CO Environmental Web Application Administrator Help

March 2012
Updated June 2012
Updated March 2014

Contents

GETTING STARTED

Welcome to CO Environmental

Welcome to Colorado Environmental (CO Env), a Web application developed to manage environmental sampling data collected from oil and gas project locations and associated laboratory analytical results data. Oil and gas operators, their third-party laboratories, agency environmental scientists and field inspectors can use the application to upload data in Excel or EPA WQX-derived XML or via secure data entry pages.

The CO Env application is a part of the Ground Water Protection Council's (GWPC's) national RBDMS Environmental program, which was developed through a grant from the U.S. Department of Energy, Office of Fossil Energy. RBDMS Environmental software is used to manage environmental and laboratory information associated with source water quality protection programs and regulatory oversight of fossil-fuel extraction and various types of mining operations.

This administrator's manual for the CO Env Web application is meant to supplement, but not duplicate, the user's manual. Therefore, the developers recommend that administrators be familiar with the content of both manuals. Programming for the RBDMS CO Env application was provided by Virtual Engineering Solutions, Inc., with GIS programming by Coordinate Solutions, Inc.

Note: For the March 2014 update, the CO Env application has been re-skinned. This change eliminated the use of a third-party control and enabled hiding the menu and tool bars on the Facility and Sample Data Upload wizard, essentially making wizard access in CO Env a seamless transition from the CO eForm dashboard. This change also updated the placement of tool bars and layout of some pages in the CO Env Silverlight application.

Installing CO Environmental on a Web Server

An installer package named **RBDMSEnv.zip** was provided to the COGCC, along with an installer for the RBDMSWindowsService called **RbdmsEnvWindowsServiceSetup.zip** . To install the CO Environmental application on a Web server, follow these steps:

1. Open IIS Manager on the server.
2. In the left panel, select the **Default Website**.
3. Click the **Import Application…** link in the bottom right panel.
4. Click the **Browse** button and select the **RbdmsEnv.zip** file.
5. Click **<Next>**.
6. Uncheck the **Deploy SQL database** option since it is already there.
7. Click **<Next>** and then **<Next>** again to accept the default *Application Path*.
8. Choose *No, just append the files in the application* and click **<Next>**.
9. The application will install.
10. Open Windows Explorer to the **E:\Inetpub\COGIS\RbdmsEnv** folder.
11. Delete the just-installed **web.config** file.
12. Make a copy of the **web_<servername>.config** file and rename it **web.config**.

The **RbdmsEnvWindowsService** manages data validations for facility IDs, locations, EDD parsing, laboratory result quality control. The Windows service was developed to use SMTP protocol for the Alert module. The COGCC staff have modified it to conform to the requirements of the DNR mail application. The Visual Studio 2010 solution for the service was provided to the COGCC in a file named **RbdmsEnvWindowsService20130903.zip**. The solution includes the following projects:

- **AlertBLL**: Business logic project. This includes the AlertJob class which includes functions for the checking the alerts. The code that sends the emails via SMTP is in the **AlertBLL** project **Notify.SendMail f**unction.
- **AlertDAL:** Data access layer. This includes the Entity Framework models.
- **RbdmsConfig**: Low-level project to expose RbdmsEnvWindowsService connection strings for all projects.
- **RbdmsEnvwindowsService:** Top-level Windows Service with method to create and StartTimer on the Notify class.
- **ztRbdmsEnvWindowsServiceTest**: Used for testing/debugging methods in the development environment.
- **RbdmsEnvWindowsServiceSetup**: Installation program for service. ***Note:*** Once this service is installed on the server, updates can be made by copying any updated .dlls and then restarting the service.

Stepping Through the Final EDD Review Process

A manual step in the process will allow a user in the *Agency* role to **Open** each data set in the user interface to review it. Each submission can then be **Verified**, which accepts the data into the primary database or **Rejected**.

The **Verify** and **Reject** buttons call the **RBDMSEnvWindows** service, which powers the Notification module, to complete the requested action. (***Note***: These calls could be automated now or in the future, if desired.) The CO Env application stores the email address of the person who uploaded the file so that the Notification module can access it for automated status alerts. This will be important in the case of EDDs that are rejected during this last-step manual review. The Notifications module will build a list of rejected EDDs for e-mail notifications to the operators who originated the submissions.

To verify an EDD submission, follow these steps:

1. On the **Data Uploads** page, set the **EDD Status** filter to *Accepted* to view the submissions that have been successfully passed the data validation checks.
2. Select a record to review by clicking in the row header on the *Uploaded Files by Status* grid.
3. Click the **Open and Review an EDD** button. The **EDD Review** page will open.
4. Review the data for the submission. If the information is not acceptable, it can be **Rejected** from the **EDD Review** page. If the information is acceptable, return to the **Data Uploads** page and, with the reviewed record selected on the grid, click the **Verify and Import** button.

Note: The option to **Reject Batch** is made available in two places: on the **Data Uploads** page and on the **EDD Review** page. The **Verify and Import** button is made available only on the **Data Uploads** page where messages from the parser are displayed**.**

Working with Quality Control Data

A **Lab Batches** page has been made available on the **Edit** menu of the CO Env application. Only *Administrative* users and power users in the *Agency* role should have *Read* and *Write* access to this page.

The hierarchy of the data grids on the **Lab Batches** page tracks that of the spreadsheet electronic data deliverable beginning at the *Batch* level. The page is most useful as a lens for data that has already been input to the CO Env application, either through the electronic data deliverables or through the facility-sample-result hierarchy of the Web application.

Using the **Lab Batches** page as a data input form in not recommended because it requires that associations of samples to facilities be forged in a direction that is counter to the usual application flow. The page is properly used to view linked quality control batch information only.

