MDSS
SYSTEM ADMINISTRATION
GUIDE

VERSION 2.3.3

Michigan Department of Community Health

April 22, 2008

11682.001.001-02
April 22, 2008

MDSS
SYSTEM ADMINISTRATION
GUIDE

VERSION 2.3.3

This User Guide was developed for the
Michigan Department of Community Health
by Altarum Institute under contract 071B6200382.

ALTARUM
SYSTEMS RESEARCH FOR BETTER HEALTH

Altarum
3520 Green Court, Suite 300 • Ann Arbor, Michigan 48105 • (734) 302-4600

Corporate Headquarters	Alexandria, VA	Washington, DC	San Antonio, TX	Portland, ME
734 • 302 • 4600	703 • 575 • 1200	202 • 828 • 5100	210 • 832 • 3000	207 • 772 • 1410

TABLE OF CONTENTS

1 SYSTEM ADMINISTRATION INTRODUCTION

Note: This guide assumes you are familiar with the MDSS Application User Guide.

The options within the **System Administration** menu are restricted to those in an administrative role such as the **SuperUser** or any role containing the name **"administrator"** or **"admin."** Other users do not have access to this menu.

There are many **Roles** defined within **MDSS** that determine the tasks each user can perform. **Roles** can relate to the type of work the person performs or their role within the system and the geography in which they perform these tasks. Depending on your state's specification, a user typically has only one role; however, more than one role can be implemented if necessary.

Permissions are defined within the application to determine the functions each **role** can perform. Different menus and options may be available depending on your role and permissions. Permissions are used to maintain case confidentiality.

Depending on your user role and permissions, the available options within the System Administration menu may differ. All of the available options regardless of role for the **MDSS** application are:

- Users
- Pending Work Queue
- Review Replaced Patients
- Administrative Reports
- NETSS Export
- NETSS Mappings
- SNOMED Mappings

- Lab Table
- Aggregate Disease List
- Legacy Aggregate Case Reporting
- Messages Menu

Note: Users of the System Administration menu and its options are used by System Administrators and are referred to as "the administrator or system administrator" throughout this guide.

Each menu option is discussed in its own section. In order to use this guide proficiently, refer to the menu option and then the specific task you need to perform.

UNDERSTANDING USER ROLES AND PERMISSIONS

A user role with the name "administrator" or "admin" within the role is able to create a new user account/user role.

User roles are typically grouped by Jurisdiction or geographic access. **Geographic access** describes the geographic location where the user has access. Some examples are: Statewide, Region, County, Hospital (including hospital lab), and Laboratory.

Refer to **Appendix C** for a list of your state's **Roles** and **Permissions**, unique instructions, and a list of terms that are used to explain the roles/permissions.

2 USERS

The **Users** option from the **System Administration** menu provides all of the functions necessary to manage the application's users.

Administrators can perform the following using the **USERS** options/buttons:

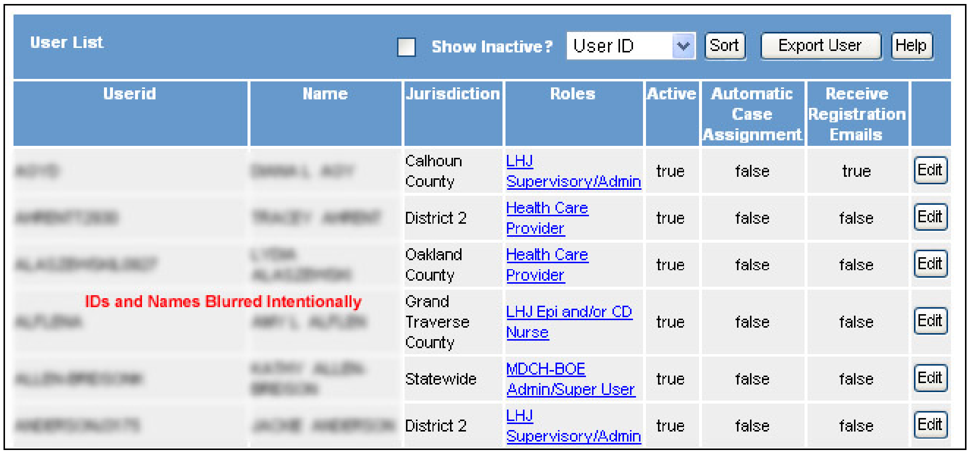
- View users
- Edit user roles
- View role privileges
- Activate or inactivate a user
- Designate automatic case assignments
- Designate which users will receive registration emails
- Invoke the email system in order to send an email to the User
- Export the user list

VIEWING USERS

To view the current list of users, perform the following:

1. Click on the **SYSTEM ADMINISTRATION** menu (located in the TopBar). The "User List" immediately appears.

Figure 2-1: User List



2. To display all users, including "inactive" users, check the "Show Inactive?" checkbox. Clear the checkbox to show only active users.

3. The fields and their descriptions are listed in the table:

Table 2-1: User List Fields

FIELD	DESCRIPTION
Userid	User Identification name of the user.
Name	Name associated with the user.
Jurisdiction	Name of the geographic access where the user is accessing the application.
Roles	Displays the role name for the user. The role name can be clicked to view the associated privileges.
Active	Indicates whether the user is active or inactive by displaying true or false, respectively.
Automatic Case Assignment	Indicates whether the user is assigned cases automatically or not by displaying true or false.
Receive Registration Emails	Indicates whether the user will receive registration emails or not by displaying true or false.

4. You can sort the list by User ID, Jurisdiction, Role, or status (Active/Inactive). To change the sort order, select one of these elements in the drop-down list (to the left of the **Sort** button) and then click **Sort**.

5. To edit user details, including role, click the **Edit** button associated with the user's row.

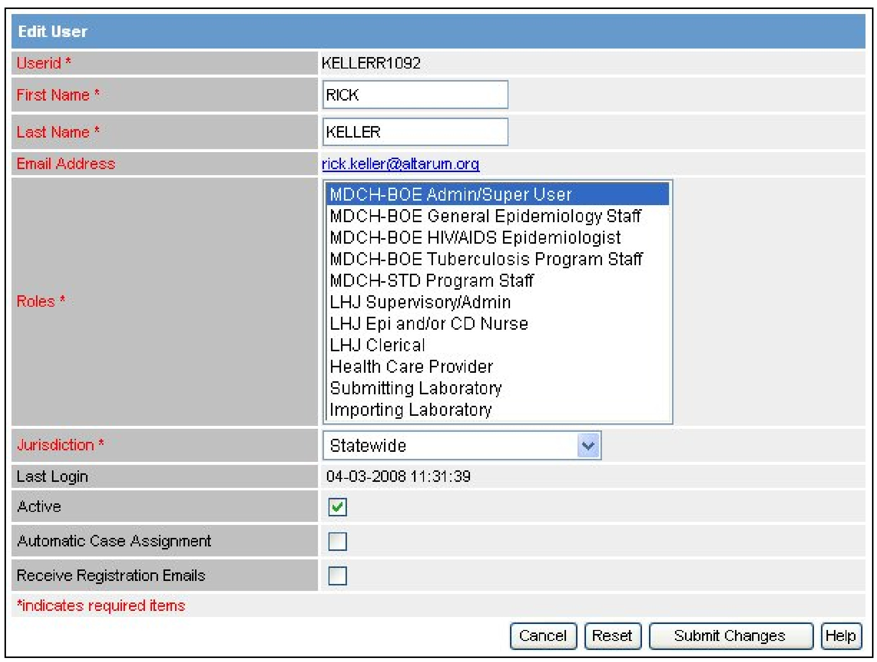
EDITING A USER'S ROLE AND OTHER SETTINGS

To **EDIT** a user's role, perform the following:

1. Click on the **SYSTEM ADMINISTRATION** menu (located in the TopBar). The "User List" immediately appears.

2. Click the **Edit** button associated with the user's row. The "Edit User" screen appears.

Figure 2-2: Edit User



Edit User

Userid *	KELLERR1092
First Name *	RICK
Last Name *	KELLER
Email Address	rick.keller@altarum.org
Roles *	MDCH-BOE Admin/Super User MDCH-BOE General Epidemiology Staff MDCH-BOE HIV/AIDS Epidemiologist MDCH-BOE Tuberculosis Program Staff MDCH-STD Program Staff LHJ Supervisory/Admin LHJ Epi and/or CD Nurse LHJ Clerical Health Care Provider Submitting Laboratory Importing Laboratory
Jurisdiction *	Statewide
Last Login	04-03-2008 11:31:39
Active	☑
Automatic Case Assignment	☐
Receive Registration Emails	☐

*indicates required items

Cancel | Reset | Submit Changes | Help

3. The fields and their descriptions are listed in the table. You can edit first and last name, selected role, selected jurisdiction, status as active or inactive, whether case assignment is automatic, and whether the user will receive registration emails.

Table 2-2: Create/Edit User Role Fields

FIELD	DESCRIPTION
Userid	User Identification name of the user.
First Name	First name of the user. This field is editable.
Last Name	Last name of the user. This field is editable.
Email Address	This field will only show on the "Edit User" window and will display an authentic email address. This is the email link that will appear when editing a user. The email address is pulled from LDAP and will not appear on the "User List" display. This field is not editable but is an HTML mail-to link. The result of clicking on the link is dependent upon the browser, but Internet Explorer will attempt to open the system's default mail client.
Roles	Displays the various role name(s) that can be assigned to the user. This field is editable.
Jurisdiction	Location of the user. Click the drop-down arrow to view/select a valid choice. This field is editable.
Last Login	Displays time and date of the user's last login.
Active	A checkbox to indicate whether the user is active or inactive. This field is editable.
Automatic Case Assignment	A checkbox to Indicate whether the user is assigned cases automatically or not. Will display true or false on the User List. This field is editable.
Receive Registration Emails	A checkbox to indicate whether the user will receive registration emails or not. Will display true or false on the User List. This field is editable.

4. At a minimum, fill in the "red* (asterisked)" fields.
5. When finished, click one of the available buttons:
   - **CANCEL** – Terminates the edit process and returns you to the "User List" screen. If you have changed

any information, a "warning prompt" is displayed asking you to verify your intention to cancel.

a) If you click the **CANCEL** button, you will return to the edit process.

b) If you click the **OK** button, you will lose any values that you entered.

- **RESET** – Erases any changes that you made.
- **SUBMIT CHANGES** – Saves the changes to the database and redisplays the "User List" screen.

DISPLAYING A USER'S ROLE DETAILS

To view the specific role details (Data Restriction, Privileges, and Program Access) for a user, perform the following:

1. Click on the **SYSTEM ADMINISTRATION** menu (located in the TopBar). The "User List" immediately appears.

2. From the "User List" locate the User whose role you want to display and click on the **ROLES** hyperlink. The "User's "Role List" appears revealing the privileges for the id.

Figure 2-3: User Role List

MDCH-BOE Admin/Super User	
Data Restriction	Statewide
Privileges	View Administrative Reports Overall System Admin Dedup View Data Modify Aggregate Cases NETSS Export Data Case Entry Dedup SNOMED Create New Users Add/Modify Alerts, All Assign Cases Edit Data
Program Access	All

3. The fields and their descriptions are listed in the table:

Table 2-3: User Role Fields

FIELD	DESCRIPTION
Role	Displays the role name of the user.
Data Restriction	Displays the user's area that is isolated for viewing.
Privileges	Lists the specific permissions the user can view/access.
Program Access	Category of access.

4. Click on a different menu option to exit the screen.

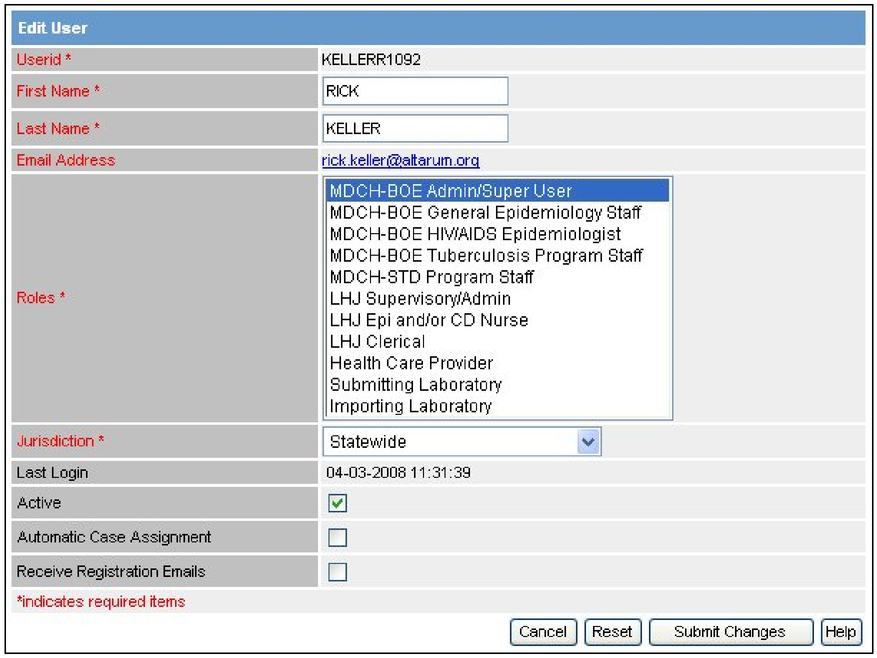
EDITING USER/ROLE INFORMATION

To edit an existing user's **USER-ID** or **ROLE** information, perform the following:

1. From the TopBar, point and click the **System Administration** menu. The current "User List" immediately appears as though you clicked the **USERS** option.

2. Click the **EDIT** button (located to the far right of the User.) The "Edit User Role" screen appears:

Figure 2-4: Edit User/Role Information



3. The fields and their descriptions are listed above in the section titled, "Editing a User's Role and Other Settings."

> ***Note:*** The **ACTIVE** field indicates whether the user is active (enabled/checked) or inactive (disabled/unchecked). Additional information is available in the section titled, "Activating/Inactivating a User."

4. Point your mouse cursor and click (or tab) to the field that you want to change. At a minimum, you must fill in the "Red*" (asterisked) fields.

5. Make the necessary changes and press one of the available buttons:

- **CANCEL** – Terminates the process of editing the user and returns to the "User List" screen. If you have changed any case information, a "warning prompt" is displayed asking you to verify your intention to cancel.

    a) If you click the **CANCEL** button, you will return to the editing process.

b) If you click the **OK** button, you will lose any edits that you entered.

- **RESET** – Erases any changes that you made.
- **SUBMIT CHANGES** – Begins a validation process and if there are no errors, saves the changes you made.

ACTIVATING/INACTIVATING A USER

Since cases are assigned to investigators by their User-ID, users cannot be deleted from the application but can be inactivated.

To activate or inactivate a user, perform the following steps:

1. Follow the steps in the section titled, "Editing User/Role Information" and then perform the following:
   - **INACTIVATE A USER** – Remove the checkmark from the "**Active**" checkbox by clicking on the checkmark. The inactive user will no longer be able to access the application; however, this does not effect the user's current application session if (s)he is currently logged in.
   - **ACTIVATE A USER**—Place a checkmark into the "Active" field by clicking inside the checkbox.
2. Click the **SUBMIT CHANGES** button.

SETTING/UNSETTING AUTOMATIC CASE ASSIGNMENT

The application assigns new cases to users who are designated to receive the automated case assignment.

To set or unset Automatic Case Assignment, perform the following:

1. Follow the steps in the section titled, "Editing User/Role Information" and then perform the following:

- **To designate the user to receive automatic case assignments**, place a checkmark in the “Automatic Case Assignment” field.
- **To stop a user from receiving automatic case assignments**, remove the checkmark from the “Automatic Case Assignment” field by clicking on the checkmark.

2. Click the **SUBMIT CHANGES** button.

SETTING/UNSETTING RECEIPT OF REGISTRATION EMAILS

To change a user’s registration email flag, perform the following steps:

1. Follow the steps in the section titled, "Editing User/Role Information" and then perform the following:

- **To designate the user to receive registration emails**, place a checkmark in the "Receive Registration Emails" field.
- **To stop a user from receiving registration emails**, remove the checkmark from the "Receive Registration Emails" field by clicking on the checkmark.

2. Click the **SUBMIT CHANGES** button.

EXPORTING THE USER LIST

This option provides the ability to **export** the **User List** to a Comma Separated Value (**CSV**) report.

The columns that will be exported are:

- Userid
- Last Name
- First Name

- Email
- Jurisdiction
- Roles (pipe delimited)
- Last Login (date and time)
- Active
- Automatic Case Assignment
- Receive Registration Emails

The email address for each user will be pulled from LDAP at the time of the export.

1. From the "User List" window, click the **EXPORT USER** button. There may be a brief "waiting" interval before the file download dialog box appears. The "waiting" interval is relative to the number of users being exported. The "File Download" dialog box will appear asking you to confirm your choice to download the export file.
2. Click the **SAVE** button. The "Save As" dialog box appears asking you to select a location on your computer to store the export file.

   Note: You may also provide a filename if you do not want to accept the default that uses the same name as the name of the search.

3. Provide the **LOCATION** for the file and either accept the default **FILENAME** or provide your own filename by typing on top of the default.
4. Click the **SAVE** button. Your exported data file will now reside on your computer in the location you specified.

3 PENDING WORK QUEUE

The **Pending Work Queue** function within the System Administration menu provides all of the functions necessary to resolve deferred duplicate patient and case records.

Patients and cases are automatically de-duplicated (or matched) by the application to reduce duplicate entries for patients and cases; thus, improving the data quality. However, there are instances when the deduplication process allows the processing of these possible duplicate records to be postponed. These instances are:

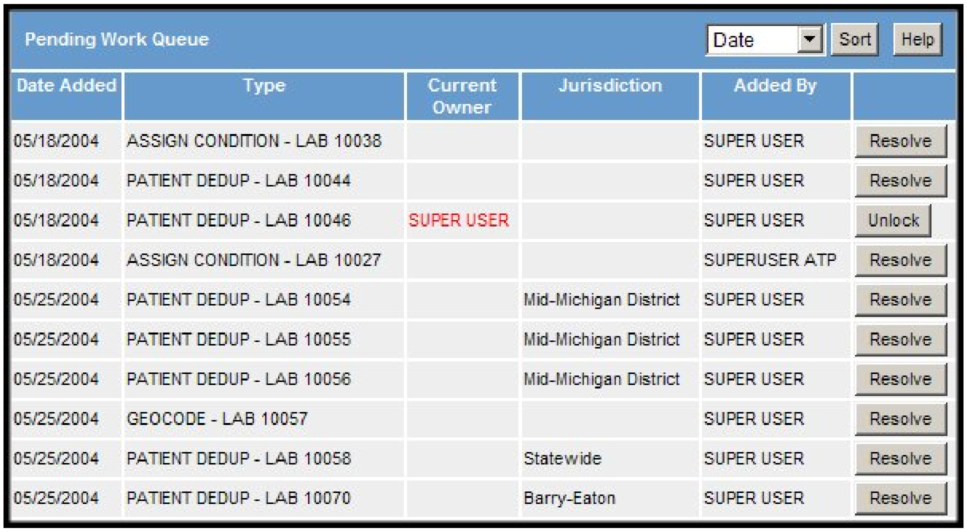
- New cases that are entered by clerical or healthcare providers (or the healthcare providers' staff.)
- Cases created from Electronic Laboratory Reports. Refer to the section titled, "View/Editing Case Details – Lab Reports Tab – Electronic Lab Reports" for more information.
- Patient or case records that have been deferred during the deduplication process. Refer to the section titled, "New Case (Adding) - Background Processing when Saving Cases - Deduplication."

When deduplication is postponed, the record is placed into the **Pending Work Queue** to resolve later.

To access the **Pending Work Queue**, perform the following:

1. From the **System Administration** menu, click the **Pending Work Queue** option from the SideBar. The "Pending Work Queue" list appears:

Figure 3-1: Pending Work Queue List



Pending Work Queue — Date | Sort | Help

Date Added	Type	Current Owner	Jurisdiction	Added By	
05/18/2004	ASSIGN CONDITION - LAB 10038			SUPER USER	Resolve
05/18/2004	PATIENT DEDUP - LAB 10044			SUPER USER	Resolve
05/18/2004	PATIENT DEDUP - LAB 10046	SUPER USER		SUPER USER	Unlock
05/18/2004	ASSIGN CONDITION - LAB 10027			SUPERUSER ATP	Resolve
05/25/2004	PATIENT DEDUP - LAB 10054		Mid-Michigan District	SUPER USER	Resolve
05/25/2004	PATIENT DEDUP - LAB 10055		Mid-Michigan District	SUPER USER	Resolve
05/25/2004	PATIENT DEDUP - LAB 10056		Mid-Michigan District	SUPER USER	Resolve
05/25/2004	GEOCODE - LAB 10057			SUPER USER	Resolve
05/25/2004	PATIENT DEDUP - LAB 10058		Statewide	SUPER USER	Resolve
05/25/2004	PATIENT DEDUP - LAB 10070		Barry-Eaton	SUPER USER	Resolve

2. The fields/columns and their descriptions are listed in the table:

Table 3-1: Pending Work Queue Columns

FIELD/COLUMN	DESCRIPTION
DATE ADDED	Date the Patient or Case record entered the Queue.
TYPE	Category of the Patient/Case record waiting in the Queue.
CURRENT OWNER	Owner of the Patient/Case record.
JURISDICTION	Geographic area of the Patient/Case record.
ADDED BY	User-ID that added the Patient/Case record to the Queue.

