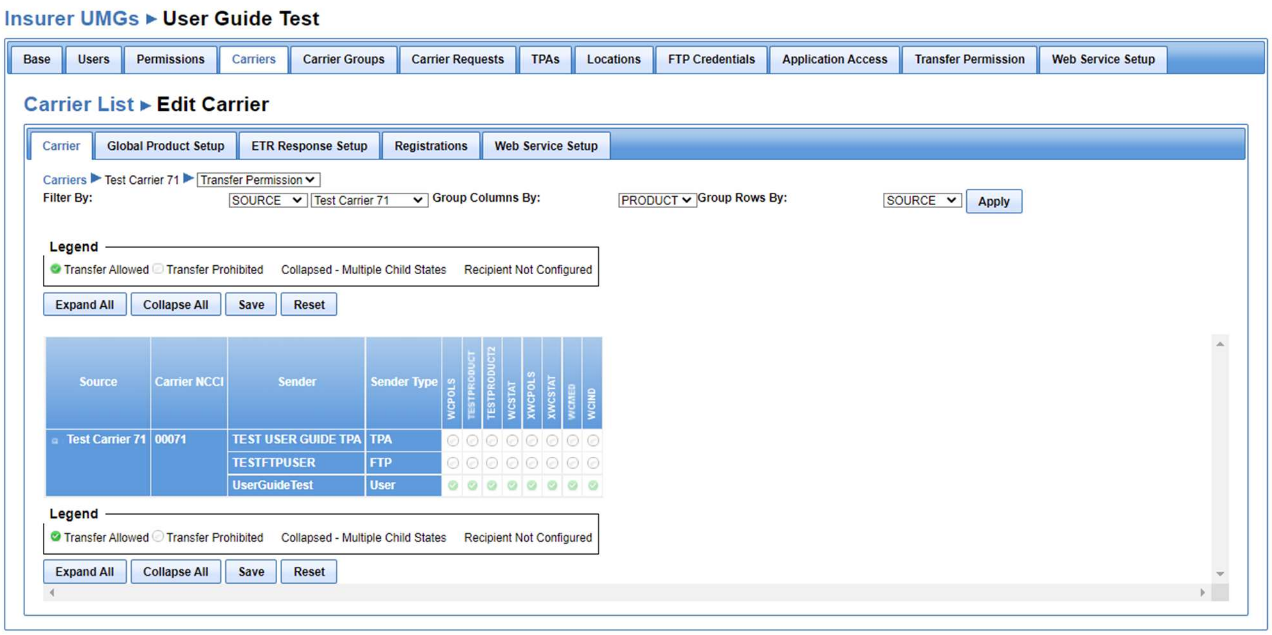
Once a TPA is linked to your UMG, there are a couple of additional steps you will need to complete in order for the TPA to begin accessing and submitting data.

- Application Access – Grant the TPA administrator access to the applicable CDX products (e.g. PEEP, BEEP)
- Transfer Permissions – Grant the TPA administrator access to the data types (e.g. WCPOLS, WCSTAT)

Follow the same process used to give permissions to Users (see Setup Application Access).

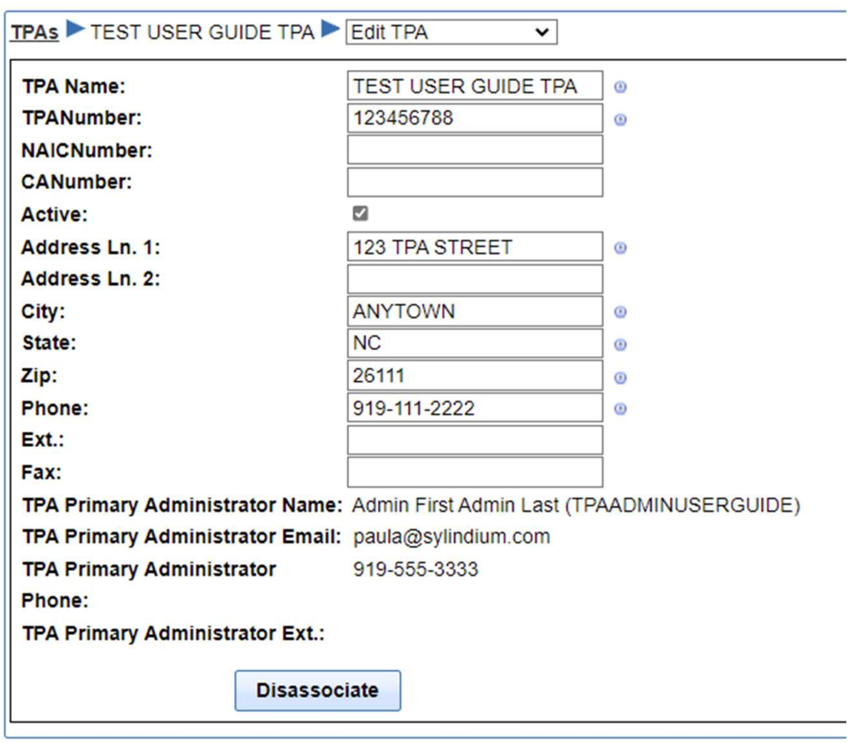
The TPA will appear on the Application Access tab as a User with User Type TPA and in Transfer Permissions as a Sender with Sender Type TPA:





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.

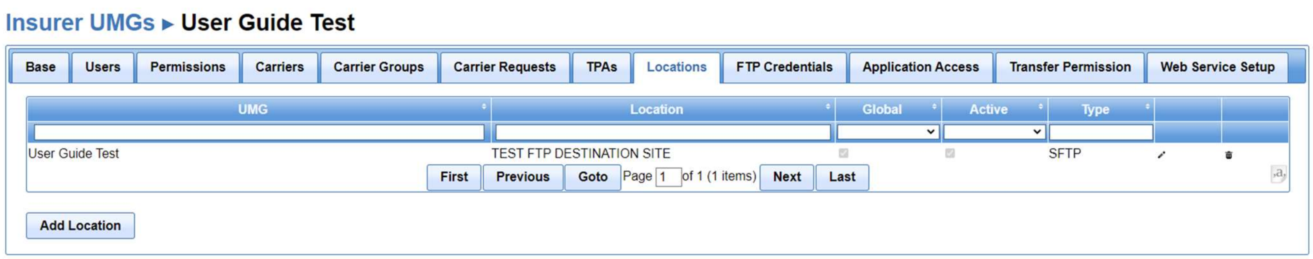


- An “Are you sure…” confirmation box will pop up. Select OK.
- A “Successfully disassociated…” confirmation box will pop up. Select OK.
- The TPA will no longer appear in the list of TPAs for the UMG and the TPA will no longer be able to report or view data for the carrier(s) in the UMG.

Locations

Locations specify the list of options for how carriers will receive files that are sent from the DCOs. The two choices for file receipt are either electronically to the carrier network utilizing Secure File Transfer Protocol (SFTP) or manually by logging into the CDX website and performing a file download (Web Pick-up).

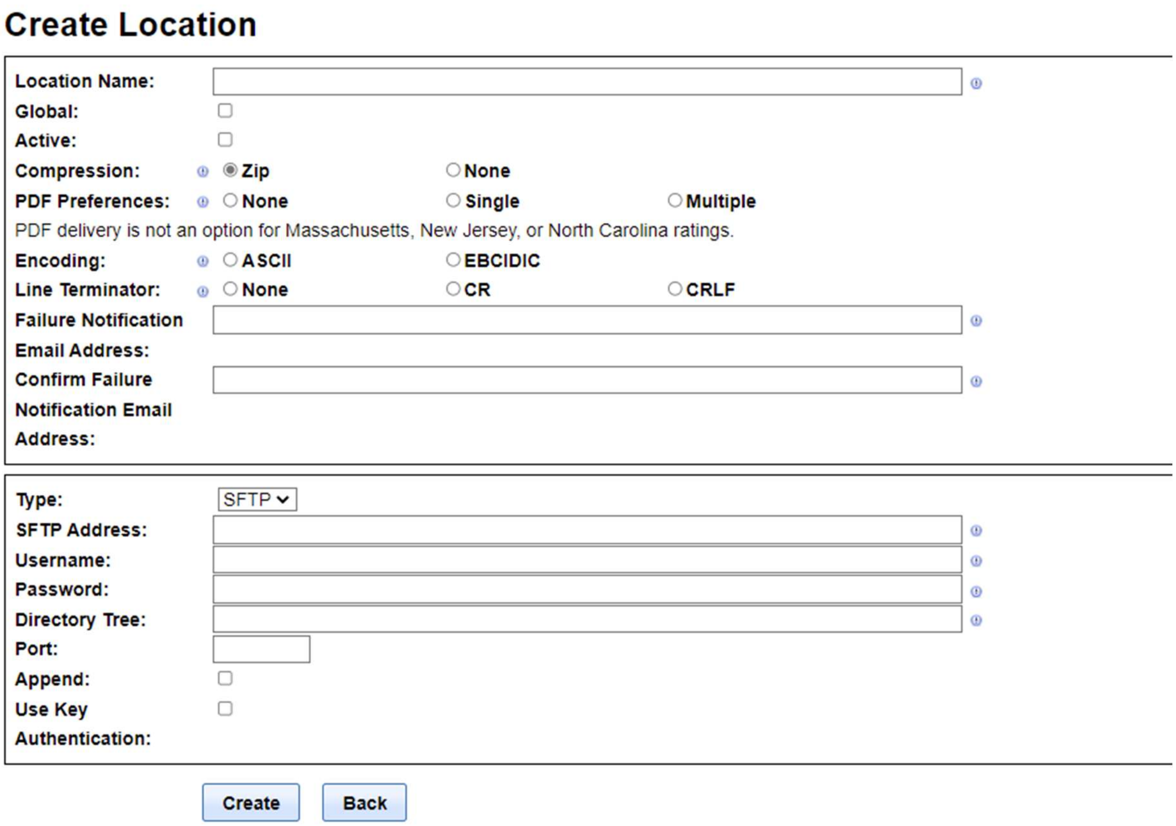
To access, Select the ADMIN menu, select My UMG, and then Locations.