Be sure to set an active project before using the **Lab Batches** page. The **Sample** combo box on the **Result Batch** tab shows only those samples that are available in the active project. Be sure to **Refresh** the **Sample** combo box when you change the active project.

To create a new record in the grids on the **Lab Batches** page for data entry, you can either click **Add**  or double-click in the **New Record**  row.

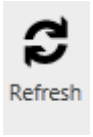
Creating Parameter Definitions

The **Parameter Definitions** page should be restricted to one or two power users in the *Agency* role (*Data Administrators*) and to users in the *Administrative* role.

The CO Env application uses the **Parameter** table to store analysis codes. The form for maintaining this information is available from the **References | Parameter Definitions** menu selection. Establishing this list is typically a one-time requirement for readying the CO Env application for use, although updates may be needed on occasion. The **Parameters** page tracks the parameter name, description aliases, allowable decimal places, significant figures, holding times, milliequivalent factors, and other calculations.

The **Parameter Definitions** page includes a grid list of the **Parameters** being tracked in the database in the left pane. The main window fills dynamically with each selection in the left pane to show the specification for each parameter. To add a new parameter to the parameter definitions included in the CO Env Web application, follow these steps:

1. In the *Parameters* grid on the left, click **Add** + to create a new parameter record in the right pane.
2. Complete the form and click **Save** 

.
3. Check to see if the parameter you added is now available to you on the Analysis Lists page. You will need to **Refresh** 

the combo box for **Analysis** in the *CollParameters* grid.

To delete a parameter from the CO Env application, follow these steps:

1. ***Warning:*** *Consider carefully whether the deletion is needed. This action will cascade through the analysis lists and the results that include this parameter, with a data-destroying outcome*.
2. Locate the record on the **Parameters** page you wish to delete. One way to do this is to enter the name of the parameter in the **Search** pane and click **Search** . The list will filter to show your entry.
3. Mark the entry you created for deletion by clicking to select the row and then clicking the **Delete** − button.
4. **Save** 

your changes.

Note: **The cascading effects of this action cannot be undone.**

Creating Analysis Lists

Creating and Using Analysis Lists

Analysis lists are user-defined sets of parameters that can be applied to sample records in the CO Env application. These lists are built from selected items defined in the **Parameter** table in the database. So, for example, to prepare a list of metals analyses that will be used either for a specific project or as a department-wide standard reference list, you would use the **Analysis Lists** builder page of the CO Env application to assign a meaningful name to that collection (e.g., "MetalsClientID175," or if it is a generic collection that you intend to use routinely, "Standard Metals"). You would then select the specific parameter and test IDs of interest to you for that purpose, e.g., calcium, potassium, chromium, lead, arsenic, etc., and then save the list for future use.

For data entry purposes, the CO Env application includes a shortcut on the **Analysis** tab of the **Sample Editor** for users to assign this list of metals analyses or another pre-defined list to any given sample with just one mouse click rather than many.

The **Analysis Lists** page, available from the **References** menu, includes a *Lists* grid in the left pane that displays the analysis sets that are already available to the application. As you select list names in the left-pane grid, the right pane dynamically displays the members of the lists.

Note: Deleting an analysis set from the **Analysis List** builder page will not delete the component list items from the database. Likewise, deleting a list member from the *Coll Parameters* grid will remove that item from the list it was in, but this action will not delete the underlying **Parameter** table record.

To create a new analysis list, follow these steps:

1. From the **References** menu, open the **Analysis Lists** page
2. In the *Lists* grid in the left pane, click **Add** +. A new record will be created and the right pane will clear so that you can enter data associated with your new analysis list.
3. Enter the **List Name** at the top of the main page**.** This will be the name that will be displayed for the list that you will create throughout the application.
4. Add a short **Description** of what the list is and how it should be used.
5. In the *Coll Parameters* grid, begin building your list by clicking in the first row and selecting an **Analysis** from the combo box (***Hint:*** You can "type ahead" in the combo box to filter to relevant selections). Tab to the **Result Method** and select an entry from the combo box. Continue to complete the relevant information across the row.
6. Repeat by clicking in the next row and continuing until your list is complete.
7. If you create a row in error or wish to delete a row, click in the row header to select the line and click **Delete** −. The deletion will be committed when you save the page.

8. Click to **Save** 

your changes. Your list is now ready to be used throughout the application.

About Working on the Analysis Lists Page

1. You cannot change the **Result Method** for a specific *CollParameters* member after the list is saved because the **Result Method** is part of the primary key and cannot be updated. You must add a new record with the new method.
2. Saving the page as each new list is added will avoid confusion if an error occurs on a list that is not current.
3. Agency power users or other individuals who are tasked with creating project-specific lists of analyses should have access to the **Analysis Lists** page.

The **Analysis Lists** page is read-only for *Agency* users unless the user has *DataAdministration* permission.

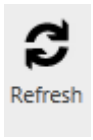
For the Database Administrator: The Hidden Use of Analysis Lists

On the **Reports** page, when a user opts to run a report with the auto select option for the analysis list, the application creates a temporary analysis list named <*zt* + a guid>. So that these temporary lists do not cause a visual clutter on the **Analysis Lists** page, a bit column named *Temporary* was added to the **Coll** table. The *CollsForParameter* query filters out of visibility any set in the **Analysis Lists** page if *Temporary* = "True."

Specifying Analytical Methods

Analytical test, preparation, and other types of methods are tracked in the CO Env application as lookups on a page that surfaces the fields in the **ResultMethod** table in the database. This **Methods** page is available from the **References** menu. Access should be restricted to *Agency* power users (*Data Administrators*) and *Administrative* users. To add a new method to the CO Env application follow these steps:

1. From the **References** menu, open the **Methods** page.
2. Click **Add**  to create a new result method record.
3. Complete the form fields in the right pane for the new record and click **OK**.
4. **Save** 

your changes.
5. Check the addition to the lookup by returning to the **Analysis Lists** page and adding a new parameter to an existing list. The new result method will show up in the **Result Method** combo box in the *Coll Parameters* grid. You may need to **Refresh** 

the **Result Method** combo box first.