3. Determine the action you want to perform and continue to its respective section below. The actions that can be performed are:

- Selecting a Different Sort Order
- Resolving Deduplications
- Unlocking Pending Work Queue Items

SELECTING A DIFFERENT SORT ORDER

To select a different **SORT** order, perform the following steps:

1. Click the **SORT** drop-down menu arrow (located at the top of the screen, to the left of the "Sort" button.) to view/select a **SORT** order.

Figure 3-2: Pending Work Queue Sort

2. Click the **SORT** button to initiate the sort and the Pending Work Queue items will display in the order you specified.

RESOLVING PATIENT/CASE DEDUPLICATIONS

To resolve **Pending Work Queue** records, perform the following steps:

1. From the **System Administration** menu, click the **Pending Work Queue** option from the SideBar. The "Pending Work Queue" list screen appears:

2. Locate the Patient whose record you want to resolve and click the **RESOLVE** button (located to the far right of the patient record.)

3. Refer to the section titled, "New Case (Adding) – Background Processing when Saving Cases – Deduplication" in the Application User Guide for complete instructions.

UNLOCKING PENDING WORK QUEUE ITEMS

When resolving a **Pending Work Queue** record, the record is locked so other users cannot concurrently access the record. This lock is not released until the record is resolved. Thus, this record is unavailable to everyone.

The **UNLOCK** button on the "Pending Work Queue" screen forces the unlocking of the record. Any processing that has occurred to this record since it was locked will be lost.

Note: This button is visible to the person holding the lock and to the **SuperUser.**

4 REVIEW REPLACED PATIENTS

The Review Replaced Patients option is accessible from the System Administration menu. It displays a history for all merged patients in the system and is used to review and "**unmerge**" them if the two merged patients were not the same person.

ABOUT THE UNMERGE PROCESS

Occasionally two patient records that were thought to be the same patient, and were de-duplicated (merged), turn out to be unique patients after all. When this happens, the data for the two patients must be **unmerged** and the original two patients restored.

Directly before two patients are merged, their individual data are archived. This archived data will be used when case unmerging becomes necessary. After the **unmerge process**, all data collected before the merge is restored automatically; however, any data added after the merge must be assigned to one patient (one patient of the two) by you during the unmerge process.

In general, you must assign each data element (lab reports, addresses, investigations) to only one patient. The exception to this rule is for addresses. It is valid to assign an address to both patients during an "unmerge;" however, this leads to another issue.

Each patient in the system can be associated to any number of residence addresses and the time periods during which the patient lived at those addresses. A patient cannot live in two places at the same time, so when unmerging, if assigning an address to a patient causes such a conflict, the application requires the user to edit the address date ranges to resolve the conflicts before completing the **unmerge**.

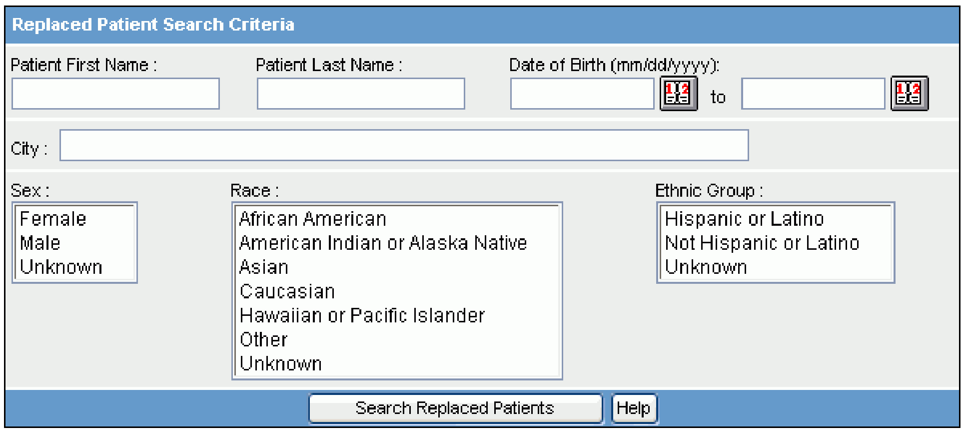
Note: Unmerge listings are not filtered by Geographic Access.

UNMERGING PATIENT INFORMATION

To "unmerge" patient information, perform the following steps:

1. From the System Administration menu, click the **Review Replaced Patients** option from the SideBar. The "Replaced Patient Search Criteria" screen appears.

Figure 4-1: Replaced Patient Search Criteria



2. You may either search for a specific patient or all patients:

- To **search for a specific patient**, type the known data into the fields.
- To **search for all patients**, do not type data into the fields.

3. Click the **SEARCH REPLACED PATIENTS** button. The "Replaced Patient List" appears.

Figure 4-2: Replaced Patient List

Replaced Patient List Help

Select Patient Replacement to Review

	Patients Replaced			Patient Replaced With			
Date of Replace	Name	Date of Birth	Gender	Name	Date of Birth	Gender	
06/08/2004	JACK SPRAT	11/27/1957	Male	JACK SPRAT	11/27/1957	Male	Review
	JACK SPRAT	11/27/1957	Male				
06/08/2004	SHARON GOTCHA	03/31/1991	Female	SHARON GOTCHA	03/31/1991	Female	Review
	SHARON GOTCHA	03/31/1991	Female				
06/08/2004	JACK BLACK	09/19/1953	Male	JACK BLACK	09/19/1953	Male	Review
	JACK BLACK	09/19/1953	Male				
06/09/2004	JEREMY GABLE	09/13/1988	Male	JEREMY GABLE	09/13/1988	Male	Review
	JEREMY GABLE	09/13/1988	Male				
06/09/2004	KEVEN MARK	12/14/1962	Male	KEVIN MARK	12/14/1962	Male	Review
	KEVIN MARK		Male				
06/09/2004	RONALD DONALD	03/17/1952	Male	RONALD DONALD	03/17/1952	Male	Review
	RONALD DONALD	03/17/1952	Male				
06/09/2004	GARY SMITH	02/13/1951	Male	GARY SMITH	02/13/1951	Male	Review
	GARY SMITH	02/13/1951	Male				
06/09/2004	HELEN MELLER	08/05/1916	Female	HELEN MELLER	08/05/1916	Female	Review
	HELEN MELLER	08/05/1916	Female				
06/09/2004	WILLIAM KYLES	09/21/1953	Male	WILLIAM KYLES	09/21/1953	Male	Review
	WILLIAM KYLES	09/21/1953	Male				
06/09/2004	SARAH MARS	11/19/1981	Female	SARAH MARS	11/19/1981	Female	Review
	SARAH MARS	11/19/1981	Female				

Revise Search Criteria

4. The fields and their descriptions are listed in the table:

Table 4-1: Replaced Patient List Fields/Columns

FIELD	DESCRIPTION
Date of Replace	Date the merge process of the patients was performed.
PATIENTS REPLACED	
Name	Name(s) of the patient that WAS replaced.
Date of Birth	Birth date of the patient that WAS replaced.
Gender	Sex of the patient that WAS replaced.
PATIENT REPLACED WITH	
Name	Name(s) of the patient that replaced those listed in the "Patients Replaced" column.
Date of Birth	Birth date of the patient that replaced those listed in the "Patients Replaced" column.
Gender	Sex of the patient that replaced those listed in the "Patients Replaced" column.

5. Locate the patient whose records you want to review and click the corresponding **REVIEW** button. The "Review Replaced Patients" screen appears.

Figure 4-3: Review Replaced Patients

	PATIENT A	PATIENT B	PATIENT C
Review Replaced Patients			
Source	Replaced Patient	Replaced Patient	Merge Result Patient
Patient ID	688118	59016	688117
Created Date	06/08/2004	06/08/2004	06/08/2004
Last Modified Date	06/08/2004	06/08/2004	06/08/2004
Patient Status	OUTPATIENT	OUTPATIENT	OUTPATIENT
First Name	JACK	JACK	JACK
Middle Name			
Last Name	WEAK	WEAK	WEAK
Date of Birth	11/27/1957	11/27/1957	11/27/1957
Gender	MALE	MALE	MALE
Race	CAUCASIAN	CAUCASIAN	CAUCASIAN
Ethnicity	NOT HISPANIC OR LATINO	UNKNOWN	NOT HISPANIC OR LATINO
Home Phone			
Other Phone			
Parent/Guardian First Name			
Parent/Guardian Middle Name			
Parent/Guardian Last Name			
Patient Addresses			
Adresses	1 NABISCO ALLEY IONIA, MI 48846 IONIA COUNTY	1 NABISCO ALLEY IONIA, MI 48846 IONIA COUNTY	1 NABISCO ALLEY IONIA, MI 48846 IONIA COUNTY

Continue Back

6. There are three columns containing demographic and case information. The three columns represent Patient A, Patient B, and Patient C.

7. Compare each field to determine if these patients should be unmerged and click one of the available buttons:

   - **BACK** – to return to the "Replaced Patient List."
   - **CONTINUE** – to go forward and continue with the unmerge process and display the "Unmerge Confirmation" screen.

Figure 4-4: Unmerge Confirmation

UnMerge Confirmation

Please review the following sections of information before continuing and finalizing the UnMerge process.

Review Replaced Patients

Merged Patient Record #688117 will be permanently lost.
Patient Records #59016 and #688118 will be recovered.

Outcome	Will be Recovered	Will be Recovered	Will be Lost
Patient ID	688118	59016	688117
Created Date	06/08/2004	06/08/2004	06/08/2004
Last Modified Date	06/08/2004	06/08/2004	06/08/2004
Patient Status	OUTPATIENT	OUTPATIENT	OUTPATIENT
First Name	JACK	JACK	JACK
Middle Name			
Last Name	WEAK	WEAK	WEAK
Date of Birth	11/27/1957	11/27/1957	11/27/1957
Gender	MALE	MALE	MALE
Race	CAUCASIAN	CAUCASIAN	CAUCASIAN
Ethnicity	NOT HISPANIC OR LATINO	UNKNOWN	NOT HISPANIC OR LATINO
Home Phone			
Other Phone			
Parent/Guardian First Name			
Parent/Guardian Middle Name			
Parent/Guardian Last Name			

Patient Addresses

Addresses	1 NABISCO ALLEY IONIA, MI 48846 IONIA COUNTY	1 NABISCO ALLEY IONIA, MI 48846 IONIA COUNTY	1 NABISCO ALLEY IONIA, MI 48846 IONIA COUNTY

Complete UnMerge | Back | Cancel

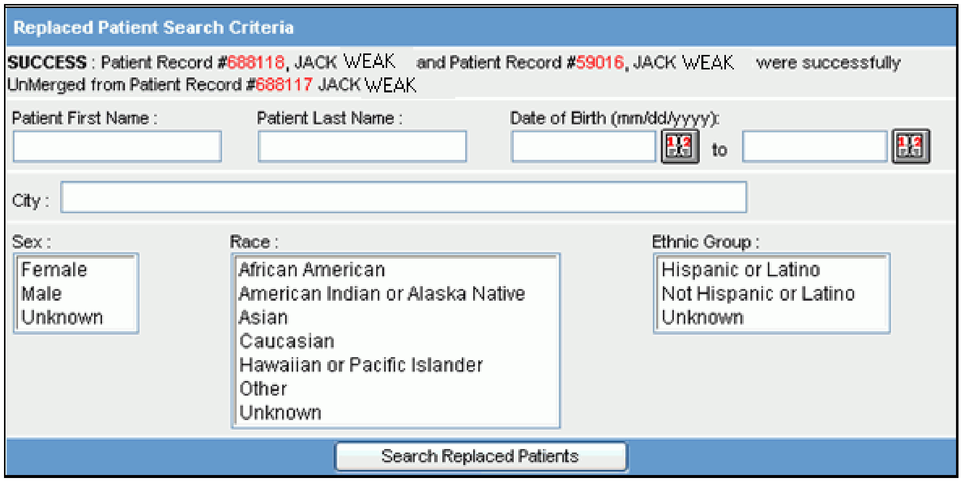
8. This is your last chance to review the patient information to determine if the records should be unmerged.

Note: Observe the specific Patient IDs that will be **Recovered** and will be permanently **Lost**.

9. Click one of the available buttons:

- **BACK** – to return to the "Review Replaced Patients" screen.
- **CANCEL** – to not continue and return to the "Replaced Patient List."
- **COMPLETE UNMERGE** – to continue with the unmerge process. The "Replaced Patients Search Criteria" screen reappears with a "success" message in the upper left corner.

Figure 4-5: Replaced Patient Search - Unmerge Success Message



10. This completes the "unmerge" process. Click a different menu and/or option to exit.

This page intentionally left blank

5 ADMINISTRATIVE REPORTS

The **ADMINISTRATIVE REPORTS** option is accessible via the System Administration menu by clicking the SideBar option.

Currently, there is only one report available, the "**Case Referral and Investigation Timeliness Summary**."

This report creates a listing of all cases that fall within the specified time period and disease information as defined by the report parameters. The case information can be further broken down by geographic boundaries by selecting the appropriate "Geographic Breakdown" radio buttons.

Access to the **Administrative Report** is limited to **Statewide** users and **Local Health Jurisdiction** administrators.

- **Statewide** users have no geographic level restrictions.
- **Local Health Jurisdiction** administrators are restricted to geographic levels from the Local Health Jurisdiction and the data from their jurisdiction.

Geographic Levels is a hierarchy of the largest to smallest geographic boundaries. Refer to the **Appendices** section for your specific state's list of User Roles and Permissions for a list of Geographic Levels.

This report can be produced in three different output formats.

REPORT OUTPUT FORMAT

The **Administrative Report** can be presented in three different formats:

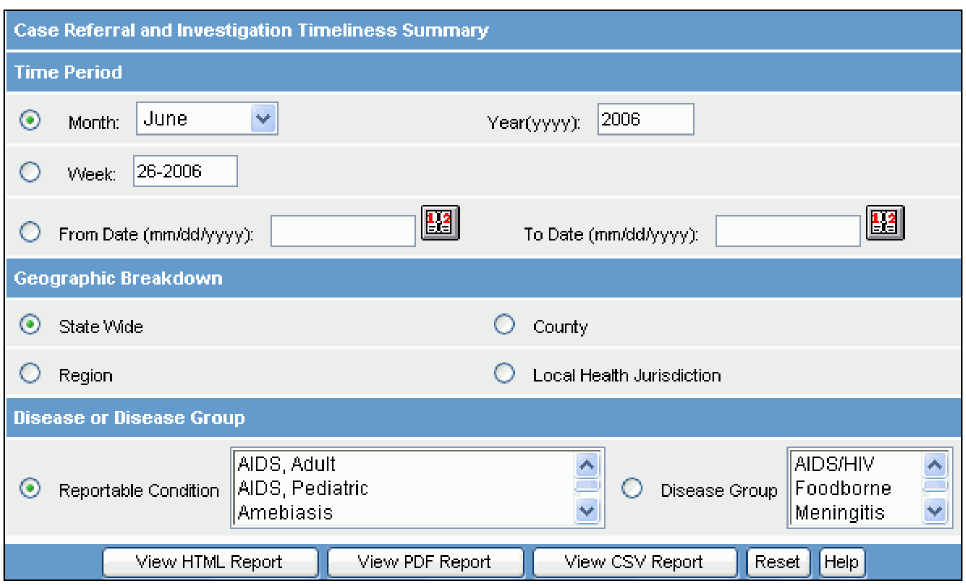
- **PDF** - Portable Document Format - a non-editable format. This report output will open in Adobe Reader.
- **HTML** – Hyper Text Markup Language - standard Web page format. This report output will open in a new browser window.
- **CSV** - Common Separated Value – a text file format. This report output can be opened and reviewed in a variety of applications such as Microsoft Word, Notepad, and Excel, depending on your PC configuration.

RUNNING A REPORT

To run a report, perform the following steps:

1. From the Top Navigation bar, click the **System Administration** menu.
2. From the SideBar, point and click the **Administrative Report** option. The "Administrative Report" selection screen appears:

Figure 5-1: Administrative Report Limitations/Selections



3. Refer to the table for a list of the major breakdown sections:

Note: This table includes every state's options, so you may not see all the categories/options listed below.

Table 5-1: Report Limitations/Selections

SELECTION AREA	DESCRIPTION
TIME PERIOD	The "Onset Date" must fall within the specified time period range. If the "Onset Date" is unavailable, the system will compare against the "Referral Date." The time period may be a selection of the following: • **Month**—limits the report to cases within the month selected. If the month radio button is selected you must select a month from the drop-down menu. • **Year**—limits the report to cases within the year provided. If the YEAR radio button is selected, you must provide a year. The year must be a valid 4-digit year and cannot be greater than the current year. • **MMR Week**—limits the report to cases within the "MMWR Week" provided. If the MMWR Week radio button is selected, you must provide a valid MMWR week in the format of a two-digit week and a four-digit year (i.e., 23-2005). • **From Date**—limits the report to cases within the date range provided. If the FROM DATE radio button is selected, you must provide a "FROM DATE" and a "TO DATE." The "From Date" must be a valid date, cannot be greater than the "To Date," and cannot be greater than the current date. The format must be mmddyyyy. • **To Date**—limits the report to cases within the date range provided. If the FROM DATE radio button is selected, you must provide a "From Date" and a "To Date." The "To Date" must be a valid date, cannot be less than the "From Date," and cannot be greater than the current date.
GEOGRAPHIC BREAKDOWN	This section provides radio buttons for selecting the geographic boundaries for the report. Each radio button is exclusive of the other options within this section. The geographic information selected will compare against the Investigation Address of the

SELECTION AREA	DESCRIPTION
	case. Only the cases that fall within the selected geographic boundary will be included on the report. • **Statewide**—All cases reported within the State will be included on the report. • **County**—All cases reported within the selected county(ies) will be included on the report. If no county is selected, then data for all counties are reported. • **Region**—All cases reported within the selected region(s) will be included on the report. No selection indicates all regions. • **(Local) Health Jurisdiction**—All cases reported within the selected jurisdiction(s) will be included on the report. No selection indicates all jurisdictions.
DISEASE **OR** **DISEASE GROUP**	This section of the screen provides the fields for selecting the Reportable Condition or the Disease Group for the report. Each radio button is exclusive of the other options within this section. Only the cases that fall within the selected reportable condition or conditions will be included on the report. Multiple disease or disease group selections are allowed. No selection indicates all diseases or disease groups. All cases matching the selected disease or disease group will be included on the report.

4. Type or select the values for the report parameters.

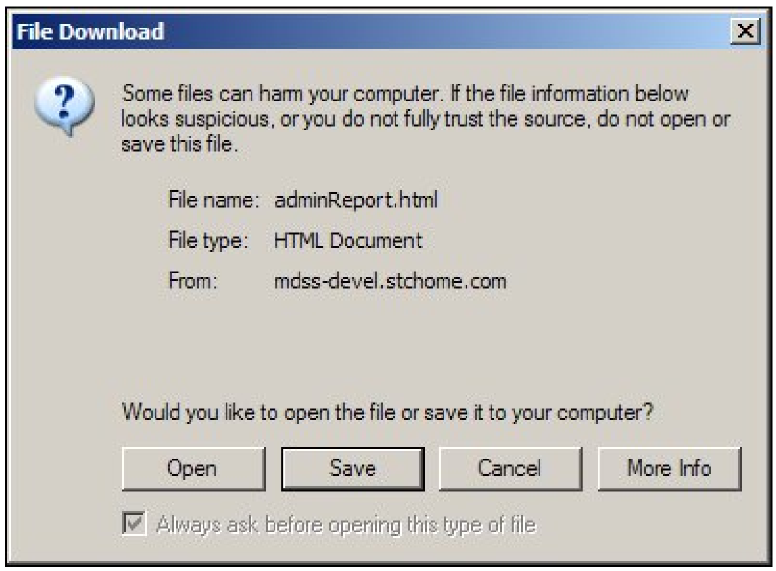
5. When you are finished selecting and defining the parameters, click one of the following buttons:

- **VIEW HTML REPORT** – opens a new window to display the report output as a standard Web document.
- **VIEW PDF REPORT** – opens Adobe Reader to display the report output as a PDF file.
- **VIEW CSV REPORT** – opens a new window to display the report output in either Microsoft Excel or Notepad; depending on the configuration of your PC.

- **RESET** – erases the values that you have supplied for the report parameters.

6. Assuming you have clicked one of the **VIEW REPORT** buttons, the following dialog box will appear asking you to confirm your choice to download the report output file. There may be a short waiting period before the "File Download" dialog box appears. The waiting period is relative to the number of cases contained in the report output file.

Figure 5-2: File Download Dialog



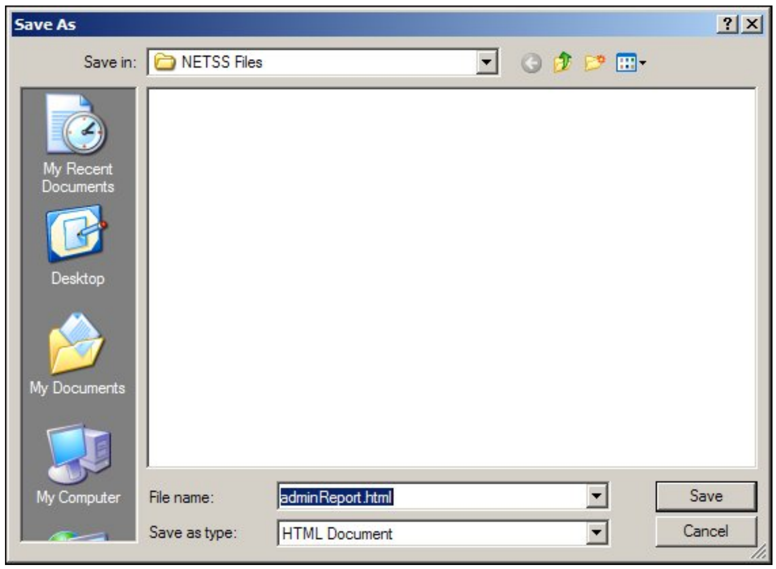
7. Click one of the available buttons:

- **OPEN** – Opens a new window to display the report output as appropriate for the report format selected. You may view and print your report output from this new window. When you are finished, you can close the window by clicking the **close** button located in the top right corner.
- **CANCEL** – Terminates the process of running and viewing the report and returns you to the report parameter screen.
- **MORE INFO** – Opens helpful information about downloading a file.

