



**SmartMsg Guide for Configuring
Campus and Citizen Alerting System
Web Portals**

SmartMsg

Secure Notification Software

Additional SmartMsg documentation is available through the Codespear website.
<http://www.codespear.com/helpcentral.asp>

Codespear is committed to providing documentation that provides full understanding of SmartMsg software. We encourage comments on any of the above documentation. This may include pointing out features that require further explanation, ambiguity in any language, inconsistencies in information or misinformation.

Send e-mails regarding any of the above-mentioned problems or any other grievances regarding any documentation to:

SmartMsgdocumentation@Codespear.com

Codespear appreciates all comments regarding any issues in order to ensure the accuracy, consistency and simplicity of all of our documentation.

Please note: This e-mail address is for comments only. If you have technical questions please contact Technical Support by visiting our website.



CODESPEAR

Federal Signal Codespear
370 E. Maple, Suite 350
Birmingham, MI 48009
www.codespear.com

This document is for informational purposes only. Codespear makes no warranties, express or implied, as to the information in this document.

©Copyright 2007 Federal Signal Codespear. All Rights Reserved. SmartMsg Documentation V5.2

Codespear Proprietary & Confidential Information

Table of Contents

Creating a Citizen/Campus Alerting Web Portal Website	4
Modifying the Settings File.....	12
SmartMsg Configuration	18

Overview

The Campus or Citizen Alerting Web Portal offers a way for users to access a SmartMsg system from a web browser. This allows citizens, students or any mass population to access a SmartMsg System to maintain their own user profile and device information. Clients access this web portal through standard web browser software, such as Internet Explorer (6 or 7), Firefox, or Opera. The setup of a website on a Microsoft IIS server is part of the configuration of a SmartMsg Campus or Citizen Alerting system. The website, in turn, accesses a SmartMsg System by means of the SmartMsg XML Interface, which is an optional SmartMsg Server module. This document is intended to guide an administrator through the process of setting up the necessary website and modules in a SmartMsg system.

Skills and Knowledge Prerequisites

This guide assumes that the reader is familiar with using IIS (Internet Information Server) to create websites and has authority to do so. The reader may also need access to view and/or edit SmartMsg Global Properties.

Server Requirements

- SmartMsg Server with the XML Interface and Mass Dial modules installed, GIS Console module and GIS Console software required for geographic-based alerting.
- CSD_XML.dll - most recent build, CSD_MassDial.dll - most recent build, CSD_GIS.dll - most recent build, SmartMSGAPI.dll
- Server running Windows 2000 Server or Windows 2003 and Internet Information Server (IIS) 5.0 or higher. (IIS and SmartMsg can be run on same server or separate servers.)
- IIS Server must have access to the SmartMsg Server via port 16887
- IIS Server must have ASP installed and enabled.
- IIS Server must have SSI (Server Side Includes) enabled (Windows 2003).
- Web Portal users must have access to the IIS server via port 80 or port 443 (SSL)*
- Enabled Parent Paths (IIS Application Configuration options)
- Scripts and Execute permission

*** Port 80 is the standard port used for web access. It is possible for an organization to use a different port for SmartMsg web access. This will require users to add the port to the end of the web address to access the site. For example: for a site with an address of smartmsg.xyzcompany.com using port 300 (instead of the default port 80), users would need to access <http://smartmsg.xyzcompany.com:300>**

SSL certificates are highly recommended for SmartMsg Web setups that will be accessed via a public IP address. Port 443 is the standard port used for SSL.

Other Important Considerations

There are many different server configurations that an organization may use and port settings are variable. For information on default ports used with SmartMsg and the Citizen/Campus Alerting web portal, please see SmartMsg Default Port Summary or SmartMsg Installation Checklist for Locally Hosted Systems. There also may be things to consider such as security issues when setting up a website through IIS. Review these topics in Microsoft's IIS help documentation.

Installing an SSL Certificate

It is recommended that a 128-bit SSL certificate is installed for the Citizen/Campus Alerting website. This will ensure that communication between the web browser and web server is secure. SSL Certificates can be obtained through companies such as Verisign, Digicert, Thawt and others.