Working with Codes

Warning: *The ability to change codes should be reserved for the system administrator. Adding, updating, or deleting codes should be done with great care. Improper adjustments to the codes can make the output of some reports invalid*.

The CO Env application makes extensive use of codes to specify types of actions, results of actions, and types of equipment. A master codes table is used for storing all code types and a description of each. You can access the administrative codes in CO Env with the **References | Codes** menu selection.

Use of a master codes table ("code groups") increases the flexibility of the CO Env application. Administrators can easily add new types of equipment or testing methods through the Codes page.

For code group members, be sure that the code is the appropriate data type for the associated field. If it is a text field, make sure that it does not exceed the maximum field length. The *Tag* and *Value* fields are optional fields used to store text and/or numeric information when needed for special codes.

If a code will not be used anymore, turn its *Active* status off. When a code's **Active** flag is off, it will not be available in combo boxes on data entry forms, but it will still appear on reports.

The following steps describe the process of creating a new code group and adding code members:

1. From the **References** menu, select **Codes**.
2. In the **Code Groups** pane, click **Add**  . The page will display blank fields to accept your new record. Enter a new code **Group** name. For example, create a code group called "OdorLevels." You can add a **Source**, **Comment**, **Max Length**, and **Code Type**, if desired.
3. If you need to specify the **Tables** to which the codes apply, enter the table names. For multiple entries, separate the names with commas.
4. With the *OdorLevels* record in the *Code Groups* grid selected, add code group members in the *RefCodes* grid. Exercise both the **Add**  button and **New Record**  row functionality to add new refCodes.
5. **Save**  your changes.

To delete code groups or code members,

1. Select the record by clicking in the row header. Then click **Delete** ..
2. **Save**  your changes.

Warning: *The ability to change codes should be reserved for the system administrator. Adding, updating, or deleting codes should be done with great care. Improper adjustments to the codes can make the output of some reports invalid*.

Customizable Views

A variety of views have been added to the CO Env database to serve as data sources for the varchar codes used in the application. These views are currently drawing from the **RefCodes** table, but COGCC can modify these views to get data from other databases.

Note: Changing the queries underlying these views is allowable, but deleting columns from these views has the potential to cause dependent objects to fail. Therefore, when you edit the data source, leave the existing column names and data types intact.

The following views have been added:

- viewActive
- viewAnalysis
- viewAnalysisMethod
- viewAquifer
- viewCodeSubReason
- viewCodeType
- viewCollectionPoint
- viewCollFilter
- viewCollParameter
- viewCollSample
- viewEDDStatus
- viewEWDir
- viewFacilityStatus
- viewFacType
- viewFormation (mrdb.dbo.formation_code)
- viewFractiontype
- viewFrequency
- viewImages
- viewInventoryType
- viewLab
- viewMatrix
- viewMediaType
- viewMeridian
- viewNSDir
- viewParameter

- viewPermissionID
- viewPrepMethod
- viewPrePost
- viewProjectType
- viewQCType
- viewQualifier
- viewSampleType
- viewSubMethod
- viewSubReason
- viewUnits
- viewVerified
- viewVolUnits
- viewWaterSource
- viewZoneID

Configuring CO Env to Connect to Other Databases

The connection strings to link the CO Env Silverlight Web client are found in the **web.config** file in the installation folder. A connection string must be set for each data source used in the CO Env application. You may add as many custom connection strings as needed to establish links with other ADO databases.

Warning: *Errors introduced during application configuration file editing will cause the CO Env application to malfunction. Therefore, if you edit the application configuration file, the developers recommend that you make a backup of the last good version before you start making changes.*

`<connectionStrings>` used by the CO Env application include the following:

The Security Database

```
<add name="_IntrinsicData" connectionString="Data
Source=RbdmsOnline.org;Database=COEnvLS;uid=RbdmsUser;Pwd=*********;" />

<!-- Security Database -->

<add name="RbdmsSecurityConnectionString" connectionString="Password=*********;Per
sist Security Info=True;User ID=RbdmsUser;Initial Catalog=COEnvLS;Data
Source=RbdmsOnline.org" providerName="System.Data.SqlClient" />

<add name="EnvLSData" connectionString="Data Source=RbdmsOnline.org;Initial
Catalog=CoEnvLS;Persist Security Info=True;User ID=RbdmsUser;Password=*********" />

<add name="0ca2b826-28f4-4c1a-aa30-c9e583668aa6" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=CoEnvLS;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" />
```

The CO Env Production SQL Server Database (Internal Agency Users)

```
<!-- COEnv Database -->

<add name="EnvEntities" connectionString="metadata=res://RbdmsEnv.Data/EnvModel.cs
dl|res://RbdmsEnv.Data/EnvModel.ssdl|res://RbdmsEnv.Data/EnvModel.msl;provider=Sys
tem.Data.SqlClient;provider connection string=&amp;quot;data
source=RbdmsOnline.org;initial catalog=CoEnv_A;persist security info=True;user
id=RbdmsUser;password=*********;multipleactiveresultsets=True;Enlist=false;App=Ent
ityFramework&amp;quot;" providerName="System.Data.EntityClient" />

<add name="RbdmsEnvConnectionString" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=CoEnv_A;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" providerName="System.Data.SqlClient" />

<add name="EnvData" connectionString="Data Source=RbdmsOnline.org;Initial
Catalog=CoEnv_A;Persist Security Info=True;User ID=RbdmsUser;Password=*********" />

<add name="RefData" connectionString="Data Source=RbdmsOnline.org;Initial
Catalog=CoEnv_A;Persist Security Info=True;User ID=RbdmsUser;Password=*********" />

<add name="be3ec3a4-3ae8-42bc-82f8-6e78ea6b68cb" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=CoEnv_A;Persist Security Info=True;User
```

```
ID=RbdmsUser;Password=*********" />

<add name="c06f96db-88f7-4ad3-85de-1a9154fd9f98" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=CoEnv_A;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" />

<add name="7fb8c376-1781-4503-b7f4-e3ab79c11a87" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=CoEnv_A;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" />
```

