Appendices

APPENDIX A - SOFTWARE REQUIREMENTS / SETTINGS

Software requirements for using the MDSS application are listed below. Current versions of the required software can be downloaded from their respective sites:

- <u>Internet Browser</u>

    Microsoft Internet Explorer is recommended – version 5.5 SP2 or higher.

    http://www.microsoft.com/windows/internet-explorer/default.aspx

- <u>Adobe Reader</u>

    Version 5.1 or higher is recommended. 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 blank forms and entering investigation information into the application.

    http://www.adobe.com/products/reader/

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

INTERNET EXPLORER SETTINGS

The following settings must be setup using Internet Explorer:

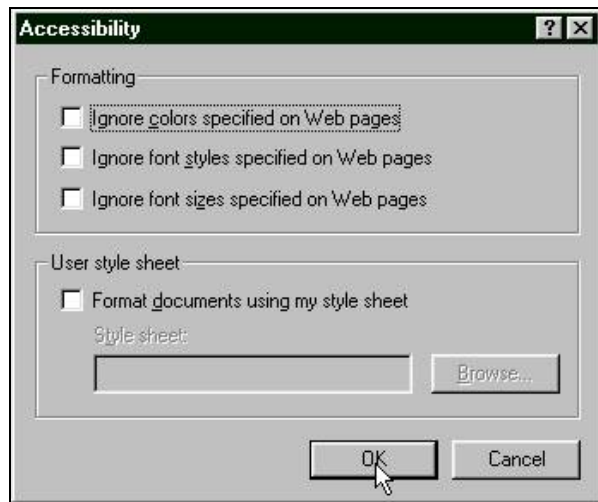- Font Styles

- 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 A-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 A-2: Internet Explorer Text Size**
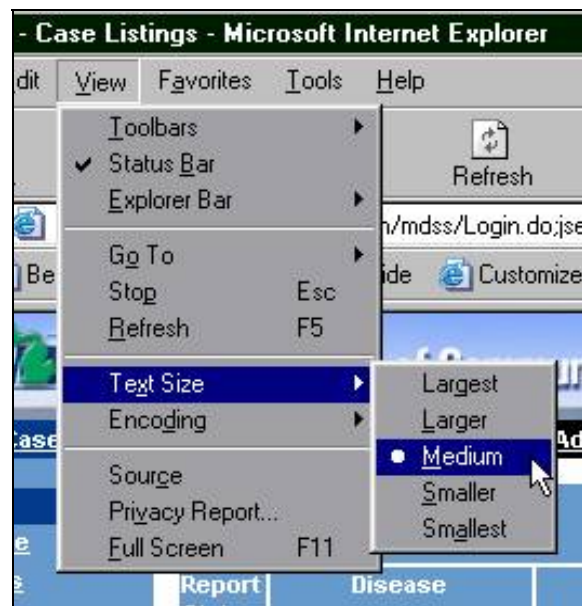
AUTO-COMPLETE

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, the Michigan Department of Community 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 A-3: Internet Options – Content
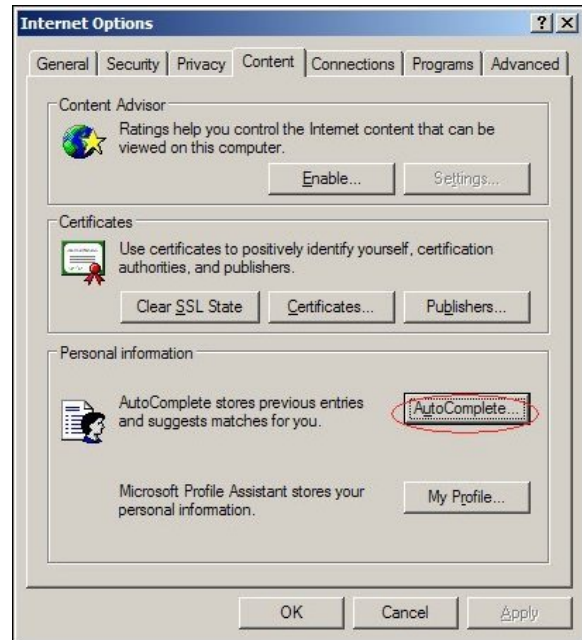
4. In the "Personal Information" section, click the **AUTOCOMPLETE** button. The "AutoComplete Settings" window appears.

