Photos courtesy of USDA NRCS.

NetDMR System Administrator User's Guide

Version 1

October 17, 2008

CONTENTS

Page

1.0 Introduction to NetDMR Help 1
1.1. Background 1
2.0 Getting Started 1
2.1. System Requirements 1
2.2. Types of Users and Roles 1
2.3. Contacting the NetDMR Team 1
2.4. Login 1
2.4.1 Common Login Problems 1
2.5. Other Resources 1
2.6. Enabling Session Cookies 1
2.7. Termination of Active Session 1
3.0 Navigating NetDMR 1
3.1. Common Links Displayed on the NetDMR Login Page 1
3.1.1 Login 1
3.1.2 Frequently Asked questions (FAQs) 1
3.1.3 Getting Started 1
3.1.4 Register for a New Account 1
3.1.5 Forgot Username? 1
3.1.6 Forgot Password? 1
3.1.7 Checking Your Permit ID? 1
3.1.8 Expired Password 1
3.1.9 Disabled Account 1
3.1.10 Locked Account 1
4.0 Managing Your Account 1
4.1. My Account 1
4.1.1 General Account Information 1
4.1.2 Selected Security Questions 1
4.1.3 My Permits 1
4.2. Edit Account 1
4.2.1 General Account Information 1
4.2.2 Security Questions and Answers 1
4.2.3 Change Your Password 1
4.2.4 Lock Your Account 1
4.2.5 Account Information Tips 1
4.3. Logout 1
4.3.1 Session Time Out 1
5.0 System Administrator 1
5.1. Create Instance 1
5.2. Manage Instances 1
5.2.1 View Instance Status 1
5.2.2 Edit Instance 1
5.2.3 Delete Instance 1
5.3. Manage Downtime 1
5.4. Manage Settings 1
6.0 Acronyms and Definitions 1

1.0 Introduction to NetDMR Help

This User's Guide provides step-by-step instructions and guidance on how to use NetDMR.

1.1. Background

The Environmental Council of States, the Texas Commission on Environmental Quality, 12 states, EPA's Office of Environmental Information, and EPA's Office of Enforcement and Compliance Assurance partnered under an EPA Challenge Grant to design, develop, and demonstrate NetDMR. NetDMR is a web-based application that will allow National Pollutant Discharge Elimination System (NPDES) permittees to submit electronic discharge monitoring reports (eDMRs) to EPA's data system for discharge information, the Integrated Compliance Information System (ICIS)-NPDES database. NPDES permits are issued under the authority of the Clean Water Act.

NetDMR includes the following key components:

- **Common Functionality**: Create an account, request access to a permit and associated DMRs/and copies of record (CORs), edit account information, retrieve a forgotten user name or reset a forgotten password, and enable a disabled account.
- **System Administrator**: Configure a NetDMR installation and customize settings for each instance associated with an installation.
- **Internal Administrator**: Manage user accounts; set additional customization options for an instance; approve signatories; and search, view, and download DMRs and CORs submitted for permits administered by the regulatory authority associated with the instance.
- **Permit Administrator**: Manage user read and write access to DMRs for a specific permit.
- **Search Functionality**: Search and view permit details.
- **DMR Functionality**: Search, view, edit, sign and submit DMRs; import DMR data.
- **Copy of Record Functionality**: Search, view, and download copies of record for DMRs.
- **Data flows**: Retrieve data from and submit data to a NPDES system using a Node and the Exchange Network. NetDMR includes the following data flows: basic permit data flow, empty slot data flow, error message data flow, and DMR submission data flow.
- **Database**: Store information needed by NetDMR or generated by NetDMR users.
- **Help System**: Provide on-line instruction on how to use specific elements of NetDMR functionality.

2.0 Getting Started

The following sections describe what you need to know to begin using NetDMR.

2.1. System Requirements

NetDMR requires the following:

Internet Access Requirements

- High-speed access to the Internet, such as DSL, cable-modem, T1, or partial T1.

Hardware Requirements

- Minimum Pentium III processor and 128 megabytes of RAM.

Browser Requirements

- Microsoft Internet Explorer Version 6.x or higher.
- Firefox 2.0 or higher.

Other Requirements

- Cookies Enabled
- Screen Resolution (recommended)
  - 1024 × 768.
- JavaScript enabled

2.2. Types of Users and Roles

There are several types of NetDMR users, and each user can be assigned one or more roles.