The CO Env DMZ Database

```
<!-- COEnvDMZ Database -->

<add name="EnvDmzEntities" connectionString="metadata=res://RbdmsEnv.Data/DmzModel
.csdl|res://RbdmsEnv.Data/DmzModel.ssdl|res://RbdmsEnv.Data/DmzModel.msl;provider=
System.Data.SqlClient;provider connection string=&quot;data
source=RbdmsOnline.org;initial catalog=CoEnvDmz;persist security info=True;user
id=RbdmsUser;password=*********;multipleactiveresultsets=True;Enlist=false;App=Ent
ityFramework&quot;" providerName=" System.Data.EntityClient" />

<add name="EnvDmzData" connectionString="Data Source=RbdmsOnline.org;Initial
Catalog=CoEnvDmz;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" />

<add name="RbdmsEnv.Data.EnvDomainService" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=CoEnvDmz;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" />

<add name="CoEnvDmzConnectionString" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=CoEnvDmz;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" providerName="System.Data.SqlClient" />

<add name="98512d17-01a9-4475-a70b-2981976a9bf6" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=CoEnvDmz;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" />

<add name="01fa9569-0871-4336-8007-813b30505724" connectionString="RbdmsEnv.Data.E
nvDomainService" />
 ..........................................................................................
 ..........................................................................................
```

The mrdb Database

```
<!-- mrdb Database -->

<add name="mrdbData" connectionString="Data Source=RbdmsOnline.org;Initial
Catalog=mrdb;Persist Security Info=True;User ID=RbdmsUser;Password=*********" />

<add name="e1c24928-5017-40e9-b197-a3a4c850807c" connectionString="Data
Source=RbdmsOnline.org;Initial Catalog=mrdb;Persist Security Info=True;User
ID=RbdmsUser;Password=*********" />
 ..........................................................................................


 ..........................................................................................
```

Configuring the EnvWindowsService

The CO Env application includes a Notification (also referred to as an "alert") module. Alerts are automated messages that can be customized to respond to quality control data flags, program- or date-specific requirements or actions, or workflow process step notifications. Alerts are generated through .NET procedures that are stored in a business layer (AlertBll) separate from the user interface, and alert sets can be shared or customized to specific users. Users can define the notification frequency of their subscribed alerts.

The Notification module is powered by the **RbdmsEnvWindowsService**, a Windows Service application that creates eNotify records and sends out e-mail notifications. The default location for the installation of the **RbdmsEnvWindowsService** on the development server in the C:\Program Files\GWPC\EnvWindowsService directory. Before starting the service, agency staff will need to edit the **EnvWindowsService.exe.config** file to update the following:

- ConnectionStrings
- ApplicationSettings:
    - SmtpHost
    - MailFromAddress
    - MailFromDisplayName
    - SmtpUserName
    - SmtpPassword

When the service is started, it writes an entry into the computer event log to indicate that it started. The service then creates an instance of the **envBLL.Notify** class.

When the Notify *StartTimer* function is called, the *NotifyFrequency* setting is read from the .config file. The *NotifyFrequency* includes multiple date intervals (in decimal day units). The initial setting is for 0.0034722,0.041667,1 which represents 5 minutes, 1 hour, and 1 day, respectively. A list of *NotifyInterval* objects is created for each value.

The application .config file also includes a *NotifyInterval* setting. The *NotifyInterval* specifies the interval in minutes for triggering the timer elapsed event. Each time the timer elapsed event occurs, a query is performed to select alerts (**CollAlerts** table) that are due to be performed. These alerts are performed, eNotify records created and the **LastRunDate** of the alert is updated to the current date.

The **eNotify** table is also queried for notification records that are due to be sent to subscribers. For example, if a subscriber has specified a notification interval of one day, the program will wait until one day since the last notifications email and then construct a new email with a table of all the notifications that have accumulated since the last email. The 1-day interval starts at 12:00AM, the 1-hour intervals start on the hour, and 5-minute intervals start at the 5-minute interval immediately less than the current time (i.e., if the current time is 1:37 a.m., then the interval will begin at 1:35 a.m.).

The query will order the results by *UserID, DueDate* and *FormKey*, if appropriate. The program loops through the query results and creates a single email for each user with a table containing the eNotify records for the user ordered by *DueDate* and *FormKey*. Each

loop is wrapped in a transaction, and once the transaction is complete, the *NotifyComplete* value for the records in each email is set to "True." System administrators may choose to delete eNotify records with *NotifyComplete* = "True" after a month or so.

Validating Incoming Data

Alerts are programmed warnings of incoming data that violate data integrity requirements. For example, at release, the following data validation checks for *Facility* exist in the CO installation of RBDMS Env:

- The facility name is required and cannot be empty.
- The UTM x, y (or latitude and longitude) must be within specified range. For example, an alert is needed to determine if a reported facility is less than 100 feet from an existing facility, since this could indicate a problem with the Facility ID assignment.
- The prime meridian must be reported.
- QtrQtr-S-T-R are present and within appropriate ranges.

Data validation checks for *Sample* in the CO installation of RBDMS Env include the following:

- The sample date is required and must be less than or equal than today's date.
- The location of the sample must be within a specified tolerance of the known facility location.
- Alerts for data warnings and errors will include the Sampler field to facilitate review.
- Sample data orphaned in the DMZ beyond an allowable time period must be reviewed.