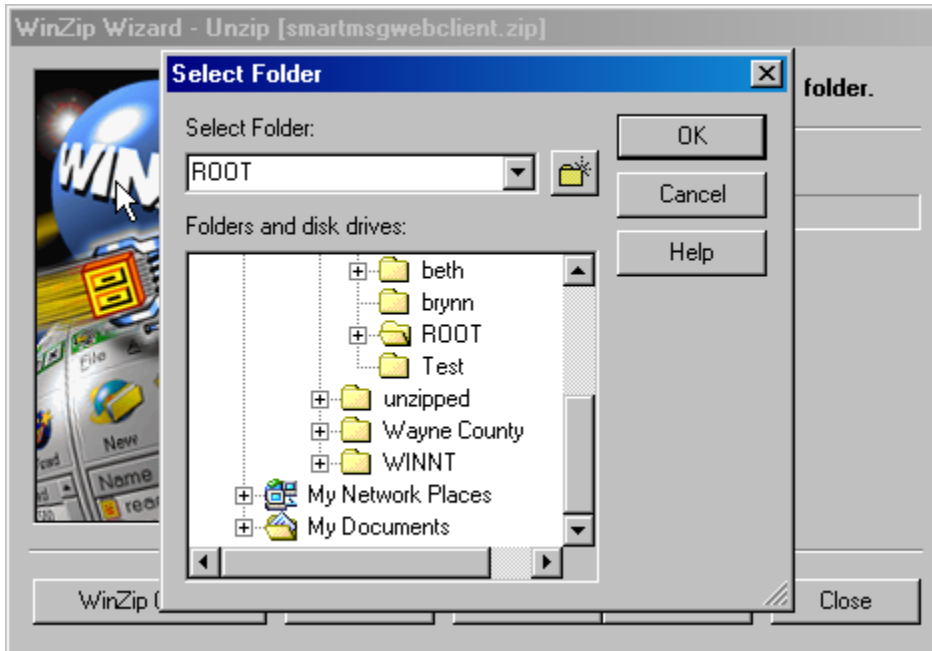
SmartMsg Dialing Configuration

If the Citizen/Campus Alerting system will include voice dialing, this must be configured in the Mass Dial module settings, under Call Manager. See Codespear Dialing Documentation for more information.

Creating a Citizen/Campus Alerting Web Portal Website

Download Files

1. Attain the web zip file from Codespear. (Example file name: SmartMsgCITIZEN/CAMPUS ALERTING.zip).
2. Unzip and extract these files to your web root folder (or other designated directory) that will be used as the root folder for the SmartMsg portal website.



NOTE: The following instructions reference the %systemroot% folder. This is the windows system root folder. The exact path to this folder can vary from system to system. Normally, the folder is c:\windows or c:\winnt. It can also be located on drive other than c: (Examples: The Windows system root folder could be d:\windows or e:\winnt, if the Windows operating system is located on a non-default drive.) To determine where your system root folder is located, type "Set" and hit Enter at a windows command prompt. All system variable values will be listed.

SmartMSGAPI.dll and Ateksc.dll Setup

- a. Stop all SmartMsg applications on the computer – including the SmartMsg server service, SmartMsg Client application, SmartMsg Admin Tool, and any other SmartMsg applications.
- b. If %SystemRoot%\System32\SmartMSGAPI.dll already exists, unregister the current DLL using this command from a Windows Command Prompt:
`regsvr32 /u %SystemRoot%\System32\SmartMSGAPI.dll`

YOU SHOULD RECEIVE A MESSAGE SAYING THE FILE UNREGISTERED SUCCESSFULLY.

- c. Copy SmartMSGAPI.dll and AtekCSE.dll (from the unzipped file in step# 2) to %SystemRoot%\System32 folder, overwriting the existing files if they already exist.
- d. Register the new copy of SmartMSGAPI.dll using this command from a Windows Command Prompt:
regsvr32 "%SystemRoot%\System32\SmartMSGAPI.dll"
- e. Open Windows Explorer to the system32 folder using this command:
explorer.exe /e,/root,"%SystemRoot%\System32"
- f. If prompted, click the "Show files" link to expose these files in the file pane.
- g. Right click on the SmartMSGAPI.dll file and choose Properties.

Note: Steps h-s need to be completed for the AtekCSE.dll file as well. Do them for the SmartMSGAPI.dll file and then come back and do them for the AtekCSE.dll file.