Figure A-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 previously existing saved application data. An "Internet Options Confirmation" dialog box appears.

Figure A-5: Internet Options Confirmation Dialog Box
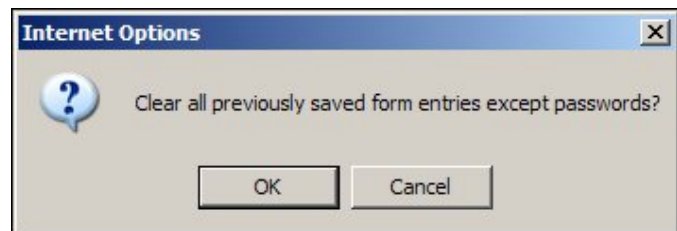
7.   Click the **OK** button. The "Auto-Complete Settings" window reappears.

8. Click the **OK** button. The "Internet Options" window reappears.

9. Click the **OK** button.

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 A-6: Display Properties - Settings
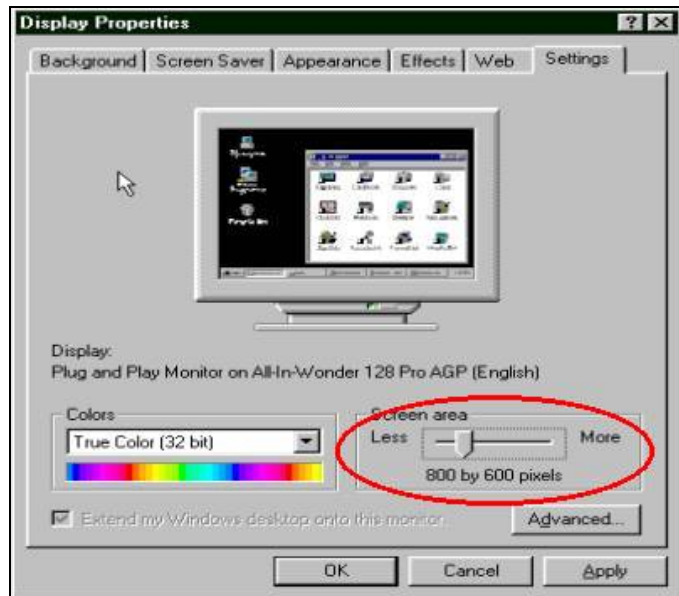
6. In the "Screen Area" section (bottom right hand corner), drag the slider until the setting reads "800 by 600 pixels."

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

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

Figure A-7: Font Size Settings
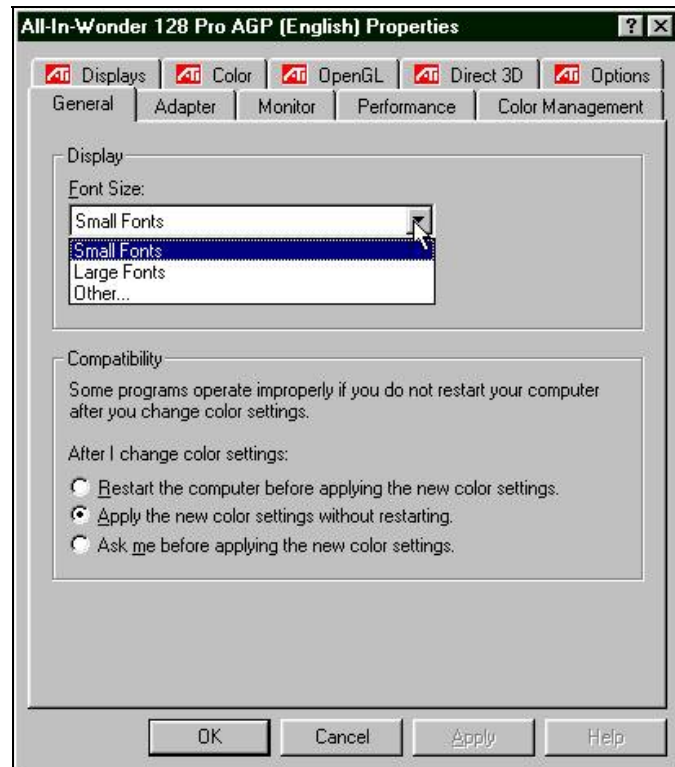
9. In the "Display – Font Size" section of the window, click the drop-down arrow and select **SMALL FONTS**.

