Welcome to NC4 Training

Module: Application Administration

Table of Contents

Table of Figures

1 Module: Application Administration

Administration of the NC4 application is critical to the operations of the tool and must be completed before any individual can access the system. In order for the system to operate properly, many key elements must be defined and managed.

All the key elements that must be defined will be outlined in this module. The Application Administration module will familiarize you with each element and its proper definitions.

VERY IMPORTANT AND WORTHY OF YOUR CONSIDERATION:

APPLICATION CONFIGURATIONS IMPLEMENTED USING THIS MODULE HAVE A SYSTEM WIDE IMPACT. AS A RESULT, PLEASE BE MINDFUL THAT THE CHANGES REFLECT YOUR OPERATIONS STRATEGIC GUIDELINES. IT IS MANDATORY THAT YOU DESIGNATE A PRIMARY INDIVIDUAL TO EFFECT THE CHANGES AND A SECONDARY PERSON AS A BACK UP.

2 General Overview

This section of the module provides an overview of Application Administration's key elements. Readers of this module will learn to create and view each of the elements, and then perform them during selected practice exercises provided at the end of the section.

The Application Administration reports are accessed by viewing the **Full Menu** to select the Administration section.

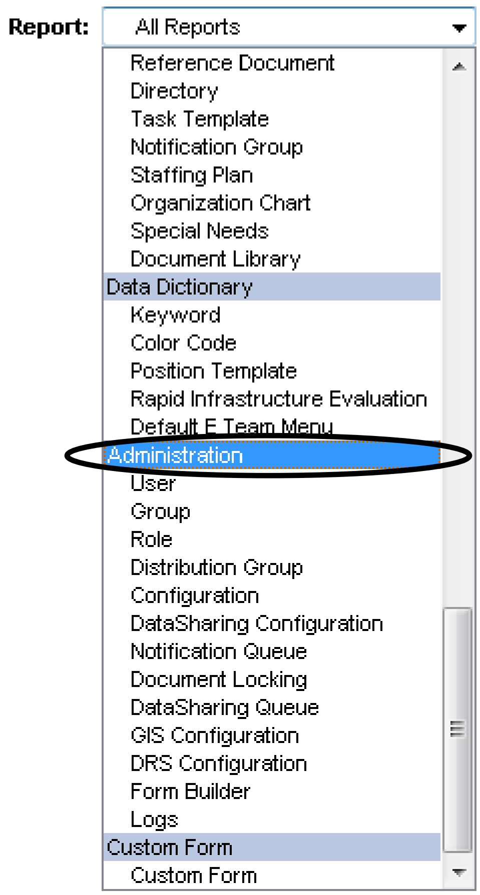


Figure 1 Locating Application Administration

The **Application Administration** module will discuss each of the following Reports as shown in Figure 1.

- User
- Group
- Role
- Distribution Group
- Configuration
- Data Sharing Configuration
- Notification Queue
- Documentation Locking
- DataSharing Queue
- GIS Configuration
- DRS Configuration
- Logs

3 Users

The Application Administration team must define the individuals or "users" that will be utilizing the NC4 Application. Users must be provided with a log in and password and given privileges to reports and features by being added to groups.

This section of the module provides an overview of the User section's key highlights. You will become familiar with the layout of the **User Administration** form and understand how to enter, modify, delete, and view users.

Learning Objectives

After completing this section, you will be able to:

- Create, edit, and delete a User.
- Associate a User with a Group.

3.1 Creating, Editing, and Deleting Users

3.1.1 Creating Users

The following steps describe the process of creating a new user by completing the information required in the **User Administration** form, as shown in Figure 2 and Figure 3.

Step 1: Select **User** from the **Report** navigation drop down menu.

Step 2: Click the **Create** button in the **User by Name** summary screen.

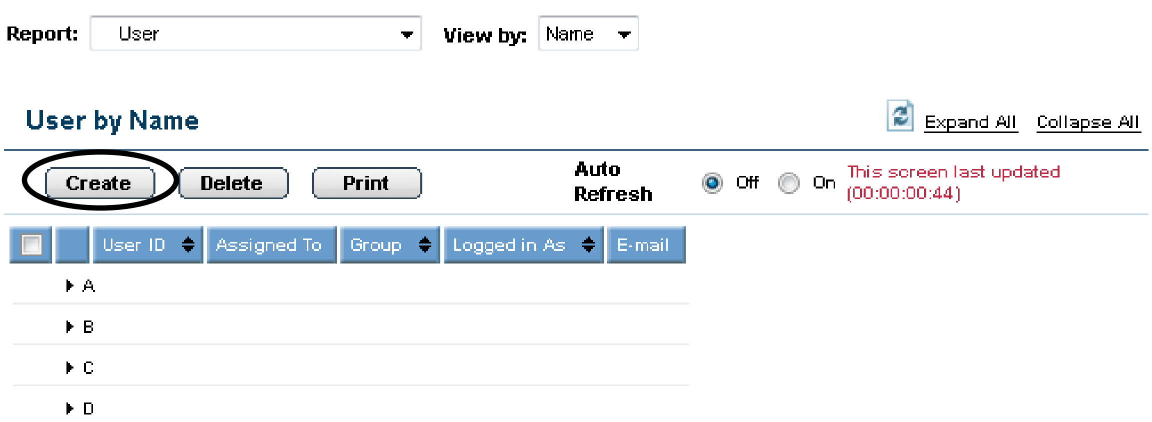


Figure 2 Users by Name Summary Screen

Step 3: Enter a **Login ID** for the new user in the **User Administration** form, as shown in Figure 3. Note: It is recommended that when assigning Login IDs and using names of personnel, that you enter the first initial and last name which will make it easier to locate users when using the **User by Name** or **User Administration** forms.

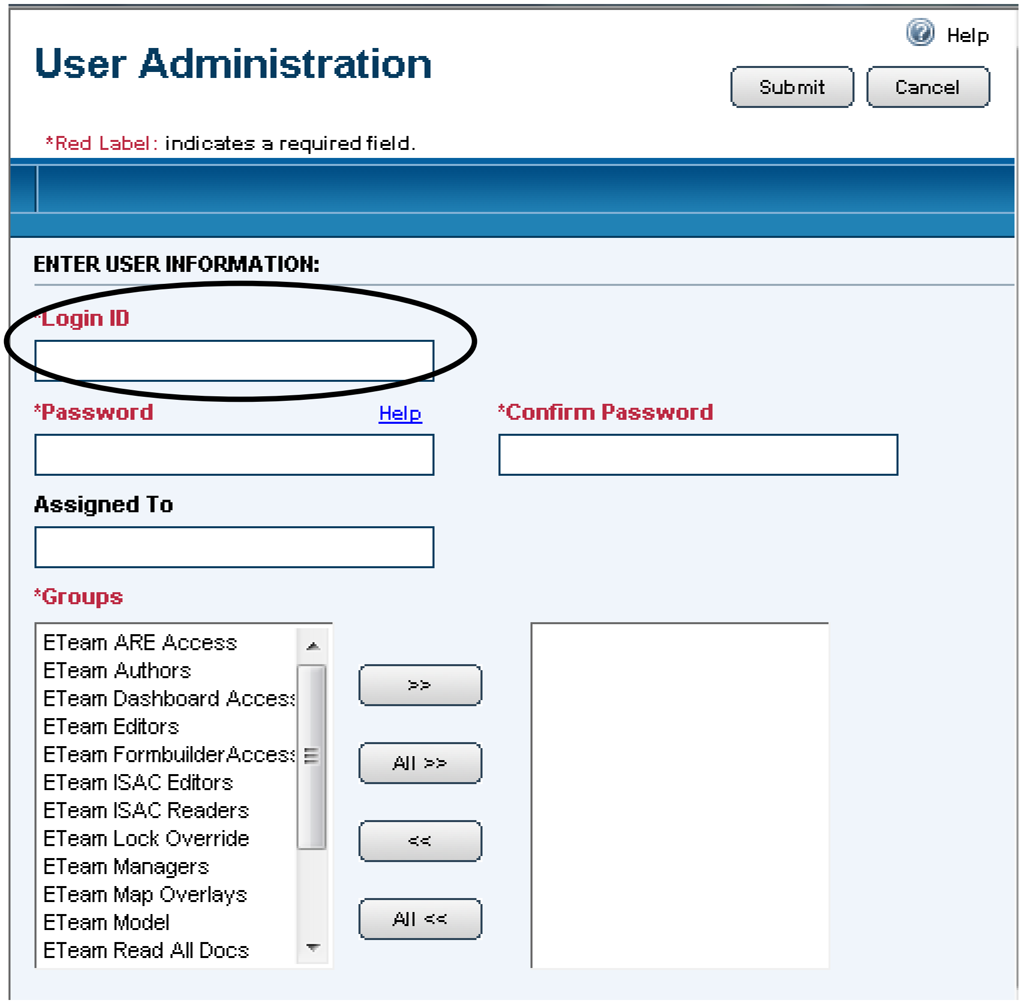


Figure 3 User Administration Form in *Create* Mode

Step 4: Enter the password in both the **Password** and **Confirm Password** fields. The password MUST be a minimum of 6 and a maximum of 20 characters. The password cannot be the same as the Login ID.

Step 5: Enter the name of the individual to whom this login and password will be assigned in the **Assigned To** field.

Step 6: Highlight a **Group(s)** in the left window by clicking on the selection. To make multiple selections, hold the control key and click each selection. This will highlight each selection. To understand the level of access associated with each group, please refer to Section 4 **Groups**.

Click the >> button to move the selected group(s) to the right box to assign the user to the group(s). In order to assign the user to all groups, click the All >> button. Assigning the user to all groups is not recommended.

In order to remove the user from a group(s), highlight the group(s) in the box on the right and click the << button or the All << button to remove the user from all groups.

Step 7: Click the **Submit** button to save the newly created user.

Step 8: View the newly created user in the **User Administration** form as shown in Figure 4.

3.1.2 Editing Users

An existing user's information can be edited at any time. Select a user from the **Users by Name** listing as shown in Figure 2. All data input for the selected user will be displayed in the **User Administration** form as shown in Figure 4. Click the Update button to modify the data on the existing user.

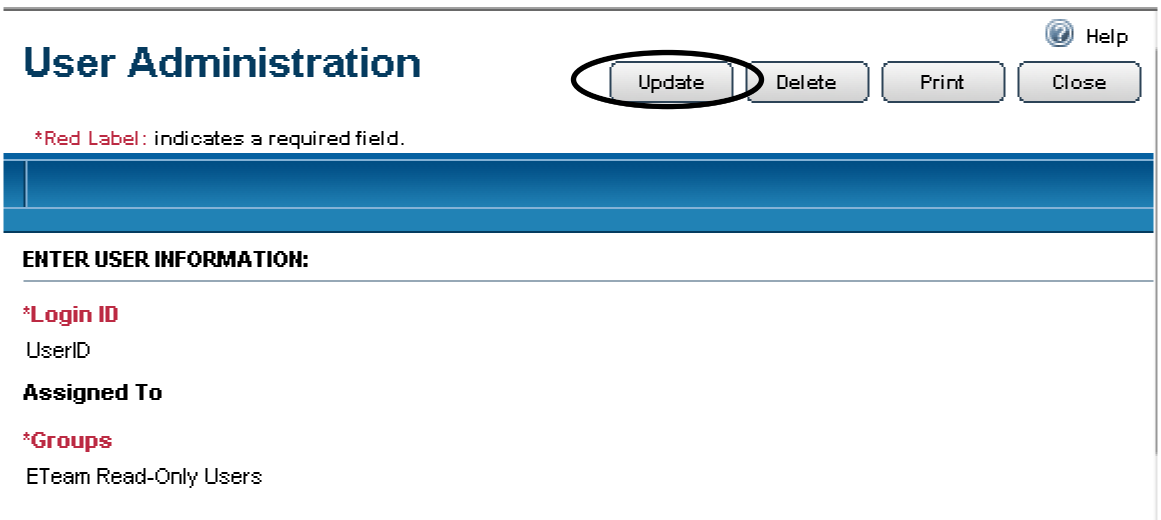


Figure 4 User Administration Form in *View* mode

The data can be modified as needed in the **User Administration** form as shown in Figure 5 then click the Submit button in the upper right corner. All data will be saved and the modified data will now be displayed in the **User Administration** form.

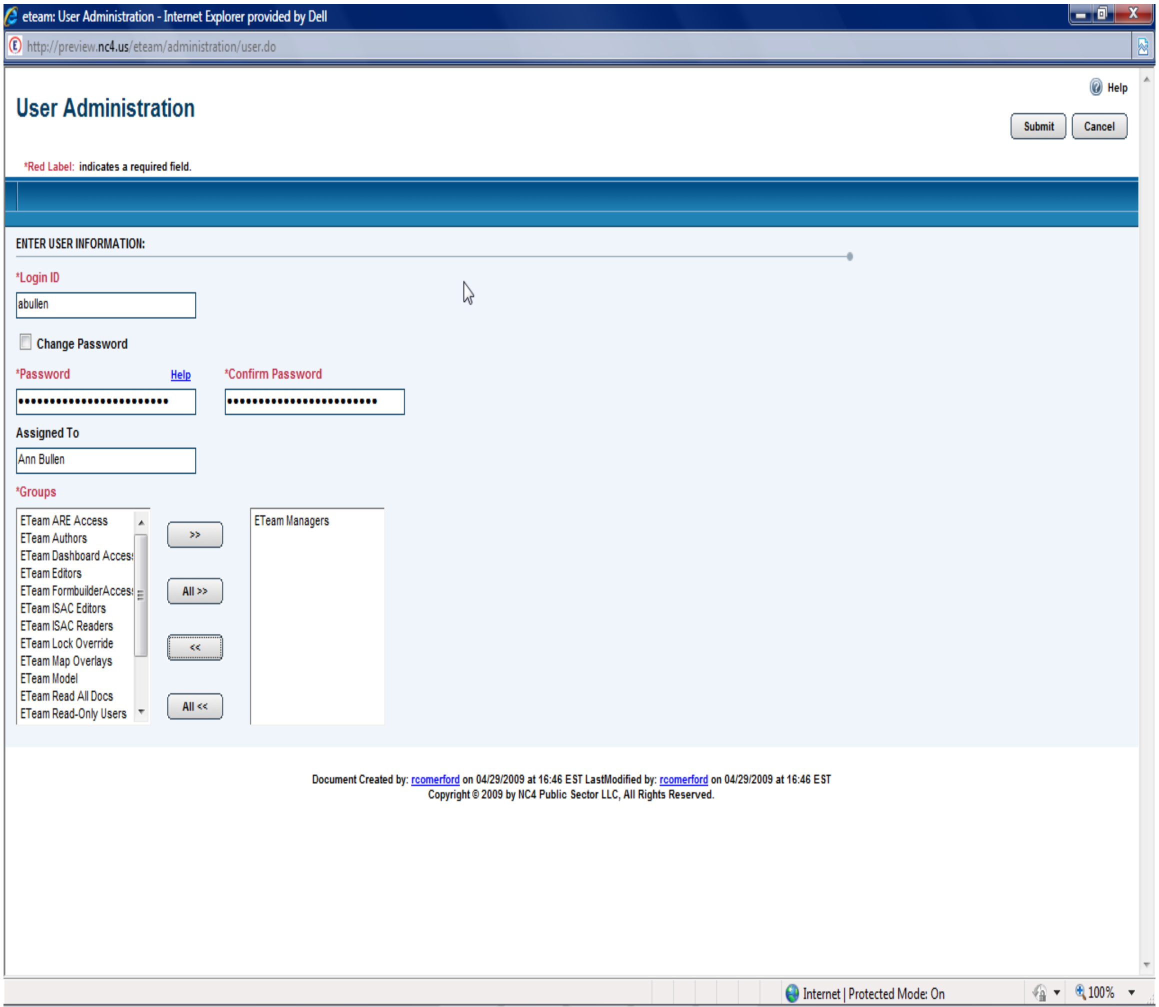


Figure 5 User Administration Form – Edit mode

3.1.3 Deleting Users

An existing user can be deleted at any time. Select the user from the listing as shown in the **Users by Name** form as shown in Figure 2. The user's information will be displayed in the **User Administration** form shown in Figure 6.

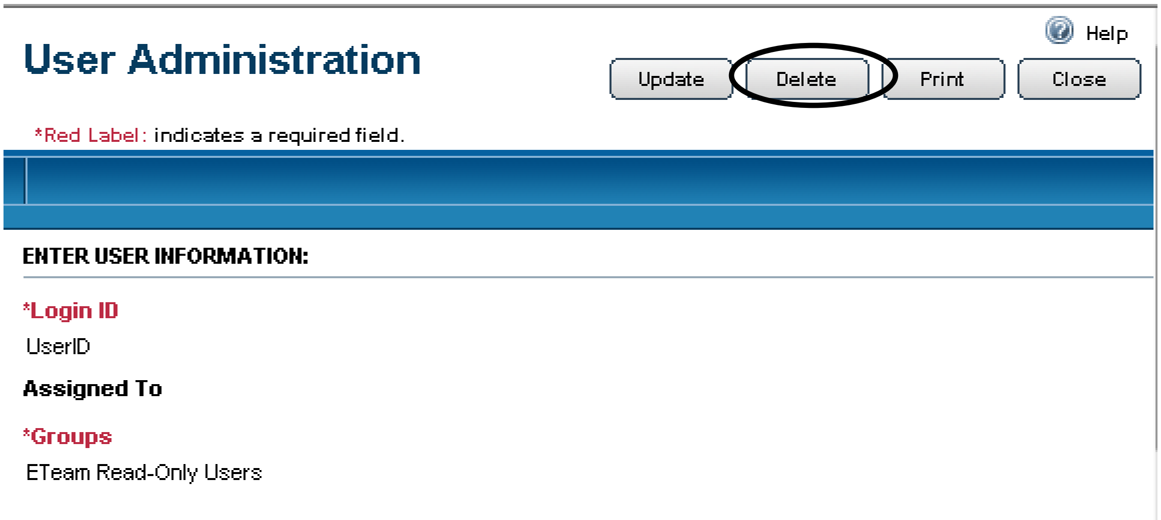


Figure 6 User Administration Form – Delete button

Click the 

button in the top right corner of the form. Once the deletion has been completed, a confirmation message will be displayed on the screen.

3.2 Viewing Existing Users

As we have seen in the previous section in Figure 2, the default view is governed by the sorting techniques. For existing users, the view is sorted by **"Name"** or **Login ID**. However, existing users can also be sorted by **"Group".** As shown in Figure 7, a **View by** drop down menu is available next to the **Report: User** which displays all sorting techniques for the report which in **User** are **"Name" and "Group"**.

In order to change the view for existing users, click **"Group"** from the **View by** drop down menu as shown in Figure 7.

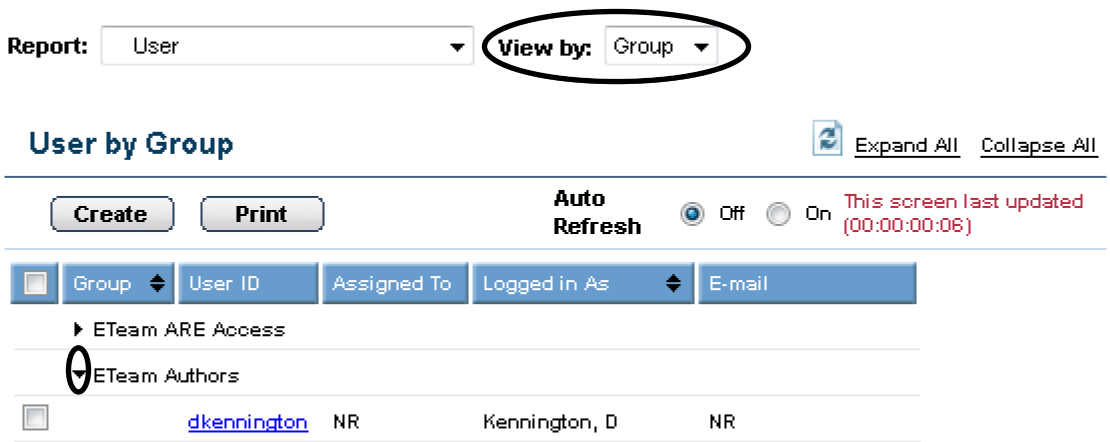


Figure 7 Users by Group

In order to view the existing users under each Group, click the button to the left of the **Group** name as shown in Figure 7.

Groups are covered in more detail in Section 4 of this module.

4 Groups

Groups establish which roles and privileges the user will have when working with the NC4 Application. Roles are associated with Groups, and the Groups in turn are associated to a User. Groups are based on logical groupings of users who need to perform similar tasks or functions. By grouping these functions, administration requirements in maintaining the application are greatly reduced.