NetDMR Users

- **Permittee User** – you work for an organization that is required to submit Discharge Monitoring Reports (DMRs) under a National Pollutant Discharge Elimination System (NPDES) permit.
- **Internal User** – you work for or support a State environmental agency that administers NPDES permits, or support EPA administration of NPDES permits.
- **Data Provider** (e.g., analytical laboratory, consultant) – you support an organization that is required to submit DMRs as part of a NPDES permit.

NetDMR Roles

- Permittee Read-only: view DMRs associated with the permit, but cannot update or modify DMR data.
- Edit access: view and modify DMRs and DMR data.

- Signatory: authority to sign and submit DMRs on behalf of your organization. A request for the signatory role requires submission of a subscriber agreement to the organization that administers your NPDES permit.
- Permit Administrator: approve all DMR read only and edit requests for a Permit.
- Internal Administrator: approve internal read-only requests for DMR Copies of Record; customize NetDMR software and certain properties.
- Internal Read-only: view DMR copies of record (CORs) after signed and submitted by permittees for the permits you administer, but cannot view in-progress DMRs or modify DMR data.
- System Administrator: configures the NetDMR software and certain properties.

2.3. Contacting the NetDMR Team

If you would like to contact the NetDMR team, click the email link on the ***NetDMR Login*** page. This link will allow you to email questions or comments to the NetDMR support team.

Alternatively, you can click the Contact the NetDMR Team link at the top of the page to view additional contact information for the NetDMR support team.

2.4. Login

After you create a NetDMR account, you can login by:

1. Accessing the ***NetDMR Login*** page.
2. Entering your username.
3. Entering your password.
4. Clicking *Submit*.

2.4.1 Common Login Problems

If you cannot log in to your account, below are steps to resolve common login issues. These directions are applicable only after you have created a NetDMR account.

Retrieve Forgotten User Name

1. Click Forgot User Name? on the ***NetDMR Login*** page.
2. Enter the email address you used to create your NetDMR account.
3. Click *Submit*.
4. Answer the security question that is displayed.
5. Click *Submit*.
6. If you provided an email address that is in the NetDMR database and answered the security question correctly, your user name will be displayed.

Reset a Forgotten Password

1. Click Forgot Password? on the ***NetDMR Login*** page.
2. Enter the email address you used to create your NetDMR account.
3. Click *Submit*.
4. Answer the security question.
5. Click *Submit*.
6. If you provided an email address that is in the NetDMR database and answered the security question correctly, a message with information on how to reset your password will be forwarded to your email account.
7. Click on the link provided in the email to access the ***Complete the NetDMR Password Reset Request*** page.
8. Answer the security question.
9. Enter a new password. (Note that your new password must be different than the last **10** passwords you specified for your account.)
10. Enter the new password again.
11. Click *Submit*.

Expired Password

After a certain time period, your password will expire and you will need to create a new one. If your password has expired, after logging in to NetDMR the ***Expired Password*** page will display. Follow these directions to reset an expired password.

1. Answer the security question.
2. Enter your current password.
3. Enter a new password. Your new password must be different than the last **10** passwords you used for your account.
4. Enter the new password again.
5. Click *Submit*.

Disabled Account

If your account is disabled due to too many invalid authentication attempts, the ***Disabled Account*** page will display after you attempt to login. Follow these directions to enable a disabled account.

1. Answer the security question.
2. Click *Submit*.

If you respond correctly to the security question, you will be directed back to the ***NetDMR Login*** page to login to your account.

Locked Account

If your account is locked, the ***Locked Account*** page will display after you attempt to login. Contact your regulatory authority and request to have your account unlocked.

2.5. Other Resources

The ***NetDMR Login*** page has links to additional resources that will give you more information on NetDMR. These menu options are always listed at the top of the ***NetDMR Login*** page and include:

- **FAQs**: frequently asked questions and answers.
- **Getting Started**: instructions on how to get started using NetDMR.
- **Contact the NetDMR Team**: contact information for the NetDMR team.

2.6. Enabling Session Cookies

NetDMR requires that you enable session cookies to function properly. A cookie is a small text file containing information that a Web site copies to your computer. NetDMR will automatically detect whether you have cookies enabled after login and provide instructions on how to enable cookies if needed. All cookies generated by NetDMR are removed once you close your browser.

After you enable cookies, log into NetDMR again. The following cookies will be used by NetDMR:

- JSESSIONIID: A number generated by the NetDMR to identify your browser. This cookie is removed once you close your browser and contains no personal identifying information.

- COOKIETEST: A cookie that has the value of 1. This cookie is set only to test that your browser allows cookies. This cookie contains no personal identifying information.