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 <u>Single Sign-On (SSO) User ID</u> 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 <u>Permission to Access MDSS</u>. Requesting Access will walk you through the steps of requesting access.

3. You must complete the <u>MDSS User Registration</u>. User Registration will walk you through the steps of registering.

4. You must be assigned a <u>Role</u> within MDSS. Getting a User Role will discuss the process of obtaining a user role.

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

The Michigan Department of Information Technology maintains the Single Sign-On (SSO) portal which allows a user to access the MDSS, as well as other state applications, with one User-ID and password.

Users who have a valid Single Sign-On User-ID and password (e.g., Michigan Care Improvement Registry (MCIR) 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 "State of Michigan Single Sign On" screen will appear:

Figure B-1: State of Michigan Single Sign On

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

Figure B-2: 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 B-3: SSO Registration – Step 2

State of Michigan Single Sign On

REGISTRATION- Step 2

Please Enter a four digit number to create a unique UserID : **example** [   ]   Why should I enter this number?
(OR)
Please generate a random four digit number for me   : ○ Yes ⊙ No

Enter the number as it is shown in the box below *   : [   ]

[Back] [Continue] [Clear]   [42657]

Copyright © 2008 State Of Michigan. All rights reserved

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 B-4: Why enter a 4-digit number dialog box
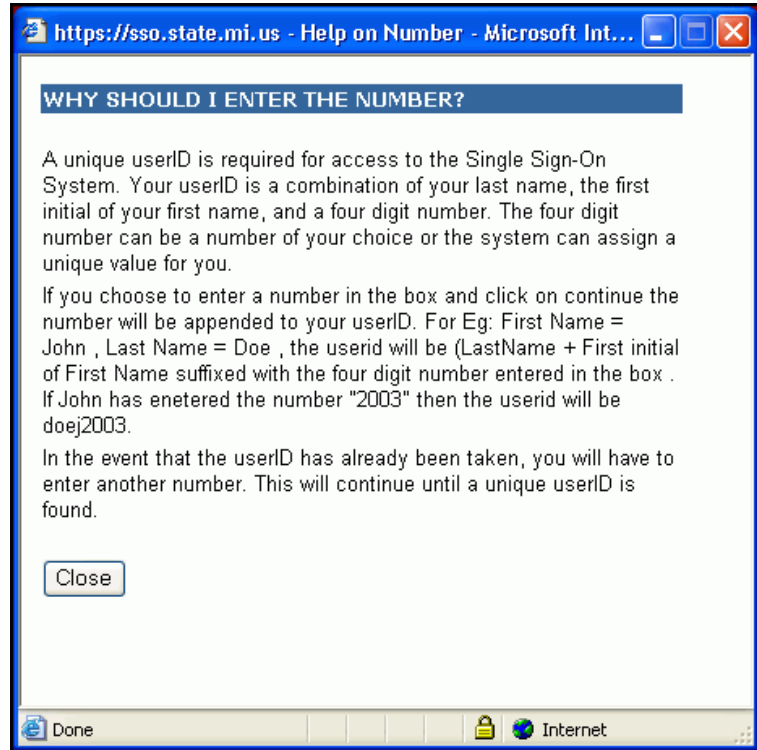
8. After reading the dialog box, click the **CLOSE** button to return to the "Registration – Step 2" window.