Analytical results in the CO Env application are checked for the following data validations:

- **Cation-Anion Ratio:** Generates alerts where the cation/anion ratio is not within limits. The milliequivalents are calculated by dividing the Result.ResultValue by the Parameter.MEQFactor column.
- **Exceedance:** For a given analysis, an acceptable range of Upper and Lower Criteria is specified (e.g., the pH must be 4-10), and this range is applied to all facility locations. This alert requires the specification of an analysis list.
- **Holding Time:** Generates alerts for analyses that have not been reported and with the current date greater than the sample date + holding time or with the analysis date > sample date + holding time.
- **Missing Analysis:** Samples are compared to the earliest sample collected for the location (Loc). If the earliest sample has ParameterIDs that are not in the current sample, then an eNotify record is added.
- **Dissolved vs. Total:** Creates an alert record if a dissolved analysis is greater than a total analysis.
- **% Difference from Baseline:** Compares current results to previous results against a specified deviation allowed for a confidence interval (if adequate data present). Location-specific warnings are then generated. This alert requires the specification of an analysis list.

- **Sodium Absorption Ratio:** The ratio of sodium milliequivalents to calcium plus magnesium milliequivalents is calculated, and the result is compared to an upper and lower limit.

The **RbdmsEnvWindowsService** generates records in the **eNotify** table for use in e-mailed alerts to subscribed users. The following list details the way in which those alerts that the COGCC Environmental Scientists specifically requested are handled at initial rollout:

Requested Alert	Type	Details
Any submitted value exceeds Table 910-1 standards	Exceedance	Create analysis list for 910-1 and set criteria
Cation anion balance is not within 20%	Cation/Anion	Sample must include analysis for major cations/anions.
pH not between 4-10	Exceedance	Add pH to analysis list for exceedance and set upper and lower limits.
Any detect on 8260 and 8270 list of compounds above detection limit	Exceedance	Create analysis list for 826 and 8270 compounds. Add true/false field for exceedance if detected.
Sodium, potassium, chloride, alkalinity, TDS, calcium, sulfate, magnesium change by 50% over previous sample data	Trend	Modify trend alert to use a specified percent change (new field called PercentChange) if the new field is set.
Methane > 1.0 mg/L	Exceedance	Add methane to analysis list for exceedance and set upper limit to 1.0
Methane increase by 5 mg/L over previous sampling data	Trend	Modify trend alert to look for an absolute specified difference for analysis in a list.
C2-C6 > 0.5 mg/L	Exceedance	Add to exceedance list.
Isotopic analytical data in EDD	Exceedance	Create isotopic analysis list, set new detected field to true and run exceedance alert.
New unique ID of sample location lies within ¼ mile of previously established location	New	Existing COGCC algorithms that are dependent on the lat/long values reported for a new *FacilityID* will be used to assign these alerts to the Area Environmental Protection Specialist (EPS).

Creating Alerts

Alerts are managed from the **References | Alerts** menu. Users can create multiple Alert Lists, and each Alert List can contain multiple alerts. Multiple users can subscribe to each Alert List, and this is managed via the **Subscribers** tab. Each alert in the list specifies the following:

1. An **Alert Method** (e.g., *Exceedance*) from a drop down list.
2. A **Project** to specify the *Facilities* to be used.
3. An **Analysis List** to specify the analysis to be checked and the criteria limits (e.g., *Upper Criteria*).
4. The **Frequency** that the alert should be performed. ***Note:*** If the data does not change, the alert will not be rerun for a specific record. This is the frequency with which the alert will search for new or updated records.
5. The **Last Run** read-only field displaysthe last run date for this alert.

Before setting up an Alert, the appropriate Project and Analysis List must exist or be created. To set up an alert, perform the following steps:

1. Create or reuse a project and assign facilities to the project (**Edit | Projects** menu).
2. Create or reuse an analysis list and set criteria appropriately (**References | Analysis Lists** menu).
3. Open the **Alerts** page (**References | Alerts** menu).
4. Create a new Alert List by clicking the **Add** + button on the top left section of the page. A new record will be added to the Alert Lists and the properties (*List Name, Description,* etc.) displayed on the top right.
5. Enter an appropriate *List Name* and *Description* in the top right section of the page.
6. On the **Alerts** tab on the bottom half of the screen, click the **Add** + button or click in the **New Record** row to add a new Alert to the list.
7. Select an Alert from the drop down list (e.g., *Exceedance*).
8. Select a *Project* by clicking the **Expand** ... button to open a dialog box used to select the project.
9. Select an *Analysis List* from the drop down list.
10. Specify a *Frequency* to run the alert check.
11. Repeat the previous 5 steps to add as many Alert records as needed for this project.
12. Click the **Subscribers** tab and add as many subscribers as needed from the lookup list of ASPNET users. You can type ahead in this combo-box to filter the results or scroll through the list to make a selection.

13. **Save** 

your changes.

If the **RbdmsEnvWindowsService** is running on your network, then subscribers to the alerts will receive an email with any alerts generated from their subscriptions since the previous email interval.

You can edit your alert set to add, to delete, or to modify any of the notifications you have specified at any time. You can navigate to a specific alert set to edit it by filtering and sorting the *Alert Lists* grid.

Tracking Alerts

The **Search Notifications** page is available on the **Edit** menu to agency users with data administrator privileges. The page allows users to filter, sort, and track the status of alerts generated by the CO Env application. Where the **References | Alerts** page allows the creation and subscription to the automated alerts, the **Search Notifications** page presents a view of the actual performance of the notification module. Creation dates, the status of the notification, the recipients' email addresses, and the frequency with which the alerts are being run on the server can be tracked on this page. A filter control at the top of the page allows you to evaluate specific alert operations.