The NC4 Application assists its clients by predetermining the logical groups that most individuals would enact as parts of the team. The predetermined groups that cannot edited are identified in Appendix A. However, if a need for a new group is determined, the system is flexible enough to add as many as desired.

Learning Objectives

After completing this section, you will be able to:

- Create, edit, and delete a Group.
- Associate a User(s) to a Group.

This section of the module will provide an overview of Group key highlights. You will become familiar with the layout of the **Group Administration** form and understand how to enter, modify, delete, and view groups.

4.1 Creating, Editing, and Deleting Groups

Before creating a new group, please refer to the groupings that are included in the system. The description and access of each group is defined in Appendix A: Groups. This section will discuss how new groups can be created if needed for your organization.

4.1.1 Creating Groups

The following steps describe creating a new group by completing the information required in the **Group Administration** form, as shown in Figure 8 and Figure 9.

Step 1: Select **Group** from the **Report** navigation drop down menu.

Step 2: Click the **Create** button as shown in Figure 8.

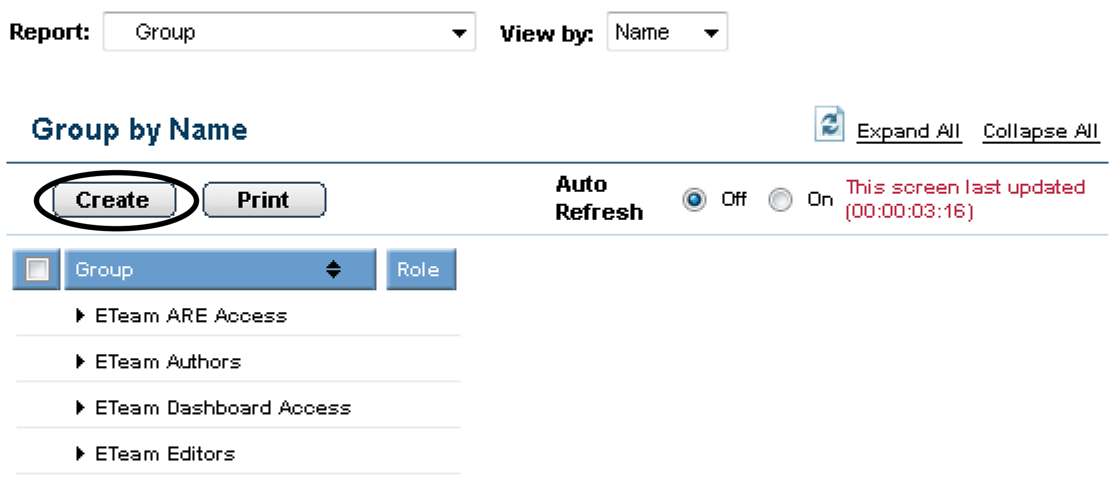


Figure 8 Locating Group by Name

A new **Group by Name** form opens as shown in Figure 9.

Step 3: Enter a distinct **Group Name** for the new group in the required field on **Group Administration** form, as shown in Figure 9.

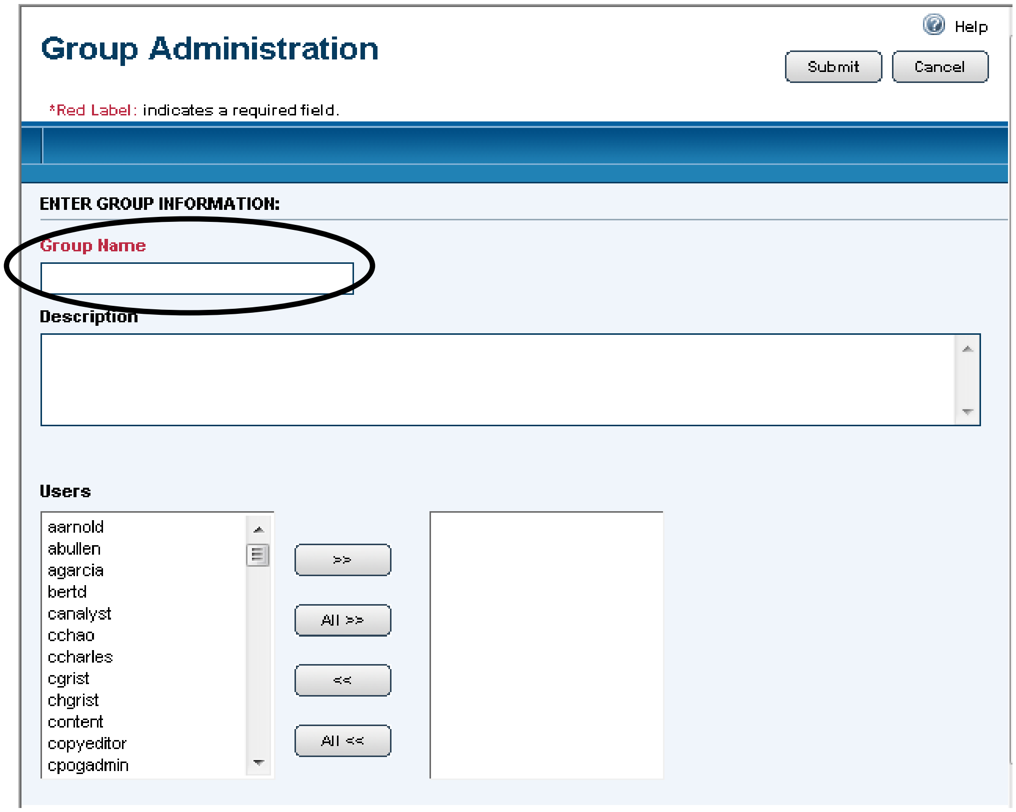


Figure 9 Group Administration Form in *Create* Mode

Step 4: Enter a **Description** for the new group in the required field.

Step 5: Highlight the **user(s)** and click the button to move the selected user(s) to the **right box** to assign the user(s) to the group. In order to assign all users to a group, click the button.

In order to remove the user(s) from a group, highlight the **user(s)** in the box on the right and click the button or the button to remove the user(s) from the group.

Step 6: Click the **Submit** button in the upper right to save the newly created group.

Step 7: View the newly created group in the **Group Administration** form as shown in Figure 10.

4.1.2 Editing Groups

You can only edit groups that you have created, such as Dashboard and Form Builder Access. Locate the **Groups by Name** listing as shown in Figure 8.

Click the button to the left of the **Group** name to review all the **Role** Name links for the selected group. Click the appropriate **Role** Name link and all current data for the selected **Group** will be displayed in the **Group Administration** form as shown in Figure 10.

If you can modify the group, the button will be available for you to click as shown below.

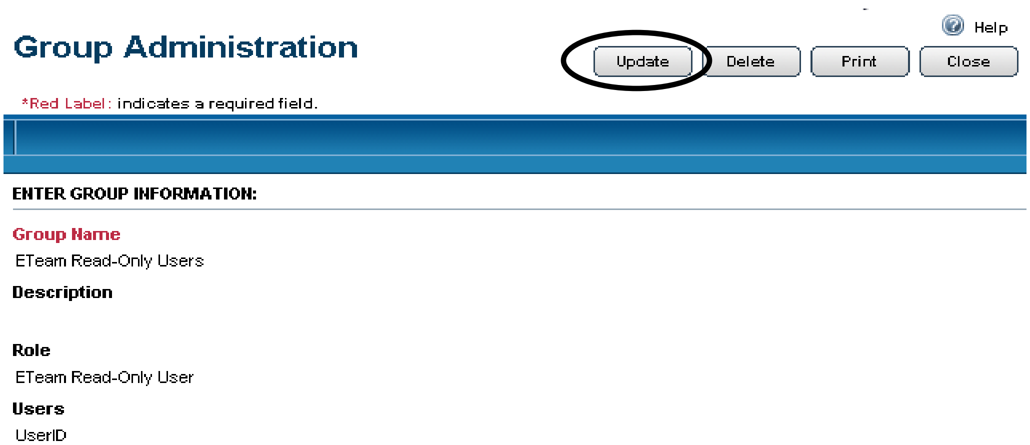


Figure 10 Group Administration Form in *View* mode

The **Group Administration** form will display in *Edit* mode and the data can be modified as needed. When you have completed the changes, click the button in the upper right corner of the form as shown in Figure 9. All data will be saved and the modified data will now be displayed in the **Group Administration** form in *View* mode.

4.1.3 Deleting Groups

You can only delete groups that you have created. The default groups that were supplied with the application do not contain a **Delete** button for the user to modify. An existing group that you created can be deleted at any time. Select the group from the listing as shown in the **Groups by Name** form. The group's information will be displayed in the **Group Administration** form. Click the button in the top right corner of the form. Once the deletion has been completed, a confirmation message will be shown on the screen.

4.2 Viewing Existing Groups

You can only edit groups that you have created. The default groups that were supplied with the application do not contain an Update button for the user to modify the group. As we have seen in Figure 8, **Group by Name**, the default view is governed by the sorting techniques. For existing groups, the view is sorted by "Name". However, existing groups can also be sorted by "Role". As shown in Figure 11, a **View by** drop down menu is available next to the **Group** report which displays sorting techniques for the report which are **"Name", "Role", and "History"**.

In order to change the view for existing users, select **"Role"** in the **View by** drop down menu as shown in Figure 11.

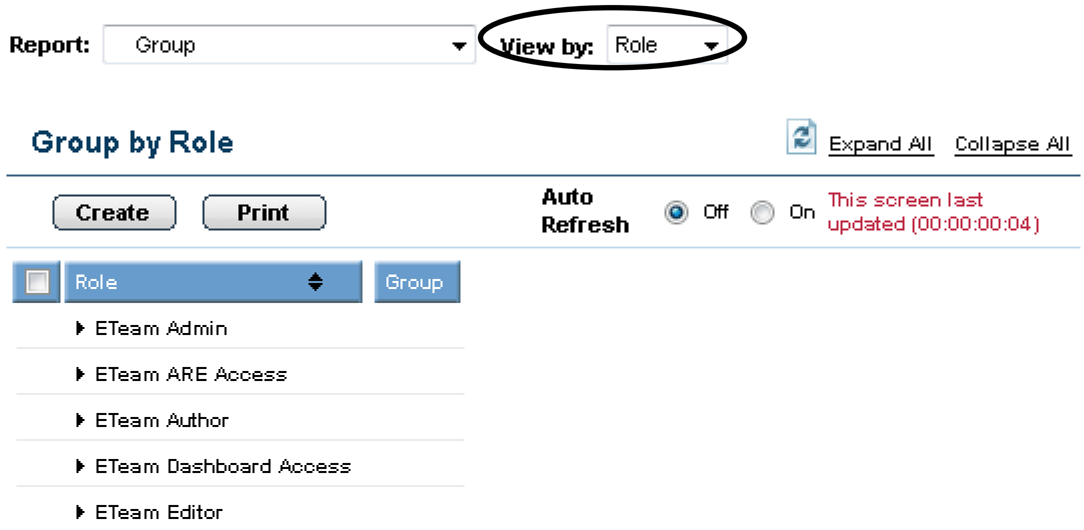


Figure 11 Groups by Role

In order to view the existing **Groups** under each **Role,** click the ▸ icon to the left of the **Role** name as shown in Figure 11.

Roles are covered in more detail in Section 5 of this module.

5 Roles and Privileges

Once the users of the system have been defined, it is time to determine the level of access each user has to the system. The NC4 Application has been delivered with pre-defined levels of access or privileges to specific reports and features. These privileges are then associated to a role.

The NC4 Application assists its clients by predetermining the roles that most individuals would enact as parts of the team. The predetermined roles and corresponding privileges are identified under Appendix B: Roles; Appendix C: Privileges. This organization of roles allows system participants to utilize the system quickly and understand the boundaries of their particular role. However, if a need for a new role is determined, the system is flexible enough to add as many as desired.

Learning Objectives

After completing this section, you will be able to:

- Create, edit, and delete a Role.
- Associate a Privilege to a Role.

This section of the module will provide an overview of **Role** and **Privilege** key highlights. You will become familiar with the layout of the **Role Administration** form and understand how to create, modify, delete, and view roles and privileges.

5.1 Creating, Editing, and Deleting Roles

Before creating a new role, please refer to the groups, roles and privileges that have been installed with the system. These can be found in a matrix in Appendix A: Groups, Appendix B: Roles and Appendix C: Privileges. This section will discuss how new roles can be created if needed for your organization.

5.1.1 Creating Roles

The following steps describe creating a new role by completing the information required in the **Role Administration** form, as shown in Figure 12 and Figure 13.

Step 1: Select **Role** from the **Report** navigation drop down menu.

Step 2: Click the **Create** button as shown in Figure 12.

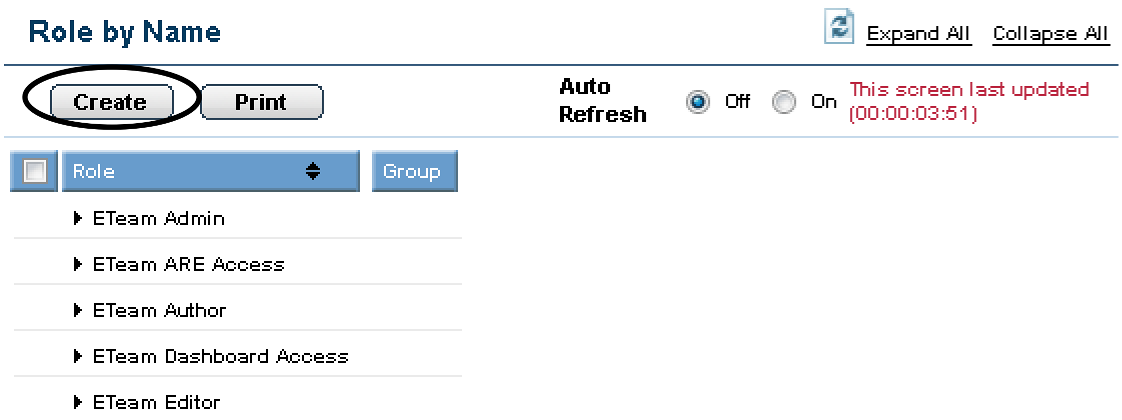


Figure 12 Role by Name

You will be presented with a Role **Administration** form as shown in Figure 13.

Step 3: Enter a distinct **Role Name** for the new role in the **Role Administration** form, as shown in Figure 13.

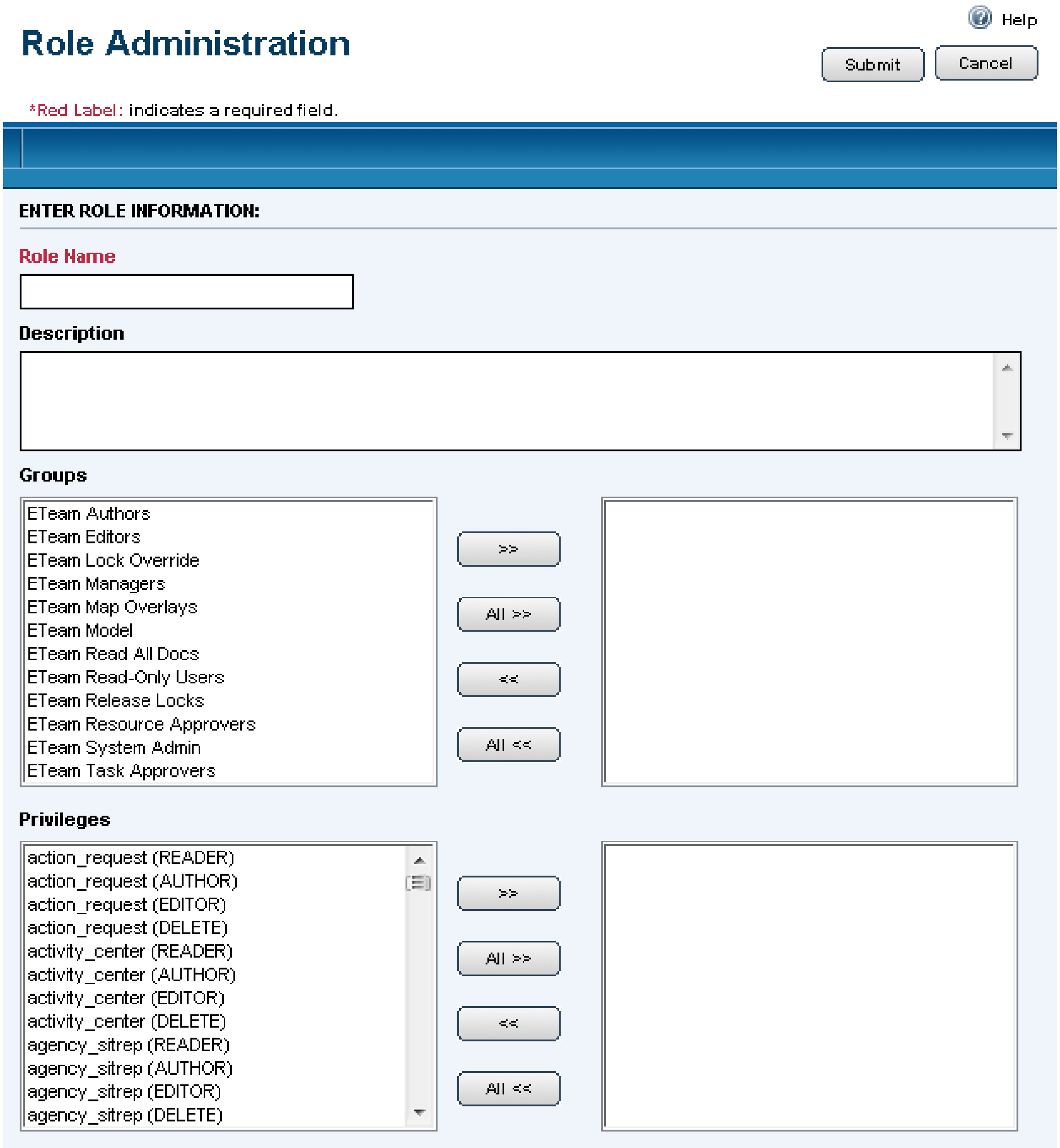


Figure 13 Role and Privileges Administration Form

Step 4: Enter a **Description** for the new role.

Step 5: Highlight a group in the left window by clicking the selection. Click the >> button to move the selected group(s) to the right box to assign the group(s) to the role. In order to assign all the groups to a role, click the All >> button.

In order to remove the group(s) from a role, highlight the group(s) in the box on the right and click the << button or the All << button to remove the group(s) from the role.

Step 6: Highlight a Privilege(s) in the left window by clicking on the selection. To make multiple selections, hold the control key and click each selection. This will highlight each selection.

Click the >> button to move the selected privilege(s) to the right box to assign the privilege(s) to the role. In order to assign all the privileges to a role, click the All >> button.