9. 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 Figure B-3 as an example, the number to type would be: 42657

10. 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** – continues 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 B-5: User Registration Confirmation

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

- **BACK** – displays the "SSO Registration – Step 2" window.
- **SUBMIT** – continues 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 B-6: Request for Registration -Acknowledgment

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

13.   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 B-7: SSO Registration Email
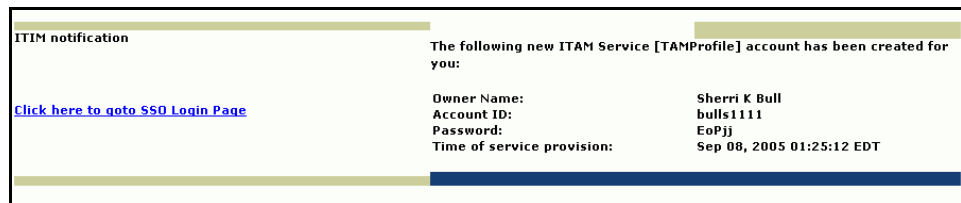
If you attempt to login before getting the email, you will get a message stating, "Login failed. You have used an invalid username, password or client certificate."

14.   After you receive the SSO registration email, click on the hyperlink labeled, "**Click here to go to SSO Login Page.**" The "State of Michigan Single Sign On" window appears.
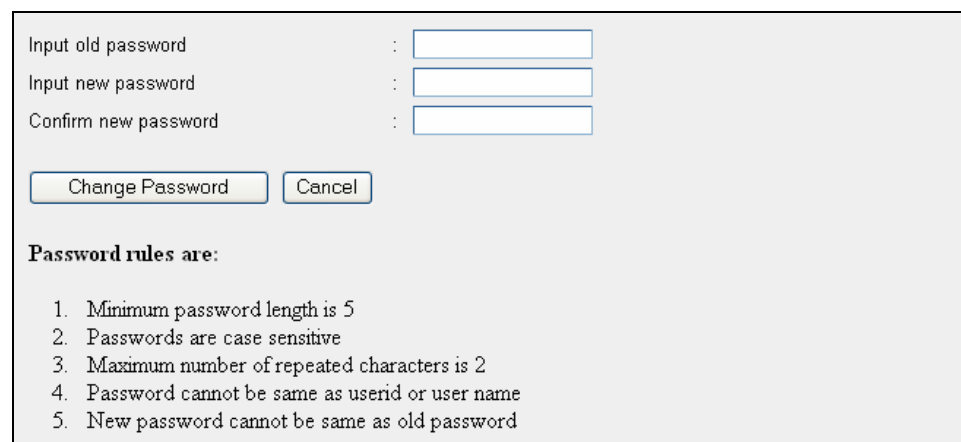
Figure B-8: State of Michigan Single Sign On

15. 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 B-9: SSO Expired Password

16. 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. Passwords can not

contain more than 2 repeated characters and must be different from the userid, username and old password.

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

Figure B-10: Change Challenge/Response Answers

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

19. 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 B-11: Change Challenge/Response Answers Acknowledgment
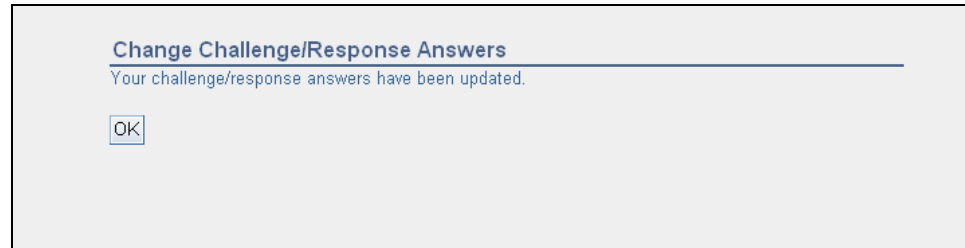
20.   Click the **OK** button. The "Account Maintenance" screen appears.