The Location screen will display the UMG and the current Location setups. Once Locations are setup, the Primary Administrator or User with Admin permissions will be able to specify the target file location for each of the products utilizing the Global Product Setup page. Carriers can elect to set up a single location for all file types, or to create separate locations for the different file types (e.g. one location for WCPOLS, a separate location for WCSTAT).

Add Location

- Select ADMIN, My UMG, then the Locations tab.
- Select the ‘Add Location’ button.
- The ‘Create Location’ screen will appear.



- **Location Name** - Name to identify the destination and file type (e.g. WCPOLS SFTP).
- **Global** - This field is no longer used and will be removed in a future version of the software
- **Active** – Helps to identify current vs. discontinued locations.
- **Compression** - Choose either Zip or None
- **PDF Preferences** – Utilizing to specify the file type for receipt of WCRatings files. If PDF is not selected, the DCO will send WCRatings files in the WCIO flat file format. Note: Not all DCOs support delivery of PDF files and the PDF files.
- **Encoding**: Choose either ASCII, or EBCIDIC to indicate the encoding that should be applied to the files that are received at the specified location. ASCII is the default, EBCIDIC is typically only used for files that need to be processed by a mainframe.
- **Line Terminator**: Choose either None, CR (Carriage Return) or CRLF (Carriage Return Line Feed). Linux servers typically utilize CR and Windows servers utilize CRLF.
- **Failure Notification E-mail**: The email address that should receive notifications when a file transfer fails. CDX currently only supports a single email address. Carriers can enter a distribution group email address if you would like multiple recipients to receive the notifications.

- **Type**: Choose how you would like to receive the file: either SFTP or Web.

For SFTP

- **SFTP Address** - The destination SFTP server address
- **Username** - The username that should be utilized to authenticate to the SFTP site.
- **Password** - The password that should be utilized to authenticate to the SFTP site.
- **Directory Tree** - Input the directory tree relative to the root that should be used when transferring files (e.g. \In). If left empty/blank, files will be transferred to the root directory.
- **Append** - In most cases, this should be left unchecked. Check the box if you want the system to open the target file and append vs. overwrite files if the file name already exists on the destination directory.
- **Use Key Authentication** – This option provides password-less authentication using SSH key authentication and requires manual setup by CDX. Please contact CDX Central Support if you would like more information about this option.

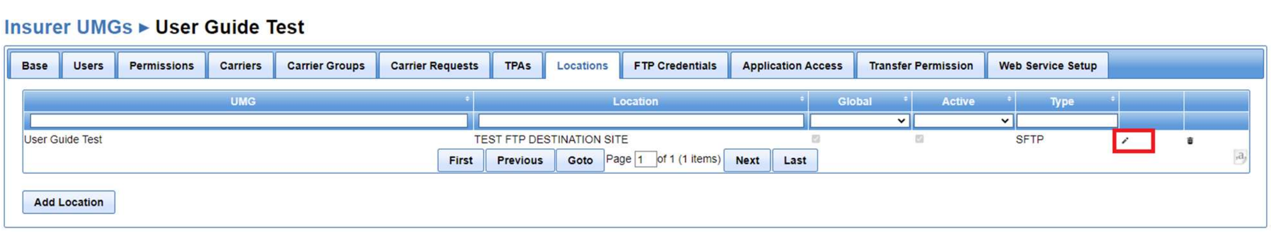
For Web

No additional information is needed beyond that entered in the top section. When Web is chosen in the Type section, the Type section will collapse.

Click the 'Create' button to save the location.
Click the 'Back' button to cancel out of creating a location.

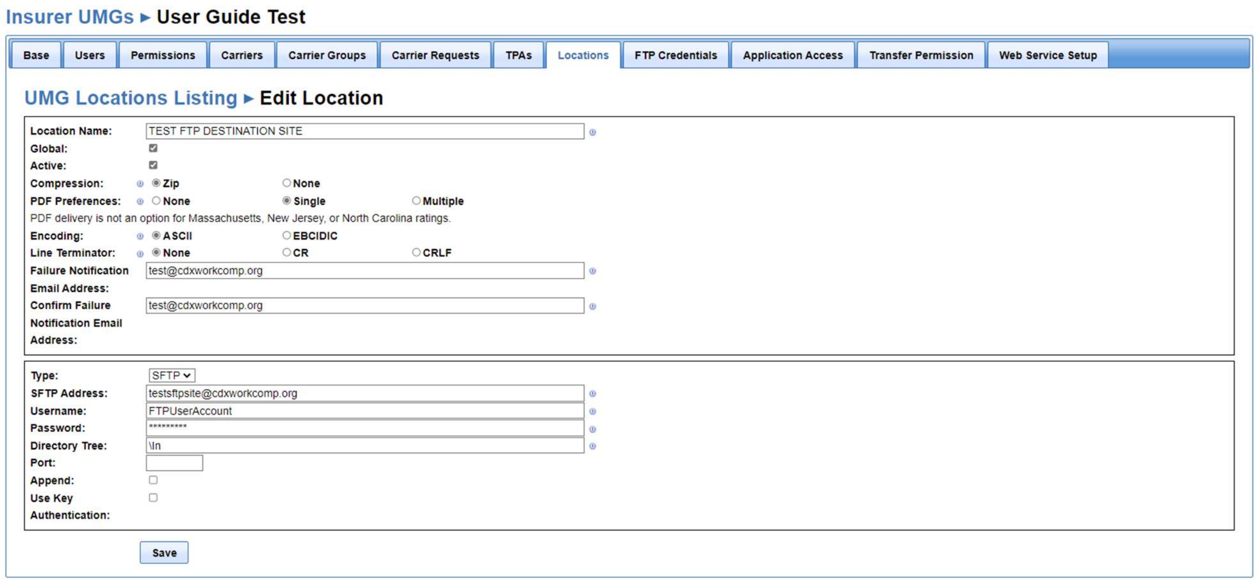
Edit Location

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



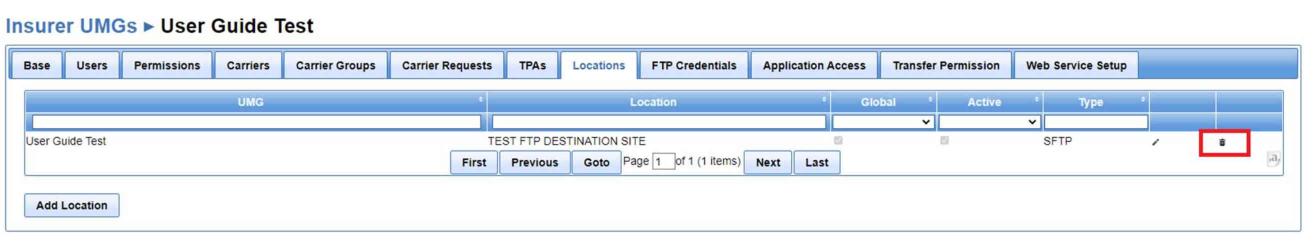
- The 'Edit Location' screen will appear, and you can change any of the fields. Click the 'Save' button to save the changes.
- To cancel out of this page, click the UMG Locations Listing or one of the carrier

tabs.