- **SAVE** – Allows you to save the report output on your PC in the format selected. Continue to the next step.

8. If you selected to **SAVE** your report output file, you will be asked to select a location on your computer to store the report output file and a file name.

Figure 5-3: Save File Dialog



9. Once you have entered the requested information, click the **Save** button. Your report output file will now reside on your computer in the location that you specified.

6 NETSS EXPORT

As the application collects information on disease events, a subset of this information is transmitted weekly to the CDC through NETSS.

The **NETSS** Export function in the System Administration menu provides the ability for the SuperUser to prepare a NETSS compliant extraction file.

NETSS transmission specifications are directed by the CDC. Although personal identifiers such as patient name and address are usually entered into the application, this information is not transmitted.

CASES THAT GET EXPORTED

Case Investigations with the Case Status of "Confirmed" or "Probable" and the Investigation Status of "Completed" will be reported to the CDC.

An exception is made for corrections where a case that was initially reported as "Confirmed" is changed to "Not a Case." In this instance, a "Deletion Record" will be included in the NETSS Export. Please refer to the section titled, "Deletion Records" for more information.

The information transmitted to the CDC is dependent on the type of record created and the specific reportable condition.

TRANSMITTED INFORMATION / RECORD TYPES

The **RECORD TYPES** that get transmitted are:

- Verification Records
- Core Records
- Deletion Records

VERIFICATION RECORDS (V RECORDS)

Verification records contain year-to-date counts for a particular disease. These records do not contain disease specific or patient identification information.

Verification records are used to synchronize the disease counts between the application and the CDC.

Verification records are identified within the NETSS Export file as "V Records."

CORE RECORDS

Information contained within a core record is determined by the record type, Individual (single case) or Summary (aggregate case.)

Summary record types are identified within the NETSS Export file as "S Records." The data contained within a summary record relates to the counts provided weekly using the Aggregate Case entry option.

Individual record types are identified within the NETSS Export file as "M Records." Extended information for these NETSS records is sent for the following Reportable Conditions:

- Hepatitis

- Meningitis
- Lyme Disease
- Measles
- Mumps
- Rubella
- Pertussis
- Tetanus
- Tuberculosis

DELETION RECORDS

If an application's "completed case" (which has already been exported) is changed to "Not a Case," a deletion record is created and sent to the CDC via the NETSS Export. This deletion record is used to correct the CDC information.

CREATING A NETSS EXPORT

The NETSS Export function creates a file that can be saved locally and then transmitted to the CDC. Once the file resides locally, the State will combine this file with other NETSS export files (from AIDS and STD program areas) and transfer the combined file to the CDC.

Upon exporting a Basic Export or Disease Specific (PDF) Export, the column names are SAS compliant.

There are two types of Exports that can be created:

- **WEEKLY** – to generate an export file for a specific MMWR Ending Week.

- **YEAR TO DATE** – to generate an export file for the entire year up to the current date. This option is used to synchronize the State and CDC data.

To generate an **EXPORT** file, perform the following steps:

1. From the System Administration menu, click the **NETSS EXPORT** option from the SideBar. The "NETSS Export" screen appears:

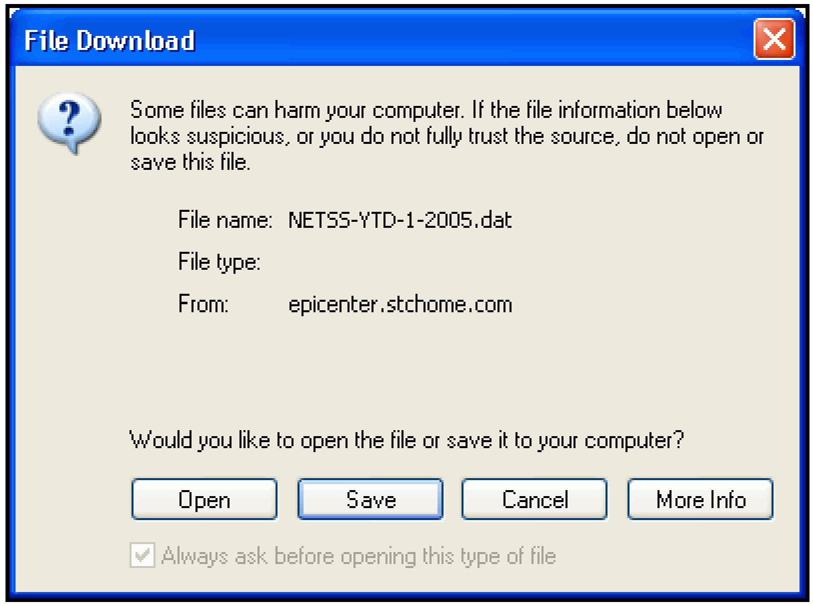
Figure 6-1: NETSS Export Screen

Note: This screen indicates the current week-ending date (at the very top of the window) along with the corresponding MMWR Publication Week.

2. Determine the type of **EXPORT** you want to perform. To export data for:
   - **WEEKLY** – type the MMWR Week desired in the "MMWR Ending Week" field using the two-digit week and four-digit year format (WW-YYYY) and click the EXPORT button.
   - **YEAR TO DATE** – Verify the MMWR Week is the current week and click the YEAR TO DATE RESET button.
3. The "File Download" dialog box appears asking you to confirm your choice to download the NETSS Export file.

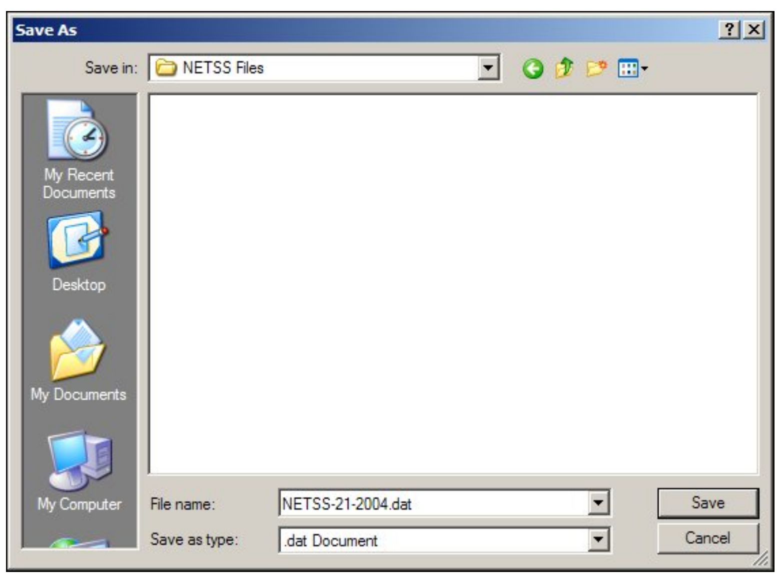
   Note: There may be a short waiting period before the "File Download" dialog box appears. The waiting period is relative to the number of cases being exported. The NETSS export is emailed to the email address designated in the MDSS properties file.

Figure 6-2: File Download Dialog



4. Click the **SAVE** button. The "Save As" dialog box appears asking for a location on your computer to store the export file and a name for the export file.

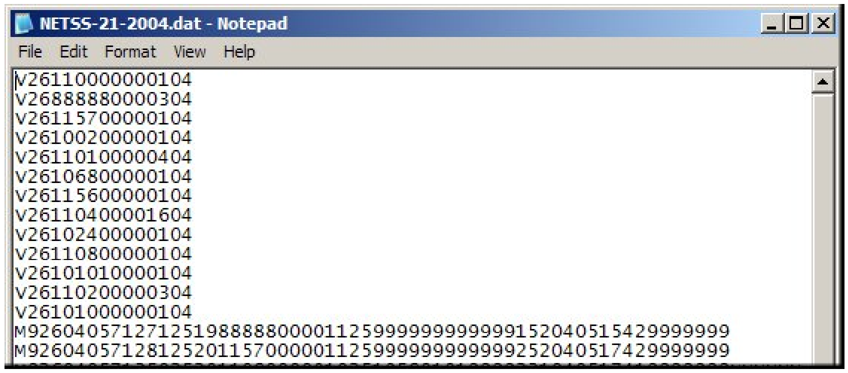
Figure 6-3: Save As Dialog



5. Once you have entered the requested information, click the **SAVE** button. Your **NETSS** Export file will now reside on your computer in the location that you specified.

A sample of the Weekly Export File (viewed with Microsoft NotePad) is shown below:

Figure 6-4: Weekly NETSS Export File



7 NETSS MAPPINGS

When the **NETSS** Export is executed, the application's Reportable Condition that is assigned to a case must be translated into a code that the CDC uses to identify the Disease Event. This CDC code is referred to as the NETSS Code.

The **NETSS** Mappings option in the System Administration module is used to maintain the association between the NETSS Code and the application's Reportable Condition.

Within the **NETSS** Mapping table, a single Reportable Condition is associated with a single NETSS code. Duplicate NETSS codes and duplicate Reportable Conditions are not permitted.

- If a Reportable Condition is not associated with a NETSS code, that Reportable Condition will not be exported by the NETSS Export.
- If a Reportable Condition is mapped to a NETSS code, it must also be set to either "Verification" or "Core" Reportable to be exported.

For more information regarding the NETSS Export, please refer to the section titled, "NETSS Exports."

CREATING A NETSS MAPPING

To **CREATE** a new **NETSS** Mapping, perform the following steps:

1. Click the **NETSS Mapping** option from the SideBar. The “NETSS List” screen appears:

Figure 7-1: NETSS List

Displaying results **1-10** of **115** found
[|< First] **1** 2 3 4 5 6 7 8 9 10 11 12 [Next >>] [Last >|]

NETSS List — Create Mapping | Help

NETSS Code	MDSS Code		
10010	Meningitis - Aseptic	Edit	Delete
10020	Brucellosis	Edit	Delete
10030	Chickenpox (Varicella)	Edit	Delete
10040	Diphtheria	Edit	Delete
10050	Encephalitis, Primary	Edit	Delete
10051	Encephalitis, St. Louis	Edit	Delete
10052	Encephalitis, Western Equine	Edit	Delete
10053	Encephalitis, Eastern Equine	Edit	Delete
10054	Encephalitis, California	Edit	Delete
10056	West Nile Virus	Edit	Delete

[|< First] **1** 2 3 4 5 6 7 8 9 10 11 12 [Next >>] [Last >|]

2. Click the **CREATE MAPPING** button (located at the top right corner). The "Create Mapping" screen appears:

Figure 7-2: Create Mapping

Create Mapping	
NETSS Code *	
Condition *	AIDS, Adult
Verification Reportable	☐
Core Reportable	☐

*indicates required items

Cancel | Reset | Create Mapping | Help

3. Move to the fields on the screen with mouse or **TAB** key.

4. The fields and their descriptions are listed in the table:

Table 7-1: Create Mapping Fields

FIELD	DESCRIPTION
NETSS Code	The CDC code that identifies the reportable condition. This is a required field.

FIELD	DESCRIPTION
Condition	The Reportable Condition. Click the drop-down menu arrow to view/select a reportable condition. Multiple selections are not permitted.
Verification Reportable	A checkbox indicating that the Reportable Condition is exported via the NETSS Export as a "Verification Record." This checkbox must be checked for this Reportable Condition to be included in a NETSS Export.
Core Reportable	A checkbox indicating that the Reportable Condition is exported via the NETSS Export as a "Core Record." This checkbox must be checked for this Reportable Condition to be included in a NETSS Export.

5. At a minimum, you must type/select values for the Fields displayed in Red* (with an asterisk).

6. When you are finished adding the information, click one of the available buttons:

- **CANCEL** – Terminates the process of adding a mapping and returns you to the "NETSS List" screen. If you have entered any information, a warning prompt is displayed asking you to verify your intention to cancel.

  a) If you click the **CANCEL** button, you will return to the adding process.

  a) If you click the OK button, you will lose any data that you have entered.

- **RESET** – Erases any entries that you made and remains on the same screen.

- **CREATE MAPPING** – Begins a validation process and if there are no errors, saves the new NETSS Mapping. You will return to the "NETSS List" screen.

EDITING A NETSS MAPPING

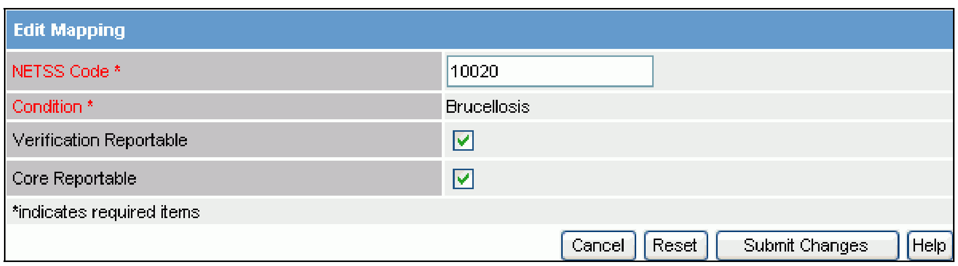
To edit an existing **NETSS** Mapping, perform the following steps:

1. Click the **NETSS MAPPING** option from the SideBar. The "NETSS List" screen appears.

2. From the "NETSS List" screen, locate the specific mapping you want to edit.

3. Click the **EDIT** button (located to the right of the specific mapping). The "Edit Mapping" screen appears with the previous values:

Figure 7-3: Edit Mapping



4. Point/click your mouse or click the **TAB** key to position your cursor in the field you want to change.

5. Make the necessary changes and press one of the available buttons:

- **CANCEL** – Terminates the process of editing a mapping and returns you to the "NETSS List" screen. If you have changed any information, a warning prompt is displayed asking you to verify your intention to cancel.

  a) If you click the **CANCEL** button, you will return to the editing process.

  a) If you click the **OK** button, you will lose any changes that you have made.

- **RESET** – Erases any changes that you made and remains on the same screen.

- **SUBMIT CHANGES** – Begins a validation process and if there are no errors, saves the changes to the NETSS Mapping. You will return to the "NETSS List" screen.

Note: If you attempt to navigate to another screen without clicking **RESET** or **SUBMIT CHANGES**, a warning message appears.

DELETING A NETSS MAPPING

Note: If you delete a NETSS Mapping record, the associated reportable condition will no longer be included in future NETSS Exports.

To **DELETE** a **NETSS Mapping**, perform the following steps:

1. Click the **NETSS MAPPING** option from the SideBar. The "NETSS List" screen
2. From the "NETSS List" screen, locate the specific mapping you want to **DELETE**.
3. Click the **DELETE** button (located on the far right of the NETSS Mapping.) A "warning dialog" box is displayed asking you to verify your intention to delete this mapping.
   - If you click the **OK** button, the mapping will be deleted and you will return to the "NETSS List" screen.
   - If you click the **CANCEL** button, the mapping will NOT be deleted and you will return to the "NETSS List" screen.

This page intentionally left blank

8 SNOMED MAPPINGS

When the State Public Health Laboratory confirms the diagnosis of a Reportable Condition, the laboratory sends this information to the application. The Electronic Laboratory Reports do not identify the Reportable Condition. Instead, these reports identify a positive test result (or numeric result within a confirming range) for a specific SNOMED (Systematized Nomenclature of Medicine) test code.

As the Electronic Laboratory Reports are processed, the SNOMED code provided in the report is used to lookup the associated Reportable Condition.

The **SNOMED** Mappings option on the System Administration menu is used to maintain the association between the SNOMED code and the application's Reportable Condition.

Within the **SNOMED** Mapping table, each SNOMED code is listed only once; however, a single Reportable Condition can have multiple SNOMED codes associated with it. If a SNOMED code is received that isn’t associated with a Reportable Condition, the Reportable Condition is left blank and the resulting case will be assigned to the State.

CREATING A SNOMED MAPPING

To **CREATE** a new **SNOMED** Mapping, perform the following steps:

1. From the **SYSTEM ADMINISTRATION** menu, click the **SNOMED MAPPING** option from the SideBar. The "SNOMED List" screen appears:

Figure 8-1: SNOMED List

Displaying results **1-10** of **315** found

[|< First] **1** 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 [Next >>] [Last >|]

SNOMED List — Create Mapping | Help

SNOMED Code	Condition		
L-10028	Gonorrhea	Edit	Delete
L-12202	Anthrax	Edit	Delete
L-12801	Pertussis	Edit	Delete
L-12921	Lyme Disease	Edit	Delete
L-13200	Brucellosis	Edit	Delete
L-13201	Brucellosis	Edit	Delete
L-13202	Brucellosis	Edit	Delete
L-13203	Brucellosis	Edit	Delete
L-13204	Brucellosis	Edit	Delete
L-13205	Brucellosis	Edit	Delete

[|< First] **1** 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 [Next >>] [Last >|]

2. Click the **CREATE MAPPING** button (located at the top of the screen). The "Create Mapping" screen appears:

Figure 8-2: Create Mapping

Create Mapping	
SNOMED Code *	
Condition *	AIDS, Adult
Description	
*indicates required items	

Cancel | Reset | Create Mapping | Help

3. Using your mouse or **TAB** key, move to the appropriate fields within the screen. The fields and their descriptions are listed in the table:

Table 8-1: Create SNOMED Mapping Fields

FIELD	DESCRIPTION
SNOMED Code	The standardized test code as assigned by SNOMED. This is a required field.
Condition	The Reportable Condition. Click the drop-down menu arrow to view/select a reportable condition. Multiple selections are not permitted.
Description	This field is optional. It is used to provide a brief description of the SNOMED/Reportable Condition association.

4. At a minimum, type/select the values for "Red*" (red asterisked) fields.
5. When finished, click one of the available buttons:
   - **CANCEL** – Terminates the process of adding a mapping and returns you to the "SNOMED List" screen. If you have entered any information, a "warning dialog" prompt is displayed asking you to verify your intention to cancel.
     - a) If you click the **CANCEL** button, you will return to the adding process.
     - a) If you click the **OK** button, you will lose any data that you have entered.
   - **RESET** – Erases any entries that you made and remains on the same screen.
   - **CREATE MAPPING** – Begins a validation process and if there are no errors, saves the new SNOMED Mapping and returns to the "SNOMED List" screen.

EDITING A SNOMED MAPPING

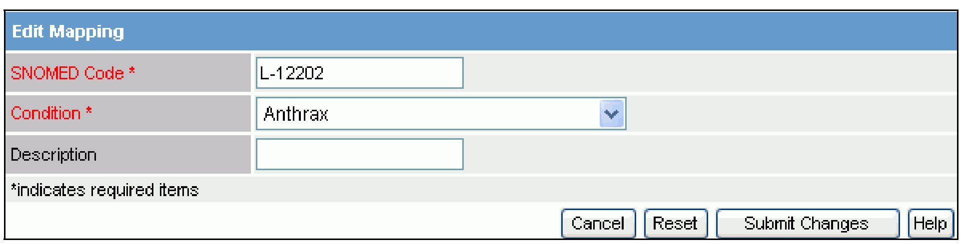
To **EDIT** an existing **SNOMED MAPPING** code, perform the following steps:

1. From the **SYSTEM ADMINISTRATION** menu, click the **SNOMED MAPPING** option from the SideBar. The "SNOMED List" screen appears.

2. From the "SNOMED List" screen, locate the specific code you want to edit.

3. Click the **EDIT** button (located to the right of the SNOMED code). The "Edit Mapping" screen appears:

Figure 8-3: Edit Mapping



4. Point/click your mouse cursor (or tab) to the field that you want to change.

5. Make the necessary changes and press one of the available buttons:

- **CANCEL** – Terminates the process of editing a mapping and returns you to the "SNOMED List" screen. If you have changed any information, a "warning dialog" prompt is displayed asking you to verify your intention to cancel.

  a) If you click the **CANCEL** button, you will return to the editing process.

  a) If you click the **OK** button, you will lose any changes that you have made.

- **RESET** – Erases any changes that you made and remains on the same window.

- **SUBMIT CHANGES** – Begins a validation process and if there are no errors, saves the changes to the SNOMED Mapping and returns to the "SNOMED List" screen.

Note: If you attempt to navigate to another screen without clicking **RESET** or **SUBMIT CHANGES**, a "warning dialog" prompt appears.

DELETING A SNOMED MAPPING

To **DELETE** a **SNOMED Mapping**, perform the following steps:

1. From the **SYSTEM ADMINISTRATION** menu, click the **SNOMED MAPPING** option from the SideBar. The "SNOMED List" screen appears.

2. From the "SNOMED List" screen, locate the specific code you want to **DELETE**.

3. Click the **DELETE** button (located on the far right of the SNOMED Mapping.) A "warning dialog" prompt is displayed asking you to verify your intention to delete this mapping.

- If you click the **OK** button, the mapping will be deleted and you will return to the "SNOMED List" screen.

- If you click the **CANCEL** button, the mapping will NOT be deleted and you will return to the "SNOMED List" screen.

This page intentionally left blank

9 LAB TABLE

The **LAB TABLE** option is used by the System Administrator to add names of facilities into the application.