Figure B-12: Account Maintenance
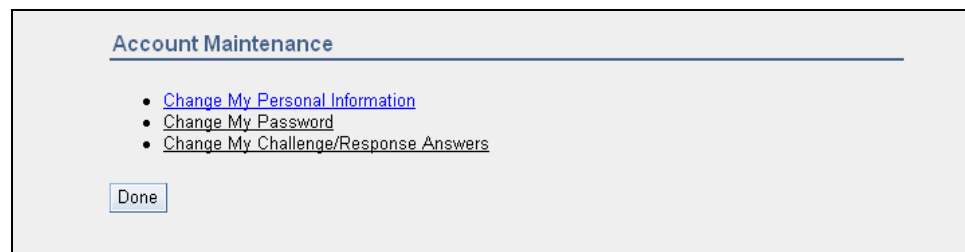
21.   Click the **DONE** button. The "Application Portal" screen appears.

Figure B-13: Application Portal
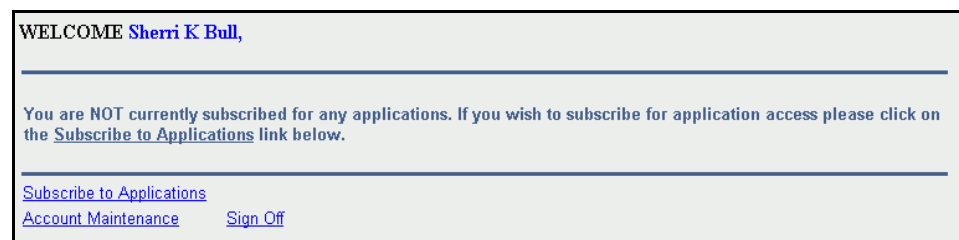
• You now have a valid SSO User ID and Password. Continue to the next section titled, "Requesting Permission to access MDSS."

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 "Michigan Single Sign On" screen appears.

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

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

Figure B-14: Application Portal

WELCOME Sherri K Bull,

You are NOT currently subscribed for any applications. If you wish to subscribe for application access please click on the Subscribe to Applications link below.

Subscribe to Applications
Account Maintenance   Sign Off
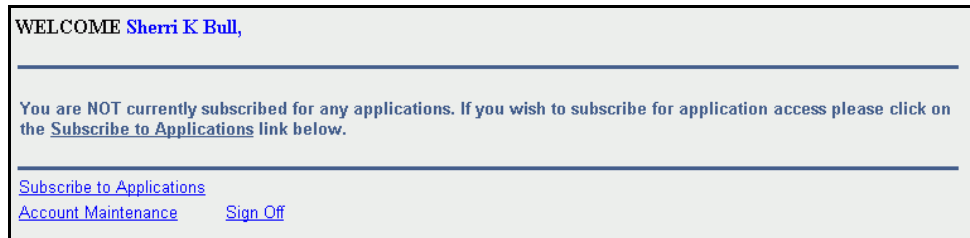
Note: If you see the link **MICHIGAN DISEASE SURVEILLANCE SYSTEM** within your list of registered applications, you already have permission to access MDSS. Continue to the section titled, "Registering with MDSS."

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

Figure B-15: Subscription Selection

6.   From the "Dept of Community Health" list, click the "Select App" drop-down arrow to view the application options and point/click to "Michigan Disease Surveillance System."

7.   Click the **NEXT** button. The "Subscription for: Michigan Disease Surveillance System" page appears.

Figure B-16: 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 B-17: User Enrollment Confirmation

User Enrollment Confirmation For: MDSS

Please review the following information. Click Submit or Back.

User Info

Username	: bulls1111
Email Address	: Sherri_Bull@stchome.com
Full Name	: Sherri K Bull
Phone Number	: 602-241-1502

[Submit] [Back]

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

- **BACK** – displays the previous screen.

- **SUBMIT** – continues 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 B-18: Enrollment Acknowledgement

Your subscription request has been submitted successfully. You will be notified upon approval.

[Close]

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. A sample approval email shown below; however, please be aware that some email spam filters will prevent the email from reaching your inbox even if your access to the MDSS has been approved.