- h. Click the "Security" tab.
- i. Click the "Add" button.
- j. If the computer you are working from is a member of a Windows domain, you will need to make sure the Computer name (not a domain name) is selected in the *Look In* drop down list.
- k. Type the following into the text box under the list:
IUSR_{computername}; IWAM_{computername}

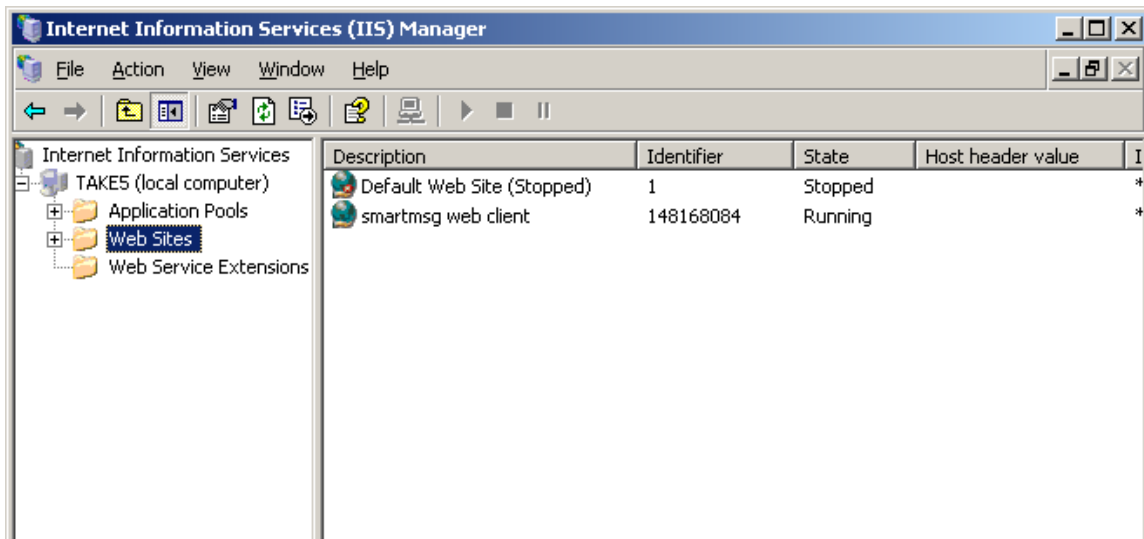
IUSR is the user IIS runs as. IWAM is the service account IIS runs as. Both of these accounts need 'Execute' access to SmartMSGAPI.DLL.

- l. Click the "Check Names" button. Make sure that the names are underlined and no errors are shown.
- m. Click "OK" button, to close the dialog.
- n. Select the IUSR_{computername} user in the list at the top.
- o. In the permissions pane, make sure that "Read & Execute" is checked.

- p. Select the IWAM_{ computername} user at the top of the list.
 - q. In the permissions pane, make sure that "Read & Execute" is checked.
 - r. Click the "Apply" button.
 - s. Click the "OK" button.
3. Open Internet Information Services (IIS) Manager. You can find this in your Control Panel under Administrative Tools.

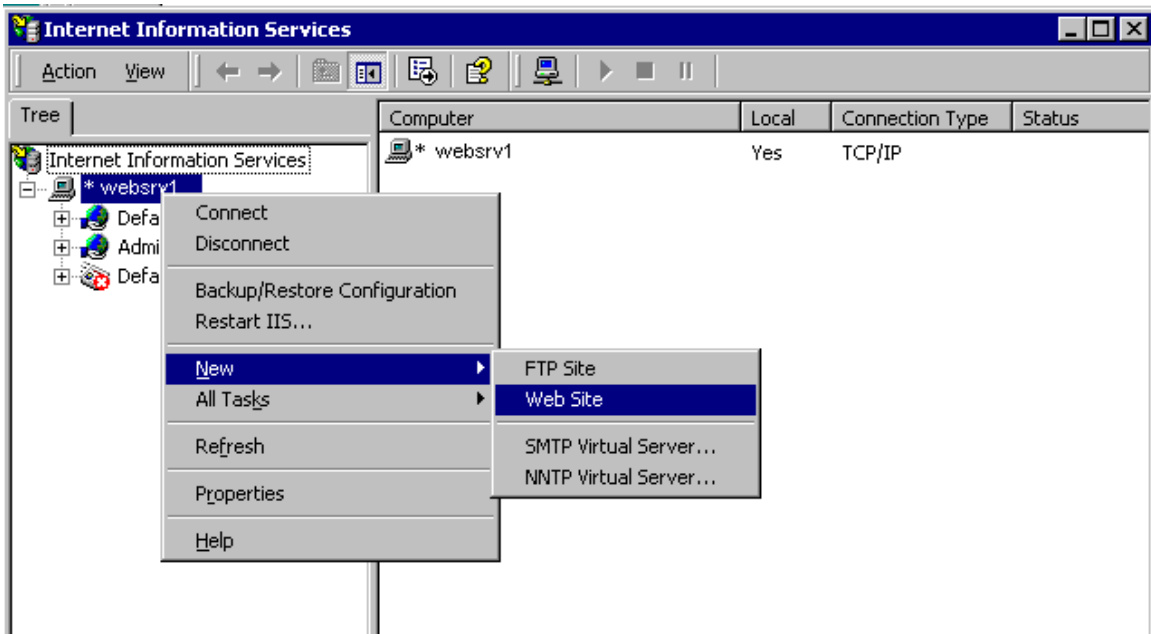
The IIS user-interface varies slightly based upon what Operating System is used.