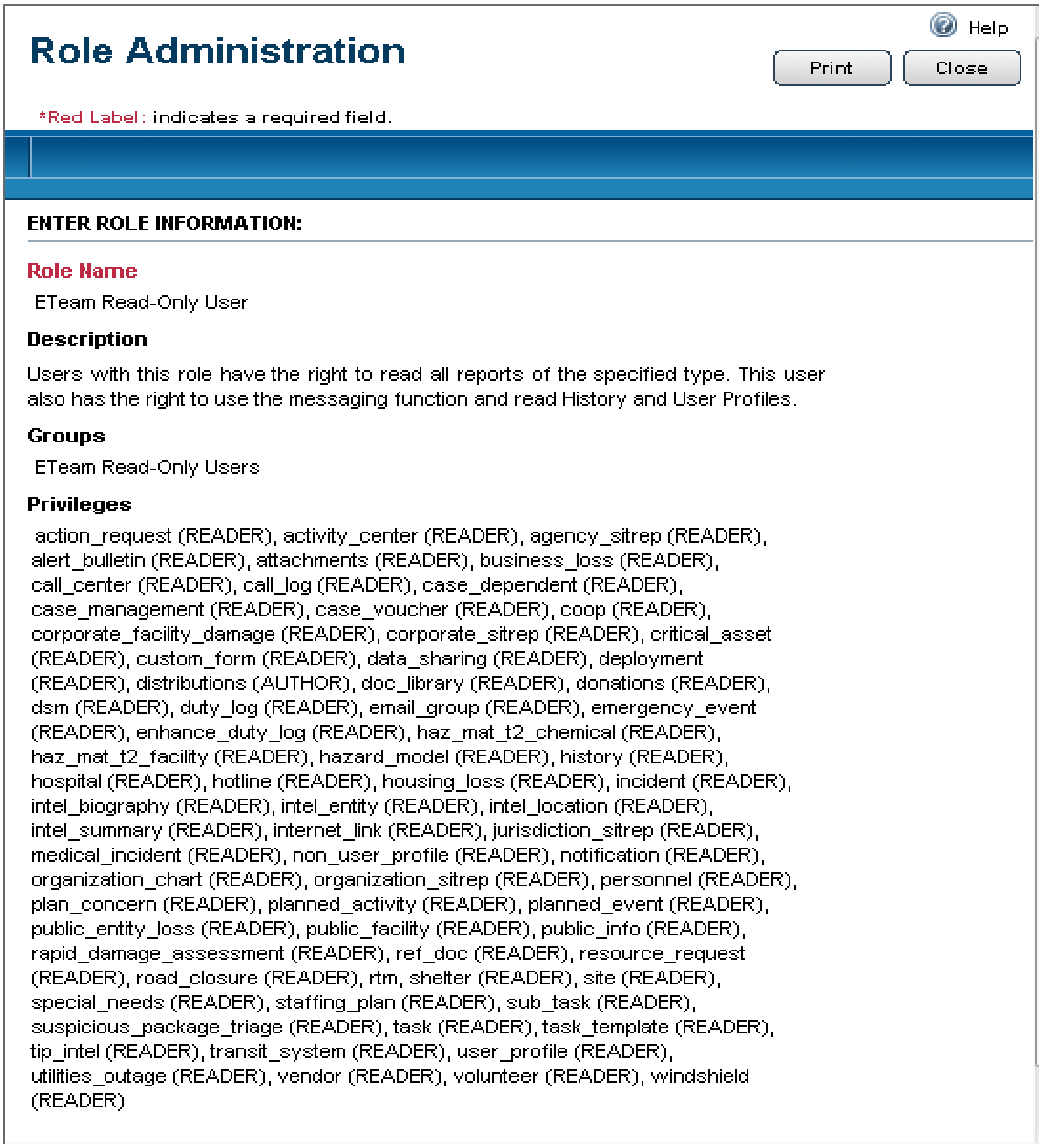
In order to remove the privilege(s) from the role, highlight the privilege(s) in the box on the right and click the << button or the All << button to remove the privilege from the role. For additional information on Privileges, please refer to Appendix C: Privileges.

Step 7: Click the **Submit** button to save the newly created role along with the associated privileges.

Step 8: View the newly created role in the **Role Administration** form as shown in Figure 14.

5.1.2 Editing Roles

You can only edit roles that you have created. Select a role from the **Roles by Name** listing, by clicking the Name link in the **Group** column. All current data for the selected role will be displayed in the **Role Administration** form as shown in Figure 14. In order to modify the data, click the Update button.



Role Administration

Help

Print Close

*Red Label: indicates a required field.

ENTER ROLE INFORMATION:

Role Name

ETeam Read-Only User

Description

Users with this role have the right to read all reports of the specified type. This user also has the right to use the messaging function and read History and User Profiles.

Groups

ETeam Read-Only Users

Privileges

action_request (READER), activity_center (READER), agency_sitrep (READER), alert_bulletin (READER), attachments (READER), business_loss (READER), call_center (READER), call_log (READER), case_dependent (READER), case_management (READER), case_voucher (READER), coop (READER), corporate_facility_damage (READER), corporate_sitrep (READER), critical_asset (READER), custom_form (READER), data_sharing (READER), deployment (READER), distributions (AUTHOR), doc_library (READER), donations (READER), dsm (READER), duty_log (READER), email_group (READER), emergency_event (READER), enhance_duty_log (READER), haz_mat_t2_chemical (READER), haz_mat_t2_facility (READER), hazard_model (READER), history (READER), hospital (READER), hotline (READER), housing_loss (READER), incident (READER), intel_biography (READER), intel_entity (READER), intel_location (READER), intel_summary (READER), internet_link (READER), jurisdiction_sitrep (READER), medical_incident (READER), non_user_profile (READER), notification (READER), organization_chart (READER), organization_sitrep (READER), personnel (READER), plan_concern (READER), planned_activity (READER), planned_event (READER), public_entity_loss (READER), public_facility (READER), public_info (READER), rapid_damage_assessment (READER), ref_doc (READER), resource_request (READER), road_closure (READER), rtm, shelter (READER), site (READER), special_needs (READER), staffing_plan (READER), sub_task (READER), suspicious_package_triage (READER), task (READER), task_template (READER), tip_intel (READER), transit_system (READER), user_profile (READER), utilities_outage (READER), vendor (READER), volunteer (READER), windshield (READER)

Figure 14 Role Administration Form in *View* mode

The **Role Administration** form will display and the data can be modified as needed.

When you have completed the changes, click the Submit button in the upper right corner of the form as shown in Figure 13. All data will be saved and the modified data will now be displayed in the Role Administration form.

5.1.3 Deleting Roles

An existing role can be deleted at any time, if there is a **Delete** button. Select the role from the listing as shown in the **Roles by Name** form. The role's information will be displayed in **the Role Administration** form. Click the Delete button in the top right corner of the form. Once the deletion has been completed, a confirmation message will be shown on the screen.

5.2 Viewing Existing Roles

The default view is governed by the sorting techniques. For existing roles, the view is sorted by **Name**. However, existing roles can also be sorted by **Group**. As shown in Figure 15, a **View by** drop down menu is available next to the **Role** report which displays all sorting techniques for the report which are **"Name", "Group", and "History**".

In order to change the view for existing roles, click **"Group"** in the **View by** drop down menu as shown in Figure 15.

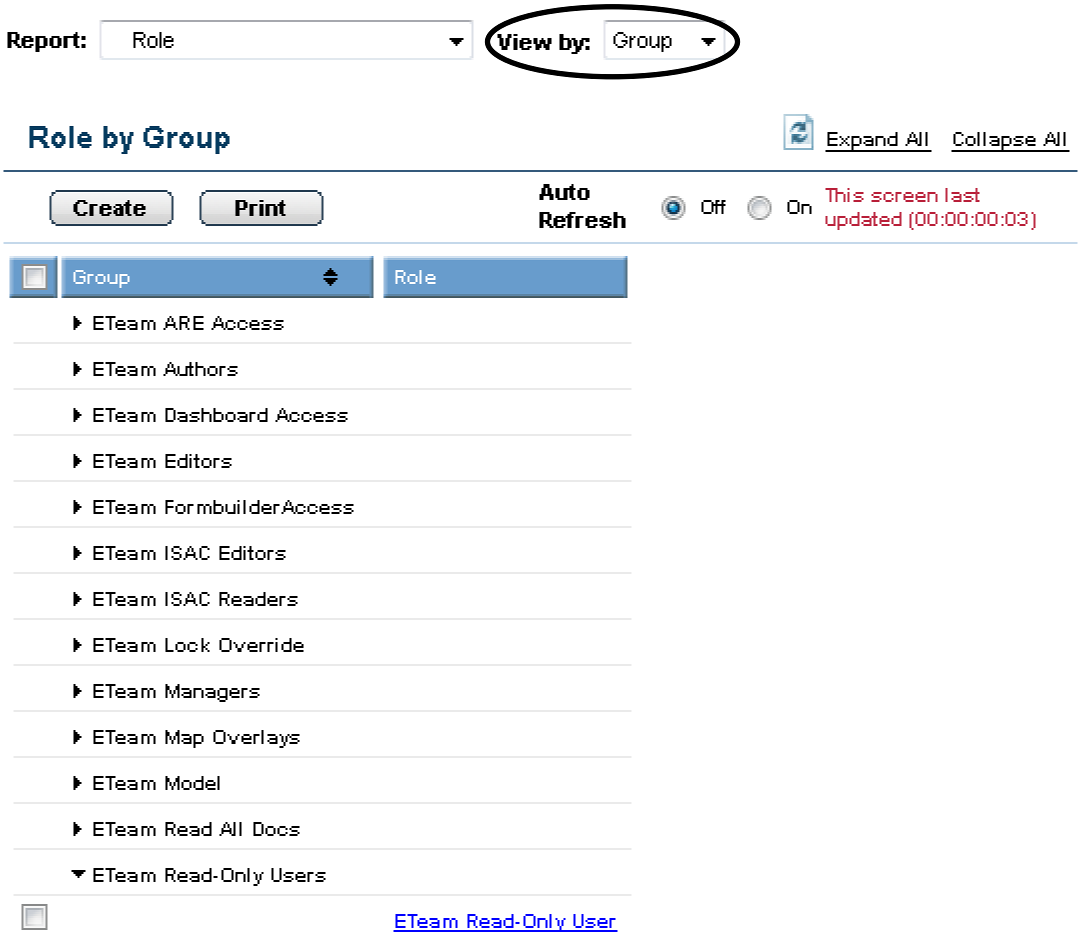


Figure 15 Roles by Group

In order to view the existing Roles within each Group, click the ▸ icon to the left of the **Group** name as shown in Figure 15.

6 Distribution Groups

Distribution Groups create the ability to limit access to system information on a user-by-user basis in a networked environment.

All reports generated within the system modules are viewable by all users. In order to partition the viewing of these reports, each module utilizes the Distribution and Sharing Tab at the top of the form or within a section of the form to specify which Distribution Groups, Individual Users, or Organizations outside the system will have access to the reports. This section will detail the creation of Distribution Groups that can be utilized for this purpose.

Distribution Groups are created for use by the organization as needed. There are no predefined Distribution Groups included in the system.

Learning Objectives

After completing this section, you will be able to:

- Create, edit, and delete a Distribution Group.
- Associate a User(s) or Group(s) to a Distribution Group.

This section of the module will provide an overview of **Distribution Group** key highlights. You will become familiar with the layout of the **Distribution Group Administration** form and understand how to create, modify, delete, and view distribution groups.

6.1 Creating, Editing, and Deleting Distribution Groups

6.1.1 Creating Distribution Groups

Step 1: Select **Distribution Group** from the **Report** navigation drop down menu.

Step 2: Click the **Create** button as shown in Figure 16.

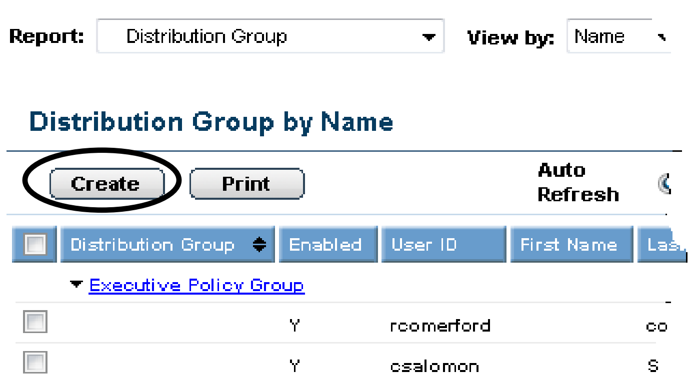


Figure 16 Distribution Group by Name

Step 3: Enter a distinct **Distribution Group Name** for the new group in the corresponding field, as shown in Figure 17.

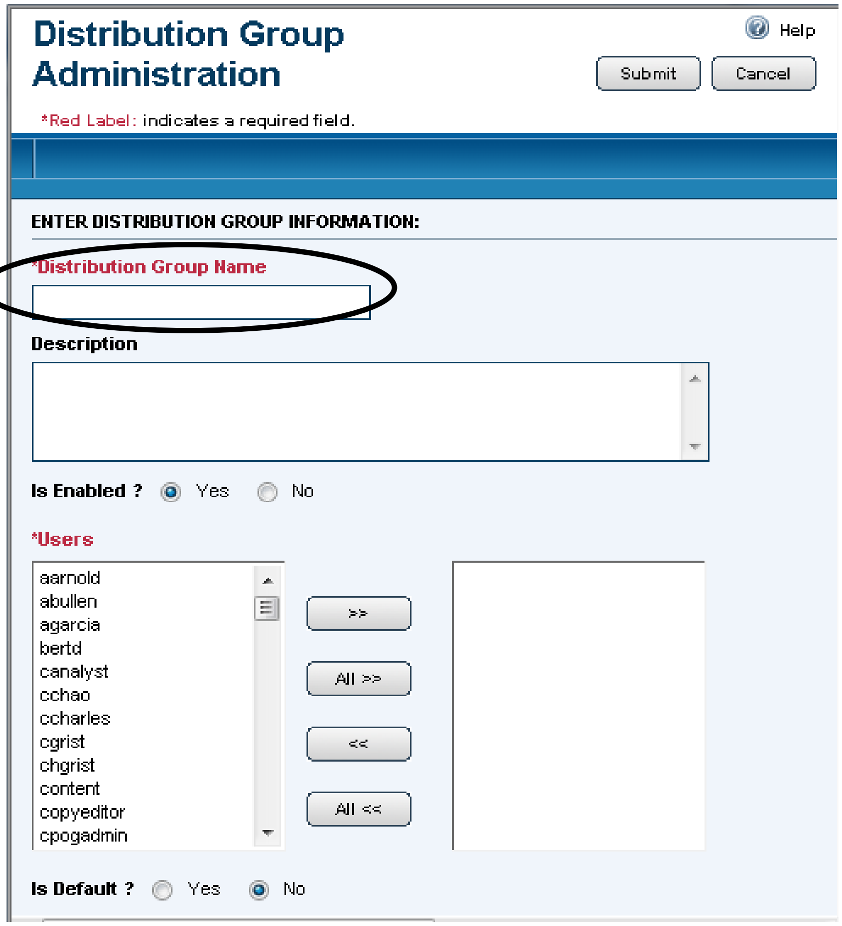


Figure 17 Distribution Group Administration Form in *Create* mode

Step 4: Enter a **Description** for the new Distribution Group.

Step 5: Click the **"Yes"** radio button for **"Is Enabled?"** if you intend for this **Distribution Group** to be displayed for selection on any system reports. If **"No"** is selected, the **Distribution Group** will not be displayed for selection on any system reports.

Step 6: Click the 

button to move the selected user(s) to the right box to assign the user(s) to the group. In order to assign all users to a group, click the 

button.

In order to remove the user(s) from a group, highlight the user(s) in the box on the right and click the << button or the All << button to remove the user(s) from the group.

Step 7: Click the **"Yes"** radio button for "**Is Default?"** if you intend for the reports to be displayed only to those within this Group. If **"No"** is selected, all the users activity will be displayed for everyone to view. Selecting No is the preferred selection.

Step 8: Click the **Submit** button to save the newly created **Distribution Group**.

Step 9: View the newly created group in the **Distribution Group Administration** form as shown in Figure 18.

Step 10: Once the **Distribution Group** has been created, you will be able select the **Distribution Group** from any of the "**Distribution and Sharing**" tabs or sections.

6.1.2 Editing Distribution Groups

Existing distribution groups can be edited at any time. Select a group from the **Distribution Groups by Name** listing as shown in Figure 16. All current data for the selected group will be displayed in the **Distribution Group Administration** form as shown in Figure 18. In order to modify the data, click the Update button as shown below.

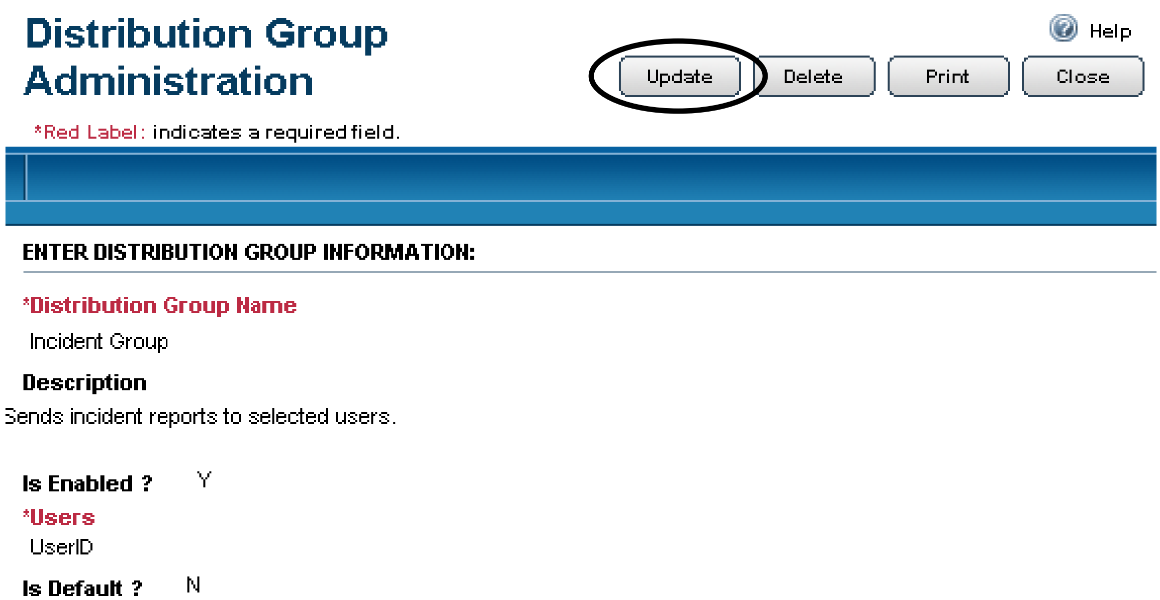


Figure 18 Distribution Group Administration Form in *View* mode

The **Distribution Group Administration** form will display, and the data can be modified as needed. When you have completed the changes, click the Submit button in the upper right corner of the form as shown in Figure 17. All data will be saved and the modified data will now be displayed in the **Distribution Group Administration** form.

6.1.3 Deleting Distribution Groups

An existing Distribution Group can be deleted at any time. Select the group from the listing as shown in the **Distribution Groups by Name** form. The group's information will be displayed in the **Distribution Group Administration** form. Click the Delete button in the top right corner of the form. Once the deletion has been completed, a confirmation message will be shown on the screen.

6.2 Viewing Existing Distribution Groups

The sorting path for viewing existing **Distribution Groups** is by **"Name"** as in Figure 16 and **"History"** as shown in Figure 19.

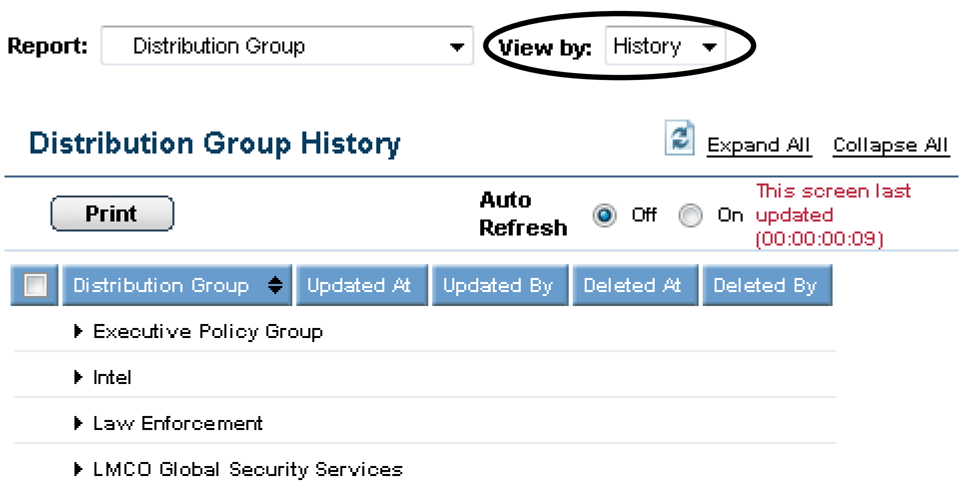


Figure 19 Distribution Groups by History

7 Configuration

The Application consists of four (4) system configuration documents. General Configuration is first discussed in this document. The information detailed in this configuration is critical to the use and maintenance of the system.

This section of the module will provide an overview of **General Configuration** key highlights. The information that is populated in the fields within this section will also be used in the **Data Sharing Configuration** section. You will become familiar with the layout of the **General Configuration** form and understand how to modify it.

Learning Objectives

After completing this section, you will be able to:

- Edit the General Configuration.

7.1 Viewing and Editing the General Configuration

7.1.1 Viewing the General Configuration

Created during the installation process, the **General Configuration** is comprised of system settings and preferences that are specific to the local organization. The **General Configuration** logs settings and preferences are on four tabs; **Basic Info, Additional Info, Mail Server, and Agent**. Details for each of the tabs can be viewed in Figure 22, Figure 23,Figure 24, Figure 25, Figure 26, Figure 27, Figure 28, Figure 29 and Figure 30.
In order to view the **General Configuration**, follow the steps below.

Step 1: Select **Configuration** from the Report navigation drop down menu.

Step 2: Click the hyperlink to the **General Configuration** form as shown in Figure 20.