Managing Passwords

The CO Env Web application enforces password strength. Passwords are case-sensitive and must include a mix of special characters, numbers, and letters, e.g., “Password!123.”

Potentially all users could be allowed to manage their own passwords after initial registration, subject to roles-based rules. Non-administrative users can change their passwords by clicking the **Change Password** link on the top corner of the dashboard. This link pops up a short form for completion.

This security feature can be used to impose self-management of passwords at designated intervals that are specified in the configuration file of the CO Env Web application. The relevant portion of the **web.config** file is reproduced below.

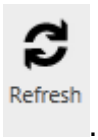
```
 <membership defaultProvider="AspNetMembershipProvider">
      <providers>
        <clear />
        <add name="AspNetMembershipProvider" type="System.Web.Security.SqlMembersh
ipProvider" connectionStringName="RbdmsSecurityConnectionString" applicationName="
RbdmsEnv" requiresUniqueEmail="false" requiresQuestionAndAnswer="false" />
        <!--<add name="AspNetMembershipProvider"
type="RbdmsWcfBase.RbdmsMembershipProvider, RbdmsWcfBase, Version=1.0.0.0,
Culture=neutral" connectionStringName="RbdmsSecurityConnectionString"
enablePasswordRetrieval="false" enablePasswordReset="true"
requiresQuestionAndAnswer="false" applicationName="RbdmsEnv"
requiresUniqueEmail="false" minRequiredPasswordLength="5"
minRequiredNonalphanumericCharacters="0" passwordFormat="Hashed"
maxInvalidPasswordAttempts="5" passwordAttemptWindow="10"
passwordStrengthRegularExpression="" />-->
      </providers>
 </membership>
```

Users in the *Administrator* and *Operator Administrator* roles can re-set passwords on the **Users** page.

Defining Roles

Application users are generally grouped into roles depending on their required usage of the application. For example, general users may have limited rights to do more than read certain data views or access various reports or editors, whereas power users might be granted the ability to perform advanced searches or to create objects such as report filters. Creating specialized user profile groups that define a set of common functions, such as *Inspectors*, also might be useful. Access to the Roles page should be restricted to the system administrator.

1. From the **Administration** menu, select **Roles** to open the **Roles** page. The page will open to display three grids: ***Roles, Permissions,*** and ***Users in this Role***.
2. **Add** + a new role in the *Roles* grid.
3. With the new role selected, **Add** + the level of access that will be allowed for that role in the *Permissions* grid.
4. **Save** 

your changes.
5. The *Users in this Role* grid is a read-only pane. To add users to the role you just created, open the **Users** page from the **Administration** menu and add a user in the role. Then return to the **Roles** page, and click **Refresh** 

. Your addition will display in the *Users in this Role* grid.

Note: An existing role cannot be updated. Allowable actions are restricted to *Add* and *Delete*.

Adding Users to Roles

Each person who will be working with the application will have to establish a user account. The following procedure steps through the process of creating a user account and assigning a role:

1. From the **Administration** menu, select **Users** to open the **Users** page.
2. **Add** + a new user in the *asp Users for Operator* grid in the left pane. The associated form fields on the right side of the page will clear.
3. Complete the **User Name, Initials, Password, Confirm Password,** and **Email** fields.
4. Make sure that the **Is Approved** check box is set to "True," and the **Is Locked Out** check box is set to "False." The **Last Password Changed Date** will default to <*Today*>, but can be overwritten.
5. Enter an optional **Comment** for the user login.
6. In the *Roles for User* grid, click **Add** + and select a role from the **Role** combo box. If the user will have operator administrator privileges, you will need to put the user in the Public role and then add the COGCC operator number as the **Option Value** in the *Profile Options* grid.
7. **Save** 

your changes.
8. Test the login by beginning a new session and logging in with the user credentials you just created. Check whether (a) the login works and (b) whether the permissions are appropriately applied. For example, logging into the application with user credentials in the *Public* role should mean that the **Administration** menu is not visible to that user.

Note: Rights are now handled as permissions, which are created at design time.

Testing Operator Administrator Accounts

Note: Although the COGCC has opted to restrict *Operator* and *OperatorAdministrator* use of the CO Env application to the **Facility and Sample Data Upload** wizard through the single sign-on of the CO eForm portal, the following discussion remains germane to the capabilities of the CO Env application.

An Operator Administrator (a "COA") can be assigned many operator numbers as profile options, at the discretion of the COGCC database administrator. However, each operator user account may belong to only one COA at a time. The COA is free to assign the user accounts he or she creates to one or more of the profile options that the COGCC has allowed to the COA. For example, a COA click the **Add All** button on the *Profile Options* grid on the **User Logins** page to create a user account that has all of the profile options available to the COA.

The person who is granted an Operator Administrator (COA) role within the CO Env application is responsible for creating, updating, and maintaining as current his or her own user accounts. Therefore, if a user leaves the employ of COA 1, then that COA must set the user's account to *Not Approved*. If this user then joins a company whose CO Env users are managed by COA 2, COA 2 must create a new user account under a new, unique user name. If the user name is not unique, account creation will not be allowed.

A *ParentUser* field was added to the **aspnet_Membership** table in the security database to accommodate this change.

The following procedure steps through the process for establishing an operator administrator role and testing the login before releasing site credentials to the user:

1. Login as a user in the *Administrator* role and open the **Administration | Users** page.
2. In the *aspnetUsers for Operators* grid, click **Add**  . A new form will open.
3. Create a new user login and assign the user to the *Operator Administrator* role in the *Roles for User* grid.
4. Enter the COGCC operator number(s) in the **Option Value** field. in the *Profile Options* grid.
5. **Save** 

the page.
6. Logout.
7. Log back in as the operator administrator you created.
8. Check the **Administration** menu to make sure only the **Users** page is visible. Check to make sure that other sensitive pages are not available, consistent with the security plan for the application. For example, users in the *Operator Administrator* and *Public* roles should not have access at all to pages that deal with Lab Batches, EDD Review, Parameters, Analysis Lists, Methods, Codes, Roles, and Tree Menus.