Figure B-19: Access Approval Email

```
****   THIS IS AN AUTO-GENERATED E-MAIL.   PLEASE DO NOT REPLY TO IT DIRECTLY.   ****

       Your request for access to the MDSS application has been approved. The
       MDSS application link will be available the next time you log into the
       Single Sign-On system.|
```

13. Now, you have permission to access MDSS. 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 "Michigan Single Sign On" screen appears.

3. Type in your **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 as Michigan Disease Surveillance System).

Figure B-20: Subscribe to Application

WELCOME Sherri K Bull,

You are currently subscribed to the following applications:

- Michigan Disease Surveillance System

Subscribe to Applications   Add new Roles to Existing Subscription
Account Maintenance   Sign Off

4. Click the **MICHIGAN DISEASE SURVEILLANCE SYSTEM** hyperlink; the "User Registration Form" appears.

Figure B-21: 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 (using your work address) and User Type. Depending on the User Type chosen, fill in the other information as appropriate. For example, if the User Type is:

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

b) Laboratory, fill in the Laboratory section.

c) Etc.

Note: In the Public Health Provider section, only MDCH users should check the *Statewide* checkbox.

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.

  b) 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.

7. You are now finished with your steps for registering with MDSS. The MDSS now sends an email to an administrator who will assign you a user role. If you click on the application hyperlink before receiving a user role, the "No Access/Privilege" screen appears.

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

> **8.**   Continue to the next section titled, "Getting a User Role."

4: GETTING A USER ROLE

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

For more information regarding user roles or activating a user, please refer to the MDSS Administration User Guide.

APPENDIX C - USER ROLES & PERMISSIONS

The MDSS role structure determines the tasks each user can perform within the application. 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, an administrator assigns that user a role. Until the role is assigned, the user can navigate to the MDSS but will see the "No Privilege" page (shown below).

Figure C-1: No Privilege Page
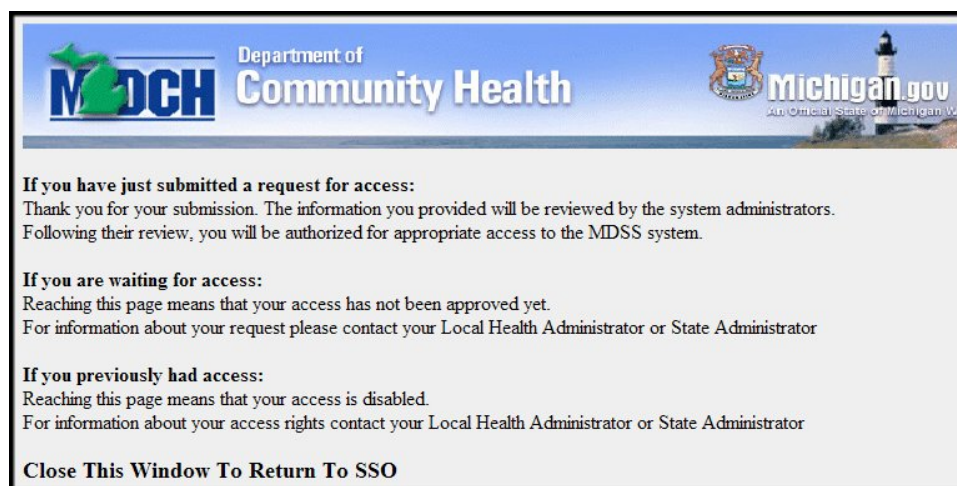
Roles enforce access limitations to disease groups, jurisdictions, and administrative functions in the application. The MDSS utilizes a role structure consisting of four elements:

- Role – Determines a user's basic level of access to the system

- Geography – Determines what geographic areas a user can access on the MDSS

- Job Function – Determines what functions or tasks a user can complete on the MDSS

- Program Areas – Determines which disease groups a user may access on the MDSS

The following table describes the options for each of these elements and the associated level of access in more detail.