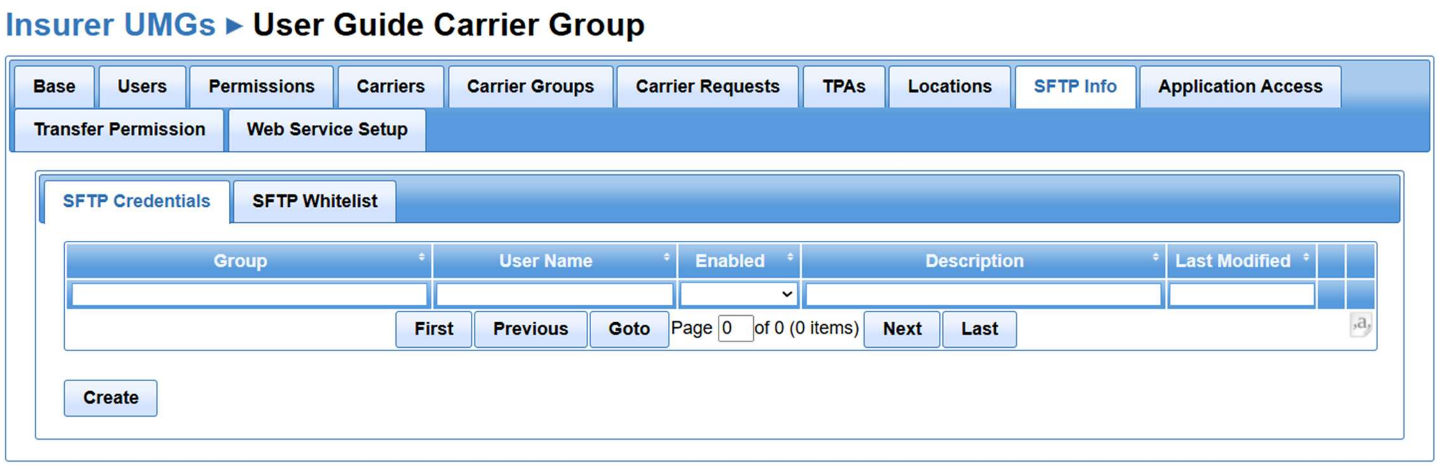
Delete Location

- 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.



SFTP Info

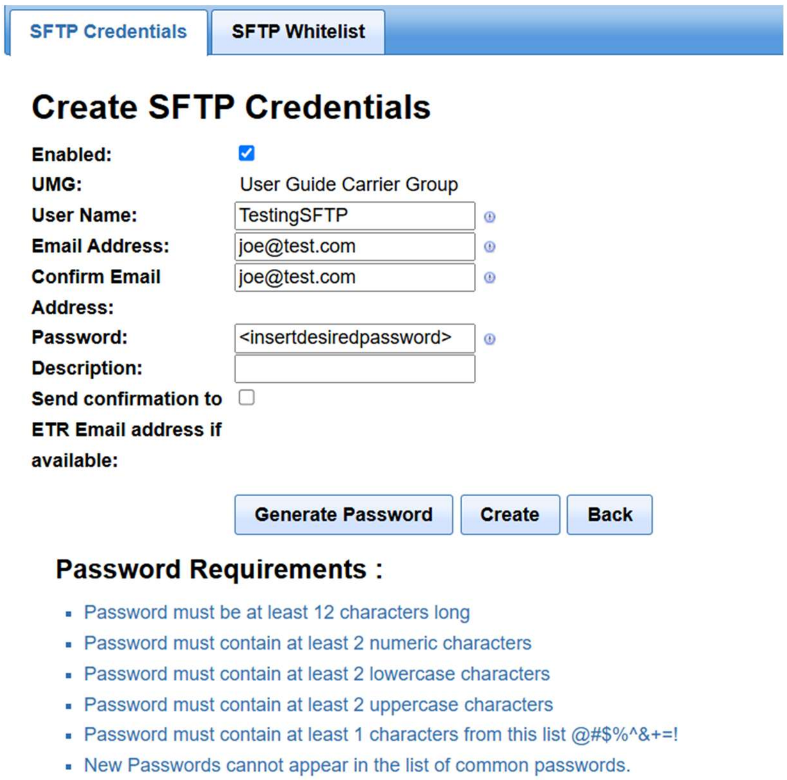
The SFTP Info tab is used to manage SFTP credentials, IP addresses and Technical Contacts.



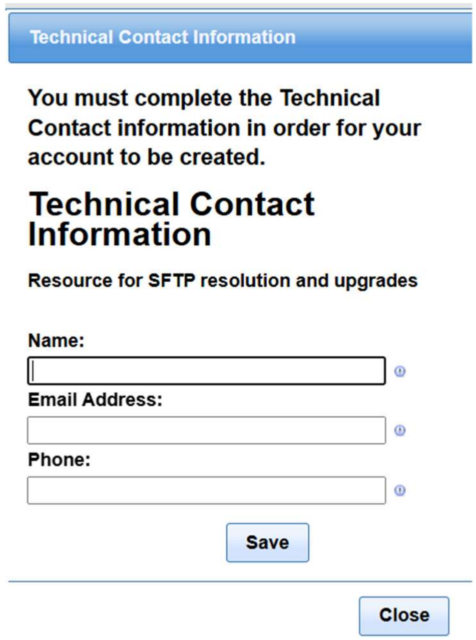
Create SFTP Credentials

In order to transmit files to the SFTP site, you will need to establish a SFTP account.

- Click ADMIN, then My UMG.
- Click the SFTP Info tab and then then SFTP Credentials tab.
- Click the ‘Create’ button.
- The Create SFTP Credentials screen will appear.



- Make sure the **Enabled** check box is checked.
- Enter a unique username for the SFTP Credentials.
- Enter a password following the password requirements or click the Generate Password button to generate a random password.
- Optionally, enter a description.
- Enter the email address that can be utilized for error notifications.
- Select the checkbox next to the ‘Send Confirmation to ETR Email address, if available’ checkbox if you would prefer for error notifications to be sent to the email address that is contained within the ETR record of each data file.
- Click the ‘Create’ button to save the SFTP Credentials.
- Click the ‘Back’ button to cancel out of creating the SFTP Credentials.
- Upon Save, if your UMG does not have a FTP Technical Contact saved, the system will prompt you to create:


Technical Contact Information
You must complete the Technical Contact information in order for your account to be created.
Technical Contact Information
Resource for SFTP resolution and upgrades
Name:
Email Address:
Phone:
Save
Close

Edit SFTP Credentials

- Click ADMIN, then My UMG.
- Click the SFTP Info tab and then the SFTP Credentials tab. Edit Credential is selected by default.
- Click the pencil icon located 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 the changes.
- To edit the SFTP Transfer Permissions, click on the down arrow next to Edit Credential to select Transfer Permission.
- 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 SFTP Credentials

- Click ADMIN, then My UMG.
- Click the SFTP Info | SFTP 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 SFTP credential?”
- Click OK to delete the SFTP Credential. You will receive a pop-up “Successfully deleted SFTP credentials.”
- Click Cancel to terminate the deletion. You will be navigated back to the SFTP Credentials screen.

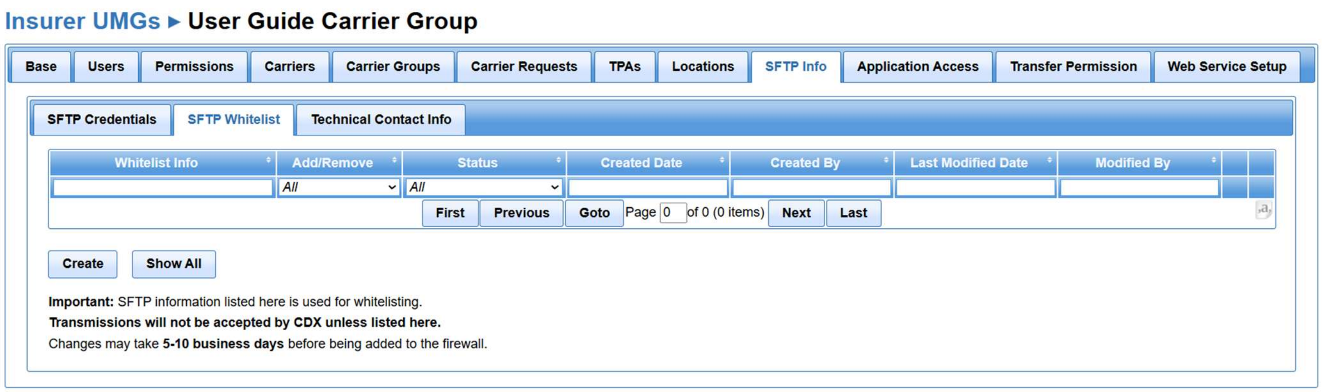
SFTP Whitelist

In order to transmit files to the CDX SFTP server, your organization's IP address must be added to the CDX firewall.

NOTE: It could take CDX up to 10 business days to add your IP address to the firewall. If you need to submit a file using the CDX platform while you wait for the firewall change, you can use the ETR File Upload option.

To access the SFTP Whitelist administrative page:

- Click ADMIN, then My UMG.
- Click the SFTP Info tab and then the SFTP Whitelist tab. By default, only the active Whitelist requests will display. To see historical, click the Show All button.