9. On the **Users** page, check to make sure that only users in the public role associated with the operator number can be created with the Operator Administrator credentials.
10. Create a public user for the operator, as in steps 1 through 5.
11. When you login as the public user, check to make sure that the **Administration** menu is invisible.

Users with *Operator Administration* permission can view and edit only those user accounts that they create under their assigned profile options.

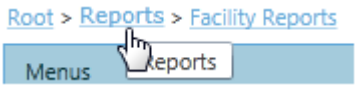
Managing the Tree Menu

The application main menu is controlled within the LightSwitch design environment. However, tree control menus, such as that for the **Reports** menu, are controlled from the **Administration | Tree Menus** page. Each report can have its own permission requirement. If the current user does not have the permission, then the report will not appear on the menu.

The **Tree Menus** page uses a 3-pane layout and a "bread-crumb" trail to manage menus. When the page first opens, the left grid displays top-level *Menus*, e.g., "Reports" and those items not currently assigned to a parent node. Selecting a menu by clicking in the row header of the left pane will display the properties associated with the node in the top center pane. If the item selected has been assigned child items, those *Menu Items* assigned to the node will display in the lower center grid.

Selecting a record in the left pane and then clicking **Zoom** will change the display of the *Menus* grid to show only the child elements associated with the selected menu and will create the "bread crumb" navigation trail at the top of the pane. This functionality reduces the amount of information clutter the user sees when building each node of the menu.

Clicking any part of the navigation trail will return you to the display for that part of the menu.

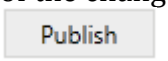


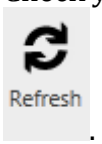
Adding a Menu Item

To add an existing item to an existing menu node such as the **Reports** menu, follow these steps:

1. Drill to the desired menu node, in this case, from the menu root, select the *Reports* record and click **Zoom**. The *Menus* pane will refresh to show you the tree nodes on the **Reports** menu.
2. Select the *Facility Information* record and observe the *Menu Items* displayed in the lower center pane.
3. In the right pane labeled **<<Select SubMenus to Add**, click in the row header to select the item you wish to add to the menu.
4. In the center *Menu Items* grid, click **Add**. The item will be added to a new line in the center pane.

5. **Save** the page. This action builds the XML underlying your changes preparatory to publishing it.
6. Return to the *Root* level of the bread crumb trail and select the Reports record in the *Menus* grid. Click **Build and Display** in the *Menus* grid tool bar to preview your change.

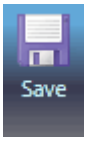
7. If you approve of the change and are ready to release the new menu to users, click **Publish**. 

8. Check your menu addition by returning to the **Home** page and clicking **Refresh** 

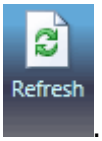
.
9. Switch to the **Reports** page and check for your addition.

Deleting a Menu Item

To delete a menu item, follow these steps:

1. In the *Menus* grid in the left, navigate to the menu item you wish to edit with the **Zoom**  button.
2. In the *Menu Items* grid in the lower center of the page, click in the row header to select the item you wish to delete.
3. Click **Delete**  to mark  the record for deletion from the menu node.
4. **Save** 

your change.
5. Return to the *Root* menu element and select the Reports record by clicking in the row header.
6. Click **Build and Display**  to check the revision.
7. Click **Publish** 

.
8. Switch to the **Home** page and click **Refresh** 

.
9. Switch to the **Reports** page to confirm the update.

Adding a New Report to the CO Env Web

To make a new .rdlc available to the application, follow these steps:

1. Upload the report (.rdlc, .xml, or .cht file) to the **/Reports** directory of the CO Env Web application on the server.
2. On the **Tree Menus** page, *Menus* grid, create a new record by clicking in the **New Record** row. Complete the form fields in the top center pane:
    a. The *Name* of the object, which can be the report name.
    b. A *Description*, which will be the text displayed on the finished menu node.
    c. The relative *File Path* to the report .rdlc template on the server.
    d. A *Tooltip*, which will be the text displayed onmouseover in the completed menu.
    e. An *Image* specification for the displayed icon used for the report. The CO Env Web application now uses the following conventions for the four available images, although the system administrator can add others in the LightSwitch environment, if desired:
    f. **Check Data** icon, used for quality control checks.
    g. **Report** icon, used for .rdlc reports.
    h. **Graph** icon, used for statistical reports.
    i. **Table** icon, used for grid-style reports.
    j. A *Tag*, which is an optional field to store additional text or numeric information when needed for special codes.
    k. *Filter*, which offers control over the sections of the **Report Data Filter** available for the report.
    l. *Skip*, which, if set to "True," will make the report item unavailable to users.
    m. *Permission ID*, the minimum level of permissions required for a user to have access to the tree menu node.
3. Save the page to commit the write operation. The item will then be available on the *<<Select SubMenus to Add* grid so that it can be added to the correct position on the **Reports** menu. Once it has been added to a node on the Reports menu, it will no longer display on the left pane *Menus* grid of the **Tree Menus** page.

About the Report Data Filter Wizard

Turning Sections of the Wizard On or Off

The **Report Data Filter** is a data wizard that includes four specific named sections. The *Visible* property of each section of the wizard can be edited to meet the data retrieval specifications of each report that is added to the CO Env report:

- Analysis, which includes the Autoselect Analysis check box and the Analysis List combo box.
- Project Select, which offers a choice of having the report pull Facility IDs or, if left blank, SampleIDs.
- Start Date, a calendar control for limiting the start date of a report data run.
- End Date, a calendar control for limiting the end date of a report data run.