4. If running Windows 2003 Operating System, right-click Web Sites, and go to New ->Website...



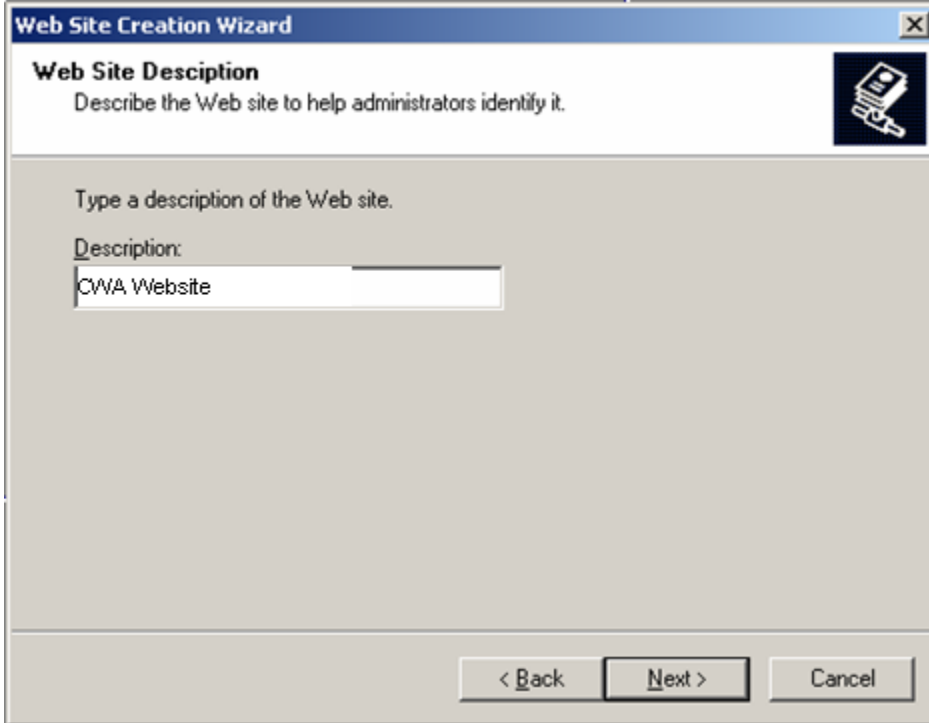
-OR-

- If running Windows 2000 Server Operating System, right-click on the Server Name ->New ->Website