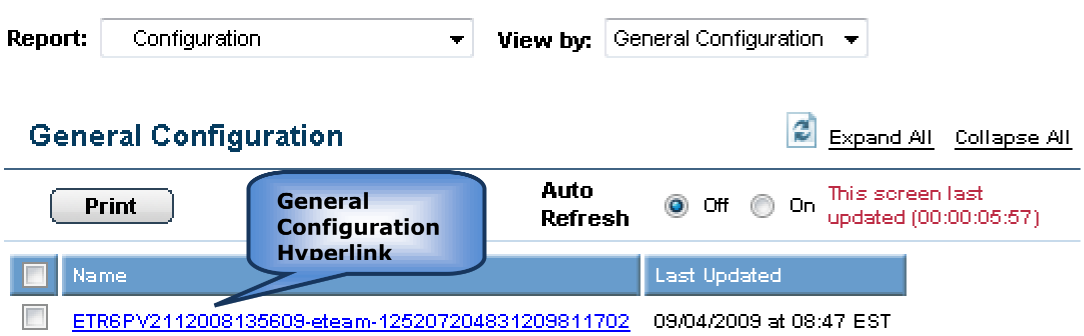
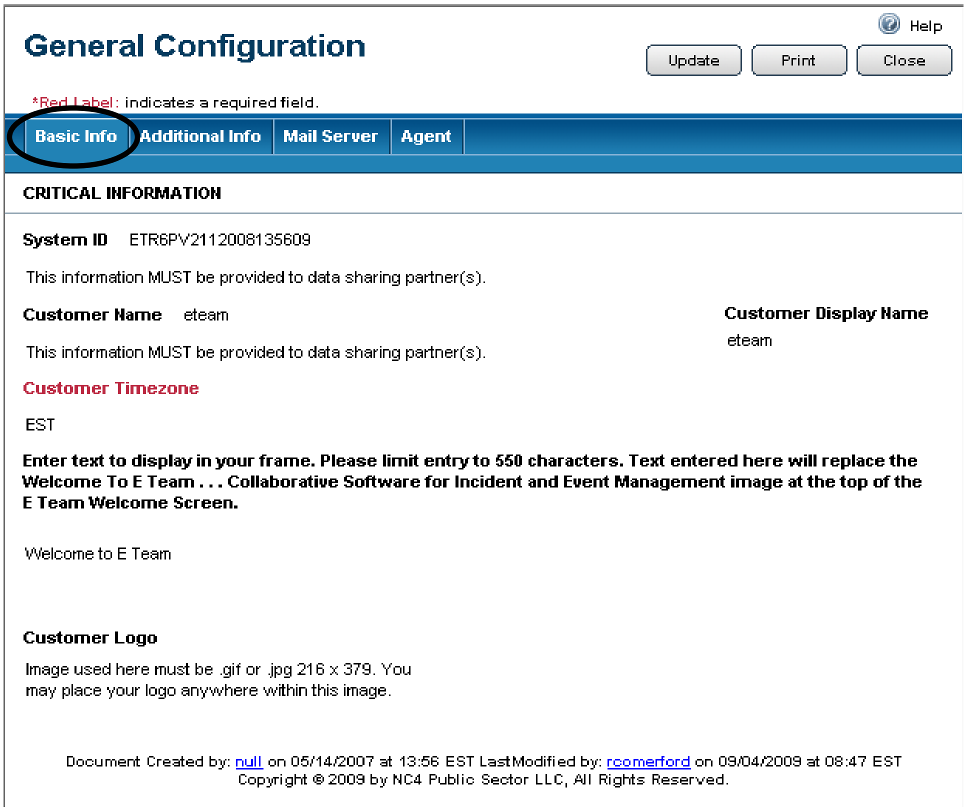


Figure 20 General Configuration Hyperlink

Step 3: The **Basic Info** tab page of the **General Configuration** form will display in the center view frame as shown in Figure 21. The remaining tab pages can be viewed by clicking the name for each tab.


General Configuration

Help

Update | Print | Close

*Red Label: indicates a required field.

Basic Info | Additional Info | Mail Server | Agent

CRITICAL INFORMATION

System ID ETR6PV2112008135609

This information MUST be provided to data sharing partner(s).

Customer Name eteam

This information MUST be provided to data sharing partner(s).

Customer Display Name

eteam

Customer Timezone

EST

Enter text to display in your frame. Please limit entry to 550 characters. Text entered here will replace the Welcome To E Team . . . Collaborative Software for Incident and Event Management image at the top of the E Team Welcome Screen.

Welcome to E Team

Customer Logo

Image used here must be .gif or .jpg 216 x 379. You may place your logo anywhere within this image.

Document Created by: null on 05/14/2007 at 13:56 EST LastModified by: rcomerford on 09/04/2009 at 08:47 EST
Copyright © 2009 by NC4 Public Sector LLC, All Rights Reserved.

Figure 21 General Configuration Form

7.1.2 Editing the General Configuration

Step 1: Select **Configuration** from the **Report** navigation drop down menu.

Step 2: Click the hyperlink to the **General Configuration** screen.

Step 3: The **General Configuration** screen will open with the **Basic Info** tab displayed as shown in Figure 21.

Step 4: Click the 

button in the upper right of the form.

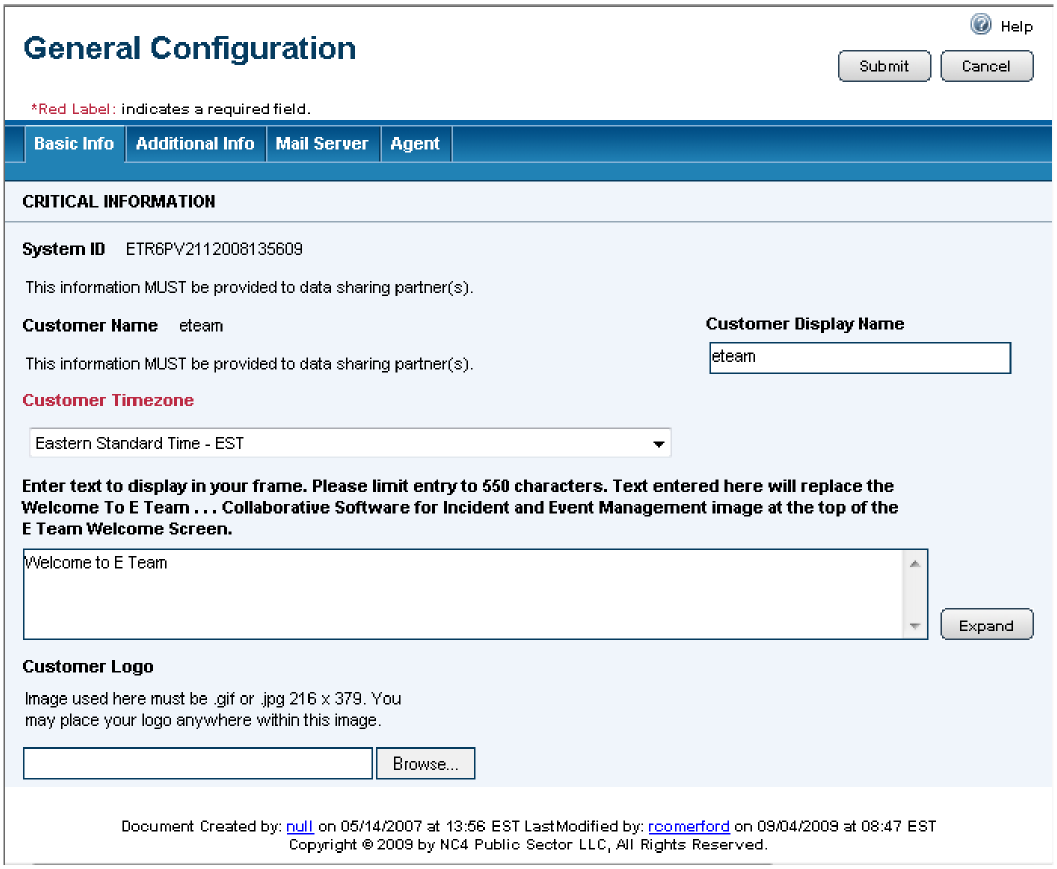
Step 5: All of the fields for the **Basic Info** tab are also defined in Figure 22. Any modifications to the data must follow the definitions outlined here.

Step 6: All of the fields for the **Additional Info** tab are defined in Figure 27. Any modifications to the data must follow the definitions outlined below.

Step7: All of the fields for the **Mail Server** tab are defined in Figure 27. Any modifications to the data must follow the definitions outlined below.

Step 8: All of the fields for the **Agent** tab are defined in Figure 29. Any modifications to the data must follow the definitions outlined below.

The output of a **Personal Profile** update request is shown in Figure 30.



Field Label	Definition
BASIC INFO TAB	
System ID	Identifies the ID given to your application during the installation process.
Customer Name	Identifies the Name given to your application during the installation process.
Customer Display Name	Type directly in the field. This is the “System” name that will appear to users at the top of the main summary screen.
Customer Time Zone	Click the arrow to display the Time Zone stamp that will be used throughout the application. The system default is PST.
Enter text to display in your frame.	Type directly in the field to create a custom Welcome Page. Use this field to include text on your Login page. See Figure 23 for an example.
Customer Logo	Click ***Browse*** to open the Choose File dialog. Used to create a custom Welcome Page. Use this field to select an image to display. See Figure 23 for an example.

Figure 22 General Configuration - Basic Info Field Label Definition

The Customer Logo and text options can be used to create a personalized **Welcome Page** to your application system. Figure 23 illustrates an example of how these two fields will look if you choose to create a custom web page.

Figure 23 Custom Webpage and Logo Example

The General Configuration-Additional Info Tab allows the user to identify several key buttons that will be displayed on the summary screen such as, the report refresh intervals, number of records per page and use of Real Time Messaging, EIM, ARE and Dashboard functionality. In addition, tracking ability relating to Password Format, and Logging activity are displayed in Figure 24.

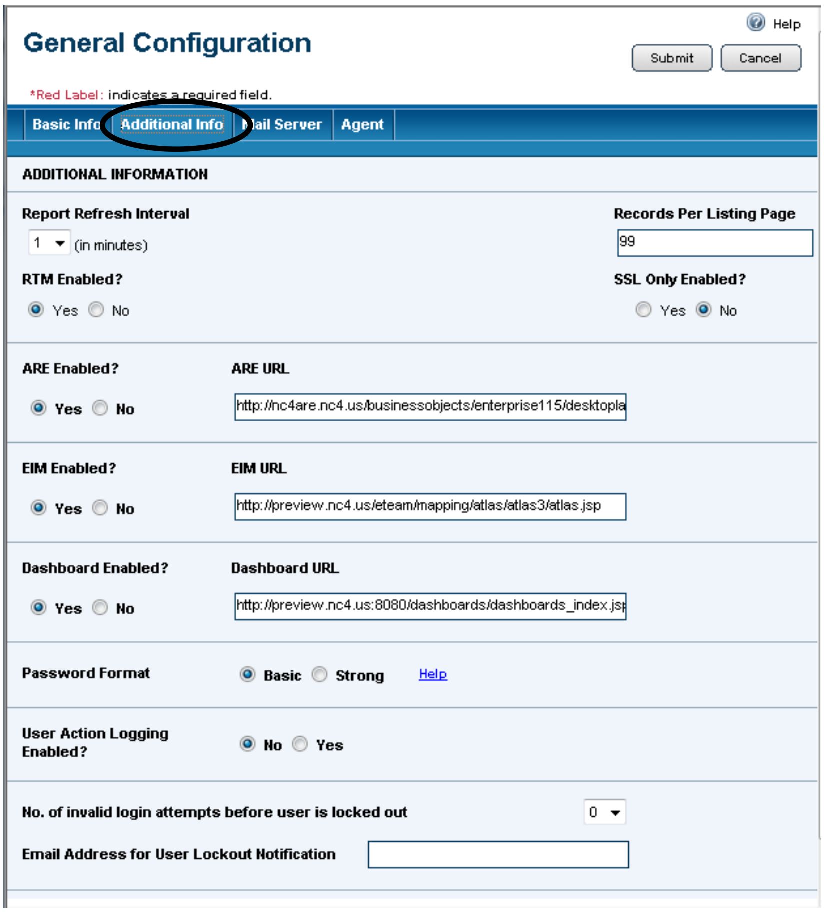


Figure 24 General Configuration – Additional Info Tab

Field Label	Definition
ADDITIONAL INFO TAB	
Report Refresh Interval	Click the arrow to establish the frequency in which views are automatically refreshed. Enter number of minutes between refresh. Valid choices are 1 thru 9. The default value is 1 minute. Note: Auto-Refresh can be turned ON or OFF by users in the Center View Frame. When ON, the NC4 application refreshes the report views at the established intervals so that the most current information is displayed. A message displays at the top of the view screen to indicate how long it has been since the last refresh.
Records Per Listing Page	Type directly in the field. Refers to the number of lines that will appear in a view. The default value is 99.
RTM Enabled?	Select the appropriate radio button. The default value is NO.
SSL Only Enabled?	Select the appropriate radio button. The default value is NO.
ARE Enabled?	If you were not provided the URL, engage the NO radio button.
ARE URL	Type directly in the field the URL you were provided.
EIM Enabled?	If you were not provided the URL, engage the NO radio button.
EIM URL	Type directly in the field the URL you were provided.
Dashboard Enabled?	If you were not provided the URL, engage the NO radio button.
Dashboard URL	Type directly in the field the URL you were provided.
Password Format	Select the appropriate radio button. Click the Help link for additional assistance.
User Action Logging Enabled?	Yes/No Radio buttons provided. The default value is NO.
No. of invalid login attempts before user is locked out	Click the drop down menu to select the appropriate value. The provided values are 0, 3 and 5.
Email Address for User Lockout Notification	Type directly in the field. This action refers situation to the email address to notify that a user is locked out of the system.

Figure 25 General Configuration–Additional Info Tab Field Label Definition

The **General Configuration**-**Mail Server** Tab allows the user to establish the protocols for email functionality, as shown in Figure 26 and Figure 27.

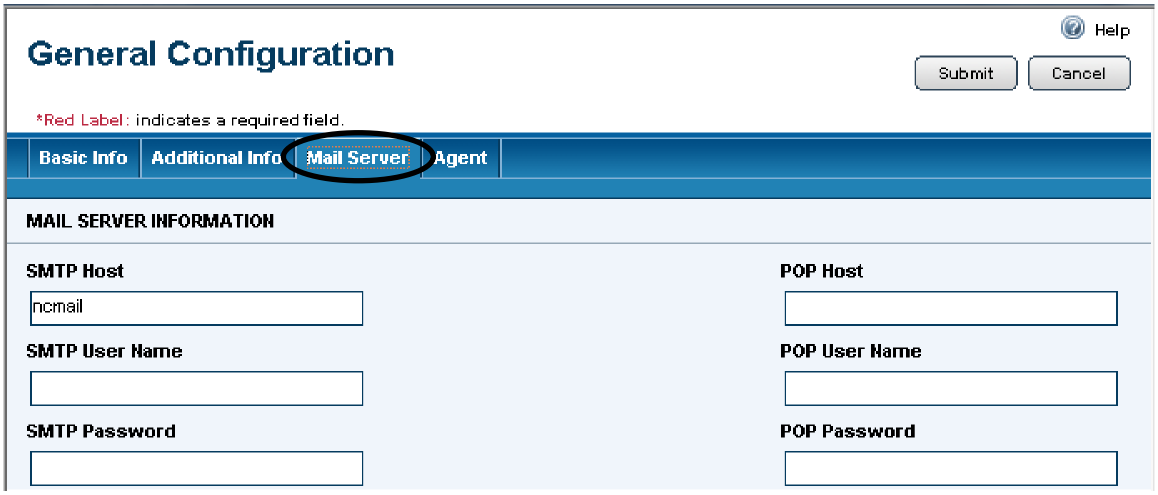


Figure 26 General Configuration – Mail Server Tab

Field Label	Definition
MAIL SERVER TAB	
SMTP Host	Outbound mail is established during the installation process.
SMTP User Name	Type directly in the field to update user name when necessary. Outbound (SMTP) mail User Name is entered during the installation process.
SMTP Password	Type directly in the field to update password when necessary. Outbound (SMTP) mail Password is entered during the installation process.
POP Host	Mail-in host is established during the installation process.
POP User Name	Type directly in the field to update user name when necessary. Mail-in (POP) User Name is entered during the installation process.
POP Password	Type directly in the field to update password when necessary. Mail-in (POP) Password is entered during the installation process.

Figure 27 General Configuration – Mail Server Tab Field Label Definition

The **General Configuration-Agent** Tab allows users to establish the protocols for Notification, Personal Profile, Password Expiration, Alert Bulletin and Data Sharing as shown in Figure 28 and Figure 29.

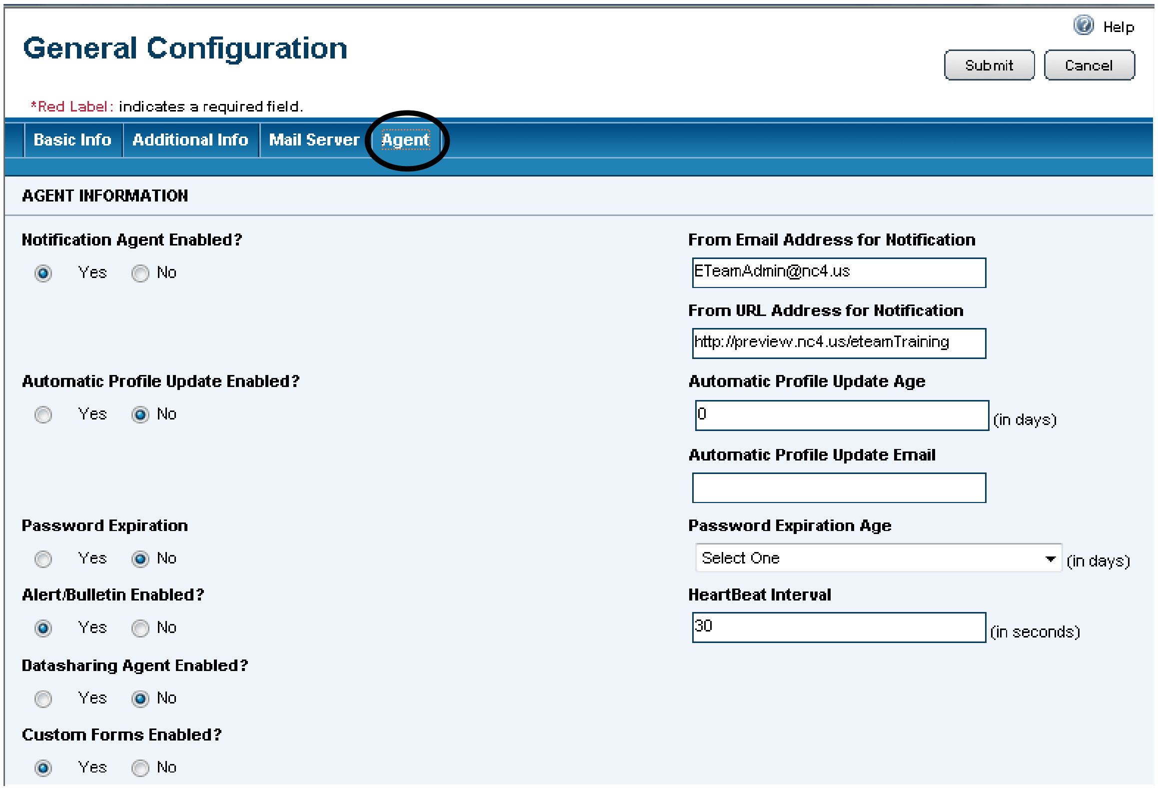


Figure 28 General Configuration – Agent Tab

Field Label	Definition
AGENT TAB	
Notification Agent Enabled?	Select the appropriate radio button. Establishes whether or not Notification is enabled. Default is YES.
From Email Address for Notification	Type directly in the field. Establishes the email address that should appear in the "from" field on notifications sent via the application.
From URL Address for Notification	Displays the application URL. This will be used when hyperlinks are contained within a notification sent via the application.
Automatic Profile Update Enabled?	Select the appropriate radio button. Establishes whether or not automatic profile update requests are to be sent. The default is NO.
Automatic Profile Update Age	Type directly in the field. Numeric entry required. The system is designed to allow for automatic update requests, via email, to system user's for which an email address has been established in their Profile Module. The email will state that their Profile has not been updated in "X" days, with "X" being the number set in this field (Refer below for an example of the email sent in Figure 30). Periodically, the system will identify profiles that meet the criteria as defined in this field. If the system identifies Profiles requiring updates, it automatically sends out an email to those users. When a user responds to the email sent by the system, incoming requests are processed automatically and the profiles are updated accordingly.
Automatic Profile Update Email	Type directly in the field. Establishes where the return Profile Update emails go for processing.
Password Expiration	Select the appropriate radio button. Default is NO.
Password Expiration Age	Click the drop down to select the appropriate amount of days in which passwords will expire.
Alert Bulletin Enabled?	Select the appropriate radio button. Establishes whether or not the Alert Bulletin Pop-up function available within the system will be used. Default is YES
HeartBeat Interval	Type directly in the field. Numeric entry required. Establishes the frequency in which: • Alert Bulletin pop-ups will display to users. Value represents number of seconds between Alerts. • Targeted Alerts panel refreshes showing latest status of all Targeted Alerts in the system. • Report locking status is reviewed. • User Locking status is reviewed. Default value is 30 seconds.
Data Sharing Agent Enabled?	Select the appropriate radio button. Establishes whether or not the Data Sharing feature will be used. Default is NO.
Custom Forms Enabled?	Select the appropriate radio button. Default is YES.