The *Filter* control on the **Tree Menus** page is used to edit the report selection criteria availability through a line of XML code. For example, for a report that is intended to list attributes of facilities only, with no associated sample or analytical data, the following XML would be entered into the *Filter* control:

```
<Filter><Analysis Visible="False"/><Project Select="Facility"/></Filter>
```

Setting the visibility of the `<Analysis />` section to "False" will hide the **Autoselect Analysis** check box and the **Analysis List** combo box in the rendered report filter wizard, and specifying "Facility" for the `<Project Select />` tag will ensure that only Facility IDs are pulled the report. To pull sample IDs and analytical results, leave the `<Project Select />` tag empty.

The Report Data Filter and Dynamic Analysis Lists

When a user opts to run a report with the **Autoselect Analysis** check box set to "True," the application creates a temporary analysis list named `<zt` *+ a guid*`>`. So that these temporary lists do not cause a visual clutter on the **Analysis Lists page**, a bit column named *Temporary* was added to the **Coll** table. The *CollsForParameter* query filters out of visibility any set in the **Analysis Lists** page if *Temporary* = "True."

Filter Persistence

Facility filtering and report filters are stored in the security database for each user, so the application will default to each user's previous session settings.

About the Facility and Sample Data Upload Wizard

The **Facility and Sample Upload** wizard is meant to provide industry operators with a simplified set of screens to guide analytical data upload through the single sign-on used for the CO eForm application. Agency users should continue to use the full data views and user interface of the CO Env Silverlight application.

The **Facility and Sample Upload** Submittal wizard consists of five screens:

1. **Firm Contact Info**, which populates contact information about the operator and the user, allowing update and save of the updates.
2. **Options**, a "Home" switchboard page that guides the user to alternative tasks available through the Wizard. Each completed operation within the wizard starts and ends on this page, thus allowing multiple paths through the wizard. Clicking **Home** from the **Options** page returns the user to the eForm dashboard, represented in the development environment by a relative link to an eForm folder.
3. **Facility Edit**, which allows users to edit location information for an existing facility associated with the operator or create a new facility.
4. **Analytical Data Upload**, which allows user to upload electronic data deliverables in either .xml or .xls formats, parse the uploaded data against the schema, and review quality control messages.
5. **Upload Review**, which allows registered users to review each data upload, add sample information, and Save the updates. Agency users also have access to a button that allows Verify and Accept actions.

Uploading information through the wizard results in EDD files passing through the following form statuses:

- *Pending:* This auto status is so brief as to elapse without the user noticing it. From there, one of two statuses is possible:
    - *Verified:* If the upload passed QC checks, the status is set to *Verified*, and the **Next-->** button becomes visible to allow the user to review the upload and edit sample attribute.
        - OR
    - *Failed:* If the upload fails QC checks, the status is set to *Failed*, and the only available action on screen 4 of the wizard is to **Return to Options**.
- *Submitted:* Once the user has reviewed and possibly added extra sample data on screen 5, clicking the **Submit EDD** button will set the upload to the *Submitted* status.
- *Accepted:* Data that the COGCC moves from the DMZ to the production database through merge replication will be flagged as having been *Accepted*.

Integrating the Facility and Sample Upload Wizard with CO eForm

Security Considerations

The operator association with the user is automatically pulled from the user profile options in the **Administrative** portion of the RBDMS Environmental Silverlight application. The system administrator should assign an *Option Type* = "Operator" and an *Option Value* (e.g., 308) for the operator number to be associated with registered public users' login.

User information for the **Facility and Sample Upload** wizard can be integrated with the same security database that the CO eForm web application is using. However, since the RbdmsOnline.org development server is not running a working copy of CO eForm, the GWPC team created a http://virtuales.com/rbdmsEnv/htmlclient/ site that allows you to login using your account credentials for *applicationName*= "PRODRBDMS.NET" and then redirects to the **Facility and Sample Upload** wizard.

For this to work in the COGCC IT environment, both applications need to have the same security-related settings in their **web.config** file, as follows:

```
    <httpRuntime maxRequestLength="1024000" requestValidationMode="2.0" requestPat
    hInvalidCharacters="" />
     <machineKey validationKey="3D0EF4C0AA642D56695A9AC65547CA434F46DF4B06BA4139A5
4A5F3DA3260224A8246E0AF0D1810F0B4C9CB5C56266C8B553F97CAA7E95955E108195279D5EFA"
                 decryptionKey="D85E821D54E1C86870718AA04816E1A8FF74EE2AFD9878658A
8636AC72A2AA8F" validation="SHA1" decryption="AES" />
     <membership defaultProvider="AspNetMembershipProvider">
       <providers>
         <clear />
         <add name="AspNetMembershipProvider" type="System.Web.Security.SqlMembers
hipProvider" connectionStringName="
RbdmsSecurityConnectionString" applicationName="PRODRBDMS.NET" requiresUniqueEmail=
"false" requiresQuestionAndAnswer="false" enablePasswordReset="true" />
                 </providers>
     </membership>
```

At deployment, this code should be added to the COGCC's eForm dashboard application and invoked from there.

URL Parameters and Dependencies

The wizard can be launched by passing the argument *?screen=AnalyticalDataSubmittal* to the URL, i.e., http://virtuales.com/RBDMSEnv/client/?screen=AnalyticalDataSubmittal.

For logins that are associated with internal agency permissions, the menu and ribbon bar for the RBDMS CO Env application are visible within the wizard. For *Operator* users of the Analytical Data Wizard, the CO Env menu and tool bar are hidden, so that the industry users' only option on exit of the wizard is to return to eForm.

Clicking **Home** from the **Options** page returns the user to the eForm dashboard, represented in the development environment by a relative link to an eForm folder. This link should be set at deployment to the appropriate URL.