Instructions for enabling cookies are provided below. There are different steps depending upon which browser you are operating. To identify what version of a web browser you are operating, click on the Help menu in Internet Explorer or Netscape and click About.

If you are using Internet Explorer 6.0 or 7.0:

1. Choose Tools, then Internet Options.
2. Click the Privacy tab.
3. Default setting is medium. Move the slider to determine which setting you prefer.
4. You can also click on Advanced for specialized cookie treatment.

If you are using Firefox:

1. Click Tools.
2. Select Options.
3. Expand the Cookies tab.
4. Select "Allow Sites to Set Cookies."

2.7. Termination of Active Session

NetDMR will automatically log you out if the page is left idle for 30 minutes. The Session Lockout Timer, which is a countdown from 30 minutes, is displayed at the top right corner of every page. The timer resets to 30 minutes every time you perform an action that refreshes the page (e.g., save, submit, cancel, etc). Once you are logged out you can immediately sign back in.

Dependent on the browser being used, the page may be automatically directed to a new screen displaying a time-out message which explains your session has logged out and you may log back in. For browsers that do not support the automatic re-direct, the user will see this new screen with the time-out message upon their next action.

3.0 Navigating NetDMR

The following sections describe how to navigate NetDMR.

3.1. Common Links Displayed on the NetDMR Login Page

Prior to logging in to NetDMR, the following links are always available on the page NetDMR.

- Login.
- FAQs.
- Getting Started.
- Contact the NetDMR Team.
- Register for a New Account.
- Forgot Username?
- Forgot Password?
- Create a NetDMR Account.
- Checking your Permit ID.

3.1.1 Login

Clicking Login directs you back to the ***NetDMR home*** page.

3.1.2 Frequently Asked questions (FAQs)

Clicking FAQs displays the ***FAQ*** page. Click the green plus sign icon to expand the FAQ list and the red minus sign icon to collapse the list.

3.1.3 Getting Started

Clicking Getting Started displays the information needed to get started using NetDMR.

3.1.4 Register for a New Account

1. From the ***NetDMR Login*** page Click register for a new account.
2. Fill out the required information and click *Save*.
3. Confirm that the information is correct and click *Confirm*.
4. You will receive an email from NetDMR in the email account you provided.
5. Click on the link in the email.
6. A new webpage will open and prompt you to answer one of the 5 security questions you created and create a password for the account.
7. Click *Submit* to complete the create account process.

3.1.5 Forgot Username?

1. Click Forgot User Name? on the ***NetDMR Login*** page.
2. Enter the email address you used to create your NetDMR account.
3. Click *Submit*.

4. Answer the security question that is displayed.
5. Click *Submit*.
6. If you provided an email address that is in the NetDMR database and answered the security question correctly, your user name will be displayed.

3.1.6 Forgot Password?

1. Click Forgot Password? on ***the NetDMR Login*** page.
2. Enter the email address you used to create your NetDMR account.
3. Click *Submit*.
4. Answer the security question.
5. Click *Submit*.

If you provided an email address that is in the NetDMR database and answered the security question correctly, a message with information on how to reset your password will be forwarded to your email account.

1. Click on the link provided in the email to access the ***Complete the NetDMR Password Reset Request*** page.
2. Answer the security question.
3. Enter a new password. (Note that your new password must be different than the last 10 passwords you specified for your account.)
4. Enter the new password again.
5. Click *Submit*.

3.1.7 Checking Your Permit ID?

You can check whether any of your permits are available for reporting in NetDMR by following the directions below. You do not have to create a NetDMR account before you can check on the status of your permits

1. Click the Checking your Permit ID link on the ***NetDMR Login*** page.
2. Enter your permit ID.
3. Click Check Permit ID.
4. A message indicating whether you can report DMRs for your Permit ID using NetDMR will be displayed.

3.1.8 Expired Password

After a certain time period, your password will expire and you will need to create a new one. If your password has expired, after logging in to NetDMR the ***Expired Password*** page will display. Follow these directions to reset an expired password.

1. Click Forgot Password? on the ***NetDMR Login*** page.
2. Enter the email address you used to create your NetDMR account.
3. Click *Submit*.
4. Answer the security question.
5. Click *Submit*.

3.1.9 Disabled Account

If your account is disabled due to too many invalid authentication attempts, the ***Disabled Account*** page will display after you attempt to login. Follow these directions to enable a disabled account.

1. Answer the security question.
2. Click *Submit*.

If you respond correctly to the security question, you will be directed back to the ***NetDMR Login*** page to login to your account.