Figure 29 General Configuration - Agent Tab Field Label Definition

Settings detailed on the **Agent** tab allow the system to automatically send **Personal Profile** update requests. An example of the update request sent to users is shown below in Figure 30.

```
Please respond to this message by replying with history.  To the right of
each field below, enter the appropriate data. Then send.
Thank you.
                        Personal Info

                           Last Name:    My last name
                          First Name:    My first name
                      Middle Initial:    My middle initial
                        Organization:    My organization
                            Position:    My position
                              Agency:    My agency
                               Title:    My title
                          Skill Sets:    My skill set
                               Phone:    My phone number
                                Cell:    My cell number
                                 Fax:    My fax number
                              E-mail:    myname@myorganization.com
                               Pager:    My pager number
                               Other:    My other information
          Pager Used in Notification:    My pager used in notification
  Mobile Device Used in Notification:    My mobile device used in notification
            Notify By Email (Yes/No):    Yes or No
            Notify By Pager (Yes/No):    Yes or No
    Notify By Mobile Device (Yes/No):    Yes or No

Please do not edit anything below this line. Thank You.
System Identification: Directory\SubDirectory\Profiles.nsf***ETQA-5SQSSV
.nsf is domino extension.
Copyright 1999-2005 by E Team, Inc.  All Rights Reserved
```

Figure 30 Personal Profile Update Request – Agent Tab

8 Data Sharing Configuration

Data Sharing creates the ability to share access to NC4 application information with other user organizations.

All reports generated within the system's modules are viewable by all system users within the originating organization. In order to share the viewing of these reports with outside organizations, each module utilizes the Distribution and Sharing section. This section will detail the creation of Data Sharing Configurations that can be utilized for this purpose.

Data Sharing Configurations are created for use by the receiving and sending organization as needed. There are no predefined Data Sharing Configurations included in the NC4 Application.

Learning Objectives

After completing this section, you will be able to:

- Create, edit, and delete a Data Sharing Configuration.

This section of the module provides an overview of **Data Sharing Configurations** key highlights. You will become familiar with the layout of the **Data Sharing Configuration** form and understand how to create, modify, delete, and view Data Sharing Configurations.

8.1 Creating, Editing, and Deleting Data Sharing Configurations

8.1.1 Preview of a completed Data Sharing Configuration

Step 1: Select **Data Sharing Configuration** from the **Report** navigation drop down menu.

Step 2: Click the **Remote System Name** hyperlink as shown in Figure 31 to view the **Data Sharing Configuration** as shown in Figure 32.

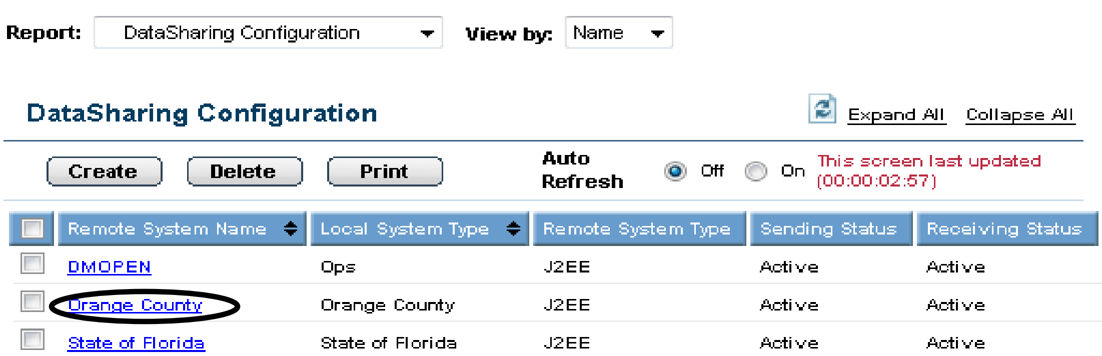


Figure 31 Data Sharing Configuration Hyperlink

Step 3: View the **Data Sharing Configuration** as shown in Figure 32. The Configuration contains system, sending, and receiving information on the **General, Sending, and Receiving** tabs. Click each tab title to review the current settings.

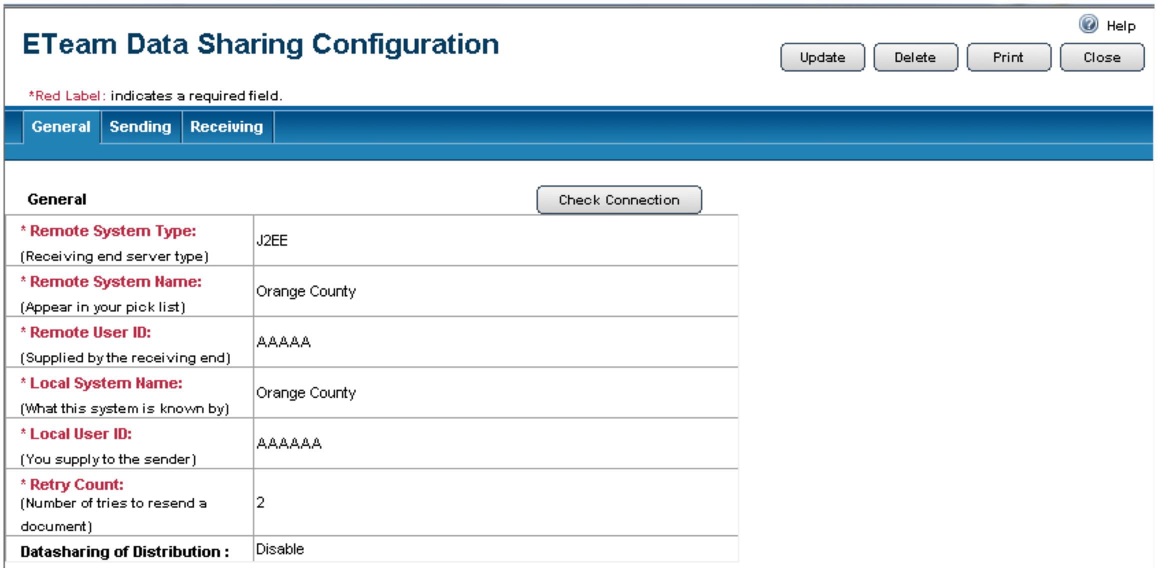


Figure 32 Data Sharing Configuration Form in *View* mode

8.1.2 Creating Data Sharing Configurations

Step 1: Select **Data Sharing Configuration** from the **Report** navigation drop down menu.

Step 2: Click the **Create** button as shown in Figure 33.

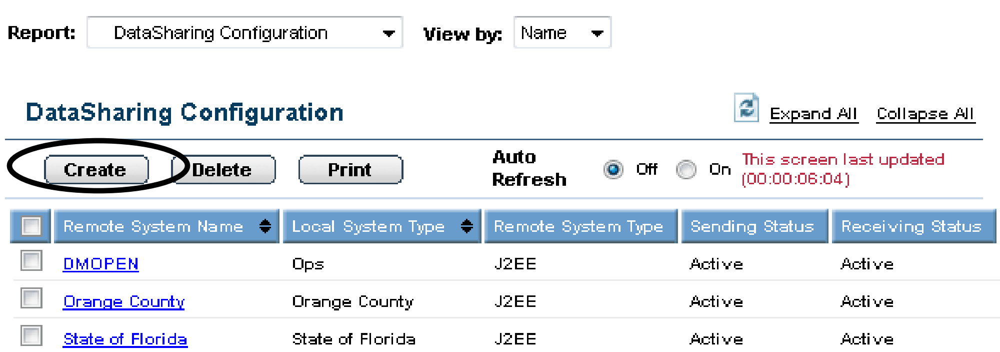


Figure 33 Data Sharing Configuration by Name Form

Step 3: The **Data Sharing Configuration** Form will open with the **General** tab displayed as shown in Figure 34. All of the fields for the **General** tab are also defined in Figure 35.

Step 4: All of the fields for the **Sending** Tab are defined in Figure 36. Any modifications to the data must follow the definitions outlined below.

Step 5: All of the fields for the **Receiving** Tab are defined in Figure 37. Any modifications to the data must follow the definitions outlined below.

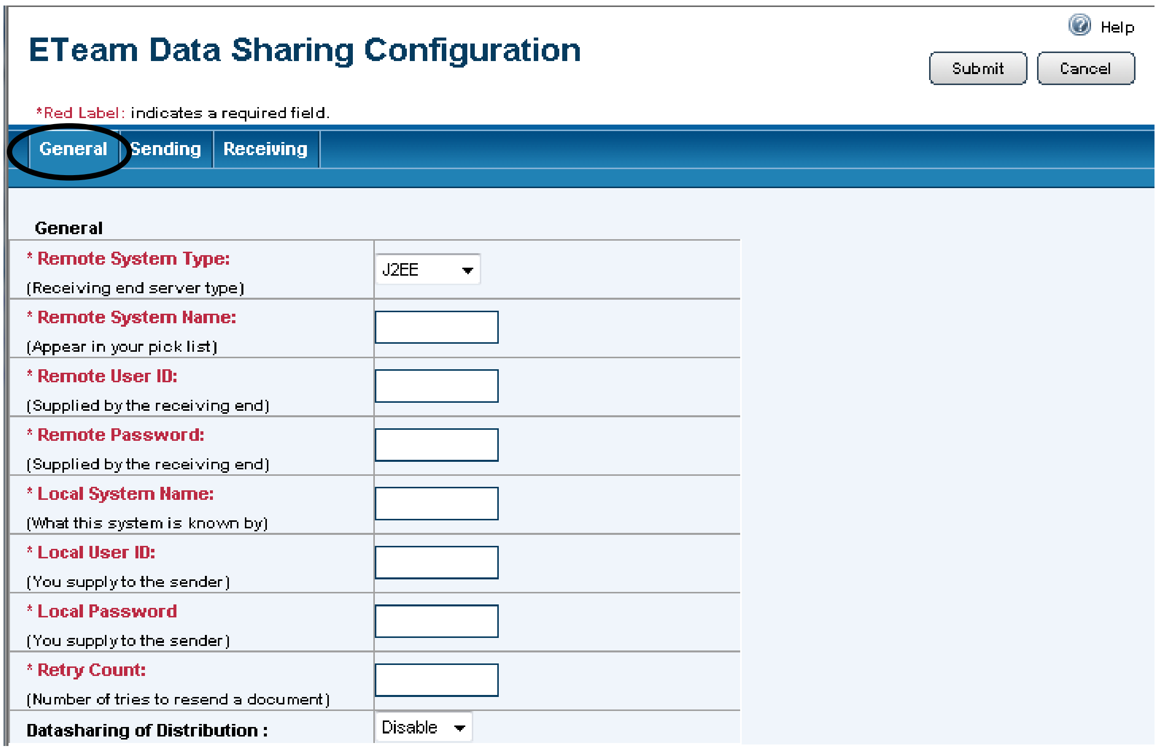
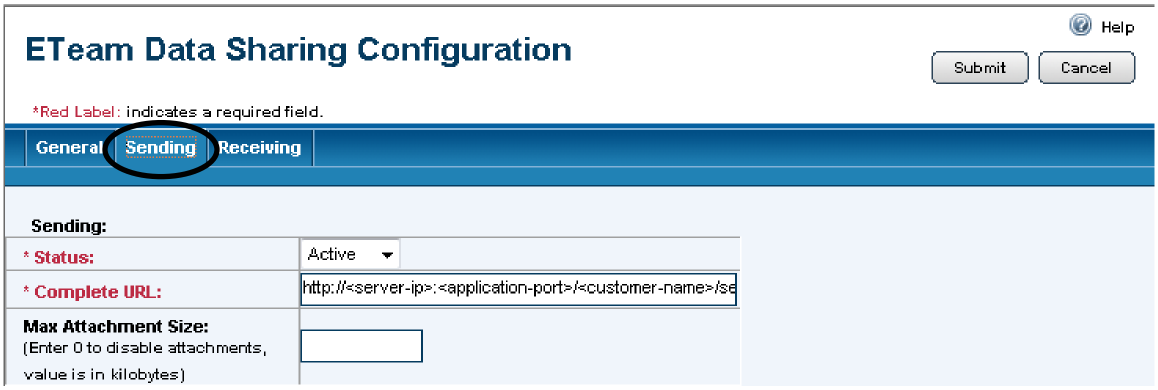


Figure 34 Data Sharing Configuration – General Tab

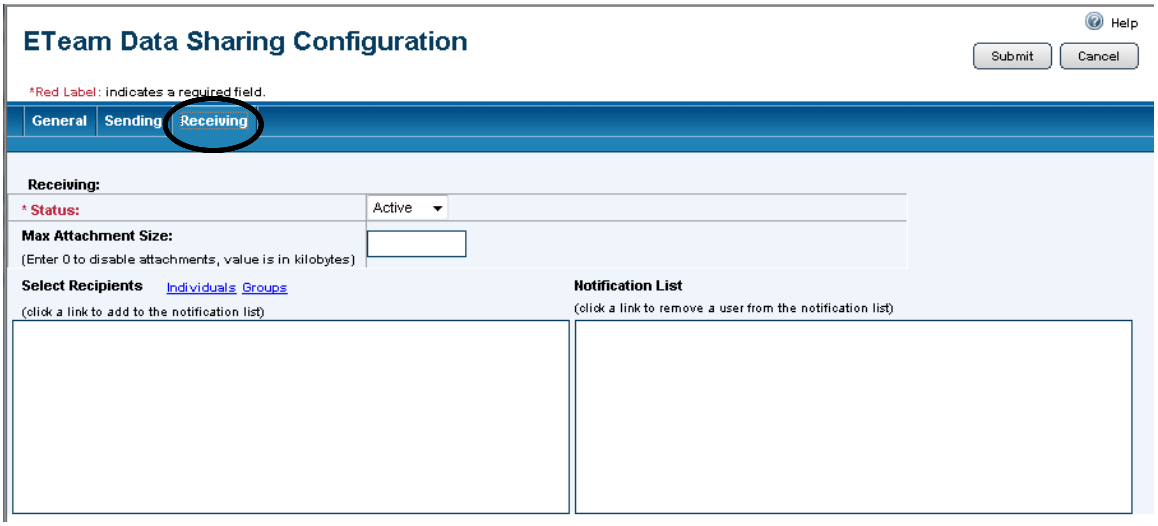
Field Label	Definition
Data Sharing Configuration – General Tab	
Remote System Type	Click the arrow to select J2EE from the drop down menu, if the data sharing partner is a J2EE system. Select DOMINO if the data sharing partner is running on DOMINO.
Remote System Name	Type directly in the field. This is your data sharing partner's **Local System Name** as used on the Data Sharing Configuration that is being set up to data share with you. This information must be obtained from the System Administrator of the Organization with which you are going to share data.
Remote User ID	Type directly in the field. This is the **Local User ID** of the remote system used on the Data Sharing Configuration that is being set up to data share with you. This information must be obtained from the System Administrator of the Organization with which you are going to share data.
Remote Password	Type directly in the field. Enter the **Local Password** of the remote system used on the Data Sharing Configuration that is being set up to data share with you. This information must be obtained from the System Administrator of the Organization with which you are going to share data.
Local System Name	Type directly in the field. Type in a valid alphanumeric combination. This is the name that your data sharing partner will have on the **Remote System Name** of his data sharing configuration.
Local User ID	Type directly in the field. Type in a valid alphanumeric combination. This is the name that your data sharing partner will have on the **Remote User ID** of his data sharing configuration.
Local Password	Type directly in the field. Type in a valid alphanumeric combination. This is the name that your data sharing partner will have on the **Remote Password** of his data sharing configuration.
Retry Count	Type directly in the field. Numeric data entry. Enter the number of times the application should retry sending the report to the remote system in case of failure on the first try. (Any number greater than one (1)).
Datasharing of Distribution	Click the arrow to select Enable or Disable from the drop down menu.

Figure 35 Data Sharing Configuration – General Tab Field Label Definition



Field Label	Definition
Data Sharing Configuration – Sending Tab	
Status	Click the arrow to display a drop down list of options to know whether or not this data sharing partner is Active or Inactive. You may change this selection at any time.
Complete URL	Type directly in the field. Enter the name by which your data sharing partner will be known to you.
Max Attachment Size	Type directly in the field. Numeric data entry. Enter the maximum file size that you will allow to be sent from your system. Enter value in kilobytes. Enter 0 to disable attachments.

Figure 36 Data Sharing Configuration - Sending Tab Field Label Definition



Field Label	Definition
Data Sharing Configuration – Receiving Tab	
Status	Click the arrow to display a drop down list of options to determine whether or not this data sharing partner is Active or Inactive. You may change this selection at any time.
Max Attachment Size	Type directly in the field. Numeric data entry. Enter the maximum file size that you will allow to be received to your system. Enter value in kilobytes. Enter 0 to disable attachments.
Select Recipients	Click the Individuals or/and Groups text links to display a list of available selections. Click an entry to move it in the Notification List window.
Notification List	Displays the list of Individuals or/and Groups selected to receive Notification. Click an entry to move it out of the Notification List window. Individuals or groups remaining in this window when the report is submitted will be notified when sharing data with this partner organization.

Figure 37 Data Sharing Configuration - Receiving Tab Filed Label Definition

Step 6: Click the **Submit** button to save the newly created configuration.

Step 7: View the newly created configuration in the Data Sharing Configuration form as shown in Figure 38.

Step 8: Click the **Check Connection** button on the **General Tab** to test the connection to the URL provided. A message box will appear to confirm the connection was successful or not.

8.1.3 Editing Data Sharing Configurations

Existing configurations can be edited at any time. Select a group from the **Data Sharing Configuration by Name** listing as shown in Figure 33. All current data for the selected configuration will be displayed in the **Data Sharing Configuration** form as shown in Figure 38. In order to modify the data, click on the Update button as shown below.

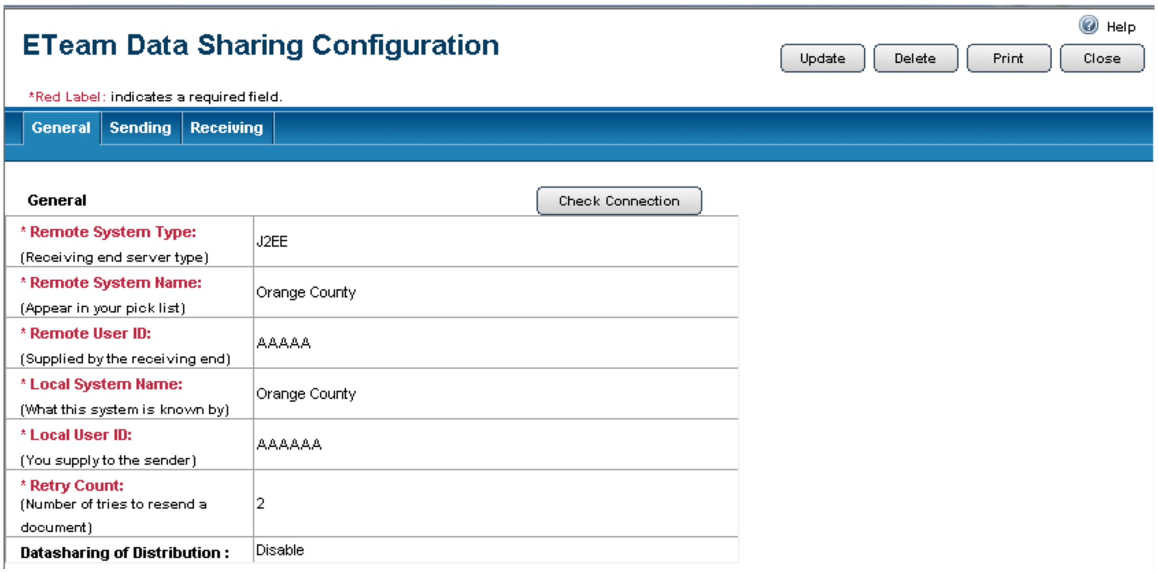


Figure 38 Data Sharing Configuration Form – Update button

The Data Sharing Configuration form will display in *Edit* mode and the data can be modified as needed. When you have completed the changes, click the Submit button in the upper right corner of the form as shown in Figure 37. All data will be saved and the modified data will now be displayed in the **Data Sharing Configuration** form.