You can perform the following using this option:

- View a list of the Facilities
- View the Users located at a specific Facility
- Create and/or Edit a Facility

VIEWING FACILITIES

To view an alphabetical list of the current facilities, perform the following:

1. Click on the **SYSTEM ADMINISTRATION** menu and then click on the **LAB TABLE** option. The “Facility List” appears.

Figure 9-1: Facilities List

Facility List

Create New Facility

CLIA	Name	Type	Street	City	County	State	Zip	Contact	Contact Phone	
46D0523979	ABC Laboratories	LAB	500 Chipeta Way	Salt Lake City		UT	84108	Shelly Smith	(800) 222-1234	Edit
23D0650909	XYZ Regional Laboratory	LAB	3350 N. Martin Luther King Jr. Blvd.	Lansing	Ingham	MI	48909	Mike Rogers	123-456-4321	Edit
33D0654233	JOE'S Hospital Laboratory	LAB								Edit

2. The fields and their descriptions are listed in the section titled, “Creating a New Facility.”
3. Determine the action to perform and continue to the respective section.

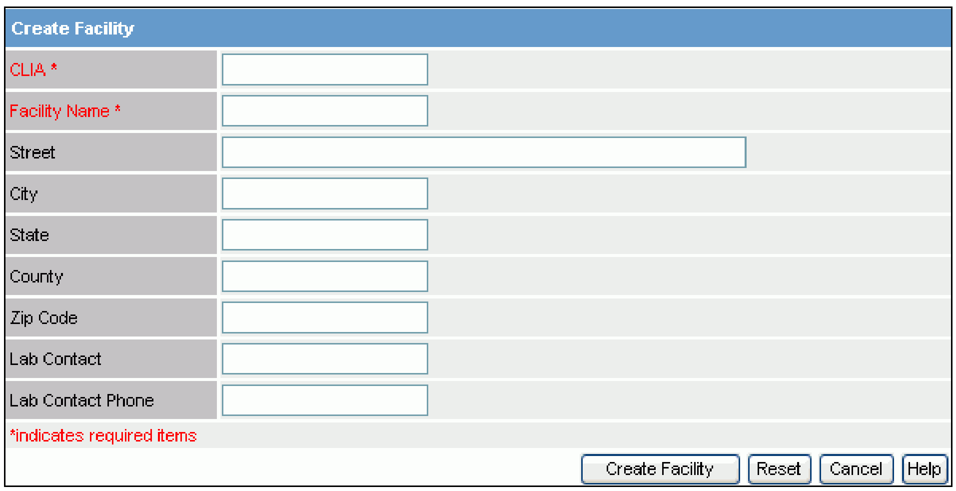
CREATING A NEW FACILITY

To create a new facility, perform the following:

1. Click on the **SYSTEM ADMINISTRATIN** menu and then click on the **LAB TABLE** option. The “Facility List” appears.

2. Click on the **CREATE NEW FACILITY** button. The “Create Facility” window appears.

Figure 9-2: New Facility



3. The fields and their descriptions are listed in the table:

Table 9-1: Create/Edit Facility Field Descriptions

FIELD	DESCRIPTION
CLIA	Identifying number associated with the facility or can be the nationwide standard code used by laboratories.
Facility Name	Name of the facility associates with the Facility CLIA id.
Type	Type of facility. Examples are: • Hospital • Physician’s Office • Laboratory
Street	Street address of the facility.
County	County name of the facility.
State	State name of the facility.

FIELD	DESCRIPTION
Zip	Zip code where the facility is located.
Contact	Name of the person that can be called.
Contact Phone	Contact person's phone number.

4. At a minimum, fill in the "red* (asterisked)" fields.

5. When finished, click one of the available buttons:

- **CANCEL** – Terminates the process of creating a facility and returns to the "Facility List" window. If you have changed any information, a "warning prompt" is displayed asking you to verify your intention to cancel.
  - **a)** If you click the **CANCEL** button, you will return to the creation process.
  - **b)** If you click the OK button, you will lose any values that you entered.
- **RESET** – Erases any changes or entries that you made.
- **CREATE FACILITY** – Saves the new facility to the database and redisplays the "Facility List" window.

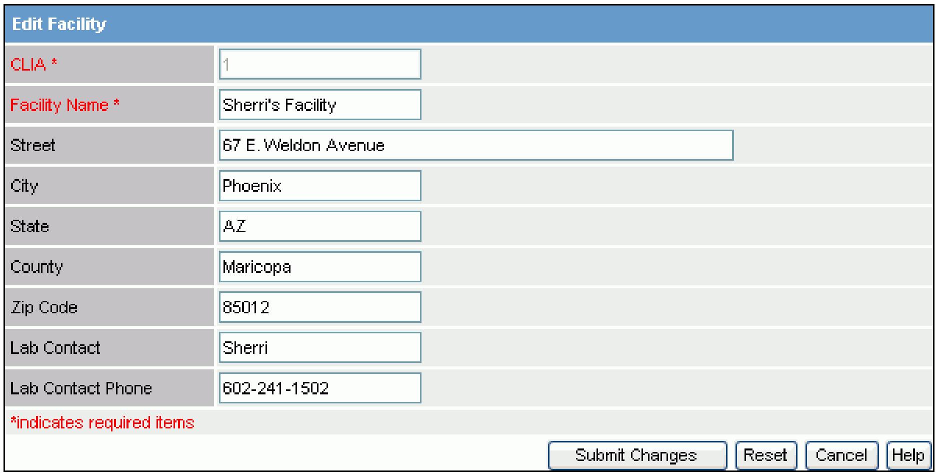
VIEWING/EDITING FACILITY DETAILS

To display and/or edit the Facility's details, perform the following:

1. Click on the **SYSTEM ADMINISTRATION** menu and then click on the **FACILITIES** option. The "Facility List" appears.

2. Locate the facility whose details you want to view/edit and click on the **EDIT** button. The "Edit Facility" window appears.

Figure 9-3: Edit Facility



3. Refer to the table titled, "Create/Edit Facility Field Descriptions" for a list of fields and descriptions.

4. Make the necessary changes and when finished, click on one of the available buttons:

   - **CANCEL** – Terminates the process of editing a facility and returns to the "Facility List" window. If you have changed any information, a "warning prompt" is displayed asking you to verify your intention to cancel.

     a) If you click the **CANCEL** button, you will return to the editing process.

     b) If you click the **OK** button, you will lose any values that you entered.

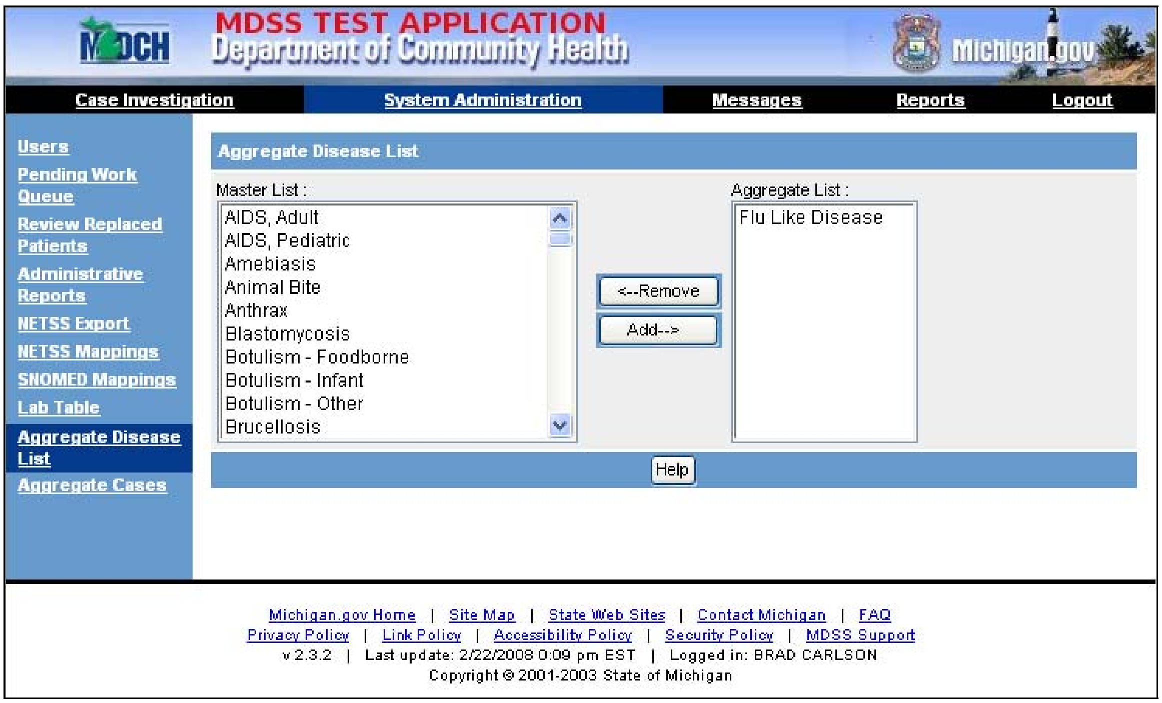
   - **RESET** – Erases any changes or entries that you made and remains on the same window.

   - **SUBMIT CHANGES** – Saves the new facility information to the database and redisplays the "Facility List" window.

10 AGGREGATE DISEASE LIST

Selecting the **AGGREGATE DISEASE LIST** menu from the Side Navigation Bar (SideBar) displays a screen where System Administrators can manage the list of diseases available for aggregate case reporting. Only the diseases moved into the Aggregate List at this screen will be reportable by users when they create new aggregate case reports.

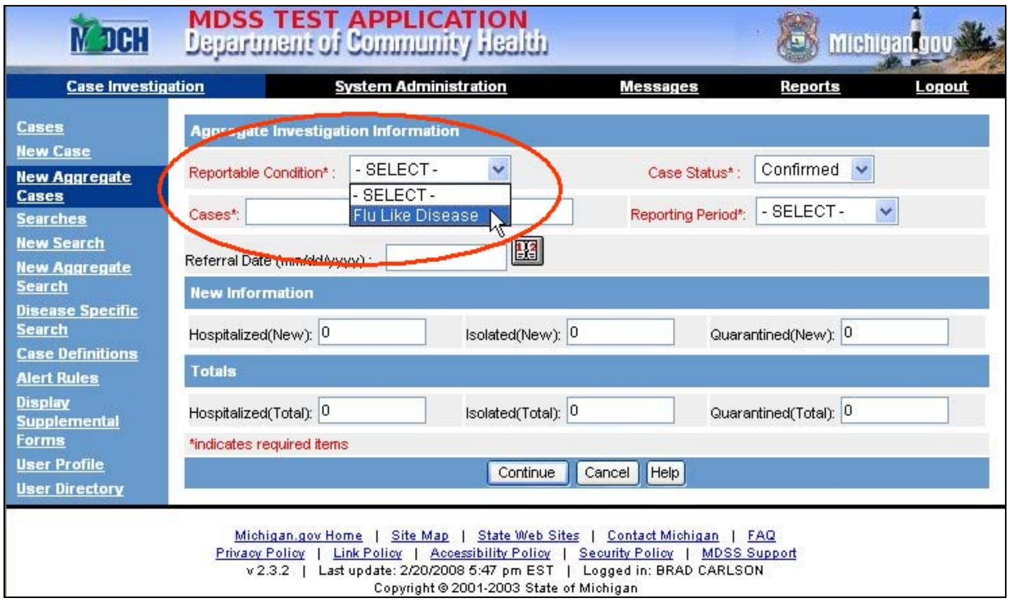
Figure 10-1: Aggregate Disease List Screen



What you add to the Aggregate List at this screen determines which Reportable Conditions users can select for new aggregate case reporting.

Note: Section 11 describes MDSS legacy aggregate case reporting, which is available from the "Aggregate Cases" link below "Aggregate Disease List" under the System Administration section. ***These two aggregate case reporting functionalities are separate and not part of the same process.*** The legacy aggregate case reporting is performed only by system administrators. The Aggregate Disease List described here modifies options for enhanced aggregate case reporting functionality for all users.

Figure 10-2: Reportable Conditions



MODIFYING THE AGGREGATE DISEASE LIST

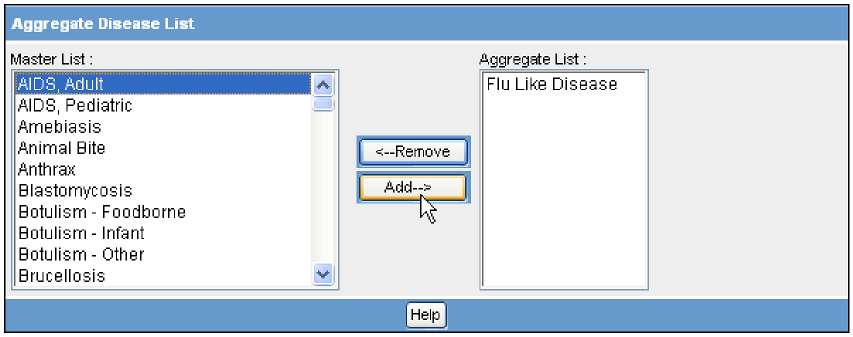
Modifying this list affects which diseases will be reportable by users when they create new aggregate cases.

To add or remove diseases, follow these steps:

1. Select **AGGREGATE DISEASE LIST** from the System Administration menu.

2. Select diseases in the Master List and click **Add** to move them to the Aggregate List. Anything you keep in the Aggregate List will be available to users as Reportable Conditions for aggregate case reporting.

Figure 10-3: Messages Menu and New Message Notification



3. Select diseases in the Aggregate List and click **Remove** to move them to the Master List. Anything you keep in the Aggregate List will be available to users as Reportable Conditions for aggregate case reporting.

4. You do not need to save your changes at this screen. Simply continue working in MDSS and your changes will be in effect.

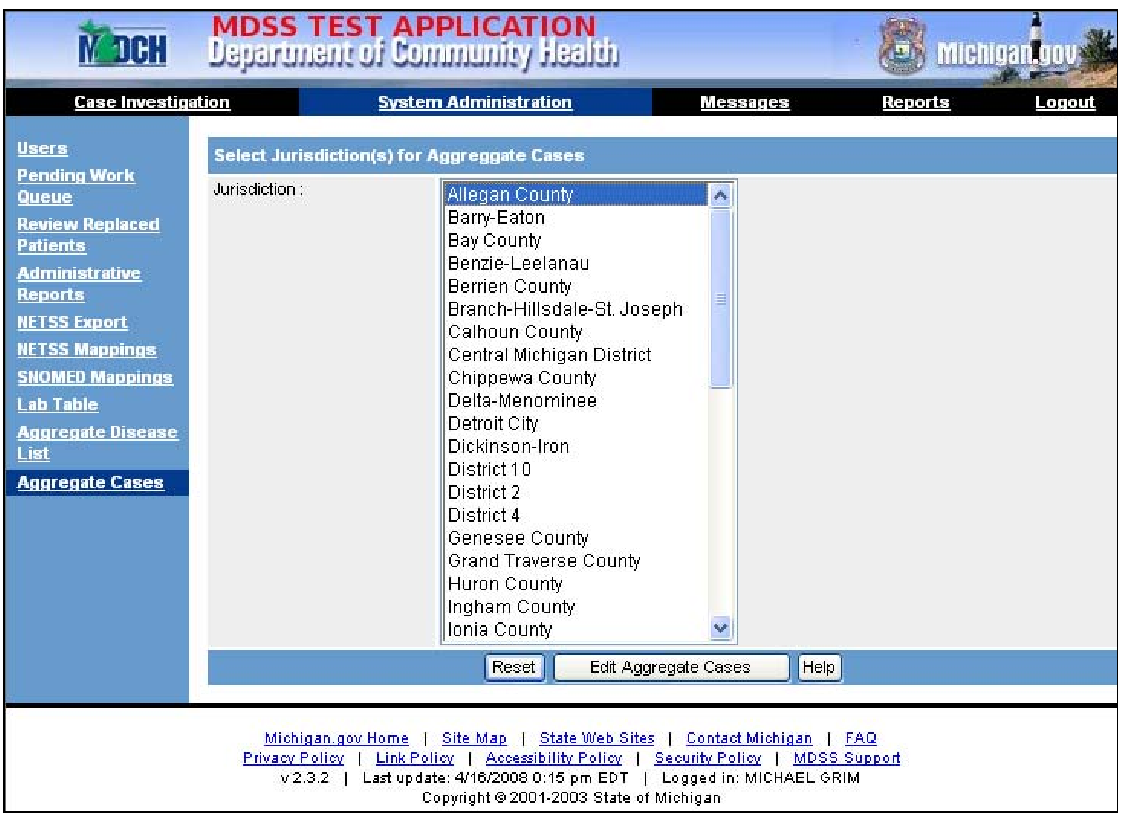
This page intentionally left blank

11 LEGACY AGGREGATE CASE REPORTING

To record the number of occurrences of AIDS by jurisdiction, system administrators can enter counts into MDSS using the "Aggregate Cases" entry screens.

Because this functionality has existed in MDSS—and to differentiate it from the ***new*** aggregate case reporting functionality available to all users in MDSS—this reporting is referred to as "legacy" aggregate case reporting in MDSS manuals. In previous MDSS versions, legacy aggregate case reporting was available from the **Aggregate Cases** link at the Case Investigation menu. To access legacy aggregate case reporting in the current MDSS, select the **Aggregate Cases** menu from the System Administration SideBar.

Figure 11-1: Legacy Aggregate Case Reporting Menu



Legacy aggregate case reporting allows system administrators to select one or more jurisdictions, specific to their role and permissions. Disease counts for AIDS are entered as a single count for each county within the selected jurisdiction(s) for the current MMWR week.

Note: The MMWR week is the MMWR publication week when the case was created. This value is assigned automatically when the case is entered into the application.

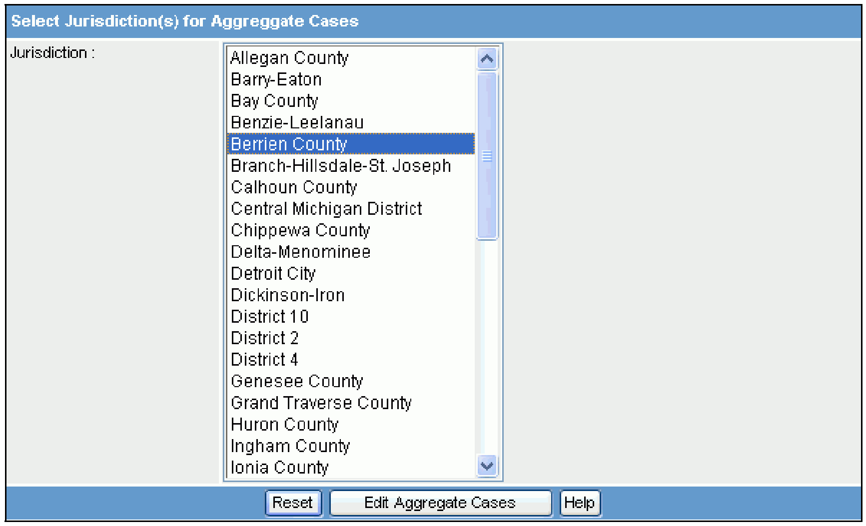
Legacy aggregate-disease counts can be edited until they are sent to the CDC. Counts are sent to the CDC via the **NETSS Export** on a weekly basis. Counts for AIDS are available within the Reports at the County, LHJ, Regional, or Statewide level. See Section 6 for more information on NETSS Export.

When you select to view legacy aggregate case information, the rules of locking take effect. These rules are designed to alleviate concurrency issues that might develop when two or more people are attempting to modify the same information at the same time. This lock remains in effect until the user cancels, saves the changes, or otherwise navigates away from the record. If the system administrators' MDSS session terminates before the lock is released, the lock will be released automatically when the user's session times out.

To Enter Legacy Aggregate Case Reports:

1. From the **SYSTEM ADMINISTRATION** menu, click on the **AGGREGATE CASES** option. The first of two screens appears:

Figure 11-2: Legacy Aggregate Cases / Select Jurisdiction(s)



2. Select the appropriate **JURISDICTION**. The following tips can help you locate and select the desired jurisdiction(s):

   - Type the **first letter** of the jurisdiction to jump to the first occurrence of the letter in the list.
   - Use the vertical slide bar to position the list and select one or more Jurisdictions.

     a) To select one item, click it.

     b) To select more than one item in a continuous list, click the first item to highlight it, and while holding the **SHIFT** key, click the last item to include in the list.