SFTP Whitelist Request Statuses

Your SFTP Whitelist Request can be in one of the following statuses:

- New: CDX has not processed your request.
- Pending Firewall Update: CDX has submitted your request to the firewall team.
- Complete: Your IP address has been added to the firewall. When your request reaches this status, you will receive an email confirmation.
- Withdrawn: Your IP address was removed from the CDX firewall.

Add a SFTP Whitelist Request

To submit a new request to CDX to add an IP address to the firewall:

- Click the ‘Create’ button.
- The Add Whitelist Request screen will appear:

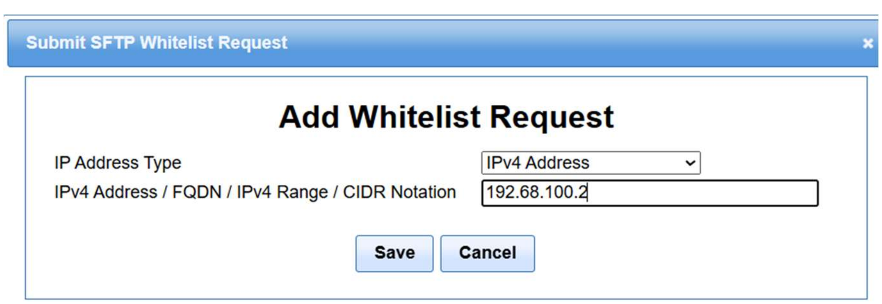
Select the type of IP Address you’d like to submit:

- IPv4 Address
- FQDN (Fully Qualified Domain Name)
- IPv4 Range
- CIDR Notation

Example IP Address Formats:

IPv4 Address:	192.28.20.1
FQDN:	ftp.example.com
IPv4 Range:	192.28.20.1-192.28.20.10
CIDR Notation:	192.28.20.0/24

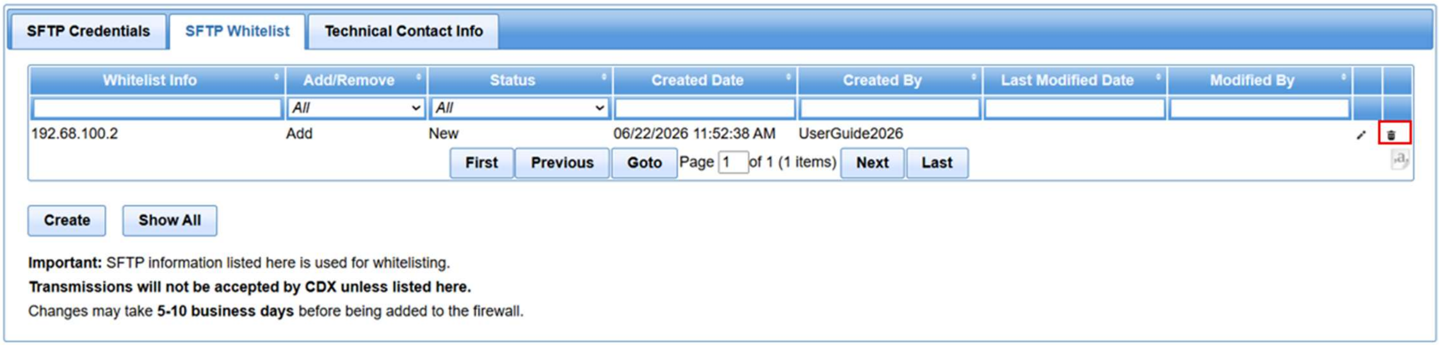
Enter the appropriate IP address value and click Save.

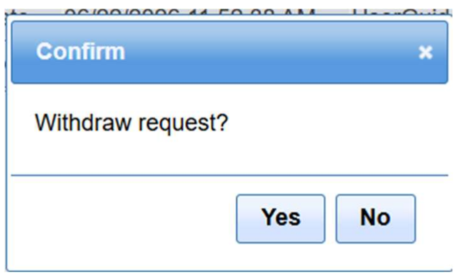


When a new request is submitted, the Status will be New and the Add/Remove option will be ‘Add’. CDX will send you an email once the IP address has been added to the firewall.

Withdrawing a Whitelist Request

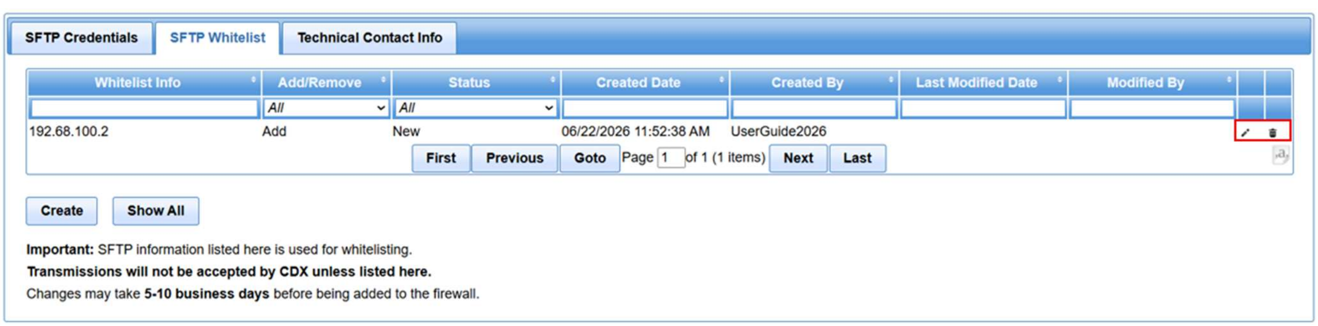
Once CDX begins processing or has completed processing your request, you can no longer modify it. If you submitted an IP address in error or your IP address has changed, you can submit to Remove your request by clicking the trash can icon on the far-right side of the row that has the IP address you'd like to remove:

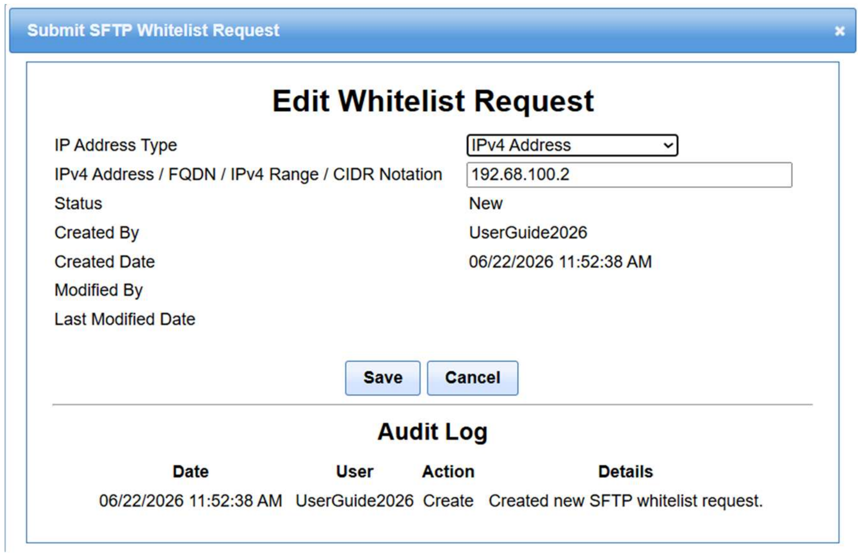




Updating a SFTP Whitelist Request

If CDX has not processed your IP address Add/Remove request yet, you can modify or delete it using the pencil icon and trashcan icons on the right side of the row:





Once CDX has started to process your request, you can no longer make modifications. Instead, you will need to either use the Withdraw feature to submit a request to have it removed, or the Create feature to submit an additional IP address.

Submitting a Change to an IP Address

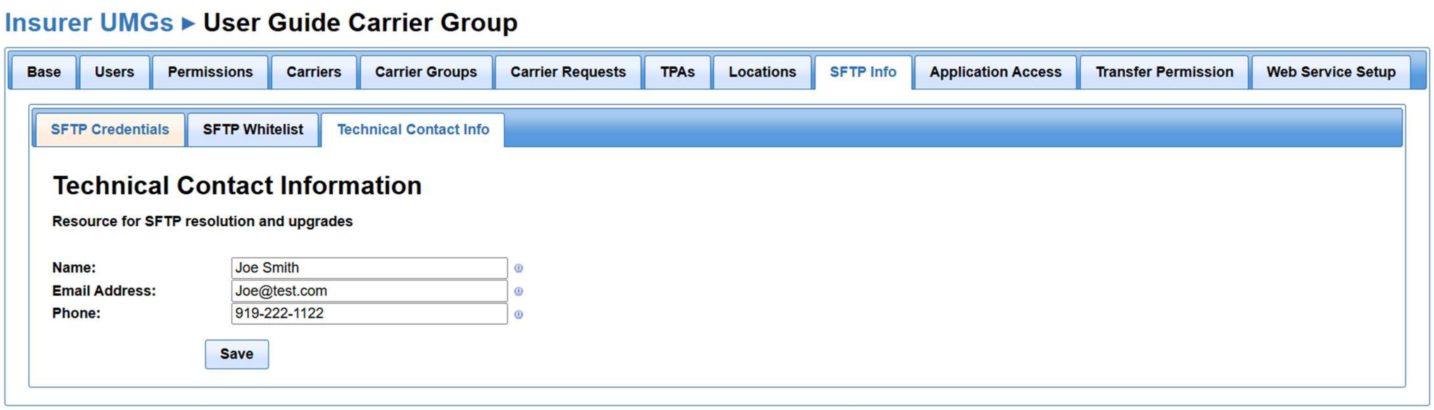
If your organization is changing your IP address(es):

- **Prior** to your organization's cut-over date to the new IP address, create a new Whitelist Request using the instructions provided above. Allow 5-10 business days to process. It is not necessary to remove your old IP address at this time. You can have multiple IP addresses in the firewall whitelist.
- **After** your organization has transitioned to your new IP address(es) and you are successfully transmitting files, you can withdraw your old IP address using the Withdraw instructions provided above.