8.1.4 Deleting a Data Sharing Configuration

An existing configuration can be deleted at any time. Select the configuration from the listing as shown in the **Data Sharing Configuration by Name** form. The configuration's information will be displayed in the **Data Sharing Configuration** form. Click the Delete button in the top right corner of the form. Once the deletion has been completed, a confirmation message will be shown on the screen.

8.1.5 Deleting multiple Data Sharing Configurations

Step 1: Select the configurations by clicking checkbox(s) next to the Remote System Name(s) as shown in Figure 33.

If you desire to delete all **Data Sharing Configurations** in the list, click the checkbox next to the headers. You will notice that all of the configurations in the list will receive a check in their corresponding checkbox as well.

Step 2: Clicking the 

button will remove all configurations listed that have a check mark in the checkbox.

8.2 Viewing Existing Data Sharing Configurations

As we have seen in the previous section in Figure 33, **Data Sharing Configuration by Name**, the default view is governed by the sorting techniques. The Data Sharing Configuration report has a **View by** drop down menu which displays all sorting techniques for the report which are **"Name"** and **"Status"**.

In order to change the view for existing configurations, click **"Status"** in the **View by** drop down menu.

9 Notification Queue

The Notification Queue displays all reports sent from within any system report. The notifications are categorized by the sending status: processed or failed. Notifications can be viewed, printed, or deleted from the queue.

This section of the module will provide an overview of the **Notification Queue** key highlights. You will become familiar with the layout of the **Notification Queue** form and understand how to view or delete each notification.

Learning Objectives

After completing this section, you will be able to:

- View and delete report notifications.

9.1 Deleting the Notification Queue

9.1.1 Viewing the Notification Queue

Step 1: Select **Notification Queue** from the **Report** drop down menu.

Step 2: Click the ▸ next to the status in order to view all the notifications as shown in Figure 39.

Step 3: Select a notification from the display. You can view the date, time, and report from which the notification was generated. Click the hyperlink of the notification you desire.

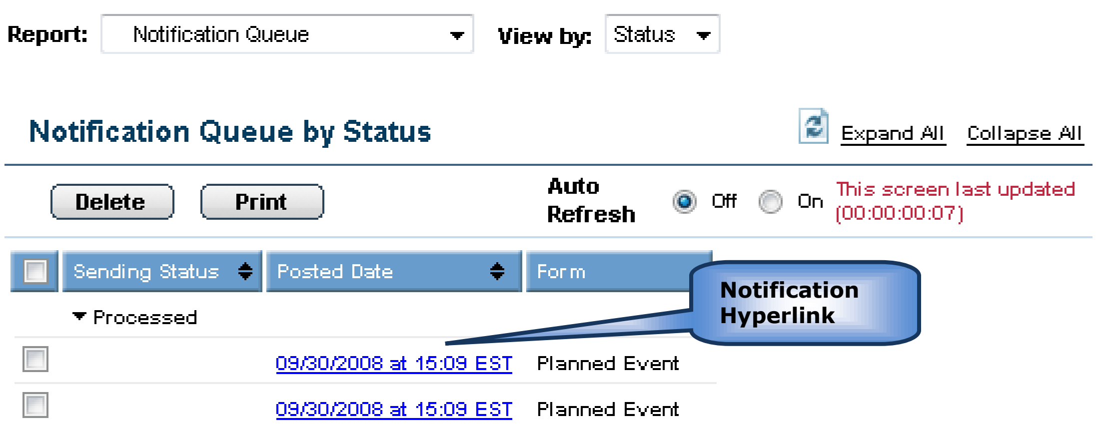


Figure 39 Notification Queue Hyperlinks

Step 4: View the **Notification Queue** information as shown in Figure 40.

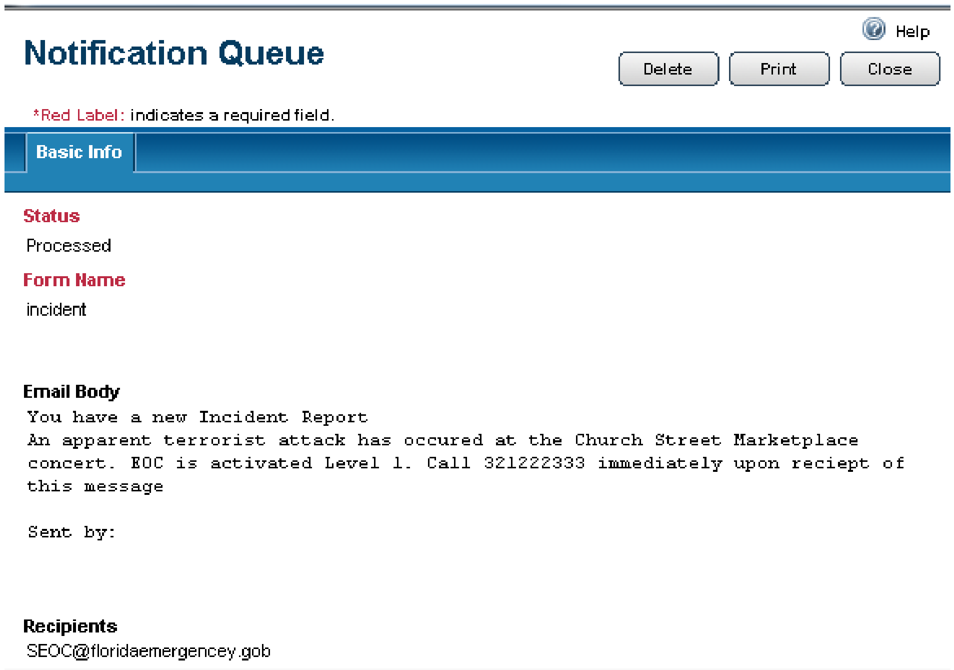


Figure 40 Notification Queue Report

9.1.2 Deleting a single data sharing queue

Step 1: Select **Notification Queue** from the **Report** drop down menu.

Step 2: Click the ▸ next to the status in order to view all the notifications as shown in Figure 39.

Step 3: Select a notification from the display. You can view the date, time, and report from which the notification was generated. Click the hyperlink of the notification you desire.

Step 4: The full notification text will be displayed in the **Notification Queue** form as shown in Figure 41.

Step 5: Click the Delete button to delete the single notification.

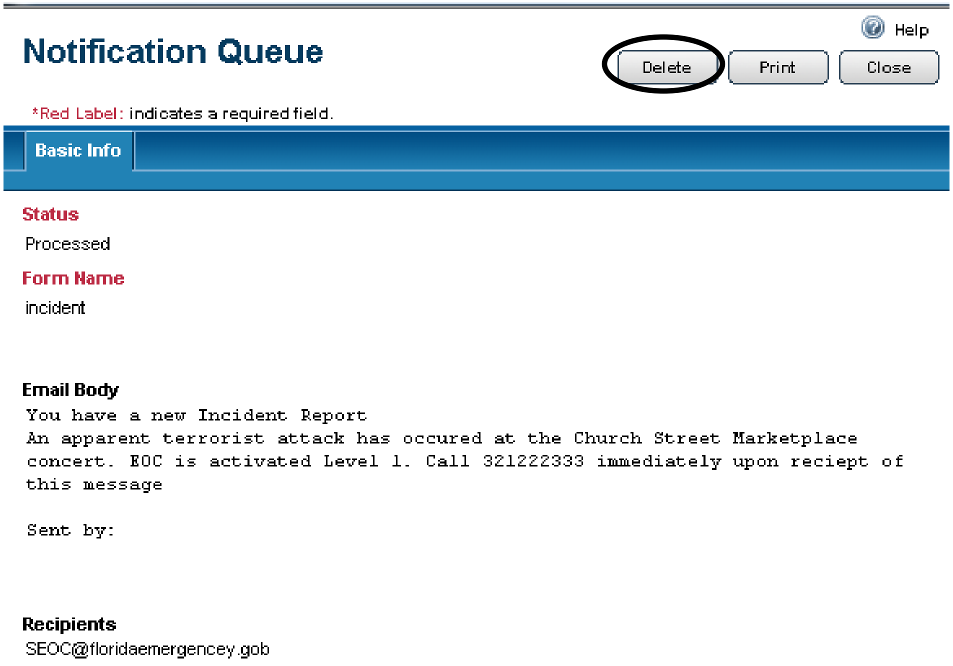


Figure 41 Notification Queue Report – Delete Button

9.1.3 Deleting multiple data sharing queues

Step 1: Select the notifications by clicking checkbox(s) next to the notification in the **Notification Queue**.

If you desire to delete all notifications in the **Notification Queue**, click the checkbox next to the headers. You will notice that all of the reports in the queue will receive a check in their corresponding checkbox as well.

Step 2: Clicking the 

button will remove all notifications listed that have a check mark in the checkbox.

10 Document Locking

Document Locking provides protection for documents that are being modified. This feature is a safety feature to keep data from being lost. However, the Document Locking feature does contain an override function for authorized users only. An authorized user is given permission when the **user login** and **password** is established.

Please note that any changes made to the report by the original user of the document will not be saved. That user will receive a message on their screen, if they attempt to save the document. The message will notify them that they are attempting to save an earlier version of the document.

This section will provide an overview of **Document Locking** key highlights. You will become familiar with the layout of the **Document Locking** form and understand how to release the documents if necessary.

Learning Objectives

After completing this section, you will be able to:

- Release a document lock.

10.1 Releasing a Document Lock

Step 1: Select **Document Locking** from the **Report** drop down menu.

Step 2: All reports being modified will be listed in the **Document Locking** form as shown in Figure 42.

Step 3: Select the report that you wish to release by clicking the checkbox next to the report on the left.

Step 4: Click the **Release** button.

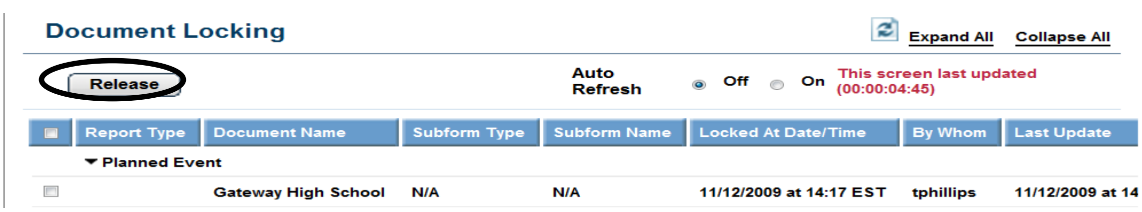


Figure 42 Document Locking Form

Step 5: A message box will display confirming your desire to release the document. Click the **OK** button.

Step 6: The document will be released and a message box will appear that verifies the release. Click the **OK** button. The document will no longer appear in the Document Locking list.

11 Data Sharing Queue

The Data Sharing Queue displays a notification and status for all reports sent from within any system report designated to be shared. The notifications are categorized by the sharing status. Data Sharing notifications can be viewed, printed, or deleted from the queue.

This section of the module will provide an overview of the Data **Sharing Queue** key highlights. You will become familiar with the layout of the **Data Sharing Queue** form and understand how to view or delete each notification.

Learning Objectives

After completing this section, you will be able to:

- View and delete data sharing notifications.

11.1 Deleting the Data Sharing Queue

11.1.1 Viewing the Data Sharing Queue

Step 1: Select **Data Sharing Queue** from the **Report** drop down menu.

Step 2: Click the ▸ next to the **Remote System Name** to view the status of the requested data and/or reports as shown in Figure 43.

Step 3: Click the ▸ next to the status in order to view all the notifications.

Step 4: Select a notification from the display. You can view the date, time, and report from which the notification was generated. Click the hyperlink of the notification you desire.

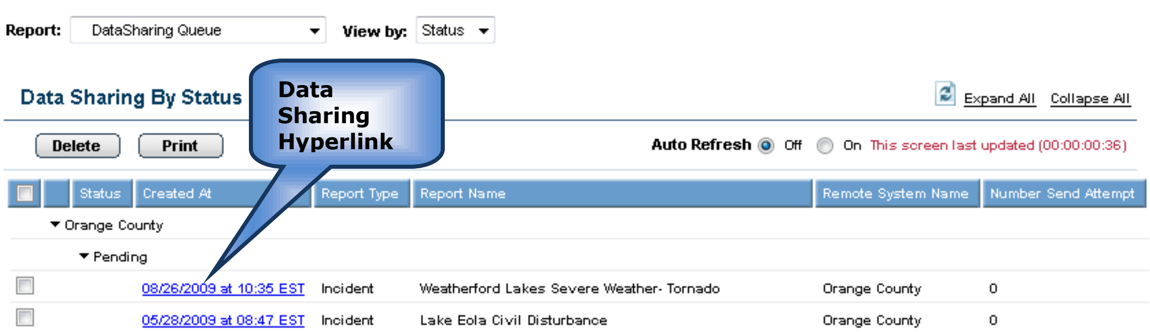


Figure 43 Data Sharing Queue Hyperlinks

Step 5: View the **Queue Information** as shown in Figure 44.

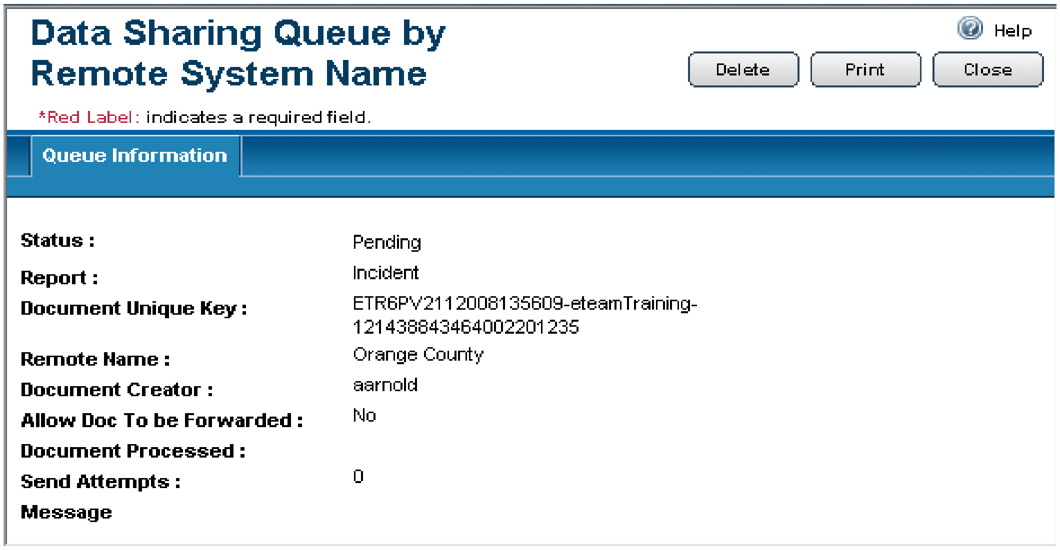


Figure 44 Data Sharing Queue Form

11.1.2 Deleting a single data sharing queue

Step 1: Select **Data Sharing Queue** from the **Report** drop down menu.

Step 2: Click the ▸ next to the **Remote System Name** to view the status of the requested data and/or reports as shown in Figure 45.

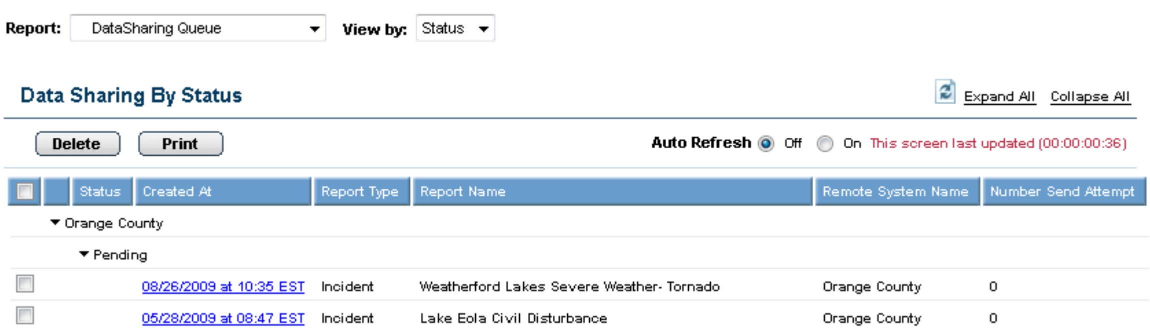


Figure 45 Data Sharing Queue

Step 3: Click the ▸ next to the status in order to view all the notifications.

Step 4: Select a notification from the display. You can view the date, time, and report from which the notification was generated. Click on the hyperlink of the notification you desire.

Step 5: The full notification text will be displayed in the **Data Sharing Queue Summary** form as shown in Figure 46.

Step 6: Click the Delete button to delete the single notification.

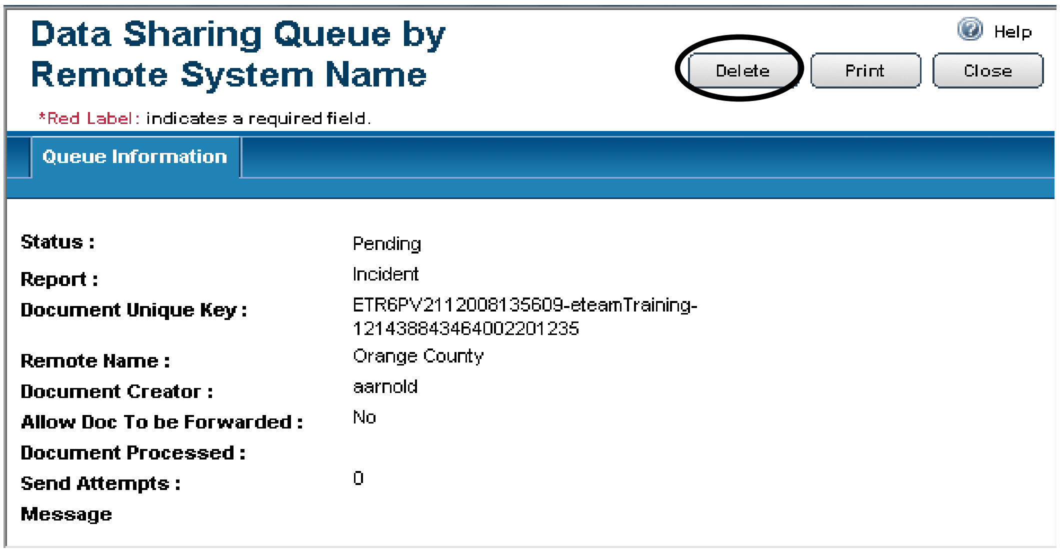


Figure 46 Data Sharing Queue Report

11.1.3 Deleting multiple data sharing queues

Step 1: Select the notifications by clicking checkbox(s) next to the notification in the Data Sharing Queue form.

If you desire to delete all notifications in the **Data Sharing Queue**, click the checkbox next to the headers. You will notice that all of the reports in the queue will receive a check in their corresponding checkbox as well.

Step 2: Clicking the Delete button will remove all notifications listed that have a check mark in the checkbox.

12 GIS Configuration

The NC4 Application consists of four (4) system configuration documents. GIS Configuration is the third configuration discussed in this document. Data Sharing and General Configurations have been addressed in preview sections of this document. The information detailed in this configuration is critical to the use and maintenance of the NC4 Application.

Within the system, on-line maps allow users to view areas being monitored in a very detailed manner. Users navigate to the Map Tab in order to view any maps that have been added to the system. In order for a map to be available to users, a GIS Configuration Document must be created.

Learning Objectives

After completing this section, you will be able to:

- Create, modify, and delete GIS Configurations.

This section of the module will provide an overview of **GIS Configuration** key highlights. You will become familiar with the layout of the **GIS Configuration** form and understand how to modify configurations.

12.1 Creating, Editing, and Deleting GIS Configurations

12.1.1 Creating GIS Configurations

Step 1: Select **GIS Configuration** from the **Report** drop down menu.

Step 2: Click the **Create** button as shown in Figure 47.