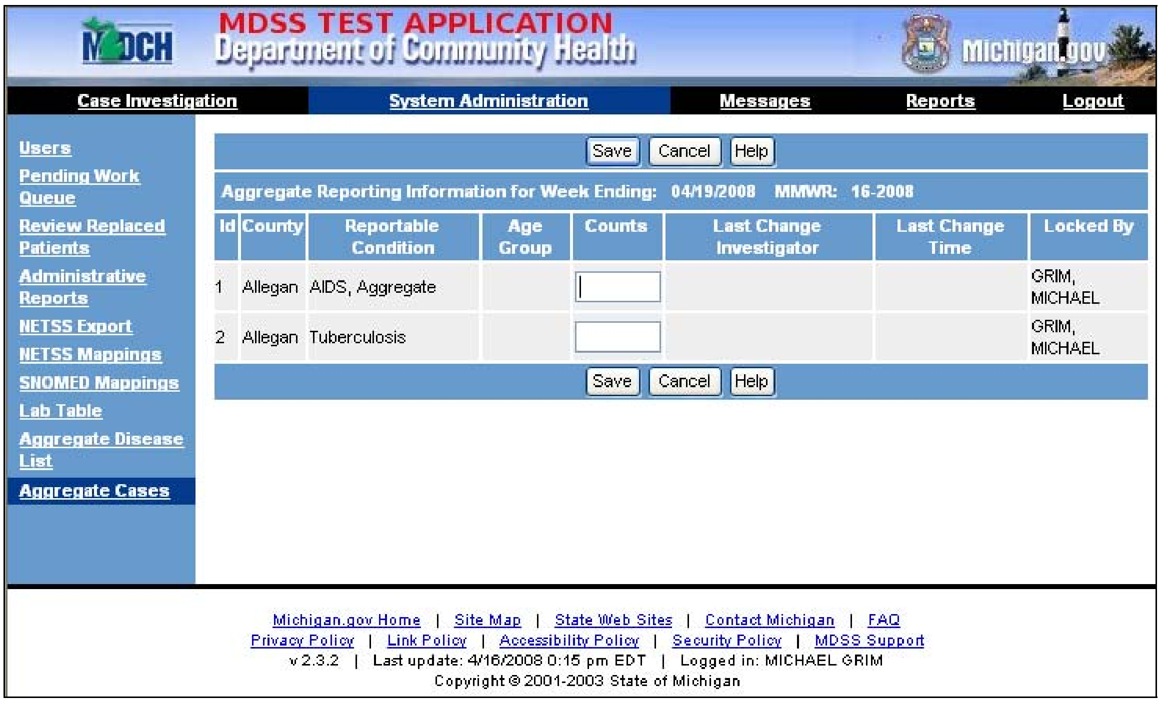
     c) To select more than one item NOT in a continuous list, click the first item to select it, and while holding the **CTRL** key, click the next item, continue until all desired items are selected.

     d) To clear your selections and start over, click **RESET**.

3. Click **EDIT AGGREGATE CASES** to display the "Aggregate Reporting Information" screen to allow the entry of counts for the selected jurisdiction(s).

4. AIDS Disease Counts are entered and updated as a single count on the "Aggregate Reporting Information" screen. Locate the desired County row and type the numeric value in the **COUNT** field/column. The **COUNTS** column will be "grayed out" when another user tries to display the same County. Refer to the table below to read more about locking by reading the LOCKED BY field/column.

Figure 11-3: Legacy Aggregate Case Reporting Information



The fields and their descriptions are listed in the table:

Table 11-1: Aggregate Reporting Information Fields

FIELD/COLUMN	DESCRIPTION
ID	Number identifying the row.
COUNTY	County name your role/permissions allow you to view. If the "Select Jurisdiction" screen appeared, these are the Jurisdictions you selected, and are grouped by county.

FIELD/COLUMN	DESCRIPTION
REPORTABLE CONDITION	Name of the condition reported during New Case Entry. Note: Though Figure 11-3 shows both AIDS and TB, only AIDS is currently used in MDSS legacy aggregate case reporting.
AGE GROUP	The groups will be labeled on the screen if they were entered; they are: • 0 to 4 years • 5 to 9 years • 10 to 14 years • 15 to 19 years • Age not specified
COUNTS	This column is used to enter the numbers for each identifying row. Counts that are left "blank" are interpreted as zero. **Note**: This column will be "grayed out" if another system administrator tries to view the same Jurisdiction while it is LOCKED by the first.
LAST CHANGE INVESTIGATOR	Name of the Investigator that made the last change. **Note**: If you are entering counts, this column will be updated to indicate your user information when you click the SAVE button.
LAST CHANGE TIME	Time the Investigator made the last change. **Note**: If you are entering counts, this column will get updated to indicate the time that you saved the count information.

FIELD/COLUMN	DESCRIPTION
LOCKED BY	Name of the system administrator that is currently working with the Jurisdiction counts record(s). The user who locked the case has the privilege of editing all of the counts. While the lock is in effect, other users will be able to view the Aggregate Reporting Information, but will not be able to edit any of the counts.

5. When finished entering the **COUNTS**, click any of the available buttons:

- **SAVE** – Begins the validation process of the field values and if the validation is successful (no errors), it saves the count information to the database and redisplays the screen. If you receive an error, you must correct it before continuing.

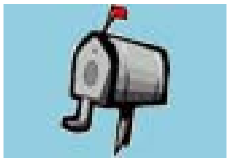
  a) The Last Change Investigator and Last Change Time columns are updated to indicate your user information and the time that you saved the count information.

- **CANCEL** – Terminates the process of entering aggregate-level disease counts. A "warning dialog" displays asking you to verify your intention to cancel.

  a) If you click the **CANCEL** button, you will return to the process of adding aggregate level disease counts.

  b) If you click the **OK** button, you will lose any data that you entered.

6. To exit the screen, click any menu or option.

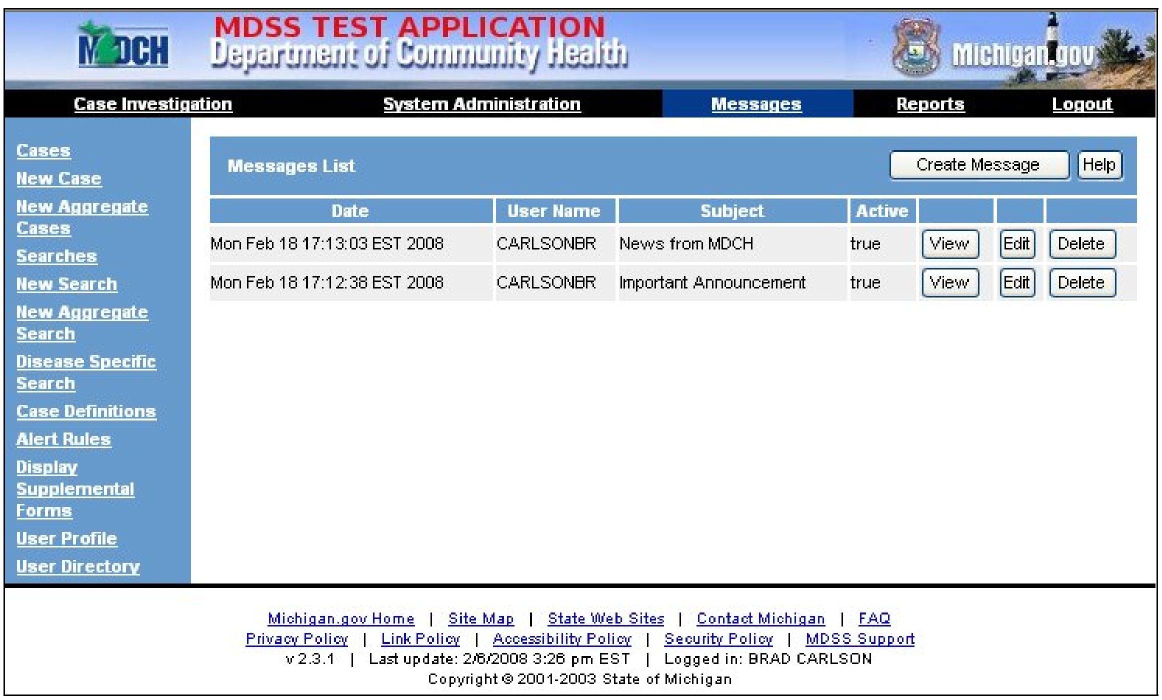


12 MESSAGES MENU

Selecting the **MESSAGES** menu from the TopBar displays a list of system-wide messages for all MDSS users. These messages can be viewed by all users, but only system administrators can create, edit, or delete them. When editing messages, System Administrators can also hide individual messages so they remain in the System Administration message list but are no longer visible to users.

When new messages are published, the "Case Listings" page displays a "New Message Waiting" link at the bottom. This link opens the same list of messages as selecting the **MESSAGES** menu from the TopBar.

Figure 10-1: Messages List (for System Administrators)

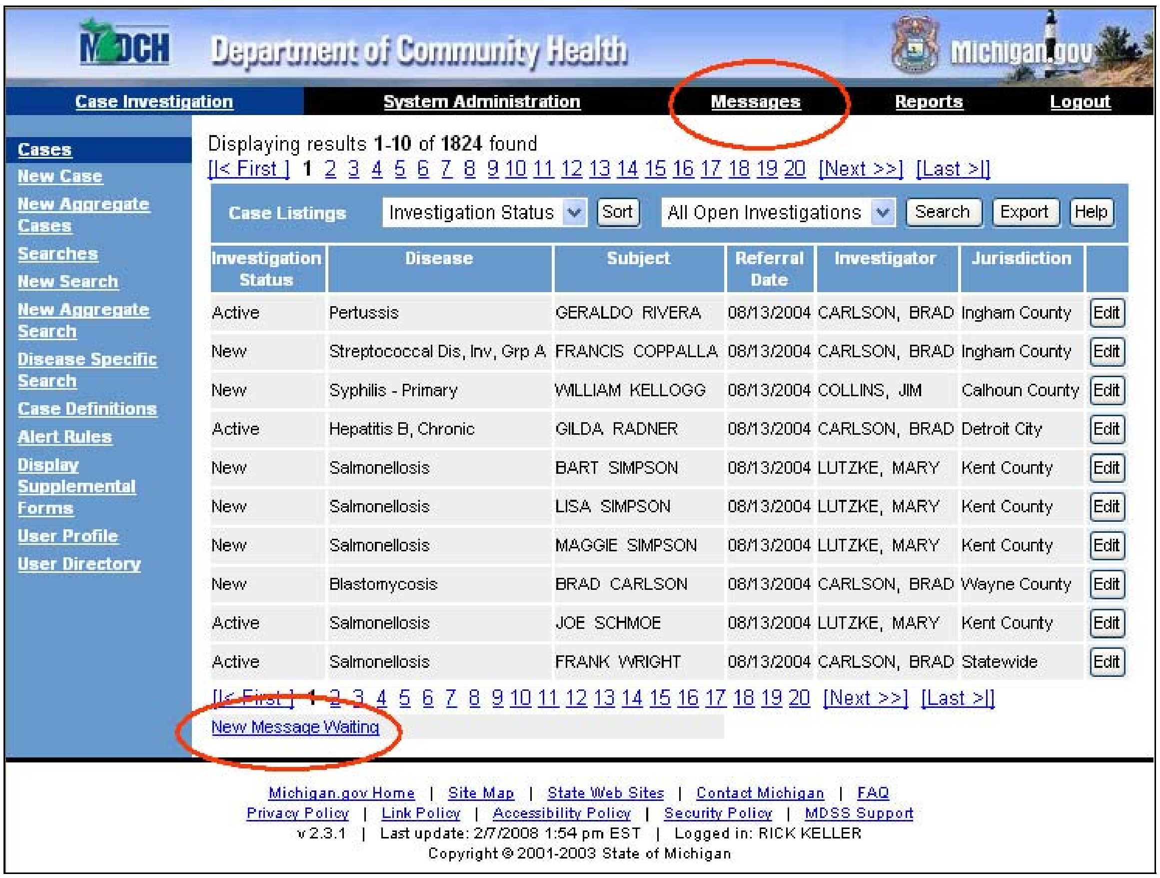


VIEWING MESSAGES

To view messages, follow these steps:

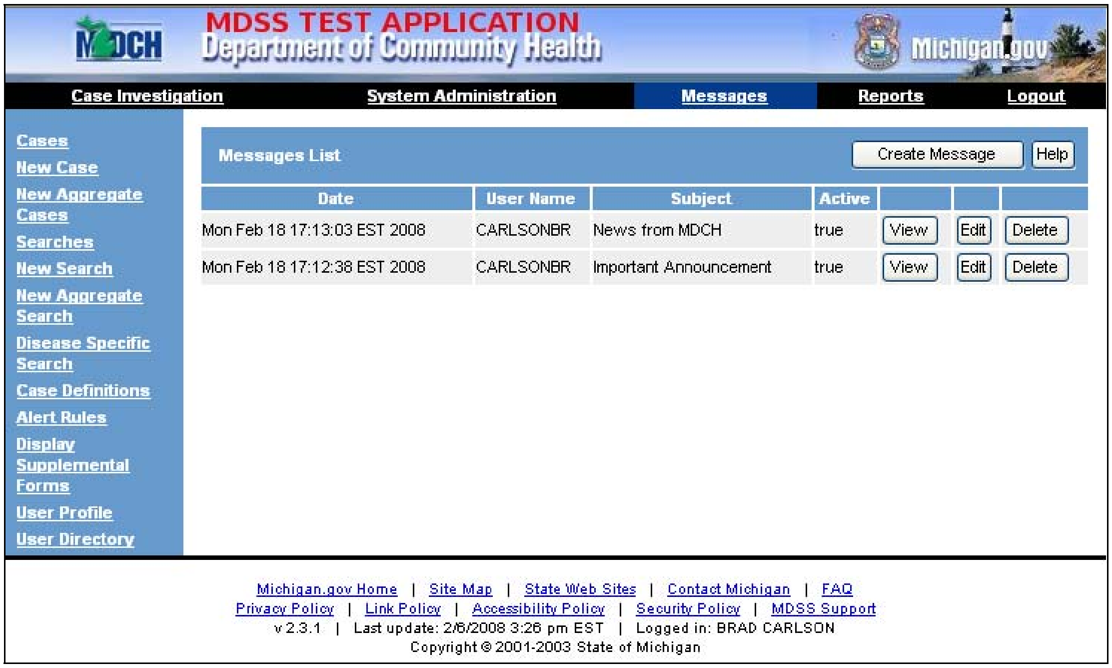
1. Select the Messages menu from the top navigation bar. You can also click the "New Message Waiting" link, if displayed, at the bottom of the "Case Listings" page.

Figure 10-2: Messages Menu and New Message Notification



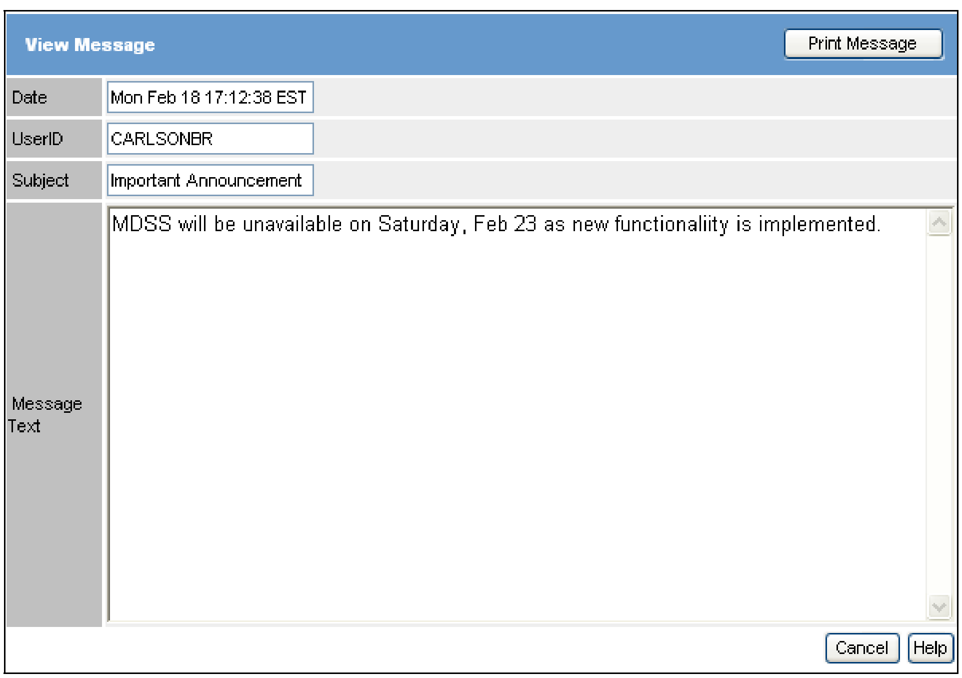
2. The "Messages List" page appears. All messages available for viewing are listed here. System Administrators have the additional options of creating new messages or editing and deleting existing messages.

Figure 10-3: Messages List (for System Administrators)



3. Click **View** to open and read a message.

Figure 10-4: View Message Screen



4. Click **Cancel** when you are finished viewing the message.
5. You can open other messages or select another menu link from the TopBar to leave the "Messages List" page.

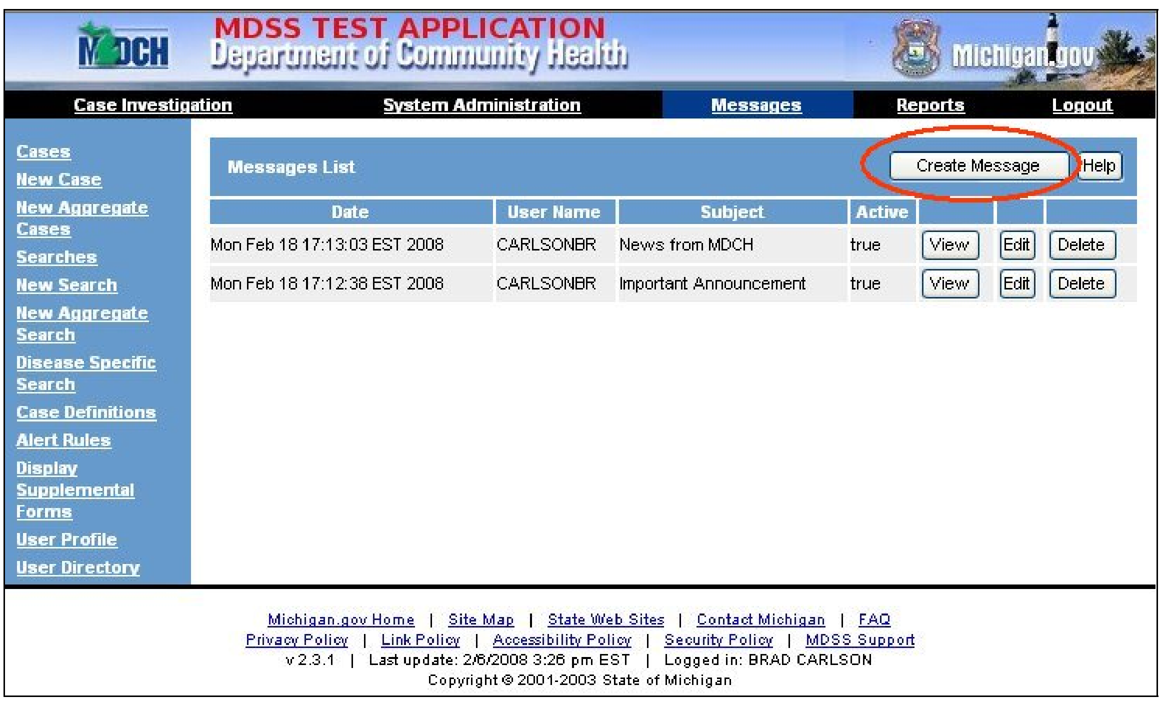
CREATING MESSAGES

System administrators can create new messages that will be displayed to all MDSS users.

To create new messages, follow these steps:

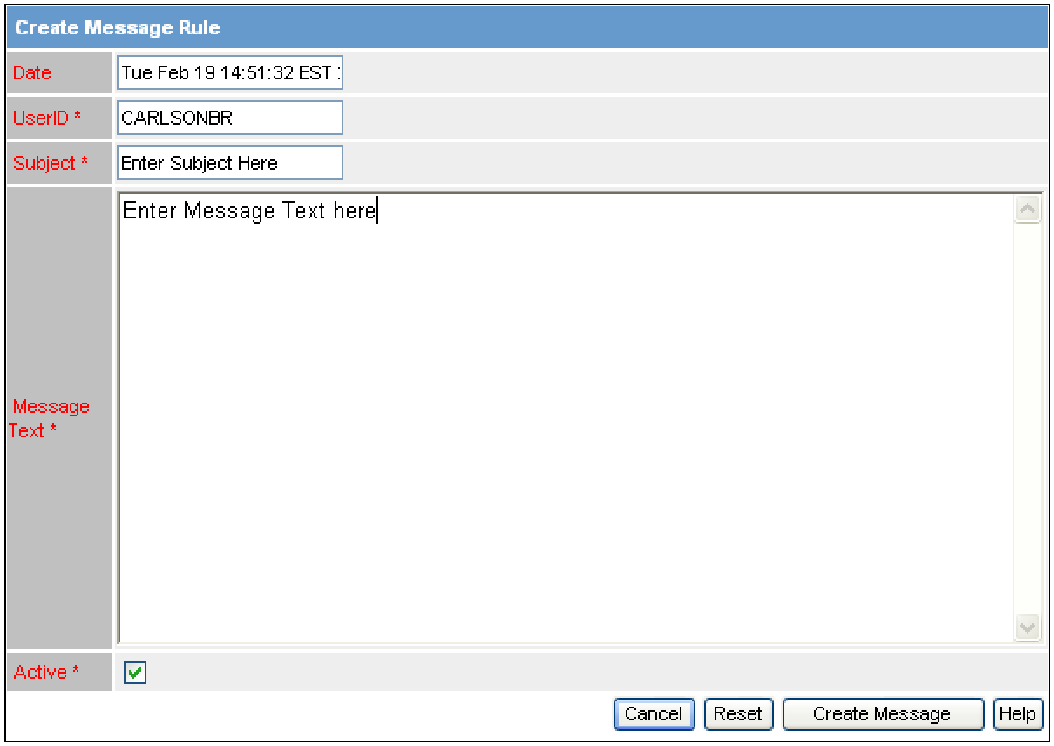
1. Select the Messages menu from the top navigation bar. You can also click the "New Message Waiting" link, if displayed, at the bottom of the "Case Listings" page.
2. At the "Messages List" screen, click **Create Message**.

Figure 10-5: Selecting to Create Messages



3. Enter a subject and message text. The date and your user ID are added automatically.

Figure 10-6: Entering Message Subject and Text



4. **Note**: The “Active” field should be selected (i.e., checked) by default. If you de-select this checkbox your new message will not display to users (though it will still exist in the System Administrator’s Messages List).
5. Optional—If you want to start over and delete all the subject and message text, click **Reset**.
6. When your message is complete, click **Create Message**.