3.1.10 Locked Account

If your account is locked, the ***Locked Account*** page will display after you attempt to login. Follow these directions to unlock a locked account.

1. Contact your regulatory authority and request to have your account unlocked.

4.0 Managing Your Account

The following section will provide you with information on how to manage your NetDMR account. These topics include:

- View your account
- Edit your account
- Logout

4.1. My Account

You can access the details of your account by clicking the **My Account** menu option on the ***NetDMR Login*** page, including: General Account Information, the Security Questions you selected, and permits that you have requested or been granted access to.

4.1.1 General Account Information

General Account Information includes the following data that you provided when you created your account:

- E-mail Address
- User Name
- First Name
- Last Name
- Telephone Number
- Organization
- Type of User

4.1.2 Selected Security Questions

This section displays the five security questions you chose when you created your account. The answers you provided are not displayed. When managing your account you will often be prompted to answer one of the five questions.

Tip: Click the green plus sign icon to display your security questions and the red minus sign icon to hide the list of security questions.

4.1.3 My Permits

The My Permits section includes a table that lists all of the permits you have been granted access to, the type of role, and all of the permits that you have requested access to, and the role you requested. Up to ten permits will be displayed by default. If more than 10 permits are associated with your account, you can navigate through the list by:

- Clicking the green forward arrow to display the next page of permits.
- Clicking the green back arrow to view the previous page of permits.

- Clicking the double green forward arrow icon to display the last 10 permits.
- Clicking the double green back arrow icon to display the first 10 permits.
- Clicking the View All link to show all permits in the table on the same page with the default sort order applied.
- Clicking the View Partial link to return from the View All display back to viewing 10 permits at a time with the default sort order applied.

You can click any underlined column title to sort the permits in ascending or descending order by the information in that column.

4.2. Edit Account

Click Edit Account in the upper right corner of the ***My Account*** page to:

- Revise your general account information
- Request changes to permit access rights
- Modify your security questions and answers
- Lock your account

Any changes you make must be confirmed and saved. Follow these directions store your edits:

1. After completing your edits, click *Save.*
2. Review your changes to confirm that they are correct.
3. Answer the Security Question and provide your current password.
4. Click *Save.*

4.2.1 General Account Information

You can modify the following account information on the ***Edit Account*** page:

- E-mail Address
- User name
- First Name
- Last Name
- Telephone Number
- Organization
- User Type (cannot be modified)

4.2.2 Security Questions and Answers

You can change your Security Questions and Answers. Click the green plus sign icon to display your security questions and the red minus sign icon to hide the list of security questions.

4.2.3 Change Your Password

You can change your Login Password by entering a new password and then reentering it in the space provided.

4.2.4 Lock Your Account

You can lock your account by checking the box next to Lock your account.

4.2.5 Account Information Tips

When entering account information, NetDMR checks for certain formats and requires certain content. A summary of these account rules is below:

Account Information	Tips and Format Requirements
Email address	• Special characters: only “@”, “.”, “-“, and “_” are allowed • Must contain the “@” symbol • Must be unique • You must have access to this email account
Username	• Special characters: only “@”, “.”, and “_” are allowed • Must be unique
First Name	• Special characters: only “’”, “.”, and “-” are allowed
Last Name	• Special characters: only “’”, “.”, and “-” are allowed
Organization	• Special characters: only spaces, “’”, “.”, and “-” are allowed
Telephone Number	• Must be in the following format xxx-xxx-xxxx
Security Questions	• What is the name of the street where you grew up? • What is your favorite color? • What is your mother’s maiden name? • What is your father’s middle name? • What is your favorite vacation destination? • What is you favorite city? • What is the name of the high school you attended? • Who was your childhood hero? • What was your high school mascot? • What was your first pet’s name?

Account Information	Tips and Format Requirements
Security Questions and Answers	• All five security questions must be different. • All five security answers must be different. • Security Answers are case sensitive. • Special characters: only spaces, “’”, “.”, and “-” are allowed • Choose security answers that are easy to remember as you will need to know them to create an account, edit your account, and retrieve forgotten passwords and user names.
Password	• Must be between 8 and 20 characters. • Must contain at least one number and one letter. • May contain both upper case and lower case letters. • Cannot contain special characters other than: !@#$^&*+= • Passwords are case sensitive.

4.3. Logout

To logout of your NetDMR account, click the **Logout** menu option at the top of the page.