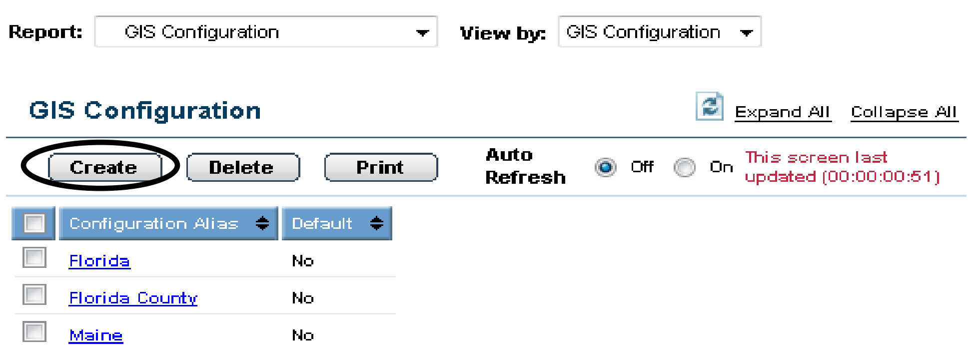


Figure 47 GIS Configuration List by Alias Form

Step 3: The **GIS Configuration Form** will display as shown in Figure 48. All of the fields for the GIS Configuration are also defined in.

.

Step 4: Enter data as described in the table provided in Figure 49.

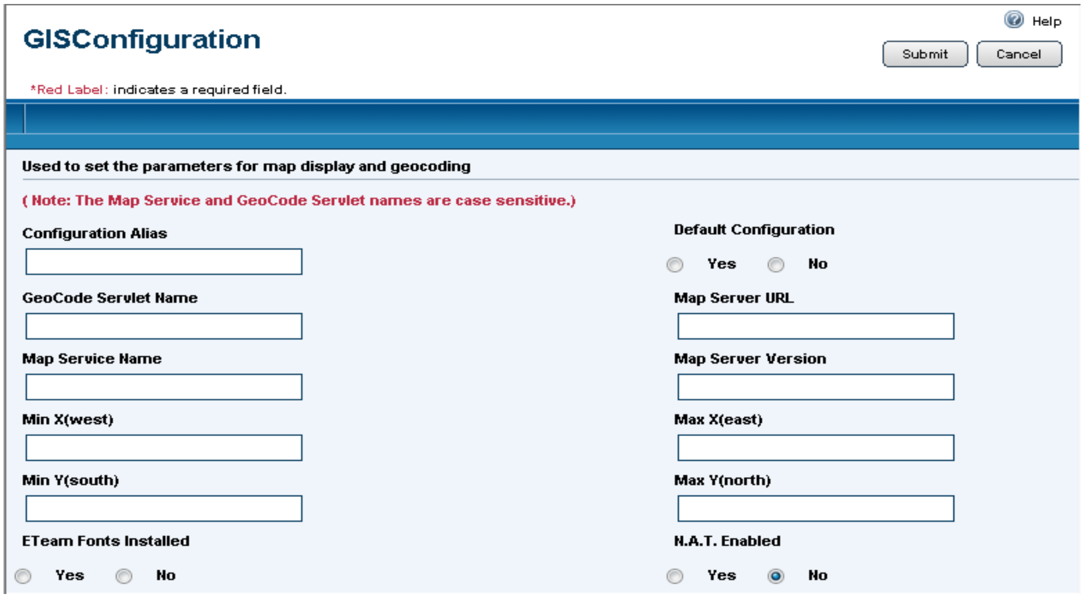


Figure 48 GIS Configuration Form

Field Label	Definition
GIS Configuration	
Configuration Alias	Type directly in the field to make changes. This information is set during installation and is used to identify the map being used. This is the name that will appear in the Available Maps drop down menu in the Map window.
Default Configuration	Select the appropriate radio button. Establishes whether or not this will be the default map that displays when a user launches the system map window. When multiple maps are being used, only one can be defined as the default map.
GeoCode Servlet Name	Type directly in the field. This defines the servlet that the geo-coder will connect to. This field is case sensitive.
Map Server URL	Type directly in the field. This establishes the path to the map server.
Map Service Name	Type directly in the field. This defines the name of the ArcIMS map service used for rendering the map (i.e., a map of Florida may be taken from a U.S.A. map service). This field is case sensitive.
Map Server Version	Type directly in the field. This refers to ArcIMS.
Min X (west)	Type directly in the field. Set the default west longitude value.
Max X (east)	Type directly in the field. Set the default east longitude value.
Min Y (south)	Type directly in the field. Set the default south latitude value.
Max Y (north)	Type directly in the field. Set the default north latitude value.
Fonts Installed	Select the appropriate radio button. Establishes whether or not the system fonts are installed on the ArcIMS server.
N.A.T Enabled	Select the appropriate radio button. Default is NO

Figure 49 GIS Configuration Field Label Definition

Step 5: Click the **Submit** button to save the newly created configuration.

Step 6: View the newly created configuration in the **GIS Configuration** form as shown in Figure 50.

12.1.2 Editing GIS Configurations

Existing configurations can be edited at any time. Select a configuration from the **GIS Configuration** listing as shown in Figure 47. All current data for the selected configuration will be displayed in the GIS Configuration form as shown in Figure 50. In order to modify the data, click on the button as shown below.

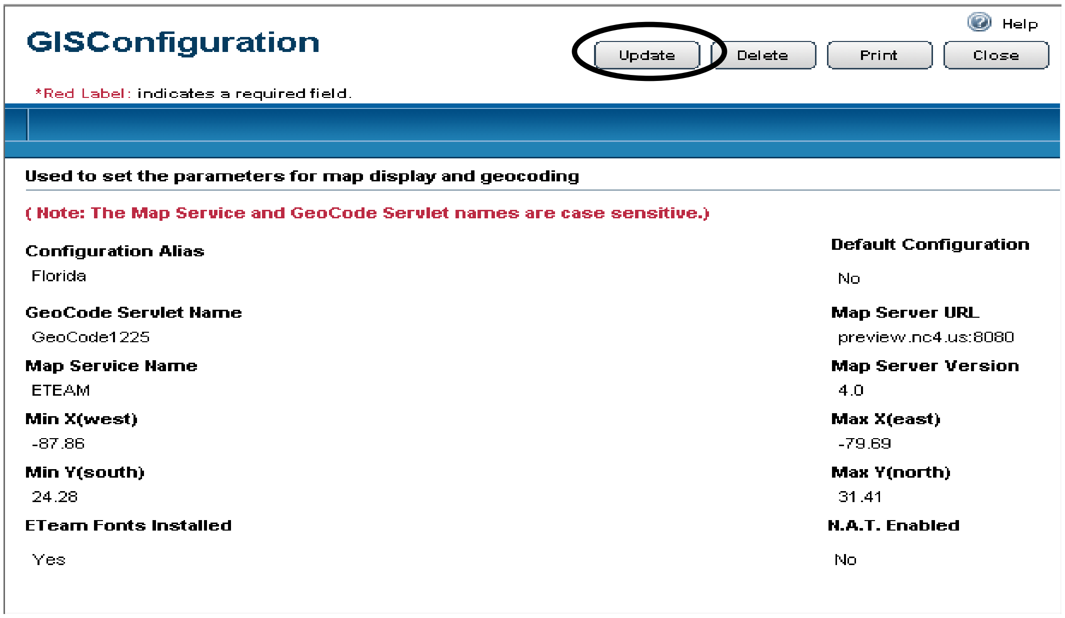


Figure 50 GIS Configuration Form in *View* mode

The **GIS Configuration** form will display and the data can be modified as needed. When you have completed the changes, click the Submit button in the upper right corner of the form as shown in Figure 49. All data will be saved and the modified data will now be displayed in the GIS Configuration form.

12.1.3 Deleting GIS Configurations

An existing configuration can be deleted at any time. Select the configuration from the listing as shown in the GIS Configuration List by Alias form as shown in Figure 47. The configuration's information will be displayed in the GIS Configuration form. Click the Delete button in the top right corner of the form. Once the deletion has been completed, a confirmation message will be shown on the screen.

12.1.4 Deleting multiple GIS Configurations

Step 1: Select the configurations by clicking checkbox(s) next to the Configuration Alias(s) as shown in Figure 47.

If you desire to delete all notifications GIS Configurations in the list, click the checkbox next to the headers. You will notice that all of the configurations in the list will receive a check in their corresponding checkbox as well.

Step 2: Clicking the Delete button will remove all configurations listed that have a check mark in the checkbox.

13 DRS Configuration

DRS Configuration is the last configuration discussed in this document. The information detailed in this configuration is critical to the use and maintenance of the system.

Data Replication Services (DRS) allows two or more installations of the system to display selected data and reports in all systems in real time. The reports from each system will be replicated in the other(s) except for time zone, non-editable General Configuration information, and GIS Configurations. However, the DRS will not replicate reports and data until a DRS Configuration has been created. Any reports or data created prior to setting up the DRS Configuration will not be replicated.

Learning Objectives

After completing this section, you will be able to:

- Create, modify, and delete DRS Configurations.

This section of the module will provide an overview of **DRS Configuration** key highlights. You will become familiar with the layout of the **DRS Configuration** form and understand how to modify it.

13.1 Creating, Editing, and Deleting a DRS Configuration

13.1.1 Creating DRS Configurations

Step 1: Select **DRS Configuration** from the **Report** drop down menu.

Step 2: Click the **Create** button as shown in Figure 51.

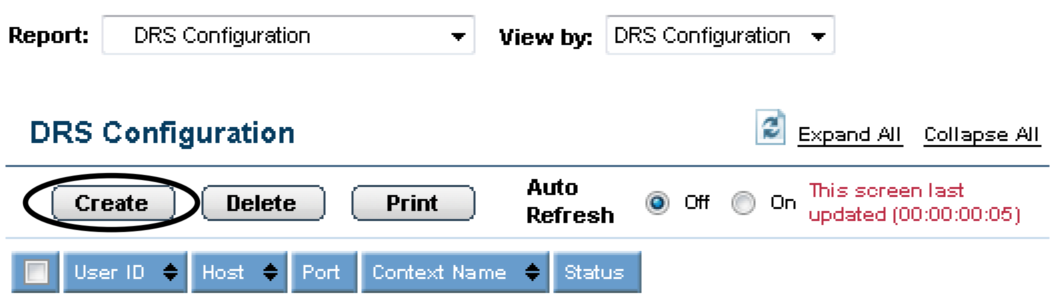
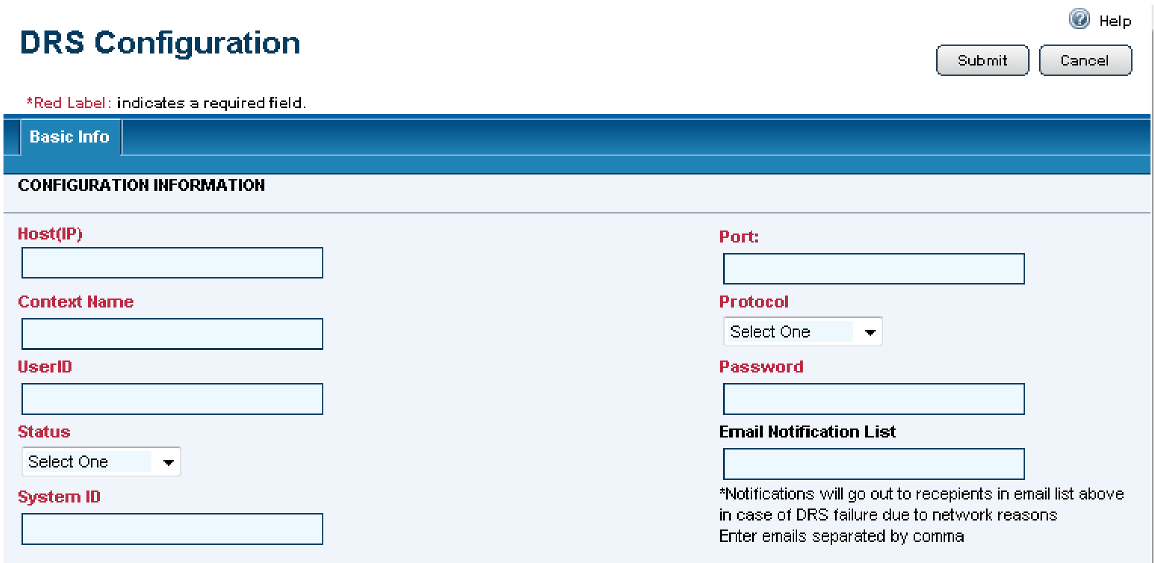


Figure 51 DRS Configuration List Report

Step 3: The **DRS Configuration** report will display as shown in Figure 52. All of the fields for the **DRS Configuration** are also defined in Figure 52.

Step 4: Enter data for all fields as described in Figure 52.



Field Label	Definition
DRS Configuration	
Host (IP)	Type directly in the field. This is the hostname or IP of the remote system you have chosen to replicate data with.
Port	Type directly in the field. This is the port on which the application server of the remote system you have chosen to replicate data with is listening on.
Context Name	Type directly in the field. This is the customer name of the remote system you have chosen to replicate data with. (assumed to be the same for all installations of a customer).
Protocol	Click the drop down arrow to display a list of options to choose from. Establishes whether the protocol for the remote server provided above is http or https.
User ID	Type directly in the field. Enter a valid username with admin privileges for the application on the remote system.
Password	Type directly in the field. Enter the Password for the username entered above.
Status	Click the drop down arrow to display a list of options to choose from. Select Enable to set replication to Active. Select Disable to set replication to Inactive .
Email Notification List	Type directly in the field. Notifications will be sent to the list in case of a DRS failure due to network reasons. Each email should be separated by a comma.
System ID	Type directly in the field. Numeric data entry. System ID of the replicating server is available from the Configuration report. (Select menu Configuration. Click the hyperlink. Configuration report page will open in View mode).

Figure 52 DRS Configuration Report

Step 5: Click the Submit button to save the newly created configuration.

Step 6: View the newly created configuration in the **DRS Configuration** report.

13.1.2 Editing DRS Configurations

Existing configurations can be edited at any time. Select a configuration from the **DRS Configuration** listing as shown in Figure 51. All current data for the selected configuration will be displayed in the **DRS Configuration** report. In order to modify the data, click on the Update button.

The **DRS Configuration** report will display and the data can be modified as needed. When you have completed the changes, click the Submit button in the upper right corner of the form as shown in Figure 52. All data will be saved and the modified data will now be displayed in the **DRS Configuration** form.

13.1.3 Deleting a DRS Configuration

An existing configuration can be deleted at any time. Select the configuration from the listing as shown in the DRS Configuration form. The configuration's information will be displayed in the DRS Configuration form. Click the Delete button in the top right corner of the form. Once the deletion has been completed, a confirmation message will be shown on the screen.

13.1.4 Deleting multiple DRS Configurations

Step 1: Select the configurations by clicking checkbox(s) next to the User ID(s) as shown in Figure 51.

If you desire to delete all **DRS Configurations** in the list, click the checkbox next to the headers. You will notice that all of the configurations in the list will receive a check in their corresponding checkbox as well.

Step 2: Clicking the Delete button will remove all configurations listed that have a check mark in the checkbox.

14 Logs

The Logging feature provides the means by which a customer can monitor use of their application. Logging is enabled in **General Configuration** by selecting the ***Yes*** option in the ***User Action Logging Enabled*** field under the **Additional Info** tab. Logs can be viewed by users with administrator rights by selecting the **Logs** option found within the menu item **Administration.**

Learning Objectives

After completing this section, you will be able to:

- View Logs

When enabled multiple user activity logs will be automatically generated each day on a 24 hour cycle beginning at 12:00am. These logs are not editable; however, they can be downloaded and saved to a file. Each downloaded log will include all line items displayed in the associated view for that log type. Each day the previous days log will be sent to history and the view will be cleared as the new daily log is created and displayed in the active view.

Log history will only be retained in the system for a seven (7) day period beginning Sunday at 12am (Sunday 00:00:00 thru Saturday 24:59:59). Customers who wish to retain all log data MUST download and save these logs to a file on a regular basis.

Note: The log clock must complete a 7 day cycle before history is cleared, therefore the first log of each type after the logging feature is enabled in the General Configuration document may contain more than 7 days.

This section of the module will provide an overview of **Logs** key highlights. You will become familiar with the layout of the **Logs** form and understand how to abstract the data.

14.1 Viewing a Log

14.1.1 Viewing Logs by User ID

Step 1: Select **Logs** from the **Report** drop down menu.

Step 2: Click the **User ID** Name link to download a log for the user id as shown in Figure 53.

Step 3: Click the **OK** button on the confirmation window.

Step 4: A window will appear asking whether you want to open or save the file. To have the file appear immediately on screen, click the **Open** button. An example of the downloaded file will appear in Figure 54.

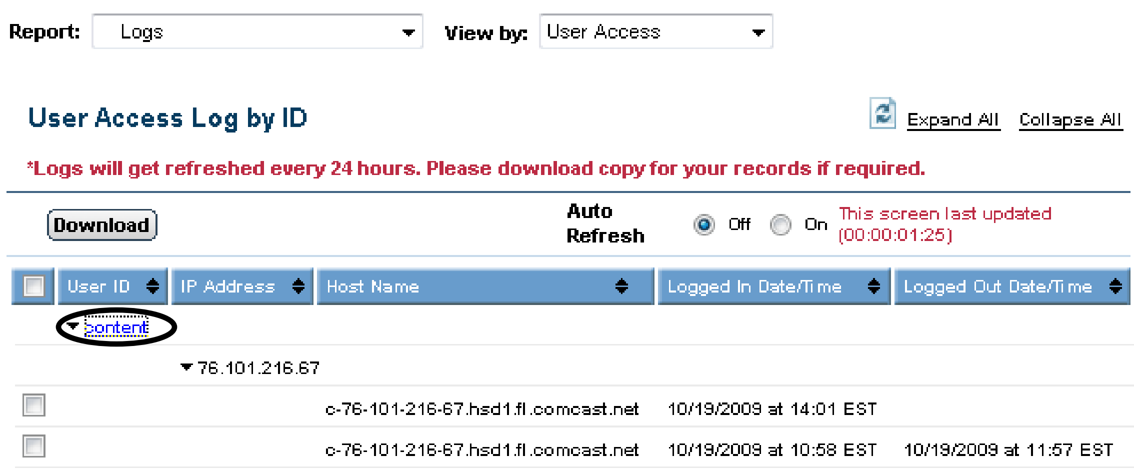


Figure 53 User Access Log by ID report

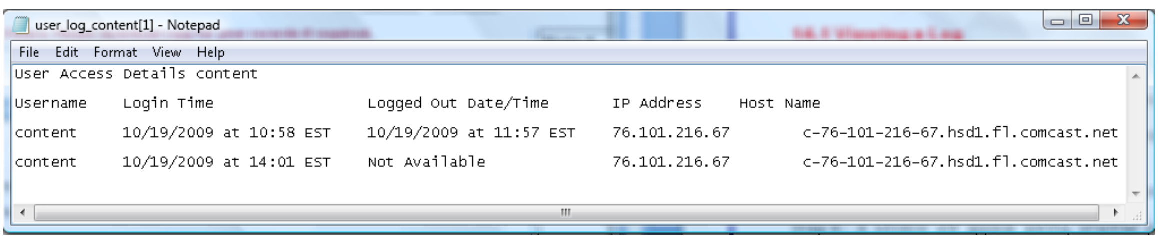


Figure 54 Log Details

14.1.2 Viewing Multiple logs by User ID

Step 1: Select **Logs** from the **Repor**t drop down menu.

Step 2: Click on the **Download** button as shown in Figure 55.

Figure 55 User Access Log for multiple User IDs

14.1.3 Viewing Existing Data Sharing Configurations

As we have seen in the previous section, the default view is governed by the sorting techniques. For existing logs, the view is sorted by **"User Access"**. However, existing logs can also be sorted by **"Invalid Login Attempts", "Locked Users", "User Actions",** and **"History".** The **Log** report has a **View by** drop down menu which displays all sorting techniques for the report.

In order to change the view for existing configurations, click one of the options in the **View by** drop down menu.

Review Exercise 1 - Putting it Together

This exercise is for class participants to login and create four users with the privileges to perform specific tasks.

In this exercise, you will login to the NC4 Application and navigate to create the **Users**, assign **Groups** and **Roles** as needed for each to perform specified tasks. You will create users with prescribed duties (low to high access) in the following scenario:

Bob Walker: The user must be able **read** all reports and features of the system, excluding system admin functions. This user will not have permission to enter any data into the system. (***Read All Docs***)

End User: The user must be able to read all reports, **create and modify** only reports **they create** in the application.**(Author)**

Kate Howard: The user must be able to **read, create, and modify** all reports and features of application, excluding system admin functions. (***Editor***)***This user will not be able to view the Data Dictionary***.