EDITING MESSAGES

System administrators can edit their own messages and any other message displayed. If you edit the message created by another System Administrator, you will assume “ownership” and be listed as the message author in the UserID field.

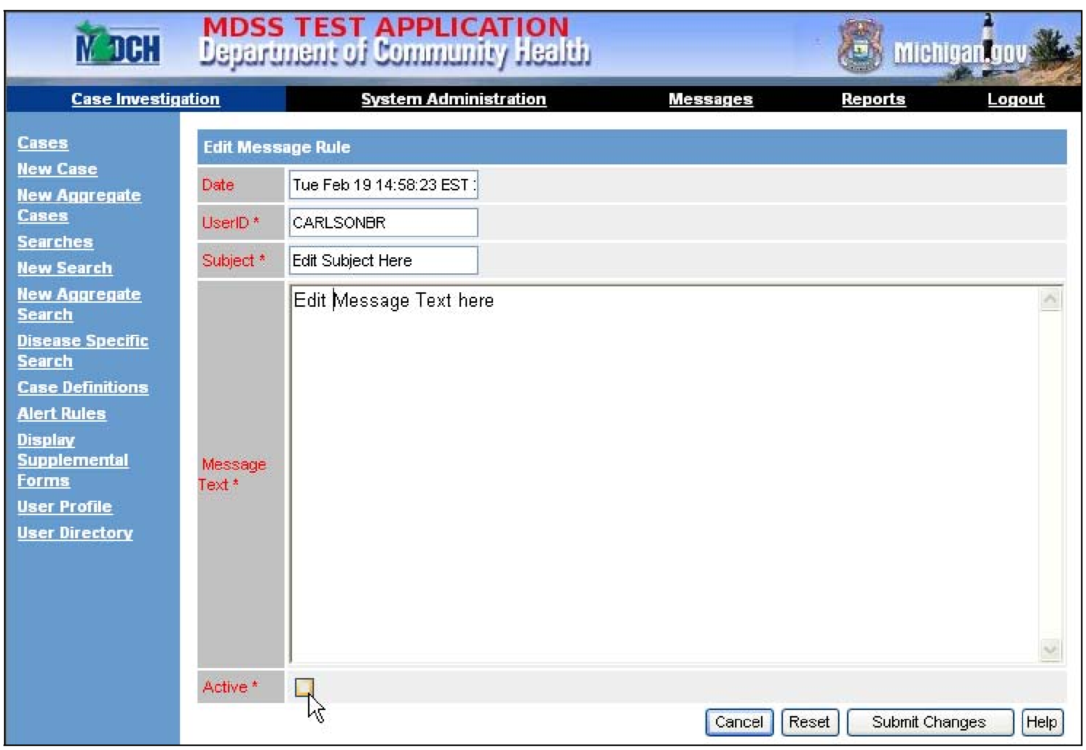
In addition to modifying the message subject or text, you can edit whether or not the message is displayed to users. System Administrators can hide individual messages so they remain in the

System Administration message list but are not visible to users. This may be useful in temporarily hiding a message that you may want to display again in the future.

To edit messages, follow these steps:

1. Select the Messages menu from the top navigation bar. You can also click the “New Message Waiting” link, if displayed, at the bottom of the “Case Listings” page.
2. At the “Messages List” screen, click the **Edit** button associated with the message you want to edit.
3. Edit the message. You have the following options:
   - Edit the subject line;
   - Edit the message text; and
   - Change whether or not the message appears to users. When the Active checkbox is selected (i.e., checked), the message will be shown to users. De-select to hide the message.

Figure 10-7: Editing Messages



4. Click **Submit Changes** when edits are complete.

You cannot edit the “Date” or “User ID” fields manually, though they will both be updated when you save changes.

DELETING MESSAGES

System administrators can delete messages that are no longer needed. Note that as an alternative to deleting, you can de-select the “Active” checkbox for a message to temporarily hide that message.

To delete messages, follow these steps:

1. Select the Messages menu from the top navigation bar. You can also click the “New Message Waiting” link, if displayed, at the bottom of the “Case Listings” page.
2. At the “Messages List” screen, click the **Delete** button associated with the message you want to remove permanently.
3. Click **OK** when asked to confirm the action.

The message is permanently removed from the “Messages List” screen.

This page intentionally left blank

13 APPENDICES

The following have been included:

- Appendix A: Software Requirements/Settings
- Appendix B: Requesting Access
- Appendix C: User Roles and Permissions
- Appendix D: ELR and HL7 Messages
- Appendix E: Additional MDSS References and Information
- Appendix F: Han Alert Configuration Properties

APPENDIX A: SOFTWARE REQUIREMENTS / SETTINGS

Software requirements for using the CEDSS application are as follows:

- **Oracle Enterprise Edition.** MDSS uses certain features that are only available in the Oracle Enterprise Edition.
- **Internet Browser. Internet Explorer is recommended** – version 5.5 SP2 or higher. Netscape Navigator version 6.0 or higher.
- **Adobe Reader version 5.1 or higher**. MDSS utilizes the power and flexibility of PDF (Portable Document Format) files for Case Management and Reports. Using the technology of PDF Forms, the disease specific forms allow for printing blanks forms and entering investigation information into the application.

To obtain current versions of the Browser or of Adobe Reader, they can be downloaded from their respective sites:

- Microsoft Internet Explorer

Http://www.microsoft.com/windows/ie/downloads/critical/ie6sp1/default.asp

- Netscape Navigator

  http://channels.netscape.com/ns/browsers/download.jsp

- Adobe Reader

  http://www.adobe.com/products/acrobat/alternate.html#51

Browser settings can affect the appearance and functionality of the application. The following settings are recommended to optimize the appearance of the application.

Note: Regardless of the type of Browser being used, do NOT use the **BACK**, **FORWARD**, and **REFRESH** buttons within the application. These buttons have been disabled to avoid concurrency errors and potential duplication of processing; however, buttons have been coded within the application to perform these processes.

INTERNET EXPLORER SETTINGS

The following settings must be setup using Internet Explorer:

- Font Styles
- Text Size
- Auto-Complete

FONT STYLES

The "Font Styles" are specified by the application. To ensure this happens, perform the following:

1. Click the **TOOLS** menu in the Internet Explorer Browser window.

2. Click the **INTERNET OPTIONS** from the menu.

3. Click the **GENERAL** tab.

4. Click the **ACCESSIBILITY** button. The "Accessibility" window appears.

Figure 13-1: Accessibility Options

5. If any of the checkboxes are checked, uncheck them by pointing and clicking them with your left mouse button:

- Ignore **colors** specified on Web pages.
- Ignore **font styles** specified on Web pages.
- Ignore **font sizes** specified on Web pages.
- Format **documents** using my style sheet.

6. Click the **OK** button. The "General Tab" window reappears.

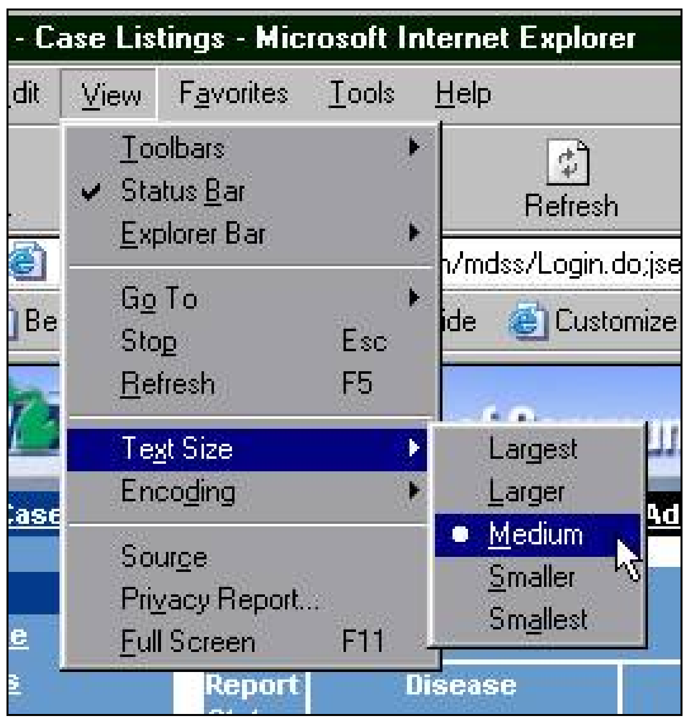
7. Click the **OK** button.

TEXT SIZE

The Text Size should be specified by the application. To access this setting, perform the following:

1. Click the **VIEW** menu in the Internet Explorer Browser window.
2. Click the **TEXT SIZE** from the menu.
3. Click the **MEDIUM** option. The menu/option flow appears similar to the one shown below.

Figure 13-2: Internet Explorer Text Size



AUTO-COMPLETE

Auto-Complete is a capability that allows the Internet Explorer to save data that is entered into online forms. When data is typed into the form, Auto-Complete will suggest possible matches. Due to the sensitive nature of the application data, State Department of Health requires that the Internet Explorer Auto-Complete does not allow the capture of this data.

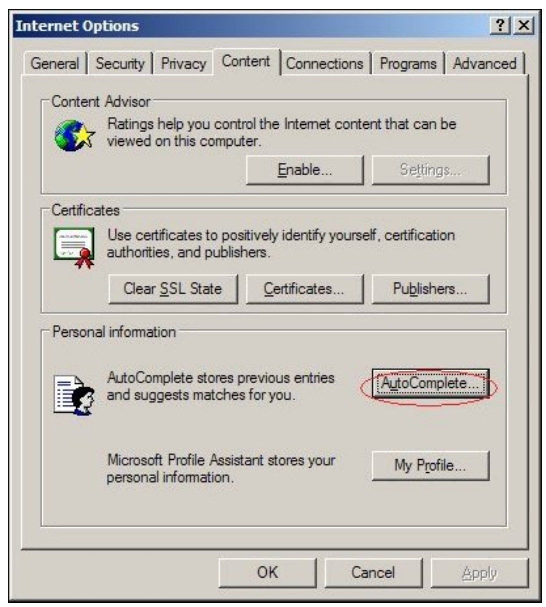
To disable the Internet Explorer Auto-Complete from capturing the application form data, perform the following:

1. Click the **TOOLS** menu in the Internet Explorer Browser window.

2. Click the **INTERNET OPTIONS** from the menu.

3. Click the **CONTENT** tab. The "Internet Options – Content" window appears.

Figure 13-3: Internet Options – Content



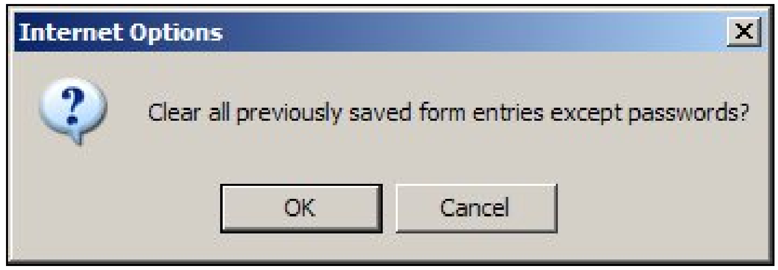
4. In the "Personal Information" section, click the **AUTOCOMPLETE** button. The "AutoComplete Settings" window appears.

Figure 13-4: AutoComplete Settings

5. In the "Use AutoComplete for" section, uncheck the **FORMS** checkbox, if checked. The window should look like the one shown above.

6. Click the **CLEAR FORMS** button to remove any existing "saved" application data. An "Internet Options Confirmation" dialog box appears.

Figure 13-5: Internet Options Confirmation Dialog Box



7. Click the **OK** button. The "Auto-Complete Settings" window reappears.
8. Click the **OK** button. The "Internet Options" window reappears.
9. Click the **OK** button.

NETSCAPE NAVIGATOR SETTINGS

The following settings must be setup using Netscape Navigator:

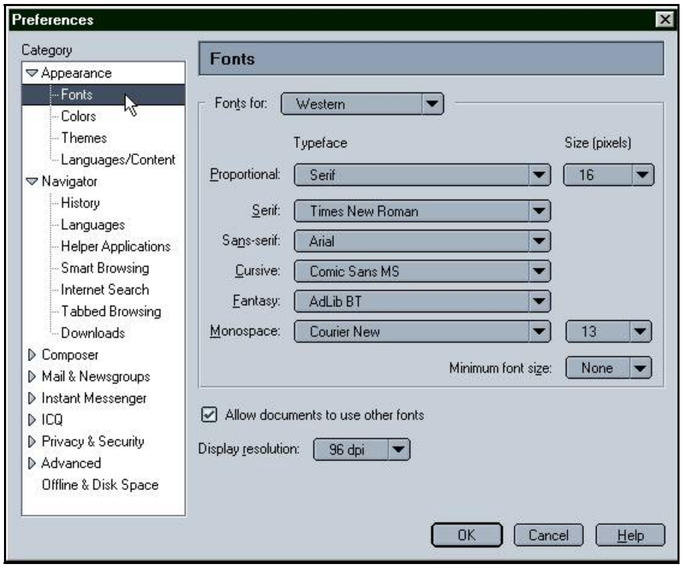
- Font Styles
- Colors and Background
- Auto-Complete

FONT STYLES

The Font Styles are specified by the application. To ensure this happens, perform the following:

1. Click the **EDIT** menu in the Netscape Navigator Browser window.
2. Click the **PREFERENCES** option from the menu.
3. Click the **APPEARANCE** category from the "Category List."

Figure 13-6: Netscape Navigator Settings – Fonts



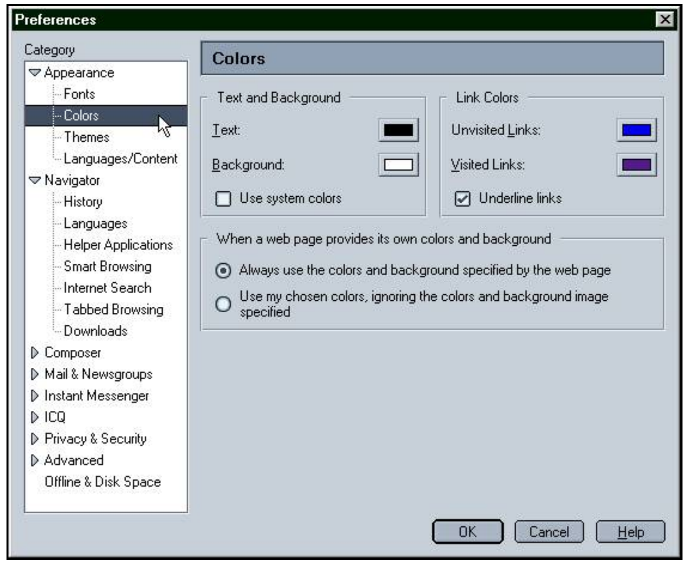
4. Click the **FONTS** option. The "Fonts" information displays similar to the one shown above.
5. If the **ALLOW DOCUMENTS TO USE OTHER FONTS** checkbox is **NOT** checked, click it to select/check it.
6. Verify the **DISPLAY RESOLUTION** setting is set to **96 dpi**. If it isn't, click the drop-down arrow to select it.
7. Click the **OK** button.

COLORS AND BACKGROUND

The Colors and Background should be specified by the application. To access these settings, perform the following:

1. Click the **EDIT** menu in the Netscape Navigator Browser window.
2. Click the **PREFERENCES** option from the menu.
3. Click the **APPEARANCE** category from the "Category List."

Figure 13-7: Netscape Navigator Colors & Background Settings



4. If the **ALWAYS USE THE COLORS AND BACKGROUND SPECIFIED BY THE WEB PAGE** radio button is not selected, click it to select it.
5. Click the **OK** button.

AUTO-COMPLETE

Auto-Complete is a capability that allows the Netscape Navigator to save data that is entered into online forms. When data is typed into the form, Auto-Complete will suggest possible matches. Due to the sensitive nature of the application data, the state requires that the Netscape Navigator Auto-Complete does not allow the capture of this data.

Disabling the Netscape Navigator Form Manager from capturing the application form data can ONLY be accomplished while using the online forms. During that time, you need to perform the following:

1. When the **Form Manager** displays a dialog box asking if you want to save the values that you've entered into the form, there are three options:
   - YES

- NEVER FOR THIS SITE
- NO

Figure 13-8: Netscape Confirmation – Auto-Complete

2. Click the **NEVER FOR THIS SITE** button. This choice will ensure that the Form Manager will not ask in the future and will not save the values.

SYSTEM SETTINGS

Your computer display and font settings will affect the appearance of the application. The following settings are recommended to optimize the appearance of the application.

These settings can be found in the **Display Properties** of your PC.

SCREEN RESOLUTION AND FONT SIZE

Screen resolution may be operated at a higher resolution, but the application was designed to have 800 x 600 pixel screen resolution.

The Display Font Size should be set to Normal Size (96 dpi).

Follow the instructions below to set the screen resolution and font size.

1. Click the **START** button located on the **STATUS BAR** at the bottom left corner of your display. The "START" menu will display.

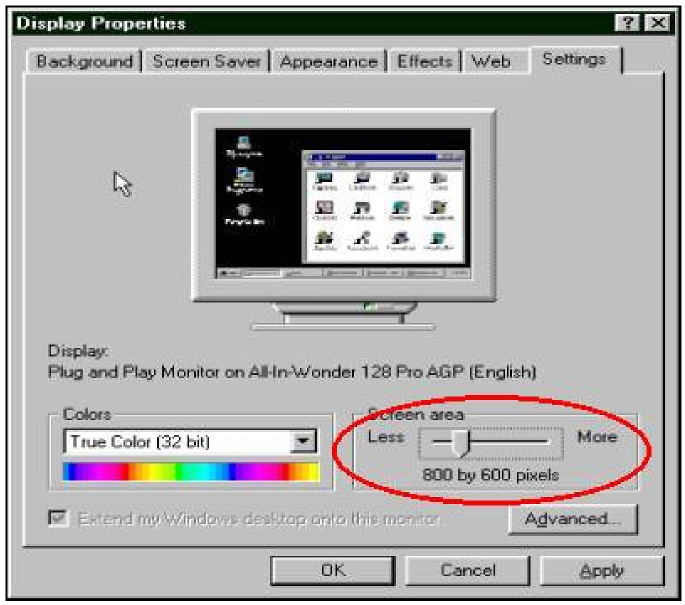
2. Select the **SETTINGS** option from the **START** menu.

3. Select the **CONTROL PANEL** option from the **SETTINGS** menu. The "Control Panel" directory will open in a new window.

4. Double-click **DISPLAY**. The "Display Properties" window will open in a new window.

5. Click the **SETTINGS** tab. The "Display Properties – Settings" window appears.

Figure 13-9: Display Properties - Settings

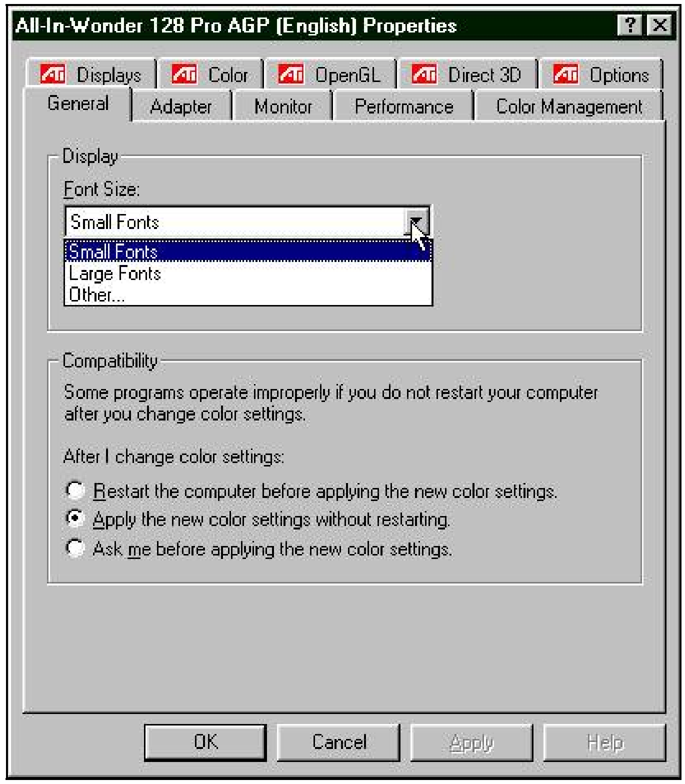


6. In the **SCREEN AREA** section (bottom right hand corner), drag the slider until the setting reads "800 by 600 pixels."

7. Click the **APPLY** button. The Screen Resolution setting is saved.

8. Click the **ADVANCED** button. The "Advanced Settings – General Tab" window appears.

Figure 13-10: Font Size Settings



9. In the "Display – Font Size" section of the window, click the drop-down arrow and select **SMALL FONTS**.

10. Click the **OK** button. The "Display Properties - Settings" window reappears.

11. Click the **OK** button.

12. Close the "Control Panel" window.

APPENDIX B: REQUESTING ACCESS

Before you can access and start using the application, the following steps must be completed in this order.

1. You must have a valid Single Sign-On (SSO) User ID and password. The Single Sign-On Registration will walk you through the steps of obtaining your SSO User-ID and password.
2. You must request Permission to access MDSS. Requesting Access will walk you through the steps of requesting access.
3. You must complete the MDSS User Registration. User Registration will walk you through the steps of registering.
4. You must be assigned a Role within MDSS. Getting a User Role will discuss the process of obtaining a user role.