Table C-1: MDSS Role Elements

Element	Options	Level of Access
Role	MDCH-BOE	Statewide data
	LHJ	Data for assigned geographies
	HCP	Data associated with assigned facility or facilities
	Lab	Data submitted by user
Geography	Statewide	All roles have statewide access, except LHJ users
	Jurisdictional	LHJ users can be assigned to one or more jurisdictions
Program Areas	All	All Disease Groups
	General CD-STD-TB	All Disease Groups except HIV/AIDS
	General CD-STD	All Disease Groups except HIV/AIDS and TB
	General CD-TB	All Disease Groups except HIV/AIDS and STD
	General CD	All Disease Groups except HIV/AIDS, TB and STD
	HIV/AIDS	Only the HIV/AIDS Disease Group
	STD	Only the STD Disease Group
	Tuberculosis	Only the TB Disease Group
	Foodborne	Only the Foodborne Disease Group
	Animal Rabies	Only Animal Rabies and Animal Bites
Job Function	System Administrator	Access to all system functions
	Administrator	Access to all administrative functions
	Epi Staff / CD Nurse	Access to all functions except user management
	General / Data Entry Staff	Access to all functions except completing cases, the pending work queue and user management
	Limited Access	Access designed for healthcare provider users

Element	Options	Level of Access
	View Access	Access designed for laboratory users
	Reports Only	Access to only the Reports Menu
	No Access	Default for new registrations not yet assigned a function

Geography – Secondary jurisdictions can only be assigned to LHJ users by the Regional Epidemiologist or State Administrator with the written permission from the LHJ MDSS Administrator of the jurisdiction that is being added. Additionally, LHJ users with more than one jurisdiction must have the same Program Area and Job Function in all assigned jurisdictions.

Program Area – Users can only be assigned to Program Areas with access to HIV/AIDS data (Program Areas "All" and "HIV/AIDS") with the approval of MDCH HIV/AIDS staff.

Job Function – To add a new LHJ Administrator, you must contact the Regional Epidemiologist or State Administrator.

The following table provides further detail regarding user permissions by Job Function:

Table C-2: MDSS Job Functions and Permissions

	Admin	Epi Staff / CD Nurse	General / Data Entry	Limited Access	View Access	Reports Only
View case listings	X	X	X	X	X	
View/Edit case details	X	X	X	X		
Export cases	X	X	X			
Assign investigator	X	X	X			
Aggregate cases	X	X	X	X		
View reports	X	X	X	X		X
Complete cases	X	X				
Entry deduplication	X	X	X			
Pending work queue	X	X				
Create alerts for self	X	X	X			
Manage other users' alerts	X					
Manage users	X					

	Admin	Epi Staff / CD Nurse	General / Data Entry	Limited Access	View Access	Reports Only
Review replaced patients	X					
Administrative reports	X					
Unassigned cases				X	X	

The MDSS System Administration User Guide contains detailed
instructions on how to assign a role to a new user or edit the role of a
current user.

APPENDIX D - HL7 / MDSS DATA ELEMENT MAPPINGS

MDSS can receive Electronic Laboratory Reports via HL7. When these HL7 elements come into the MDSS system, they will automatically populate certain input fields.

Refer to the table for a cross-reference list.

Table D-1: HL7 / MDSS Data Element Mappings

Seg	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

Seg	SEQ	Element Name	Notes
			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	
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.

Seg	SEQ	Element Name	Notes
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 Home Phone Number in MDSS.
	13.7	Home Phone Number Extension	
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		

Seg	SEQ	Element Name	Notes
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	Free Text	
	15.4	Body Site	
OBR	16	Ordering Provider	
OBR	16.2	Ordering Provider First Name	Remove OBR 16.2 mapping from "Affiliation." Map OBR16.2 and 16.3 to the Primary Physician First and Last Name in the Referrer Section.
OBR	16.3	Ordering Provider Last Name	
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		

Seg	SEQ	Element Name	Notes
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	
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	

Seg	SEQ	Element Name	Notes
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	
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	

Seg	SEQ	Element Name	Notes
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.
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	

Seg	SEQ	Element Name	Notes
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 - 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/vaWeb services/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 sent 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.

INDEX