Shaun Stevens: The user must be able to read, create, modify and delete all reports and features, excluding system functions, and also must be able to **approve** procurements. (***Manager, Approver***)***This user will not be able to view System Administration.***

Mary Banfield: The user must have access to the **System Administrative** functions and have all privileges available within the system. (***System Admin***)

Remember, all * red label fields are required. To create the four users, please follow the steps below.

1. Make a template of the Name of the User, Login ID, Passwords, Group, Role and Privileges. Based on the scenario above, fill in the information similar to the template below to assess if the predefined groups and roles will provide the correct access to the reports.

Login ID	Password	Group(s)	Role(s)	Privilege(s)
bwalker		Read Only Users	Reader	Read
enduser		Author	Author	Author,
khoward		Editors	Editor	Author, Editor,
sstevens		Managers, Approvers	Manager Approver	Author, Delete, Editor, Approve
mbanfield		System Admin	Administration	Author, Delete, Editor, Reader

2. Login to the NC4 Application.

3. Go to **User** from the drop down **Report** navigation menu.

4. Click the **Create** button on the center view frame.

5. Go to the **Login ID** field.

    a. Key in the user's ID from the Login ID column in your template.

6. Go to the **Password** field located below the Login ID field.

    a. Key in a password for the user.

7. Go to the **Confirm Password** field located next to the Password field.

    a. Key in the same password for the user.

8. Select a group name(s) listed under the **Groups** header for this user from the Group column in your template.

    a. Click the >> button to move the selected group name(s) to the right box.

9. Click the **Submit** button to complete the User creation.

10. Go to Step 3 to complete the process for the additional users.

Test for success:

Log out of the NC4 Application. On the Welcome Page, enter the Login ID and Password of the first user. Once the Personal Profile of the user appears, the username and password have been successfully tested. Press the Cancel button to return to the Welcome Page and enter the next user until complete.

Well done! Remember to log out of the NC4 Application.

Review Exercise 2

This exercise is for class participants to login and create the ability to share data with an application outside the NC4 Application.

In this exercise, you will login to the NC4 Application and navigate to create a Data Sharing Configuration.

Before logging into the system, this exercise requires that information be gathered regarding the organization with which you desire to share data.

Remember, all * red label fields are required. To complete a Data Sharing Configuration, please follow the steps below.

1. Login to the NC4 Application.
2. Go to **DataSharing Configuration** from the drop down **Report** navigation menu.
3. Click the **Create** button on the center view screen.
4. On the new Data Sharing Configuration form, note that the form opens with the **General Tab** available.
5. Go to the **General** section and locate the **Remote System Type** field:
    a. Select a **Remote System Type** from the Remote System Type drop down menu.
6. Go to the **Remote System Name** field located below the Remote System Type field.
    a. Key in the Data Sharing partner's **Local System Name.**
7. Go to the **Remote User ID** field located below the Remote System Name field.
    a. Key in the Data Sharing partner's **Local User**.
8. Go to the **Remote Password** field located below the Remote User ID field.
    a. Key in the Data Sharing partner's **Local Password**.
9. Go to the **Local System Name** field located below the Remote Password field.

   a. Key in the name that your data sharing partner has as the **Remote System Name** of his data sharing configuration.

10. Go to the **Local User ID** field located below the Local System Name field.

    a. Key in the name that your data sharing partner has as the **Remote User ID** of his data sharing configuration.

11. Go to the **Local Password** field located below the Local User ID field.

    a. Key in the name that your data sharing partner has as the **Remote Password** of his data sharing configuration.

12. Go to the **Retry Count** field located below the Local Password field.

    a. Key in the number of times the application should retry sending the report to the remote system.

13. Go to the **Datasharing of Distribution** field located below the Retry Count field.

    a. Select the appropriate response from the drop down menu.

14. On the new Data Sharing Configuration form, click the **Sending Tab**.

15. Go to the **Sending** section and locate the **Status** field:

    a. Select a **Status** from the Status drop down menu.

16. Go to the **Complete URL** field located below the Status field.

    a. Key in the URL with the following format. http://<server-ip>:<application-port>/<customer-name>/servlet/dsServlet

17. Go to the **Max Attachment Size** field located below the Complete URL field.

    a. Key in the appropriate value in kilobytes.

18. On the new Data Sharing Configuration form, click the **Receiving Tab**.

19. Go to the **Receiving** section and locate the **Status** field:

    a. Select a **Status** from the Status drop down menu.

20. Click the **Individuals** link next to the Select Recipients header to view the users of the remote system.

a. Click a link under the Name header to add the individual user to the notification list.

21. Click the **Submit** button to complete the Data Sharing Configuration.

Test for success: Data Sharing has been successfully implemented when the Recipients are receiving the selected reports.

Well done! Remember to log out of the NC4 Application.

Review Exercise 3

This exercise is for class participants to login and create a GIS Configuration based on information you provide.

The following information will be developed by the class participants with guidance from the Instructor. Once the variables are decided upon, all class participants should login to the system. Navigate to create a new GIS Configuration based on this information.

Determine the:

1. Configuration Alias
2. Default Configuration
3. GeoCode Servlet Name
4. Map Server URL
5. Map Service Name
6. Map Server Version
7. Min X (west)
8. Max X (east)
9. Min Y (south)
10. Max Y (north)
11. E Team Fonts Installed
12. N.A.T Enabled

Test for success: Go to the **Maps** tab and find the added location in the Available Maps map viewer.

Well done! Remember to use the Logout button to exit the NC4 Application.

Appendix A: Groups

The NC4 Application is delivered with several predefined groups. The most used groups contain system and report access and are categorized as follows:

SYSTEM ACCESS

1. **System Admin** – This group contains the role Admin and should be assigned only to those individuals who should have **access to all the administration functions.**
2. **Managers** – This group contains the role Manager and should be assigned to those individuals who need to have the ability to **configure the Data Dictionary keywords, color-coded status, and menus, and are authorized to delete documents within the system. Managers DO NOT have access to the administration functions.**
3. **Editors** – This group contains the role Editor and is the most often assigned group to everyday system users.
4. **Authors** – This group contains the role Author. This Group is not recommended for most users and should be used only in special circumstances, such as, a **special guest whose expertise** is required but should have very limited access to the application.
5. **Read-Only Users** – This group contains the role Reader. This group is most often assigned to **visitors or observers who have no need to enter information into the application.**

REPORT ACCESS

6. **Models** – This group contains the role Models and should be assigned to those individuals with modeling capabilities.
7. **Lock Override** – This group contains the role Override Lock and is generally given to those users with Manager and Admin roles.
8. **Read All Docs** – This group contains the role Read All and should be given with discretion as it allows a user to Read ALL documents within the application even if they have no Distribution rights to that document.
9. **Release Locks** – This group contains the role Release Locks and is generally given only to those with System Admin privileges. A user in this group can release a lock from any document within the application.
10. **Resource Approvers** – This group contains the role Resource Approver. This is generally given only to those individuals whose responsibility it is to approve procurements in the resource request report.
11. **Task Approvers** – This group contains the role Task Approver. This is generally given only to those individuals whose responsibility it is to approve tasks and subtasks.

Appendix B: Roles

The NC4 Application is delivered several predefined roles. The role consists of system access and report access. These are the roles most commonly used among customers.

SYSTEM ACCESS by Hierarchy

1. **Admin** – This role provides the user with all privileges available within the NC4 application.
2. **Manager** – This role provides the user with all privileges for reports and features not related to the Administration functions.
3. **Editor** – This role provides the user with all Editor privileges for reports and features not related to the Data Dictionary or Administration functions.
4. **Author –** This role provides the user with all Author privileges for reports and features not related to the Data Dictionary or Administration functions.
5. **Read-Only User** – This role provides the user with all Reader privileges for reports and features **not** related to the **Data Dictionary or Administration** functions.

REPORT LEVEL ACCESS

6. **Models –** This role provides users with the ability to view the Model Operator's Workspace and, if given Editor privileges, to add and delete models using the Model Operator's Workspace accessible from the Hazard Model Report.
7. **Override Lock** – This role provides users with the ability to override document locks so that another user can take control of a document.
8. **Read All –** This role provides users with the ability to view documents even though they are not a member of a Distribution Group (if Distribution was enabled on that report).
9. **Release Locks** – This role provides users with the ability to see the Document Locking view and release locks from within the view.
10. **Resource Approver** – This role provides users with the ability to see AND make changes to the **Approved By** field located on the Resource Request document.
11. **Task Approver** – This role provides users with the ability to see AND make changes to the **Approved By** field located on the Task and Sub-Task reports.

OPTIONAL

12. **ARE Access** - This role provides the user with access to the ARE option (when enabled) in the Toolbar.
13. **Dashboard Access** - This role provides the user with access to the Dashboard option (when enabled) in the Toolbar.
14. **Formbuilder Access** - This role provides the user with all rights and access to the Form Builder (Custom Forms) option (when enabled). Option is located under the Administration menu.
15. **TIP ISAC Editor** - This role provides users with the ability to read AND make changes to the ISAC ONLY sections of the Tip Submission report.
16. **TIP ISAC Reader** - This role provides users with the ability to read the ISAC ONLY sections of the Tip Submission report.

Appendix C: Privileges

There are five different types of privileges available within the NC4 Application. These privileges are identified on a report-by-report or feature by feature basis.

- **Manager** - Grants the user access to create, read, and edit reports.
- **Editor** - Grants the user access to create, read and edit reports.
- **Reader** - Grants the user access to **read** reports.
- **Author** - NOT RECOMMENDED. Grants the user the right to **create and update his/her OWN reports and read reports created by others.** However, the user cannot edit reports created by others. This access level is not recommended since if User A creates a Resource Request and sends it to User B for processing, and User B has only Author access, User B will not be able to edit the document. Similarly, if User C creates an Incident Report, and User D needs to update this report with new information, if User D has only Author access, they won't be able to update the report. It is recommended that users be given Editor access instead. You can use the History and logging functions to catch inappropriate editing of documents and take appropriate action.
- **Delete** - Grants the user the right to delete reports.

The table below defines the privileges that are available for some reports and features within the NC4 Application.

Name	Privilege(s)	Description
ETMapOverlay		Controls ability to create Map Overlays.
ETModels		Controls ability to create use the Hazard Model Operator's Workspace
ETOverrideLock		Controls ability to override locks on documents that have been placed in Update mode.
ETReadAllDoc		Controls ability to read all documents within the system regardless of individual document distribution setting(s).
ETReleaseLocks		Controls ability to release locks on documents that have been placed in Update mode.
ETResApprover		Provides user with the right to approve resource requests.
ETTaskApprover		Provides user with the right to approve tasks.
action_request	Author, Delete, Editor, Reader	Controls access to the Action Request.
activity_center	Author, Delete, Editor,	Controls access to the Incident

	Reader	Management Center (formerly Activity Center).
agency_sitrep	Author, Delete, Editor, Reader	Controls access to the Agency Situation Report.
alert_bulletin	Author, Delete, Editor, Reader	Controls access to the Alert Bulletin
attachments	Author, Delete, Editor, Reader	Controls access to the Attachments section of all reports. A user must be given these rights in addition to report rights in order to establish rights to the attachments section of a report for which they have been given privileges. Attachments AUTHOR – Users with this privilege can add attachments to a report that they created AND read attachments that have been added to reports of that type that have been created by others. The Add Attachments button should be visible in Read mode only on those reports CREATED by this user. Attachments READER – Users with this privilege can see the attachments section of a report AND can read attachments that have been added to a report for which they have been given privileges. They should NEVER see the Add Attachments button on the report while in Read mode. Attachments EDITOR – Users with this privilege have the ability to see the attachments section of a report AND to add AND read attachments to reports for which they have been given privileges. They should always see the Add Attachments button on the report while in Read Mode. Attachments DELETE – Users with this privilege are the only users that should see the DELETE

		button after clicking on an attachment link.
Business_loss	Author, Delete, Editor, Reader	Controls access to the Business Loss report
call_center	Author, Delete, Editor, Reader	Controls access to the Call Center Report.
call_log	Author, Delete, Editor, Reader	Controls access to the Call Log.
case_dependent	Author, Delete, Editor, Reader	Controls access to case Dependent information
case_management	Author, Delete, Editor, Reader	Controls access to the Case Management Report
case_voucher	Author, Delete, Editor, Reader	Controls access to Case Vouchers
config	Author, Editor, Reader	Controls access to the Configuration Report.
coop	Author, Delete, Editor, Reader	Controls access to the Coop Report.
corporate_sitrep	Author, Delete, Editor, Reader	Controls access to the Corporate Situation Report.
critical_asset	Author, Delete, Editor, Reader	Controls access to the Critical Asset Report.
Data_dictionary	Editor, Reader No DELETE privilege. Data Dictionary documents are integral system documents and cannot be deleted. No AUTHOR privilege as these documents are delivered with the system.	Controls access the Data Dictionary Keywords, Color Coded Status, Menu Modification and Default View documents. NOTE: This privilege DOES NOT control access to Building Floor Plans.
data_sharing	Author, Editor, Reader	Controls access to the Data Sharing section of all reports. You must give a user rights to a report in order to establish rights to Data Sharing. Data Sharing AUTHOR – Users with this privilege can see and update the Data Sharing section of reports that they created AND read the Data Sharing section of reports of that type that have been created by others. The UPDATE button is only visible on reports that they have created. Data Sharing READER – Users with this privilege can see the Data Sharing section of a report for which they have been given privileges however, they have no

		ability to update this section. Since they have reader-only rights, the report can only be viewed in read mode and there should be no UPDATE button visible on the report. Data Sharing EDITOR – Users with this privilege have the ability see the Data Sharing section of a report AND to make updates to reports for which they have been given privileges. They should always see the Update button on the report while in Read Mode.
datasharing_config	Author, Delete, Editor, Reader	Controls access to the Data Sharing Configuration Report.
datasharing_queue	Delete, Reader	Controls access to queue monitoring
db_password	Delete, Reader	Controls access to data base password
distribution_group	Author, Delete, Editor, Reader	Controls access to the Distribution Group Administration document.
distributions	Author, Editor, Reader No DELETE privilege. This privilege controls access to a section of a document. Deletion occurs at the document level.	Controls access to the Distribution section of all reports. You must give a user rights to a report in order to establish rights to Distribution. Distribution AUTHOR – Users with this privilege can see and update the distribution section of reports that they created AND read the distribution section of reports of that type that have been created by others. The UPDATE button is only visible on reports that they have created. Distribution READER – Users with this privilege can see the distribution section of a report for which they have been given privileges, however, they have no ability to update this section. Since they have reader-only rights, the report can only be viewed in read mode and there should be no UPDATE button visible on the report. Distribution EDITOR – Users with

		this privilege have the ability see the distribution section of a report AND to make updates to reports for which they have been given privileges. They should always see the Update button on the report while in Read Mode.
doc_library	Author, Delete, Editor, Reader	Controls access to the Document library
donations	Author, Delete, Editor, Reader	Controls access to the Donations Report
drs_configuration	Delete, Editor, Reader	Controls access to Data Replication Services
dsm	Author, Delete, Editor, Reader	Controls access to the Disease Surveillance Report.
duty_log	Author, Delete, Editor, Reader	Controls access to the Duty Log.
email_group	Author, Delete, Editor, Reader	Controls access to the Email Groups document.
emergency_event	Author, Delete, Editor, Reader	Controls access to the Emergency Event Report.
enhance_duty_log	Author, Delete, Editor, Reader	Controls access to the Enhanced Duty Log.
gis_configuration	Author, Delete, Editor, Reader	Controls access to the GIS Configuration document.
group	Author, Delete, Editor, Reader	Controls access to the Group Administration document.
hazard_model	Author, Delete, Editor, Reader	Controls access to the Hazard Model Report.
hazmat_facility	Author, Delete, Editor, Reader	Controls access to the HazMat T-II Facility Report.
history	Reader	Controls access to the History feature.
hospital	Author, Delete, Editor, Reader	Controls access to the Hospital Report.
hotline	Author, Delete, Editor, Reader	Controls access to the Hotline Report.
housing_loss	Author, Delete, Editor, Reader	Controls access to the Housing Loss Report.
incident	Author, Delete, Editor, Reader	Controls access to the Incident Report.
intel_biography	Author, Delete, Editor, Reader	Controls access to the Biography Intelligence Report.
intel_entity	Author, Delete, Editor, Reader	Controls access to the Entity Intelligence Report.
intel_location	Author, Delete, Editor, Reader	Controls access to the Location Intelligence Report.
intel_summary	Author, Delete, Editor, Reader	Controls access to the IntelligencenSummary Report.
internet_link	Author, Delete, Editor, Reader	Controls access to the Internet Links Report.

jurisdiction_sitrep	Author, Delete, Editor, Reader	Controls access to the Jurisdiction Situation Report.
medical_incident	Author, Delete, Editor, Reader	Controls access to the Medical Incident Report.
non_user_profile	Author, Delete, Editor, Reader	Controls access to **Non-User** Personal Profile documents. NOTE: This option DOES NOT refer to system User Profile documents.
notification	Author, Editor, Reader No DELETE privilege. This privilege controls access to a section of a document. Deletion occurs at the document level.	Controls access to the Notification section of all reports. You must give a user rights to a report in order to establish rights to Notification. Notification AUTHOR – Users with this privilege can see and update the notification section of reports that they created AND read the notification section of reports of that type that have been created by others. The UPDATE button is only visible on reports that they have created. Notification READER – Users with this privilege can see the notification section of a report for which they have been given privileges, however, they have no ability to update this section. Since they have reader-only rights, the report can only be viewed in read mode and there should be no UPDATE button visible on the report. Notification EDITOR – Users with this privilege have the ability see the notification section of a report AND to make updates to reports for which they have been given privileges. They should always see the Update button on the report while in Read Mode.
notification_queue	Reader, Delete	Controls access to the Notification Queue view. In this instance DELETE allows the user to select documents from within the view that should be deleted from the Queue. Documents deleted from

		the queue will be retained in the Notification Queue History.
organization_chart	Author, Delete, Editor, Reader	Controls access to the Organization Charts.
personnel	Author, Delete, Editor, Reader	Controls access to the Personnel Report.
plan_concern	Author, Delete, Editor, Reader	Controls access to the action plan concern functionality in Reports.
planned_activity	Author, Delete, Editor, Reader	Controls access to the Planned Activity Report.
planned_event	Author, Delete, Editor, Reader	Controls access to the Planned Event Report.
position_template	Author, Delete, Editor, Reader	Controls access to the Position template
position_entity_loss	Author, Delete, Editor, Reader	Controls access to the Position entity loss
public_facility	Author, Delete, Editor, Reader	Controls access to the Public Facility Report.
public_info	Author, Delete, Editor, Reader	Controls access to the Public Information (PIO) Report.
rapid_damage_assessment	Author, Delete, Editor, Reader	Controls access to the Rapid Damage Assessment Report.
rapid_infrastructure_evaluation	Author, Editor, Reader No DELETE privilege. This privilege controls access to a core document within the Data Dictionary.	Controls access to the Infrastructure Component Evaluation Table.
ref_doc	Author, Delete, Editor, Reader	Controls access to the Reference Document.
resource_request	Author, Delete, Editor, Reader	Controls access to the Resource Request.
road_closure	Author, Delete, Editor, Reader	Controls access to the Road Closure Report.
role	Author, Delete, Editor, Reader	Controls access to the Role Administration document.
shelter	Author, Delete, Editor, Reader	Controls access to the Shelter Report.
site	Author, Delete, Editor, Reader	Controls access to the Site Report.
staffing_plan	Author, Delete, Editor, Reader	Controls access to the Staffing Scheduling document.
sub_task	Author, Delete, Editor, Reader	Controls access to the Sub Task Report.
task	Author, Delete, Editor, Reader	Controls access to the Task Report.
task_template	Author, Delete, Editor,	Controls access to the Task

	Reader	Template functionality.
tip_intel	Author, Delete, Editor, Reader	Controls access to the Tip Intel Report.
tip_isac	Editor, Reader	Controls access to the Tip-Isac Report.
transit_system	Author, Delete, Editor, Reader	Controls access to the Transit System Report.
user	Author, Delete, Editor, Reader	Controls access to the User Administration document. In this instance DELETE causes the following to occur: The User Administration document is deleted but retained in History. The user is removed from all notification and distribution groups. The user's profile is no longer displayed in the User Directory views.
user_profile	Reader	Control access to User Personal Profile Documents (users must have a Login ID and password). This privilege allows users to view the profile documents of OTHER users. NOTE: System users are ALWAYS provided full access to their own Personal Profile document.
utility_outage	Author, Delete, Editor, Reader	Controls access to the Utilities Outage Report.
vendor	Author, Delete, Editor, Reader	Controls access to the Vendor Report.
volunteer	Author, Delete, Editor, Reader	Controls access to the Volunteer Report.
windshield	Author, Delete, Editor, Reader	Controls access to the Windshield Report.