SFTP Technical Contact Information

Your SFTP Technical Contact is normally an IT staff member that is responsible or familiar with your organization's SFTP setup/process. CDX utilizes this email address for sending notifications related to SFTP maintenance, outages or upgrades.

- Enter the name (first & last)
- Enter the Email address
- Enter the Phone number
- Click Save.


Insurer UMGs ▸ User Guide Carrier Group
Base
Users
Permissions
Carriers
Carrier Groups
Carrier Requests
TPAs
Locations
SFTP Info
Application Access
Transfer Permission
Web Service Setup
SFTP Credentials
SFTP Whitelist
Technical Contact Info
Technical Contact Information
Resource for SFTP resolution and upgrades
Name:
Joe Smith
Email Address:
Joe@test.com
Phone:
919-222-1122
Save

Application Access

Application Access is the screen on which the Primary Administrator or User with Admin permissions sets each User's permissions to access the CDX applications. The Primary Administrator or User with Admin permissions has the ability to set up application access by Users and by Carrier.

> *Note: A user with Admin permissions may only setup access for users in the carrier(s) for which the Admin has Manage User permissions and for only the applications for which the Admin has permissions.*
>
> *For example, if group 12345, has carriers 12345 and 13579 and the Admin has Manage User permissions only for carrier 13579, and only has access to BEEP, the Admin may only set permissions for users in carrier 13579 and for BEEP.*

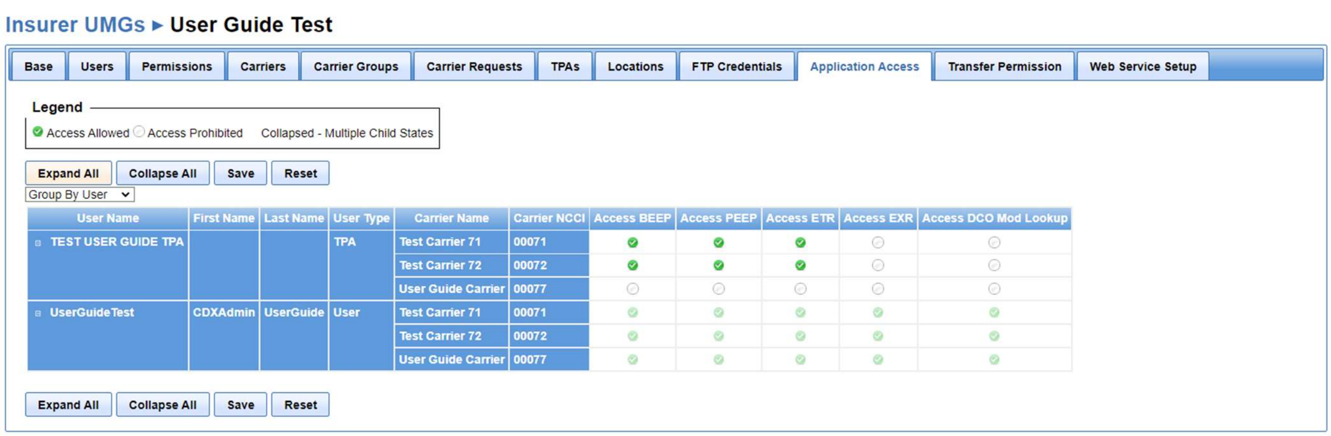
- Select ADMIN, then My UMG.
- Click the Application Access tab.

The default view is Group by User and all the users in the UMG will be listed.

- Click Expand All button to see all Carrier Names by User Name.
- Click the + icon next to the name to expand one at a time.
- Click Collapse All button to see only User Names.
- Click the – icon next to the name to collapse one at a time.

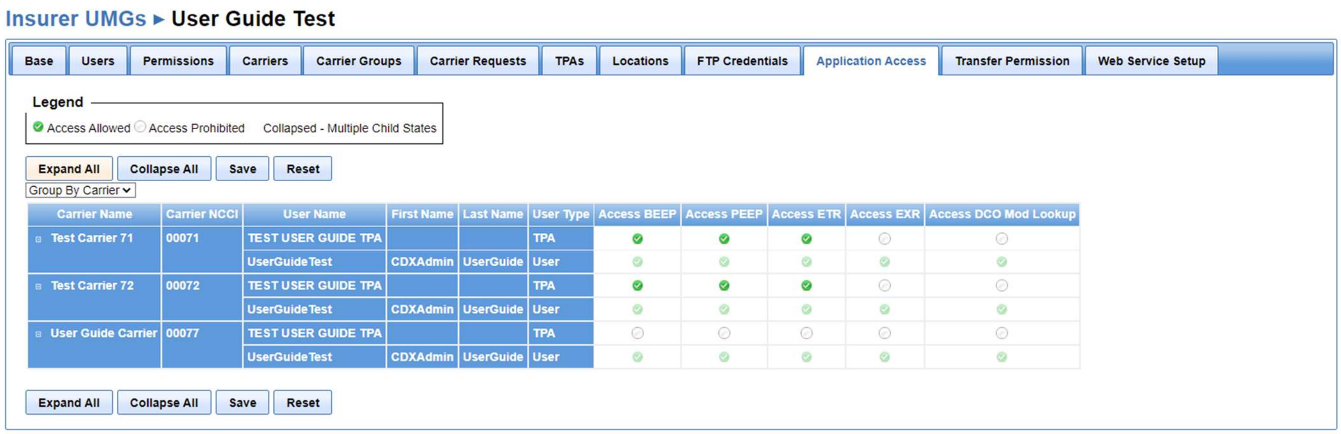
Example of Group by User

The Group by User screen displays a listing of all users and the Access Rights per carrier id.



Example of Group by Carrier

The Group by Carrier screen displays a listing of all carriers and the access rights per user.



- 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 will have a blank circle.
- 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.

Transfer Permissions

Transfer Permissions is the screen on which the Primary Administrator or User with Admin permissions sets each User’s permissions to send WCIO Products to DCOs.

Note: A user with Admin permissions may only setup transfer permissions for users in the carrier(s) for which the Admin has Manage User permissions and for only the WCIO products for which the Admin has permissions.

For example, if group 12345, has carriers 12345 and 13579 and the Admin has Manage User permissions only for carrier 13579, and only has transfer permissions for WCSTAT, the Admin may only set permissions for users in carrier 13579 and for WCSTAT.

- Click ADMIN, then My UMG.
- Click the Transfer Permission tab.

General grid behavior is as follows:

- Click Expand All button to expand all collapsed listings.
- Click the + icon next to the name to expand one at a time.
- Click Collapse All button to collapse all expanded columns.

- Click the – icon next to the name to collapse one at a time.

Fields above the Legend allow the user to filter and display the data in different ways.

Utilize the Filter By Source (Carrier List), Sender (User List) or Product (WCIO Product) to limit which data is displayed. Selecting one of these options will change the content of the second dropdown list.

The user also has the option Group Columns By Source, Sender or Product, and Group Rows By Source, Sender or Product to change the way the data is presented.

Whatever option is chosen in one field, determines what can be chosen in other fields, because all of the options must be different. For example if Filter by Source is chosen, then Source may not be selected for Group Columns By or for Group Rows By.

- To allow access, click the field to display a green checkmark circle.
- To deny access, the box will have a blank circle.
- 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.

Web Service Setup

The Web Service Setup page is used to request approval from participating DCOs to utilize the WCUnderwriting web service. This service enables a carrier to electronically receive ratings factors from participating DCOs. In order to use this service, each DCO must approve the carrier. After approved, the carrier utilizes this screen to obtain an API Authorization Key.

NOTES:
TPAs must obtain API Authorization Keys from their carriers. Please reach out to your carrier to initiate the process.

Some DCOs require the carrier to have established a Single Sign On (SSO) account first. Please see the Single Sign On (SSO) section of this guide for further instructions.

Depending on what configuration the DCOs support, Authorization Keys can be established at either the Group Level or the individual Carrier Level.