4.3.1 Session Time Out

NetDMR will automatically log you out if a page is left idle for 30 minutes. The Session Lockout Timer, which is a countdown from 30 minutes, is displayed at the top right corner of every page. The timer resets to 30 minutes every time you perform an action that refreshes the page (e.g., save, submit, cancel, etc).

Depending on your browser, you may be automatically directed to a new page displaying a time-out message explaining that your session has timed out due to inactivity. For browsers that do not support the automatic re-direct, you will be directed to the time out page after you perform an action that refreshes a page.

5.0 System Administrator

NetDMR System Administrators configure a NetDMR installation, create and manage all NetDMR instances that are part of that installation, and manage installation settings.

A NetDMR Installation is the NetDMR application as deployed in a hosting environment. A NetDMR Instance is a customized version of NetDMR, specific to a Regulatory Authority, such as a state or Region.

A single NetDMR installation can include one or more instances. An installation is analogous to enterprise email server software, and each NetDMR instance associated with the installation is analogous to an email account. Global settings, such as data flow request frequency and timing, are specified at the installation level. Instance settings, such as Agency Maps and password change frequency, and are specified at the account level.

5.1. Create Instance

An instance is a customized version of NetDMR, specific to a Regulatory Authority. Follow these directions to create a new instance in NetDMR and specify general information, create the initial internal administrator, assign Agency Maps, and update the subscriber agreement.

Update General Information

1. Log into NetDMR with the System Administrator account.
2. Click Create New Instance to access the ***Create Instance*** page.
3. On the ***Create Instance*** page:
   - Enter the name of the instance.
   - Select the time zone.
   - Select the number of security questions users must answer when creating an account.
   - Select how often users will be required to change their password.
   - Select whether to allow multiple signatory requests in a subscriber agreement.
   - Upload the graphic that will be shown in the top right corner of each page by clicking *Browse* and selecting it from your hard drive. Graphics must be in the *.jpg format. The recommended size specifications are:
     - Height: 60 pixels
     - Width: 20 pixels

     Graphics of a different size will likely appear distorted.
   - Specify the Submittal Postal Code. The DMR data flow requires that NetDMR include in the submission file name a submittal Postal Code. NetDMR uses the code you provide to properly name all DMR submission files that are submitted to CDX and ICIS. You will need to coordinate with EPA ICIS staff on the proper postal code for each instance you create.

- Specify a Contact Name. This name will be displayed on the NetDMR ***Contact Information*** page.
- Specify a Contact Email. This email will be displayed on the NetDMR ***Contact Information*** page and the ***Home*** page.
- Specify a Contact Phone. This phone number will be displayed on the NetDMR ***Contact Information*** page.

Create the Initial Internal Administrator

1. On the ***Create Instance*** page, provide the account information for the first Internal Administrator for this instance:
   - Enter the Internal Administrator's email address.
   - Confirm the Internal Administrator's email address by entering it a second time.
   - Choose whether to use the Internal Administrator's email address as the user name or create a custom user name.
   - If you choose to create a custom user name, enter the user name.
   - Enter the Internal Administrator's first name.
   - Enter the Internal Administrator's last name.
   - Enter the Internal Administrator's 10-digit telephone number in the following format (xxx-xxx-xxxx).
   - Enter the name of the organization with which the Internal Administrator is affiliated.
   - Enter a temporary password
   - Confirm the temporary password by typing it again.

Specify Agency Maps

1. On the ***Create Instance*** page, specify the Agency Maps by selecting the states or areas appropriate for this instance. You should consult with the program area or business lead for the Instance to determine appropriate Agency Maps.
   - Select the permit prefix.
   - Select the agency type code. This is the code used in ICIS-NPDES to categorize the agency that administers the permit. Options, as of August 2008, are as follows:

Agency Type Code Listing		
CNT : County	IN4 : Interstate	SC1 : State Contractor
CT1 : County	IN6 : Interstate	SC2 : State Contractor
CT2 : County	INT : Interstate	SC3 : State Contractor
CT3 : County	LC1 : Local	SC4 : State Contractor
CT4 : County	LC2 : Local	SC6 : State Contractor
CT6 : County	LC3 : Local	SO1 : Other - State
EC1 : EPA Contractor	LC4 : Local	SO2 : Other - State
EC2 : EPA Contractor	LC6 : Local	SO3 : Other - State
EC3 : EPA Contractor	LCL : Local	SO4 : Other - State
EC4 : EPA Contractor	MN1 : Municipal	SO6 : Other - State
EC6 : EPA Contractor	MN2 : Municipal	ST1 : State
EO1 : Other - EPA	MN3 : Municipal	ST2 : State
EO2 : Other - EPA	MN4 : Municipal	ST3 : State
EO3 : Other - EPA	MN6 : Municipal	ST4 : State
EO4 : Other - EPA	MUN : Municipal	ST6 : State
EO6 : Other - EPA	OF1 : Other Federal	STA : State
EP1 : U.S. EPA	OF2 : Other Federal	STC : State Contractor
EP2 : U.S. EPA	OF3 : Other Federal	STF : State - Using
EP3 : U.S. EPA	OF4 : Other Federal	Federal Credentials
EP4 : U.S. EPA	OF6 : Other Federal	STO : Other - State
EP6 : U.S. EPA	OFD : Other Federal	TR1 : Tribal
EPA : U.S. EPA	REG : Regional	TR2 : Tribal
EPC : EPA Contractor	RG1 : Regional	TR3 : Tribal
EPO : Other - EPA	RG2 : Regional	TR4 : Tribal
IN1 : Interstate	RG3 : Regional	TR6 : Tribal
IN2 : Interstate	RG4 : Regional	TRB : Tribal
IN3 : Interstate	RG6 : Regional	TRF : Tribal - Using
		Federal Credentials

— Click *Save and Add Another*.
— Repeat these steps until all the desired Agency Maps have been added to the table.

Customize the Subscriber Agreement

On the ***Create Instance*** page, customize the subscriber agreement by providing information on the Regulatory Authority and entering any specific terms and conditions

1. Provide the mailing information for the Regulatory Authority.
   — Enter name of the Regulatory Authority.
   — Enter the address.
   — Enter the supplemental address.
   — Enter the City.
   — Enter the State.
   — Enter the Zip Code.
2. Enter the opening terms of the subscriber agreement.
3. Enter the closing terms of the subscriber agreement.

4. Enter a condition for the subscriber agreement.
   — Click Save and Add Another.
   — Click on the move up arrow or move down arrow to change the order of the conditions
   — Repeat this step until all the required conditions are added to the table.
5. Click Save.
6. Review the information on the ***Confirm Create Instance*** page and click *Create*.

You will be returned to your ***Home*** page and the newly created instance will be displayed in the ***My Instances*** table.

5.2. Manage Instances

The following section provides information on how to manage your instances. These topics include.

- View Instance Status
- Edit Instance Settings
- Delete Instance

5.2.1 View Instance Status

You can access the details of your instances by logging into your account and clicking on the name of the instance in the ***My Instances*** table on your ***Home*** page. Here you will be able to view the following information on each of your instances:

- Instance Details
- Agency Maps
- Internal Administrators
- Subscriber Agreement

Note: The ***My Instances*** table is also accessible by clicking on **Instances** under the **Manage** menu.

Instance Details

The Instance Details section displays the information that you specified when you created this instance, including:

- Instance Name
- Instance Time Zone
- Number of Secret Questions
- Password Change Frequency
- Multiple requests per subscriber agreement?
- Submittal Postal Code
- Contact Name
- Contact Email

- Contact Phone

Agency Maps

The Agency Maps table displays the selected Permit Prefixes and associated Agency Type Codes. Up to ten Agency Maps will be displayed by default. If more than ten Agency Maps are associated with your instance, you can navigate through the list by:

- Clicking the green forward arrow to display the next page of Agency Maps.
- Clicking the green back arrow to view the previous page of Agency Maps.
- Clicking the double green forward arrow icon to display the last ten Agency Maps.
- Clicking the double green back arrow icon to display the first ten Agency Maps.
- Clicking the View All link to show all Agency Maps in the table on the same page with the default sort order applied.
- Clicking the View Partial link to return from the View All display back to viewing ten Agency Maps at a time with the default sort order applied.

You can click the Permit Prefix or Agency type code column title to sort the Agency Maps in ascending or descending order.

Internal Administrators

The Internal Administrators table displays the User Name, Affiliation, Email Address, and Phone Number of each Internal Administrator. Up to ten Internal Administrators will be displayed by default. If more than ten Internal Administrators are associated with your instance, you can navigate through the list by:

- Clicking the green forward arrow to display the next page of Internal Administrators.
- Clicking the green back arrow to view the previous page of Internal Administrators.
- Clicking the double green forward arrow icon to display the last ten Internal Administrators.
- Clicking the double green back arrow icon to display the first ten Internal Administrators.
- Clicking the View All link to show all Internal Administrators in the table on the same page with the default sort order applied.
- Clicking the View Partial link to return from the View All display back to viewing ten Internal Administrators at a time with the default sort order applied.