1: SINGLE SIGN-ON (SSO) USER ID REGISTRATION

Your State's Information Technology/Services Department maintains control over newly added users via the Single Sign-On (SSO) verification process. This system has been implemented to administer passwords, access, and administrative services.

Users who have a valid Single Sign-On User-ID and password (e.g., State Childhood Immunization Registry users) should proceed to the next section, Requesting Access to MDSS.

To register for **SSO**, perform the following steps:

1. Using your Internet Browser, type the following **URL** into the location/address text box:

   `https://sso.state.mi.us/`

2. Press the **ENTER** key. The "Login User-id and Password" screen will appear:

Figure 13-11: Login-User-id and Password

3. Click the **REGISTER** button. The “Registration – Step 1” page will display:

Figure 13-12: SSO Registration – Step 1

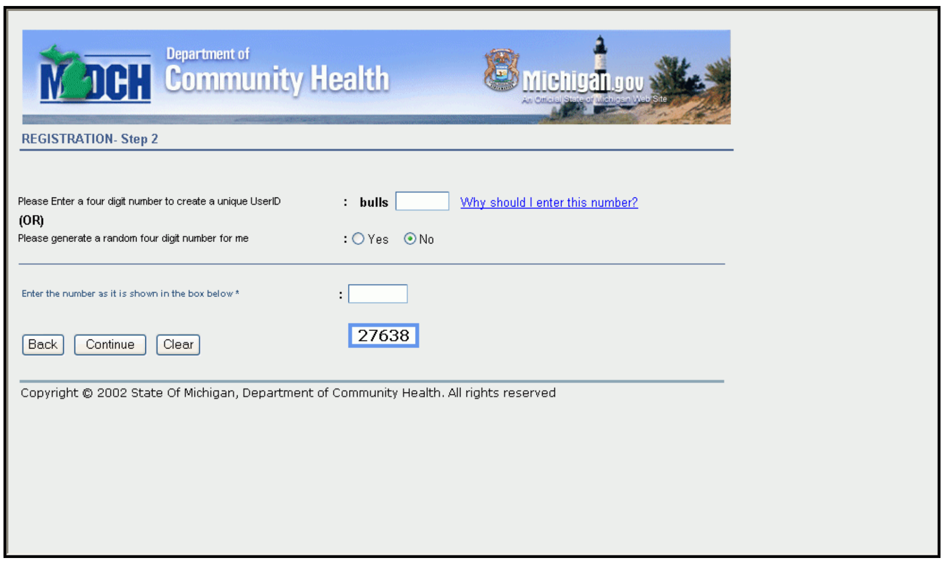
4. Using your mouse or the **TAB** key, move to the appropriate fields within the screen.

5. Type the value for the fields. Fields displayed with an asterisk (*) are required field entries. You cannot continue without supplying information for these fields.

6. When finished adding the information, click one of the available buttons:

- **CONTINUE** –begins the validation process. If no errors are detected, the "Registration – Step 2" page will display. If errors are detected, you must correct all errors before proceeding.
- **CLEAR** – erases the information that you entered into the screen and remains on the same window to re-enter data.

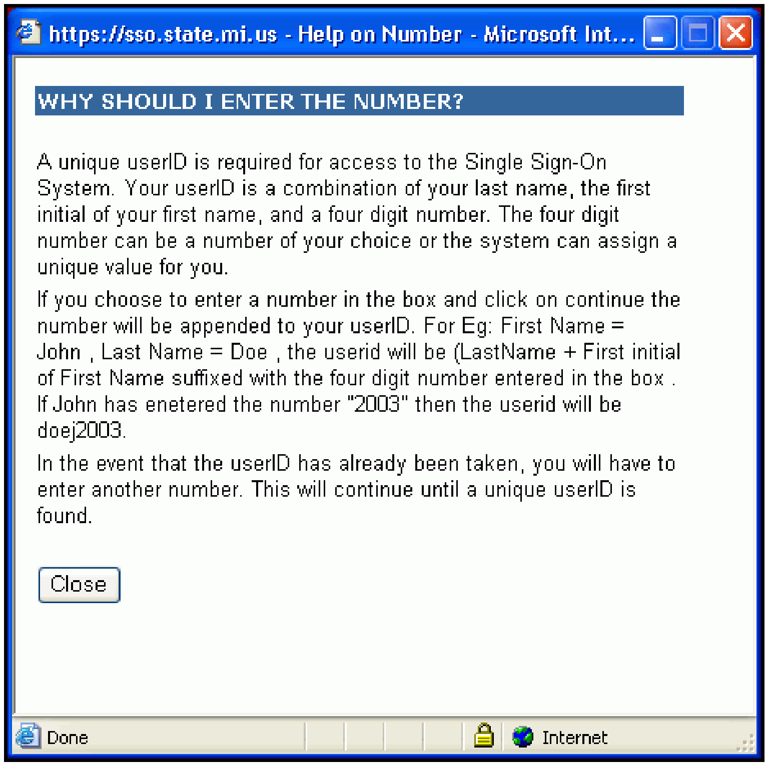
Figure 13-13: SSO Registration – Step 2



7. Type a four-digit number (to the right of the user-id) that will be included as part of your User-ID (example: jsmith1234) or you can choose to let the computer generate a number by clicking on the YES radio button. The NO radio button is chosen by default.

- For a detailed explanation, click on the "Why should I enter this number?" hyperlink. The following window appears:

Figure 13-14: Why enter a 4-digit number dialog box



a) After reading the dialog box, click the **CLOSE** button to return to the "Registration – Step 2" window.

8. The next field of entry is the field labeled, "Enter the number as it is shown in the box below."

   - This is the number displayed in the blue box. Using the figure above (SSO Registration - Step 2), the number to type would be: 27638

9. When you are finished adding the information, click any of the available buttons:

   - **BACK** – displays the "SSO Registration – Step 1" window.
   - **CLEAR** – erases the new information that you entered and remains on the same window to re-enter data.
   - **CONTINUE** – begins the validation process. If no errors are detected, the "User Registration

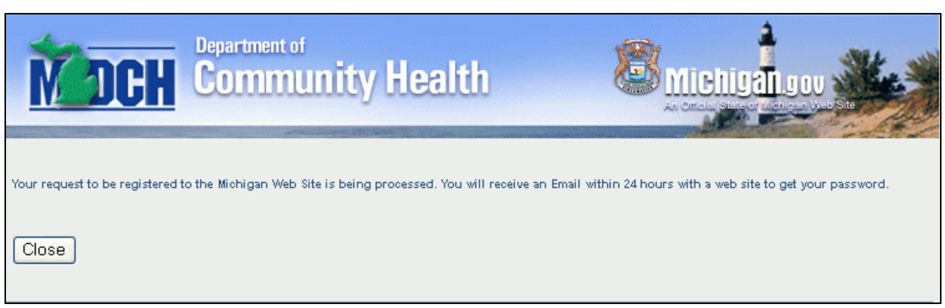
Confirmation" page appears. If errors are detected, you must correct all errors before proceeding.

Figure 13-15: User Registration Confirmation

10. Review the information displayed and click one of the available buttons:

- **BACK** – displays the "SSO Registration – Step 2" window.
- **SUBMIT** – begins the validation process. If no errors were detected, the "Request for Registration Acknowledgement" window appears. If errors were detected, you must correct all errors before proceeding. Your request is sent to the SSO Administrator.

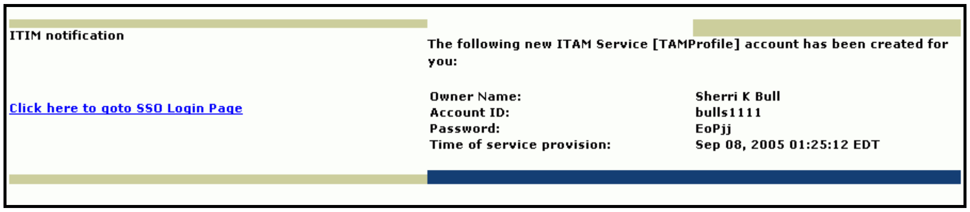
Figure 13-16: Request for Registration -Acknowledgment



11. Click the **CLOSE** button. The browser "dialog box" appears asking if you want to close the browser. Click YES to close the browser.

12. The **SSO_Administrator** responds via e-mail within two business days with your designated password. An example of the SSO registration email is shown below:

Figure 13-17: SSO Registration Email



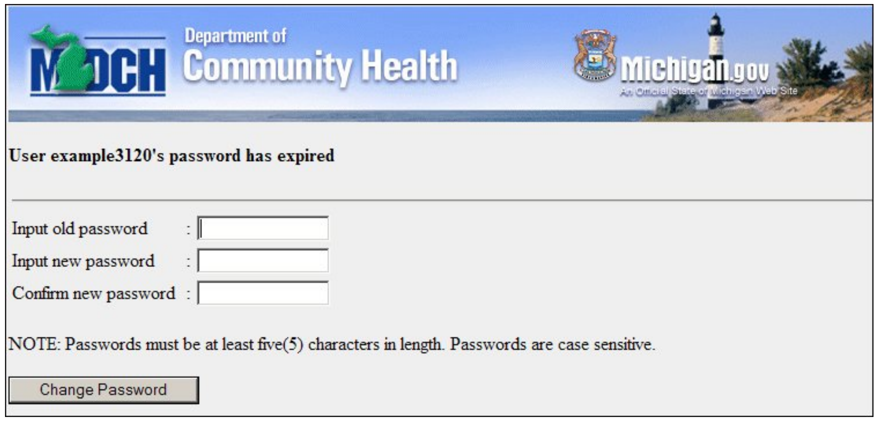
Note: If you attempt to login before getting the email, you will get a message stating, "Login failed. You have used an invalid username, password or client certificate."

13. After you receive the SSO registration email, click on the hyperlink labeled, "Click here to go to SSO Login Page." The "MDCH Sign-In" window appears.

Figure 13-18: Example: State of Michigan-DCH Login

14. Type your **User ID**, press the **TAB** key, type the provided Password from the email and click the **LOGIN** button. The "SSO Expired Password" page will display.

Figure 13-19: SSO Expired Password

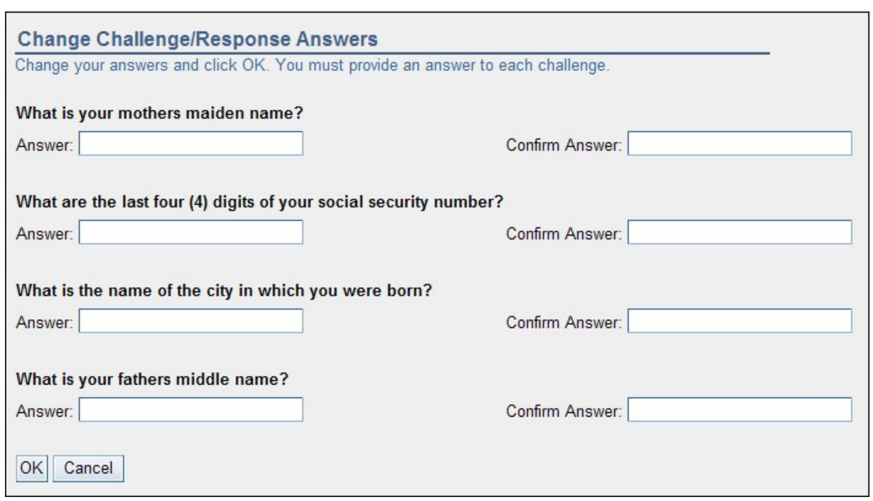


15. Change your password by typing the appropriate values for the fields.

Note: Passwords must be at least five characters in length. Password entries are case sensitive.

16. Click the **CHANGE PASSWORD** button. The "Change Challenge/Response Answers" page will display. The example provided below may not be the same questions that appear on your screen. There are several different questions selected at random.

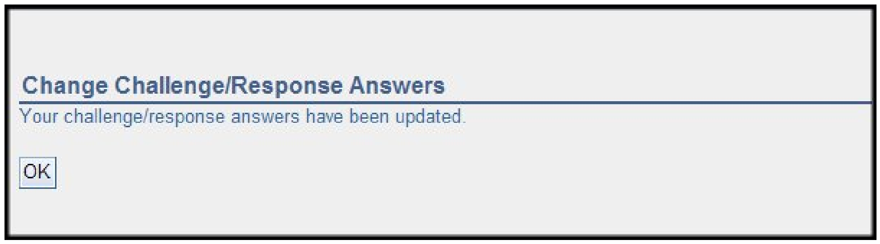
Figure 13-20: Change Challenge/Response Answers



17. Using your mouse or the **TAB** key, move to the appropriate fields within the screen.

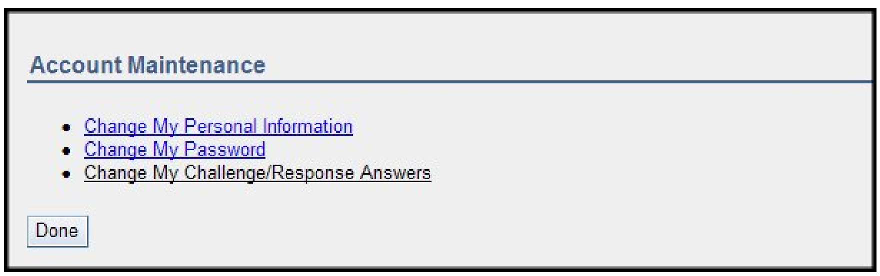
18. Type the value for each of the fields and click the **OK** button. An "acknowledgement" screen displays acknowledging the updates to your challenge/response answers.

Figure 13-21: Change Challenge/Response Answers Acknowledgment



19. Click the **OK** button. The "Account Maintenance" screen appears.

Figure 13-22: Account Maintenance



20. Click the **DONE** button. The "Application Portal" screen appears.

Figure 13-23: Application Portal

21. You now have a valid SSO User ID and Password. Continue to the next section titled, "Requesting Permission to access MDSS."

2: REQUESTING PERMISSION TO ACCESS MDSS

Once you are a registered user of Single Sign On (refer to the previous section), you need to request access to MDSS.

To request access, perform the following steps:

1. Using your Internet Browser, type the following URL into the location/address text box:

`https://sso.state.mi.us/`

2. The "Login User-id and Password" screen appears.

3. Type in your **Single Sign-On User ID**, press the **TAB** key, and type your **PASSWORD**.

4. Click the **LOGIN** button. The "Application Portal - Registration" page appears.

Figure 13-24: Application Portal - Subscription

Note: If you see the link "**Michigan Disease Surveillance System"** within your list of registered applications, you already have permission to access MDSS; hence, you do not need to complete the remainder of these steps.

5. Click the **SUBSCRIBE TO APPLICATIONS** button. The "Subscription" page displays.

6. Select "Dept of Community health" from the first drop-down list and "Michigan Disease Surveillance System" in the second.

Figure 133-25: Subscription Selection

7. Click the **NEXT** button. The "Subscription for: MDSS" page appears.

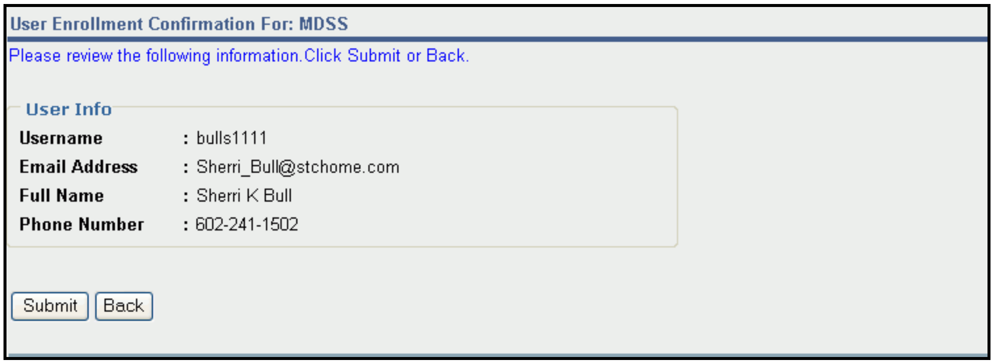
Figure 13-26: Subscription for MDSS

8. Click in the **WORK PHONE** field and type your work phone number beginning with the area code. Your e-mail address will automatically be filled in.

9. Click one of the available buttons:

- **RESET** – clears the information that you entered into the screen and redisplays the page.
- **BACK** – displays the previous screen.
- **CONTINUE** –begins the validation process. If no errors were detected, the "User Enrollment Confirmation" page displays (shown below). If errors were detected, you must correct all errors before proceeding.

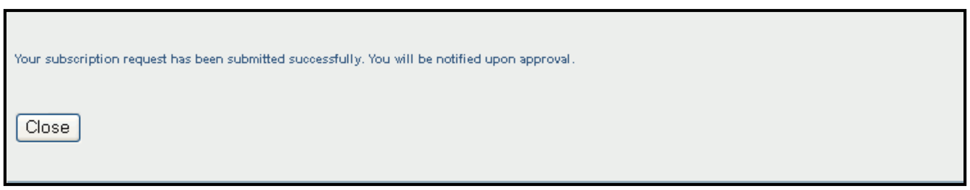
Figure 13-27: User Enrollment Confirmation



10. Review the information displayed and click one of the available buttons:

- **BACK** – displays the previous screen.
- **SUBMIT** – begins the validation process. If no errors were detected, the "Enrollment Acknowledgment" page displays (shown below). If errors were detected, you must correct all errors before proceeding.

Figure 13-28: Enrollment Acknowledgement



11. Click the **CLOSE** button. A "Browser Dialog Box" appears asking if you want to close the Browser. Click the **YES** button to close it. This will close your Internet Browser and your request will be sent.

12. Once your access to MDSS has been granted, you will receive an access approval e-mail (sample approval email shown below).

Figure 13-29: Access Approval Email

13. Continue to the section titled, "Registering with MDSS."

3: Registering with MDSS

The final step to gaining access is to register with MDSS.

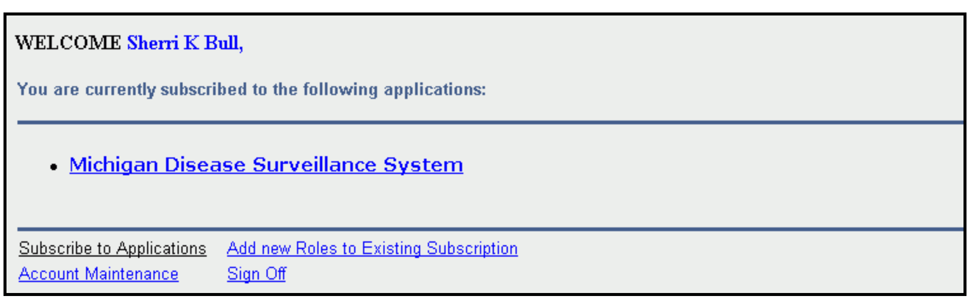
To register with **MDSS**, you must perform the following steps:

1. Using your Internet Browser, type the following URL into the location/address text box:

   https://sso.state.mi.us

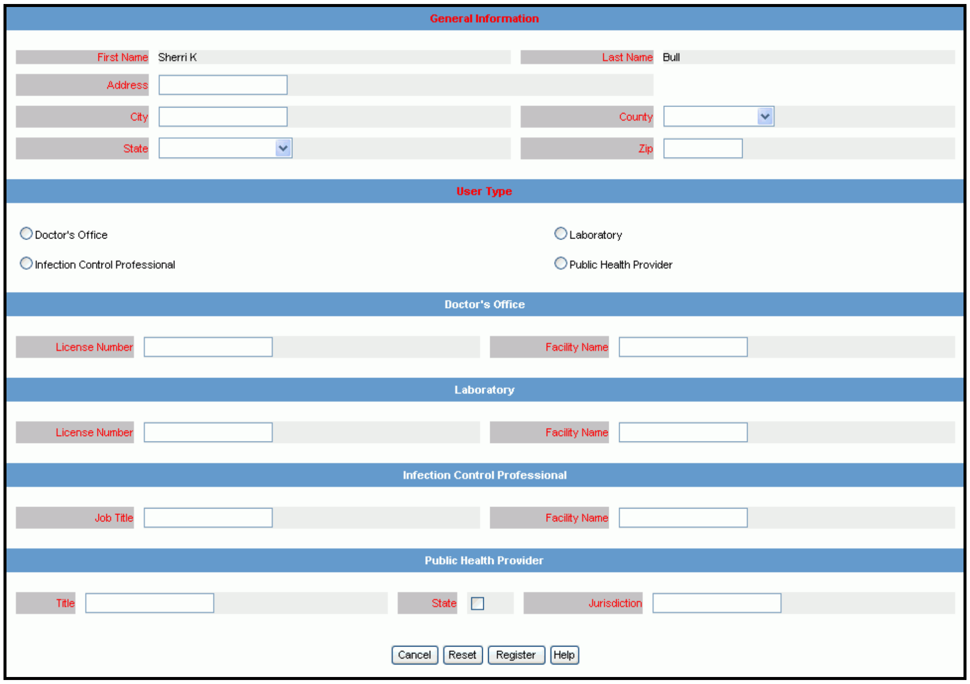
2. Press the **ENTER** key. The “Login User-id and Password” screen appears.
3. Type in your Single Sign-On User ID, press the TAB key, type your Password, and click the LOGIN button. The “Application Portal” window appears with your requested application’s hyperlink (shown below Michigan Disease Surveillance System).

Figure 13-30: Subscribe to Application



4. Click the **Michigan Disease Surveillance System** hyperlink. The "User Registration Form" appears.

Figure 13-31: User Registration Form



5. Using your mouse or the **TAB** key, move to the appropriate fields within the screen and type values for the fields.

- You must fill in the General Information and User Type. Depending on the User Type chosen, fill in the other information; i.e., if the User Type is:

  a) Doctor's Office, fill in the Doctor's Office section of the window.

  a) Laboratory, fill in the Laboratory information.

  b) Etc.