To access the Group Level, select Admin, then MyUMG and then the Web Services Setup tab.

To access the Carrier Level, select Admin, then MyUMG, then the Carrier tab. Select the carrier id link and then click the Web Services Setup tab.

ETR (Electronic Transmittal Record)

The ETR product provides access to view the status of files that were submitted to the DCO for processing. Files that have successfully been sent to the DCO have a ‘Sent’ status. Once a DCO processes a file, the status will be updated to ‘Accepted’ or ‘Rejected’.

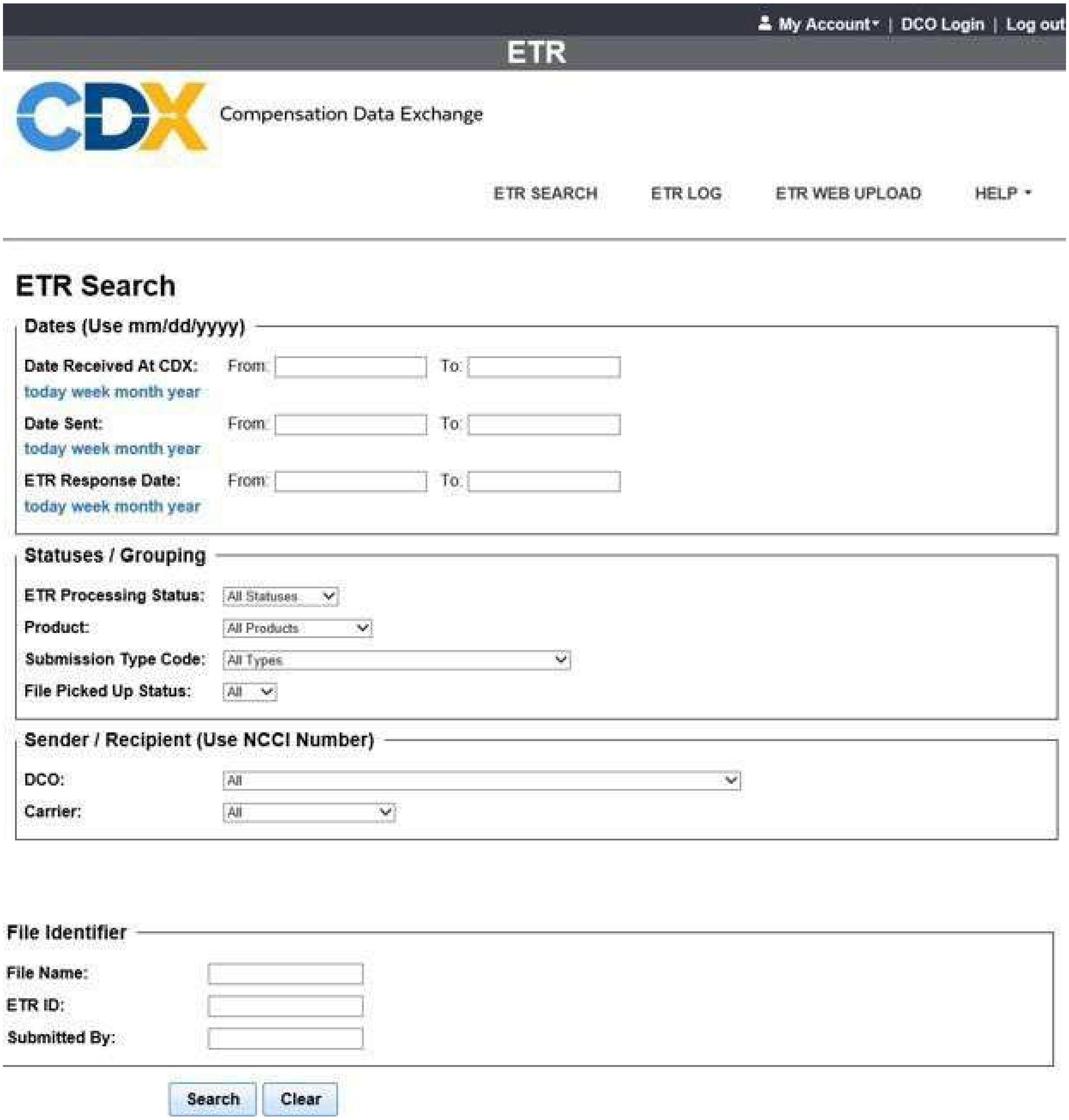
Within this menu a user has access to the ETR Search, ETR Log and ETR Web Upload.

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 displays submissions received within the previous 90 days for a UMG.

NOTE: The actual submission files are only available for 30 days.

- 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 hyper link. 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:
    - ETR Processing Status: the processing status of the file (see glossary for status explanations). Choose one from the dropdown list
    - Product: All CDX products; choose one from the dropdown list.
    - Submission Type Code: Type of file; choose one from the dropdown list.
    - File Picked Up Status: either true or false; Choose one.
  - Search by DCO or Carrier.
  - Search by File Name.
  - Search by ETR ID.
  - Search by Submitted By name.



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 each column.
- Utilize the First, Previous, Next and Last buttons to navigate the grid pages.
- The Page # field will jump you 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 icon located at the end of the row will take you to a screen which displays the details of the file, including error information, if applicable. 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 30 days 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.

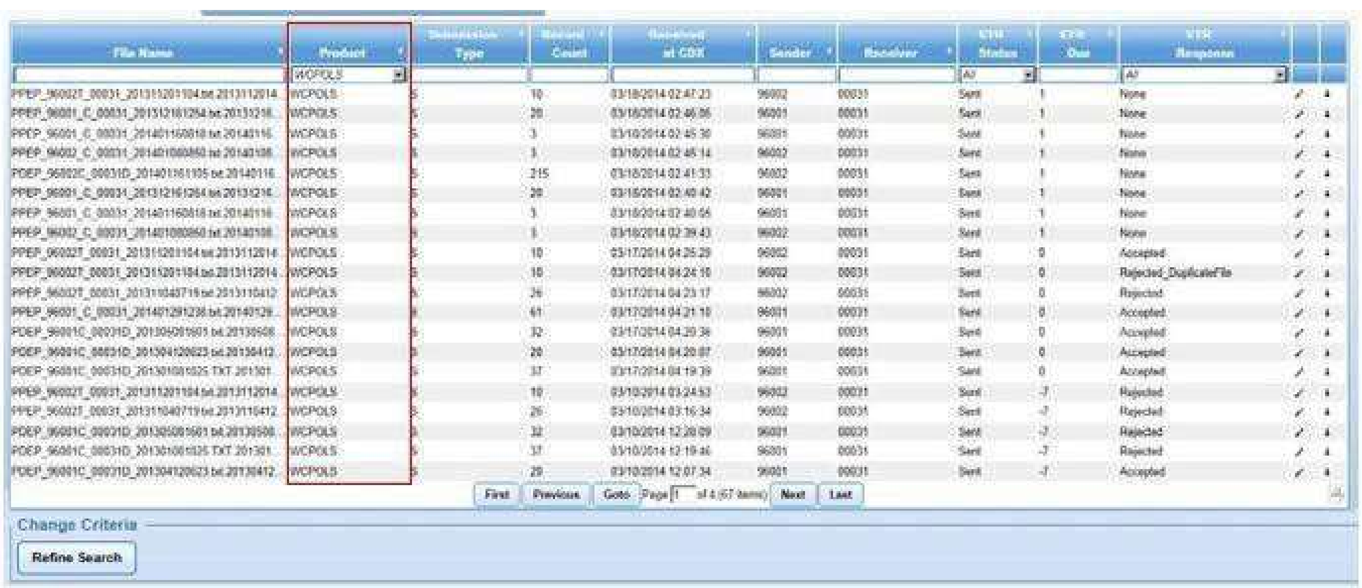
ETR Log

The ETR Log will display all files received within the last 90 days.

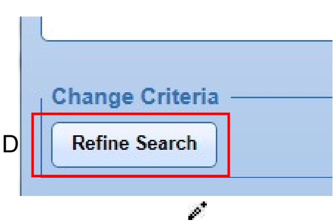
- Click the ETR menu.
- Choose ETR Log.
- The pencil icon located near the end of the row will take you to a screen which displays the details of the file. See below for further description of this screen.
- The down arrow icon at the end of the row allows you to download the file by opening or saving 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. 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.



- 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.