You can click any underlined column title to sort the Internal Administrators in ascending or descending order by the information in that column.

Subscriber Agreement

The Subscriber Agreement section displays the following information:

- Regulatory Authority Mailing Information
  - Attn
  - Address
  - Supplemental Address
  - City
  - State
  - Zip Code
- Terms and Conditions
  - Opening Terms
  - Closing Terms
  - A table displaying each condition

5.2.2 Edit Instance

You can edit instances by logging into your account and clicking on the name of the instance in the ***My Instances*** table on your ***Home*** page, then click the *Edit Instance* button. You can then modify the following information from the ***Edit Instance*** page that is displayed:

- Instance Details
- Agency Maps
- Internal Administrators
- Subscriber Agreement

Instance Details

You can edit the following information in the Instance Details section, including:

- Instance Name
- Instance Time Zone
- Number of Secret Questions
- Password Change Frequency
- Multiple requests per subscriber agreement?
- Submittal Postal Code
- Contact Name
- Contact Email
- Contact Phone

Click Save on the ***Edit Instance*** page and then click Save on the ***Confirm Edit Instance*** page to finalize your changes.

Agency Maps

You can edit the Agency Maps for the instance in the Agency Maps section.

- Delete an Agency Map: Click the icon in the delete column for the row of interest and click OK to confirm the deletion.
- Update an Agency Map: Click the pencil icon in the update column for the row of interest, click to select a new Agency Type code, and click Save to confirm the selection.
- Add new Agency Maps:
  - Select the permit prefix.
  - Select the agency type code.
  - Click Save and Add Another.
  - Repeat these steps until all the desired Agency Maps have been added to the table.
- Click *Save* on the ***Edit Instance*** page and then click Save on the ***Confirm Edit Instance*** page to finalize your changes.

Up to ten Agency Maps will be displayed by default. If more than ten Agency Maps are associated with your instance, you can navigate through the list by:

- Clicking the green forward arrow to display the next page of Agency Maps.
- Clicking the green back arrow to view the previous page of Agency Maps.
- Clicking the double green forward arrow icon to display the last ten Agency Maps.
- Clicking the double green back arrow icon to display the first ten Agency Maps.
- Clicking the View All link to show all Agency Maps in the table on the same page with the default sort order applied.
- Clicking the View Partial link to return from the View All display back to viewing ten Agency Maps at a time with the default sort order applied.

You can click the Permit Prefix or Agency type code column title to sort the Agency Maps in ascending or descending order.

Internal Administrators

You can update a view only Internal User to an Internal Administrator role by clicking in the box next to Internal Administrator, selecting the name of the user to grant Administrator access to, and click *Save and Add Another*.

You can also delete Internal Administrator access from a user by clicking the icon in the Delete column in the row for the user of interest.

To complete your changes, click *Save* on the ***Edit Instance*** page and then click *Save* on the ***Confirm Edit Instance*** page.

The Internal Administrators table displays the User Name, Affiliation, Email Address, and Phone Number of each Internal Administrator. Up to ten Internal Administrators will be displayed by default. If more than ten Internal Administrators are associated with your instance, you can navigate through the list by:

- Clicking the green forward arrow to display the next page of Internal Administrators.
- Clicking the green back arrow to view the previous page of Internal Administrators.
- Clicking the double green forward arrow icon to display the last ten Internal Administrators.
- Clicking the double green back arrow icon to display the first ten Internal Administrators.
- Clicking the View All link to show all Internal Administrators in the table on the same page with the default sort order applied.
- Clicking the View Partial link to return from the View All display back to viewing ten Internal Administrators at a time with the default sort order applied.

You can click any underlined column title to sort the Internal Administrators in ascending or descending order by the information in that column.

Subscriber Agreement

You can edit any of the following information for the Subscriber Agreement:

- Regulatory Authority Mailing Information
  - Attn
  - Address
  - Supplemental Address
  - City
  - State
  - Zip Code
- Terms and Conditions
  - Opening Terms
  - Closing Terms
- Add a new condition by entering the condition text, click *Save and Add Another*.
  - Click on the move up arrow or move down arrow to change the order of the conditions
  - Repeat this step until all the required conditions are added to the table.
- To delete a condition, click on the icon in the row of interest and click *OK* to confirm the deletion.

Click *Save* on the ***Edit Instance*** page and then click *Save* on the ***Confirm Edit Instance*** page to finalize your changes.