6. When finished adding the information, click one of the available buttons:

- **CANCEL** – Terminates the process of registering with MDSS and closes the "MDSS User Registration" window. A warning prompt is displayed asking you to verify your intention to cancel.

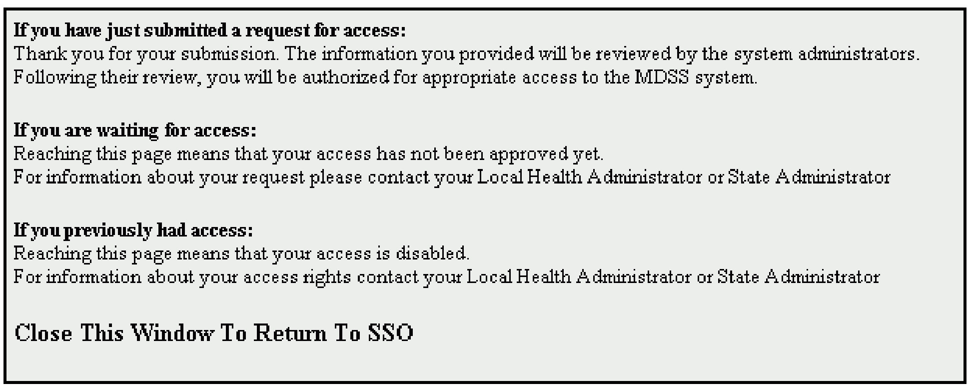
  a) If you click the **CANCEL** button, you will return to the registration screen.

a) If you click **OK**, you will lose any data that you have input.

- **RESET** – Clears the information that you entered into the screen and redisplays the page.
- **REGISTER** – Begins the validation process. If errors were detected, you must correct all errors before proceeding. If no errors were detected, the "Application Portal" screen reappears.

a) If you click on the application hyperlink before receiving a user role, the "No Access/Privilege" screen appears.

Figure 13-32: No Access/Privilege



7. You are now finished registering with MDSS and are in "wait" mode. An email is sent to the System Administrator who assigns you a User Role.
8. Continue to the next section titled, "Getting a User Role."

4: Getting a User Role

The system administrator will select the appropriate user role. Once a role is selected, you will have access to the application. Typically, the system administrator will send a notification email.

For more information regarding user roles or activating a user, please refer to the guide titled, "System Administration."

APPENDIX C: USER ROLES & PERMISSIONS

There are many Roles defined within MDSS that determine the tasks each user can perform. Roles relate to the type of work the person performs or their role within the system and the geography in which they perform these tasks. Each user can only have one role.

When the SSO registration creates a new user account, the LHJ administrator assigns that user a role. Until the role is assigned, the user can navigate to MDSS but will see the "No Privilege" page (shown below).

Figure 13-33: No Privilege Page

If you have just submitted a request for access:
Thank you for your submission. The information you provided will be reviewed by the system administrators.
Following their review, you will be authorized for appropriate access to the MDSS system.

If you are waiting for access:
Reaching this page means that your access has not been approved yet.
For information about your request please contact your Local Health Administrator or State Administrator

If you previously had access:
Reaching this page means that your access is disabled.
For information about your access rights contact your Local Health Administrator or State Administrator

Close This Window To Return To SSO

Roles enforce access limitations to disease groups, jurisdictions, and administrative functions in the organization. The following table depicts the roles defined in MDSS that are relevant to the LHJ Administrators.

Table 13-1: MDSS Roles

Role Number	Description
1	MDCH-BOE Admin/SuperUser
2	MDCH-BOE General Epidemiology Staff
3	MDCH-BOE HIV/AIDS Program Staff
4	MDCH-BOE Tuberculosis Program Staff
5	MDCH STD Program Staff
6	LHJ Supervisory/Admin.
7	LHJ Epidemiologist and/or CD Nurse
8	LHJ Clerical
9	Health Care Provider

Note: To add a new LHJ Administrator, you must contact the Regional Epidemiologist or State Administrator.

Permissions are also defined within MDSS to determine the functions each role can perform. Different MDSS menus and options may be available depending on your role and permissions. Permissions are used to maintain case confidentiality.

The following table shows the relationship between the Roles and their Permissions:

Table 13-2: MDSS Roles and Permissions

Role	Geography	Add New Users	View/Edit Identifying Data	Export Data	Assign Cases	Manage Alerts	View Reports
6	LHJ	Roles 7-9	LHJ	LHJ	Yes	All Diseases All LHJ Users	All except HIV, AIDS, TB, STD and Small Cell count for own LHJ only
7	LHJ	No	LHJ	LHJ	Yes	All Diseases Self-Only	All except HIV, AIDS, TB, STD and Small Cell count for own LHJ only
8	LHJ	No	LHJ	LHJ	Yes	All Diseases Self-Only	All except HIV, AIDS, TB, STD and Small Cell count for own LHJ only
9	No	No	Only Submitted	No	No	No	None

APPENDIX D: ELR AND HL7 MESSAGES

MSG	SEQ	Element Name	Notes
MSH	1	Field Separator	
MSH	2	Encoding Characters	
MSH	3	Sending Application	
MSH	4	Sending Facility	A separate table has been added containing the Laboratory CLIA number, laboratory name, lab address, city, state, zip code, lab contact, and lab contact phone number. The CLIA number, lab contact, and lab contact phone number is maintained in the table but will not show up in the Laboratory section of the Case Investigations screen. The system will not allow CLIA numbers to be duplicated. The HL7 message will contain the sending laboratory's CLIA number (MSH-4) which will be used to pull the lab address data and populate the file in the laboratory section on MDSS. This table is maintained under System Administration and is viewable/editable by SuperUsers only. Note: If the lab address were changed, this would not affect previously entered records. If an ELR message contains an unrecognized CLIA, the record will be rejected.
MSH	4.1	Laboratory Name	
MSH	4.2	CLIA Number (Facility ID)	Required. A pre-built table of facilities is maintained. ELR processing rejects messages containing unrecognized CLIA numbers. Lab address information is copied from the table if not available in the message.
MSH	4.3	"CLIA"	
MSH	5	Receiving Application	
MSH	6	Receiving Facility	

MSG	SEQ	Element Name	Notes
MSH	7	Date/Time Of Message	
MSH	9	Message Type	
MSH	10	Message Control ID	
MSH	11	Processing ID	
MSH	12	Version ID	
PID	5	Patient Name	
PID	5.1	Family Name	If Suffix (PID 5.4) is present, populate database and display following Family Name, with a comma separating the Family name and the suffix.
PID	5.2		
PID	5.3		
PID	5.4	Suffix	If 5.4 is present, populate database and display following family name.
PID	7	Date/Time of Birth	
PID	8	Sex	Any other values than {M,F,U} turn into Unknown.
PID	10	Race	White: W or 2106-3 Black: B or 2054-5 Asian: A or 2028-9 Amer Indian or Alaskan Native: I or 1002-5 Hawaiian or Pacific Islander: 2076-8 Other: M, O, or 2131-1 Unknown: U, null, or anything else.
PID	11	Patient Address	
PID	11.1		
PID	11.3		
PID	11.4		
PID	11.5		
PID	11.9		
PID	13	Phone Number - Home	Optional: Mapped to Home Phone number field.
PID	13.6	Home Phone Number	PID 13.6 and 13.7 is mapped to the

MSG	SEQ	Element Name	Notes
	13.7	Home Phone Number Extension	Home Phone Number in MDSS.
PID	14	Phone Number - Business	Optional: Mapped to Other Phone Number field.
	14.6	Business Phone Number	PID 14.6 and 14.7 is mapped to the Other Phone Number in MDSS.
	14.7	Business Phone Number Extension	
PID	22	Ethnic Group	Hispanic or Latino: H; Not Hispanic or Latino: N; Unknown: U or null or anything else. PID 22 is mapped to the Ethnicity field in MDSS.
OBR	3	Filler Order Number	
OBR	3.1		
OBR	4	Universal Service ID	
OBR	4.1		
OBR	4.2		The Parent Result in OBR 26.3 should be added to the "Ordered Test Name". The format for the "Ordered Test Name" should be "(OBR 4.2), (OBR 26.3)"
OBR	4.3		
OBR	4.4		
OBR	4.5		
OBR	4.6		
OBR	7	Observation Date/Time	
OBR	14	Specimen Received Date/Time	
OBR	15	Specimen Source	
OBR	15.1	specimen source name or code (CE)	
	15.3	Freetext	
	15.4	Body Site	
OBR	16	Ordering Provider	Remove OBR 16.2 mapping from
OBR	16.2	Ordering Provider First Name	

MSG	SEQ	Element Name	Notes
OBR	16.3	Ordering Provider Last Name	"Affiliation." Map OBR16.2 and 16.3 to the Primary Physician First and Last Name in the Referrer Section.
OBR	17	Ordering Provider Phone	
OBR	25	Result Status	
OBR	26	Parent Result	Add to Ordered Test Name
OBR	26.3	Parent Result	OBR 26.3 should be added to the Ordered Test Name. The format for the Ordered Test Name field should be OBR 4.2, OBR 26.3.
ZLR	1	Ordering Provider's Address	
ZLR	1.1		
ZLR	1.3		
ZLR	1.4		
ZLR	1.5		
ZLR	1.9		
ZLR	2	Ordering Facility Name	
ZLR	2.1	Ordering Facility Name	Map to "Affiliation" in the Referrer Screen section.
ZLR	3	Ordering Facility Address	If ZLR-1 is blank, map ZLR-3 to the Primary Physician's Address Information in the Referrer Screen section.
ZLR	3.1-3.5	Ordering Facility Address	ZLR 3.1 - ZLR 3.5 should be mapped to the Primary Physician Address information in the Referrer section on MDSS if the Ordering Provider information (OBR-16) is null.
ZLR	4	Ordering Facility Phone	If ORC-14 is blank, map ZLR-4 to the Primary Physician's Phone Number in the Referrer Screen section.
ZLR	4.6	Ordering Facility Phone Number	ZLR 4.6 - ZLR 4.7 should be mapped to the Primary Physician Phone Number in the Referrer section on MDSS if the Ordering Provider information (OBR-16) is null.
ZLR	4.7	Ordering Facility Phone Extension	

MSG	SEQ	Element Name	Notes
ZLR	5	Patient Age	
ZLR	5.2		
ZLR	5.3		
ZLR	6	Next of Kin/Assoc. Party Name	Mapped to parent/guardian first, last and middle name on demographics screen if ZLR-7.1 = Parent, Mother, Father, Guardian, PAR, MTH, FTH, or GRD.
ZLR	6.1 - 6.4	Next of Kin/Assoc Party	Mapped to parent/guardian first, last and middle name on demographics screen if ZLR-7.1 = Parent, Mother, Father, Guardian, PAR, MTH, FTH, or GRD.
ZLR	7	Next of Kin/Assoc. Party Relationship	
ZLR	8	Next of Kin/Assoc. Party Address	
ZLR	9	Next of Kin/Assoc. Party Phone	
ZLR	10	Reserved (Patient's Occupation)	Mapped to Occupations/Grade Field on Demographics screen.
ZLR	10.2	Occupation Text	Mapped to Occupations/Grade field on Demographics screen (after the lab address that currently is being sent in this spot is moved to ZLR21)
ZLR	11	Reserved	
ZLR	12	Reserved	
ZLR	20	Client Contact (DOH)	
ZLR	21	Lab Address	Map to Lab Address information on Lab Reports 2/Laboratory Information Screen.
ZLR	22	Outbreak Name	Map to "Outbreak Name" field in Investigation Information section of case reporting screen.
OBX	1	Set ID - OBX	
OBX	2	Value Type	

MSG	SEQ	Element Name	Notes
OBX	3	Observation Identifier	Map OBX 3.2 and 3.5 to "Reported Test Name," separated by a slash.
OBX	3.1	Observation Identifier	Map OBX 3.2 and 3.5 to "Reported Test Name," separated by a slash.
OBX	3.2	Observation Identifier	Map OBX 3.2 and 3.5 to "Reported Test Name," separated by a slash.
OBX	3.3	Observation Identifier	Map OBX 3.2 and 3.5 to "Reported Test Name," separated by a slash.
OBX	3.4	Observation Identifier	Map OBX 3.2 and 3.5 to "Reported Test Name," separated by a slash.
OBX	3.5	Observation Identifier	Map OBX 3.2 and 3.5 to "Reported Test Name," separated by a slash.
OBX	4	Observation Sub-ID	
OBX	5	Observation Value	
OBX	5.1	**CE data type*	
OBX	5.2	**CE data type*	
OBX	5.3	**CE data type*	
OBX	5.4	**CE data type*	
OBX	5.5	**CE data type*	
OBX	5.6	**CE data type*	
OBX	5.1	**SN data type*	
OBX	5.2	**SN data type*	
OBX	5.3	**SN data type*	
OBX	5.4	**SN data type*	
OBX	5.1	**ST data type*	
OBX	5.1	**TX data type*	
OBX	6	Units	OBX-6 (Units) should be placed after the result (OBX-5) with a space between the result and the units. Units value should be changed from a drop down to free text so that incoming ELR values can be accepted as they are.

MSG	SEQ	Element Name	Notes
OBX	7	Reference Range	Create a new "Reference Range" field below Coded Result in the "Reported Test Name" section. If OBX-7 is not null, map its value to this field. Suppress display of this field if null.
OBX	8	Abnormal Flags	Create a new "Abnormal Flag/Susceptibility Result" field below Reference Range in the "Reported Test Name" section. If OBX-8 is not null, map its value to this field. Suppress display of this field if null.
OBX	9	Probability	
OBX	10	Nature of Abnormal Test	
OBX	11	Observation Result Status	
OBX	12	Date Last Obs Normal Values	
OBX	13	User Defined Access Checks	
OBX	14	Date/Time of the Observation	
OBX	15	Producer's ID	
OBX	16	Responsible Observer	
NTE	1	Set ID - NTE	Create a new field called "Test Comments" in the "Reported Test Name" Section. If any NTE segments occur after an OBX, the values should be mapped to this field. Multiple NTE records should be concatenated into the Test Comment field.
NTE	3	Comment	

APPENDIX E: ADDITIONAL MDSS REFERENCES AND INFORMATION

For more information on the MDSS, please visit the MDSS Web site at www.michigan.gov/mdss.

APPENDIX F: HAN ALERT CONFIGURATION PROPERTIES

THEORY OF OPERATION

The MDSS system can be configured to generate automatic alerts when new cases are detected. An alert can be configured for a specific condition, location type and a specified number of cases within a specified number of days. Also configurable is the alert level, email only or HAN level (low, medium and high).

Han Alerts are sent to the virtual alert system using the SOAP protocol. All SOAP messages must be authenticated before they can be processed. The MDSS system logs into the SOAP system as a privileged user that is allowed to send messages for other users. All HAN alerts are additionally sent as an email to the user.

Each time a HAN message is sent, an email version is also sent to a “monitor” email address. This was requested so that a supervisor could make sure the HAN messages were being sent to the appropriate people.

If a HAN message receives a negative acknowledge (nack) from the server, an email is sent to the user and monitor email with failure information. A nack may indicate a misconfiguration on the MDSS or HAN side, or may indicate another problem with the message (attempting to alert a non-existent role for example). Specific data about the Virtual Alert API status codes can be obtained from Virtual Alert. MDSS will report the data received from the HAN nack, but does not interpret it.

All configuration properties are located in the **STC.Properties** file. They are described below.

MESSAGE FORMATTING

The Java Message Formatter is used to generate the email and HAN text messages. The available variables are assigned numbers starting with 0. A string is then composed that uses {x} to insert variable x into the string dynamically. The variables available for the alerts are listed below.

Example:

Alert properties:
MDSS User First Name = John
Condition = Aids
Number of Cases = 10
Number of Days = 5

Using the properties values below with a message string of "[0] has a new alert triggered by [5] cases of [4] in [6] days" would generate the following alert string: John has a new alert triggered by 10 cases of Aids in 5 days.

Changes to these properties will take effect after restarting the application server. No caching of these values is done by MDSS, but the application server often caches the properties file, necessitating a restart.

```
#*****************************************************
**
# alert properties
#    0   - MDSS User First Name
#    1   - MDSS User Middle Name
#    2   - MDSS User Last Name
#    3   - Jurisdiction of Case(s)
#    4   - Condition
#    5   - Number of Cases
#    6   - Time span (days)
#    7   - Alert Id
#    8   - Alert Level
#    9   - HAN User Id
#    10  - HAN Role Group
#    11  - MDSS User Id
#    12  - HAN Msg Subject
```

13 - HAN Msg Body
14 - HAN SOAP Exception (Used for monitor failed email only, otherwise null)
15 - HAN Alert Id (assigned when SOAP message is sent, used in monitor email)
#**

EMAIL PROPERTIES

These properties are used to generate the Email text.

com.stchome.mdss.alerting.EmailSubject=Michigan HAN {8} Level Alert M.D.S.S

com.stchome.mdss.alerting.EmailBody=You have received an automated {8} level alert corresponding to M.D.S.S. Alert Number, {7}, created by {0} {2}.\n\nPlease log into the M.D.S.S for additional information. If you are not an M.D.S.S. user, please contact your communicable disease program staff for assistance.

This value is used in the "from" field of the email.

com.stchome.mdss.alerting.EmailFrom=mdss_system@stchome.com

This value is no longer used and can be removed from the file.

com.stchome.mdss.alerting.EmailTo=

HAN PROPERTIES

The following properties apply to the HAN integration.

This controls the HAN integration. It must be set to "true" to enable HAN messages.

com.stchome.mdss.alerting.HAN.soap.enable=false

This sets the url of the HAN system to be used for SOAP communication. It must be uncommented (remove the #) before use.

#com.stchome.mdss.alerting.HAN.soap.url=http://michiganhan.net/vaWebservices/alert.asmx

This sets the service name to use when communicating with the SOAP server.

com.stchome.mdss.alerting.HAN.soap.servicename=AlertingServiceSoap

The following is the privileged user/pass to be used when sending messages on behalf of MDSS users.

com.stchome.mdss.alerting.HAN.soap.mdssuser=mdssadmin

com.stchome.mdss.alerting.HAN.soap.mdsspass=mihan_Pass

The following 2 values set the subject and body of the HAN messages.

com.stchome.mdss.alerting.HAN.subject=test test Michigan HAN {8} Level Alert M.D.S.S

com.stchome.mdss.alerting.HAN.body=this is a test of the api: You have received an automated {8} level alert corresponding to M.D.S.S. Alert Number, {7}, created by {0} {2}.\n\nPlease log into the M.D.S.S for additional information. If you are not an M.D.S.S. user, please contact your communicable disease program staff for assistance.

This sets the duration to be used when signaling the han. The value is in hours.

com.stchome.mdss.alerting.HAN.duration=24

This sets the email subject and body to be send when a han message is attempted and fails for any reason.

com.stchome.mdss.alerting.HAN.failed.subject=test! test! M.D.S.S. Failed Automated {8} Level HAN Alert

com.stchome.mdss.alerting.HAN.failed.body=test! test! The M.D.S.S. attempted to send a {8} level alert to the \"{10}\" using \"{9}\" as a User Id. Check to make sure \"{10}\" and \"{9}\" are valid. If you need additional assistance, contact the M.D.S.S Help Desk.

The system will send an email containing the details about each HAN alert to an authorized person. The email address to be used is set here.

com.stchome.mdss.alerting.HAN.monitor.email=brian_fox@stchome.com

These values set the subject and body of the email sent to the HAN monitor defined above.

com.stchome.mdss.alerting.HAN.monitor.subject=M.D.S.S. sent HAN message.

com.stchome.mdss.alerting.HAN.monitor.body=The following HAN Alert (Id {15}) was sent to HAN Role \"{10}\" from M.D.S.S. User \"{11}\":\n{12}\n{13}

This defines the subject and body sent to the monitor when a message fails.

com.stchome.mdss.alerting.HAN.monitor.failed.subject=M.D.S.S. Failed Automated {8} Level HAN Alert

com.stchome.mdss.alerting.HAN.monitor.failed.body=The M.D.S.S. User {0} {2} \"{11}\" attempted to send a {8} level alert to the \"{10}\" role using \"{9}\" as a User Id. Check to make sure \"{10}\" and \"{9}\" are valid. If you need additional assistance, contact the M.D.S.S Help Desk.\n\n Exception Text:{14}

These values map the alert high,medium and low to the corresponding values in HAN.

com.stchome.mdss.alerting.HAN.HIGH=2

com.stchome.mdss.alerting.HAN.MEDIUM=1

com.stchome.mdss.alerting.HAN.LOW=0

STEPS TO ENABLE HAN

Set com.stchome.mdss.alerting.HAN.soap.enable = true.

Set com.stchome.mdss.alerting.EmailFrom= to the address alert messages should come from. This is also where emails will bounce to if they have a bad address.

The following 4 field values must be obtained from Virtual Alert.

Verify that com.stchome.mdss.alerting.HAN.soap.url is pointing to the correct han address.

Verify that com.stchome.mdss.alerting.HAN.soap.servicename has the correct service name.

Set com.stchome.mdss.alerting.HAN.soap.mdssuser and

com.stchome.mdss.alerting.HAN.soap.mdsspass to the correct values.

Change com.stchome.mdss.alerting.HAN.monitor.email to contain the email that all han messages should be cc'd to. If this value is empty, then no monitor emails will be sent.

14 INDEX

T

U

V

W