Back to ETR Log

Base | ETR Response | Errors

Download File

ETR Record Base

Sender:	33333
Receiver:	00032
Product:	WCSTAT
Original FileName:	UBEP_33333_C_00032_201308190931.TXT
New FileName:	52754b37-ae07-4fcc-a51e-c2e8f56b262c/UBEP_33333_C_00032_201308190931.TXT.20130819093124
Submission Type Code:	S
Record Count:	6
Date Received:	8/19/2013 9:31:24 AM

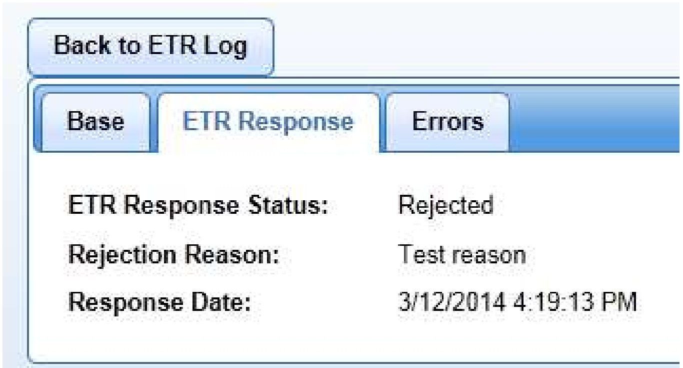
ETR Record Details

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

Contact Information

Data Provider Contact:	minnie mouse
Email:	jst@ncrb.org
Street:	2910 Sumner Blvd
City:	Raleigh
State:	NC
Zip:	27616
Phone:	9198108593
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.



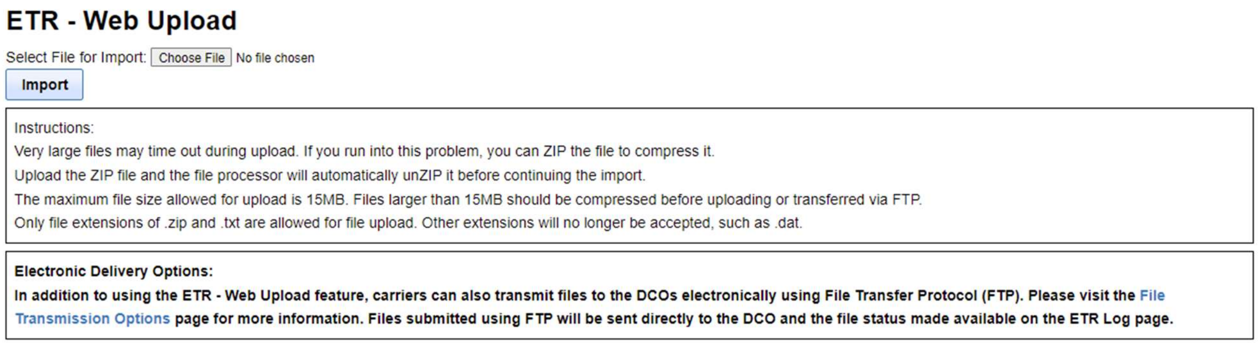
- The Errors tab displays the errors that were generated from the file if there were any. Files with an ETR Status of "Invalid" in the ETR Log or ETR Search will have an error displayed in this tab. See glossary for status explanations.
- The Back to ETR Log button will direct you back to the ETR List screen.

ETR Web Upload

If a carrier does not want to electronically submit files to the DCOs utilizing the SFTP process, the carrier can manually upload files directly to the CDX site and CDX will transfer the files to the DCO specified in the ETR record. To upload:

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

Users can either upload individual files with the .txt extension, or they can upload a compressed Zip file that contains multiple .txt files.

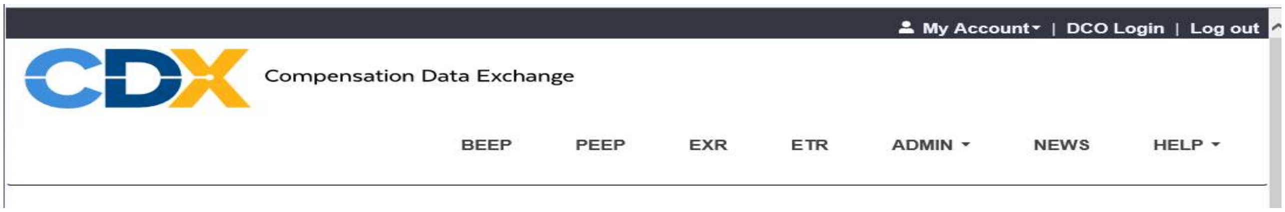


NOTE: There are two requirements to utilize the ETR Web Upload feature:

- The user must have Transfer Permissions for the file type (e.g. WCPOLS)
- The carrier must be approved by the DCO for data submissions (Admins can check this status by accessing the Admin, MyUMG, Carrier, Registrations tab)

BEEP
The BEEP application is used to enter or modify Unit Statistical Reports. Primary Administrators can grant access to this product by using the Admin | MyUMG | Application Access tab.

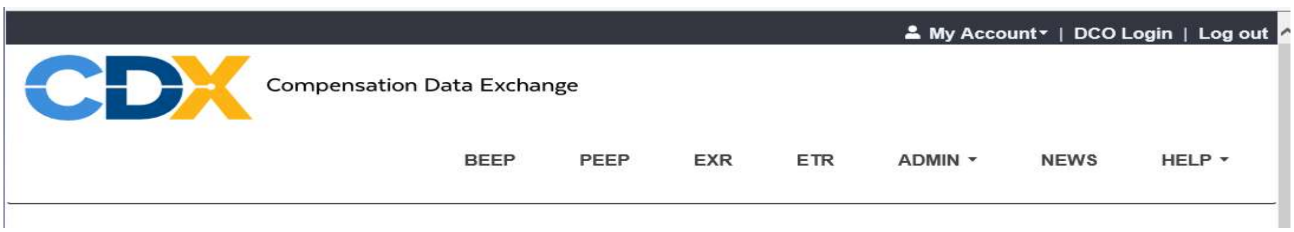
Please see the BEEP User Guide for more information.



PEEP

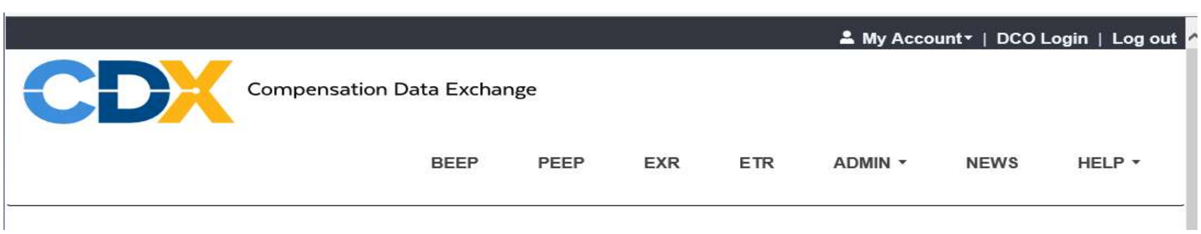
The PEEP application is used to enter or modify policy transactions. Administrators can grant access to this product by using the Admin | MyUMG | Application Access tab.

Please see the PEEP User Guide for more information.



EXR
The EXR application is used to retrieve rating worksheets from participating DCOs. Administrators can grant access to this product by using the Admin | MyUMG | Application Access tab.

Please see the EXR User Guide for more information.

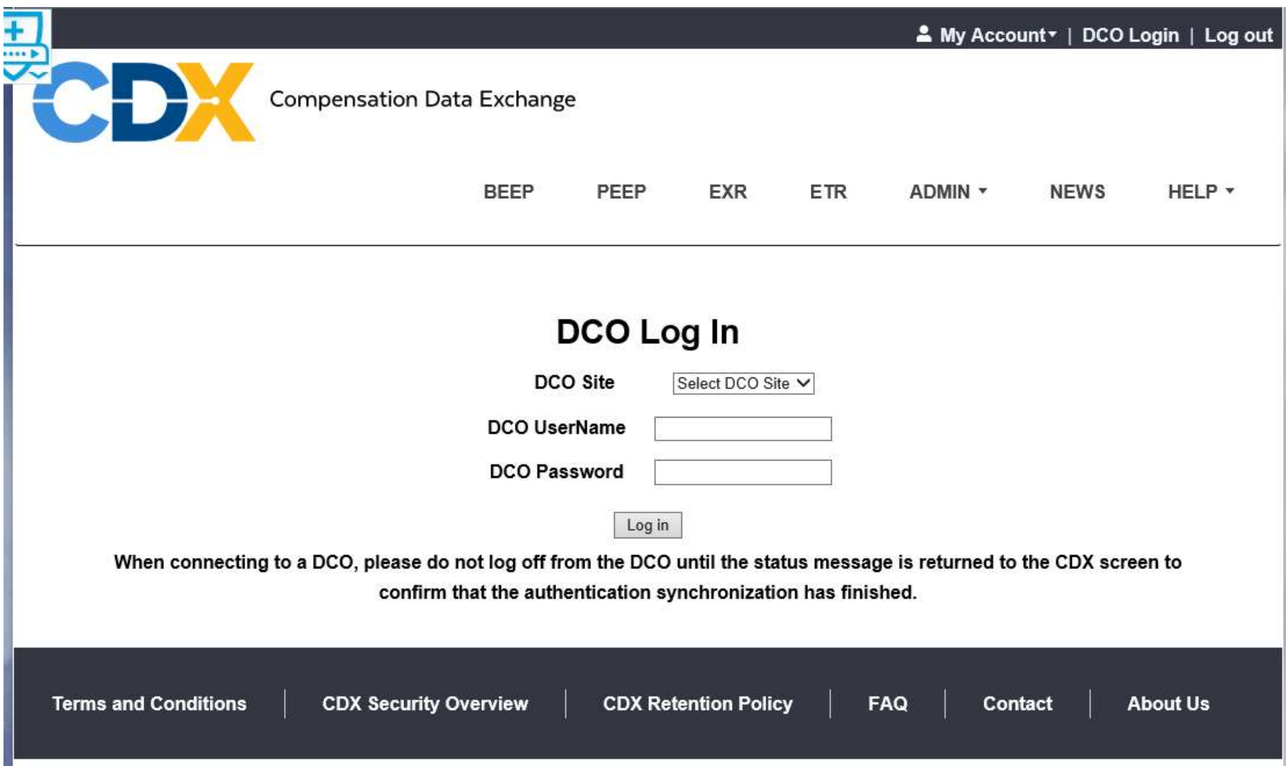


Single Sign On (SSO)