5.2.3 Delete Instance

You can delete an instance by logging into your account, and clicking the icon in the Delete column for the instance of interest on the ***My Instances*** page. Click *Delete* on the ***Confirm Delete Instance*** page to finalize the deletion. **If you delete an instance, all information associated with the instance, including users, DMRs, and CORs, will be removed and will no longer be available.**

5.3. Manage Downtime

You can schedule downtimes for any of the instances in your installation. During a downtime, external users can not access the Instance, internal users with a view role cannot access the Instance, and new user accounts cannot be created. Note that Internal Administrators can still access an Instance during a downtime. To schedule a downtime for the entire NetDMR installation or one or more instances, follow the instructions below:

1. Click **Downtimes** under the **Manage** menu on the ***Home*** page.
2. Click *Schedule Another Downtime* on the ***Instance Downtime Schedule*** page
3. Click in the box next to Take Down on the ***Schedule Downtime*** page to select all instances, or one or more specific instances.
4. Enter a Start Date and Start Time. Note that if the installation and instance time zones are different, the downtime start time must be entered in the installation time zone. For example, if your installation time zone is Eastern but the instance time zone is Central, starting a downtime at 2 pm Central would require that you set the downtime start time at 3 pm Eastern.
5. Enter an End Date and End Time. Note that if the installation and instance time zones are different, the downtime end time must be entered in the installation time zone. For example, if your installation time zone is Eastern but the instance time zone is Central, ending a downtime at 3 pm Central would require that you set the downtime end time at 4 pm Eastern.
6. Enter a message to be displayed to users.
7. Click *Save* to schedule the downtime.
8. Click *Save* again on the ***Schedule Downtime Confirm*** page.
9. Your downtime will be displayed in the table on the ***Instance Downtime Schedule*** page.

To update a downtime, click the in the row of interest on the Schedule Downtime table, update the downtime settings, and click *Save*.

To delete a downtime, click the in the row of interest on the Schedule Downtime table, and click *OK* to verify the deletion. Note that you cannot delete a downtime that has already started.

5.4. Manage Settings

Follow the steps below to view and edit installation settings:

1. Click **Setting** under the **Manage** menu on the ***Home*** page.
2. Click *Edit Settings* on the ***View Settings*** page.
3. Click in the box next to User/COR Purge Schedule to change the setting.
4. Click in the box next to Time Zone to change the setting.
5. Click in the box next to Suspect Analysis Frequency to change the setting.
6. Click in the box next to Suspect Analysis Log Data Subset to change the setting.
7. Click *Save*.
8. Click *Save* again on the ***Confirm Edit Settings*** page to finalize your modifications.

6.0 Acronyms and Definitions

Table 6-1. Acronyms

Acronym	Description and Notes
BPDF	Basic Permit Data Flow
CDX	Central Data Exchange - http://www.epa.gov/cdx/
COR	Copy of Record, legally enforceable copy of DMR submission
CWA	Clean Water Act
DMR	Discharge Monitoring Report Required under the Clean Water Act, used by permittees to report pollutant concentrations or other properties for water discharged into rivers, lakes, streams, and other water bodies as specified in a NPDES permit.
ECHO	Enforcement and Compliance System On-line http://www.epa.gov/echo/index.html
ECOS	Environmental Council of States http://www.ecos.org
eDMR	Electronic DMR System
EPA	U.S. Environmental Protection Agency http://www.epa.gov
Exchange Network	National Environmental Information Exchange Network http://www.epa.gov/exchangenetwork/index.html http://exchangenetwork.net/
ICIS	Integrated Compliance Information System http://www.epa.gov/compliance/data/systems/modernization/index.html ICIS, a Web-based system, enables individuals from states and EPA to access integrated enforcement, compliance, and NPDES data from any desktop connected to the Internet. The public can access some ICIS data through ECHO.
ICIS-NPDES	Integrated Compliance Information System - National Pollutant Discharge Elimination System http://www.epa.gov/compliance/data/systems/index.html
NEIEN	National Environmental Information Exchange Network http://www.epa.gov/exchangenetwork/index.html http://exchangenetwork.net/
NPDES	National Pollutant Discharge Elimination System
OECA	EPA Office of Enforcement and Compliance Assurance http://www.epa.gov/compliance/
OEI	EPA Office of Environmental Information http://www.epa.gov/oei/
RA	Regulatory Authority. The entity responsible for administering an NPDES permit issued under the CWA.
XML	eXtensible Markup Language