The Single Sign On (SSO) feature 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:

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



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:
- Select a DCO from the DCO Site dropdown menu.
- Type the DCO User Name and password.
- 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:

1. If the login is not successful because the DCO User Name and/or Password are invalid, the error message "Login to DCO site was unsuccessful. Please contact the DCO to resolve the issue" is displayed.

2. If the login is not successful because the DCO User Name 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 LogIn

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:
- Select a DCO from the DCO Site dropdown menu.
- 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 web services (Business to Business –B2B) provides immediate access to participating DCO data for experience modification factors, merit rating factors and related rating information. The user is able to retrieve data using Risk IDs or FEIN #s and may request a specific date range. Data returned adheres to the WCIO WCUnderwriting XML data specification file layout.

To utilize the WCUnderwriting web services, please contact your Primary Administrator to request approval by the participating DCO and to obtain a copy of the CDX WCUnderwriting Implementation Guide from CDX Central Support. The WCUnderwriting Implementation Guide provides additional details on the following:

- Requesting authorization keys for participating DCOs
- Technical details for integration with carrier systems
- XML Schemas
- Sample files

File Naming Convention for CDX

Example: AAEP_SSSSSC_RRRRR_CCYYMMDDHHMMSS.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 tapeformat*
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 = WCSTAT - ICR Data *
EC = WCCRIT - Workers Compensation Criticism Information
MC = WCMED - Medical Data Call
MK = WKMED – Medical Call Key Field Change Records
IC = WCIND - Indemnity Data Call **

Note: * WCIO tape format (EBCDIC)
** For NY, refer to the Indemnity Data Call Guide and Manual on NYCIRB’s website.
** For PA/DE, refer to the Indemnity Data Call Electric Submission Guidelines on PCRB’s website.
** For NJ, refer to the Indemnity Data Call Guide and Manual available on NJCRIB’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

Glossary of Terms

ASCII	American Standard Code for Information Interchange. A standard coding scheme for representing characters as data
ASWG	Advisory Statistical Working Group—A group within the WCIO that developed the revised USR data format, and by extension, the formats themselves.
Batch Number	Identifies groups of USRs as they are entered into BEEP® on a particular date
BEEP®	Bureau Entry & Edit Package—A web-based application designed to give Insurers the ability to enter, validate and submit Workers Compensation statistical information.
Breadcrumbs	A link to a prior screen
Bureau Version Identifier (Edition Number)	An identifier used to correspond to a specific endorsement number reported previously
Carrier Version Identifier	An identifier used to determine the version of the endorsement applied to a policy
CDX®	Compensation Data Exchange. CDX® is a secure Internet based service that facilitates the electronic transmission of Workers' Compensation data between member insurers and DCOs
Correction Report	A USR which revises previously reported data within a report level, correction reports are sequentially numbered (i.e., the first, second or third correction to a First Report)
DCO	Data Collection Organization – An organization that collects workers' compensation information. A DCO can be a bureau, jurisdiction or statistical agent
Date Entered	The date a USR was entered into BEEP® either by data entry or import
EBCDIC	Extended Binary Coded Decimal Interchange Code - A standard coding scheme for representing characters as data commonly used on mainframe computers (compare ASCII).
Edit Status	Defines the state of the transaction within PEEP® and BEEP®. Edit statuses are defined in the associated User Guide.
Employee Leasing Policy Type Code	A code used to identify the type of employee leasing policy.
Endorsement Number	An identifier used to report an endorsement number

Endorsements with Variable Data	These are the individual endorsements that are attached to a policy that contain information beyond the standard endorsement wording. Meaning the endorsement requires policy specific variable text
ETR	Electronic Transmittal Record – Is the first line of a submission file used to identify data within, and destination of a submission
Exposure Period Code	A code used to identify the period covered by the reported estimated exposure amount.
EXR	Product used to access rating data from participating DCOs
First Report	The initial USR for a policy, which reflects policy, exposure, premium, and loss information that is valued and submitted per the established USR valuation schedule
IAIABC	International Association of Industrial Accident Boards and Commissions - A non-profit trade association providing workers' compensation information and education
Import	To bring data into a computer system from an external source. PEEP® provides the facility to import policy transactions (WCPOLS) and BEEP® provides the facility to import USRs (WCSTAT).
Legal Nature of Entity Code	A code used to identify the type of entity(s) being insured. (Reported in the Name Record)
Legal Nature of Insured Code	A code used to identify the type of entity(s) being insured. (Reported in the Header Record)
Link Data	The data elements which are required to be reported consistently for all records within a transaction. Link data is used to keep these records connected for processing, storage and identifying duplicate data
Name Link Identifier	An identifier used to link names with their corresponding addresses and exposures.
PEEP	Policy Entry and Edit Package— A web-based application designed to give Insurers the ability to enter, validate, and submit Workers Compensation policy information
POC	Proof of Coverage – Data derived from a workers' compensation policy which is used by state accident boards and commission to verify workers' compensation coverage for the employers in their state.
Policy Change Effective Date	The date of change or addition reported on the record
Policy Change Expiration Date	The date of change or deletion reported on the record

Primary Administrator	The administrator responsible for a CDX User Management Group (UMG)
Replacement Report Code	A code used to report if the USR is replacing a previously submitted report
Retrospective Rating Code	A code used to report the type of retrospective rating plan applied
Secondary Administrator	A CDX User delegated some administrator privileges
SFTP	Secure File Transfer Protocol – Provides a secure method for sending or receiving files in CDX
SSL	Secure Sockets Layer – An interface between applications (such as browsers) and the Transmission Control Protocol/Internet Protocol (TCP/IP) protocols to provide server authentication, client authentication, and an encrypted communication channel between client and server.
State Unemployment Number	The unemployment number issued by a given state.
Submission File	An electronic file created to submit data.
Subsequent Report	A USR that is valued and submitted on a predetermined 12-month schedule after the First Report. Subsequent Reports provide updated information on losses from the Second Report through the Tenth Report.
TPA/TPE	Third Party Administrator/Third Party Entity – An organization that processes insurance transactions for a separate entity
Transaction Issue Date	The date of issuance of the transaction
Transaction Type Code	The code use to identify the type of transaction that is being submitted by the carrier. See the WCIO for the list of possible values.
UMG	User Management Group – Represents a group of users managed by a single Primary Administrator
Validate	The process of running edits

Summary of Changes

Page, Section, etc.	Date of Change	Change/Update
Pages 55-63	6/22/2026	Renamed FTP Credentials to SFTP Info, added instructions on new SFTP Whitelist screen
All	1/26/2026	Removed references to DCO Mod Lookup
Page 10	11/2/2022	CDX Support email address changed to support@cdxworkcomp.org
All	5/27/2022	Guide reviewed for accuracy and additional content
Page 45-46	10/13/21	Removed FTP with SSL option from Location Setup
Page 70	8/27/21	Added WCUnderwriting Product
Pages 45 to 47	4/1/21	Remove email delivery. FTP delivery now requires SSL.
Page 71	3/2/21	Change CDX File Naming Convention-WKMED
Pages 67 to 70	8/25/20	Renaming WCUnderwriting to DCO Mod Lookup
Pages 57 and 58	6/1/20	ETR Log updated to display submissions received within 90 days.
Pages 8 and 71	3/10/20	Update to Replacing an Existing Administrator, and addition to PA/DE Indemnity Data Call Information Note
Entire User Guide	10/10/19	Updates to new CDX website design.
Pages 8-13, 74-77	9/17/18	IPA Request New UMG Primary Admin User for Existing UMG, Update Contact Info for Existing UMG Primary Admin User, & WCUNDERWRITING Search User Guide Information
Pages 54-55	3/19/18	Update for Member Verification Technical Contact Information