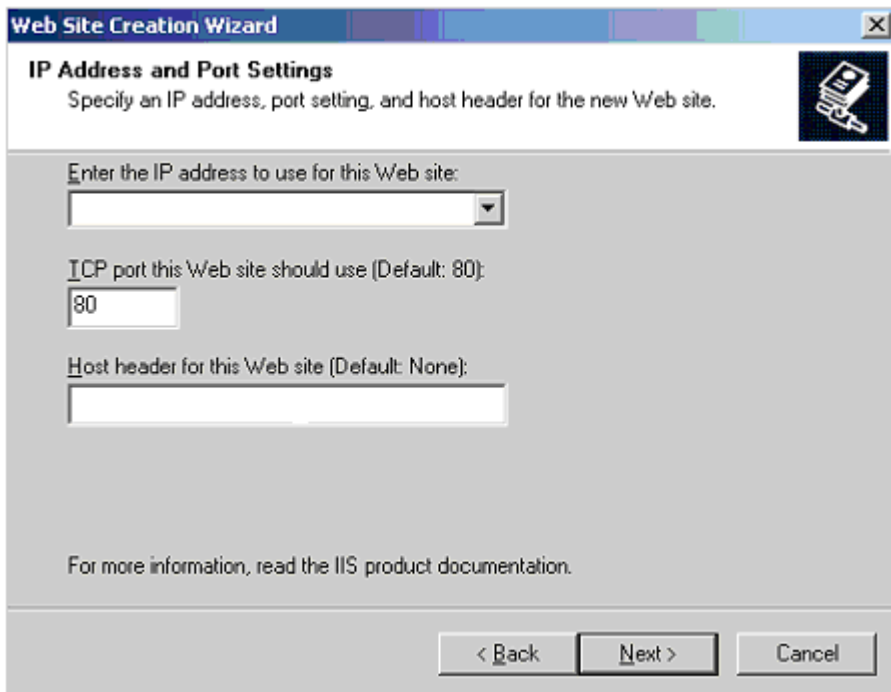
5. Click on **Next**.

6. Enter a **Description**.



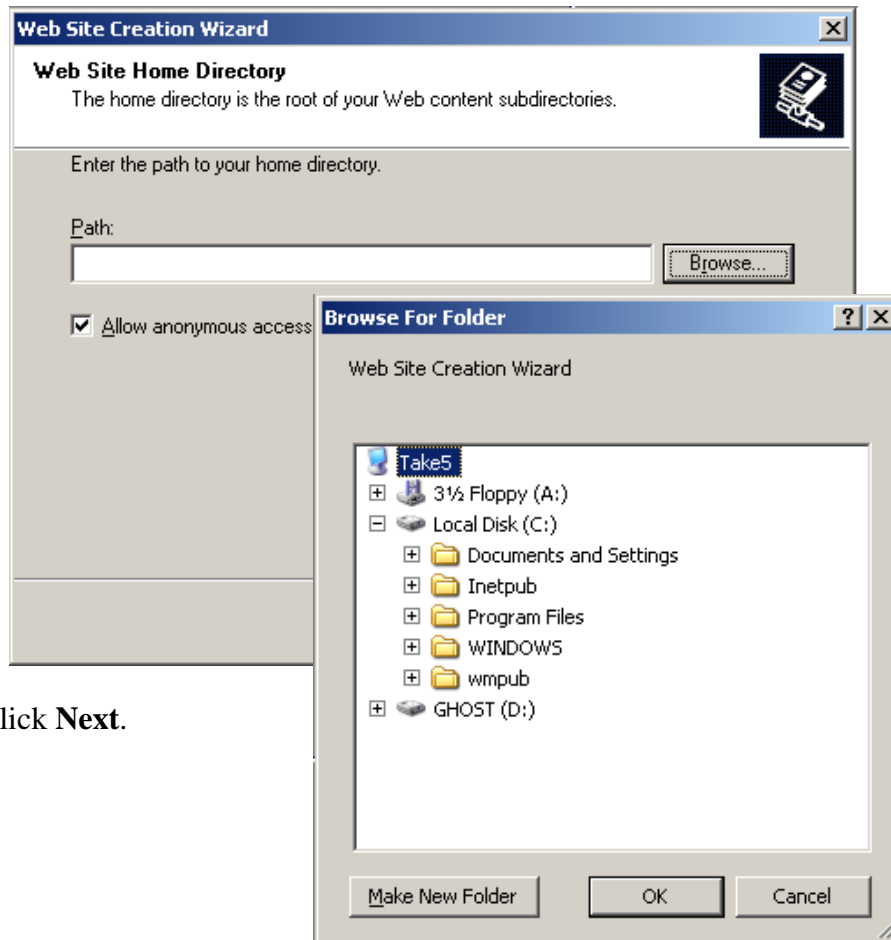
The screenshot shows a window titled "Web Site Creation Wizard" with a close button in the top right corner. The main heading is "Web Site Description" and the instruction is "Describe the Web site to help administrators identify it." Below this, it says "Type a description of the Web site." There is a label "Description:" followed by a text input field containing the text "CWA Website". At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

7. Click **Next**.
8. Pick the **IP Address** from the dropdown menu.



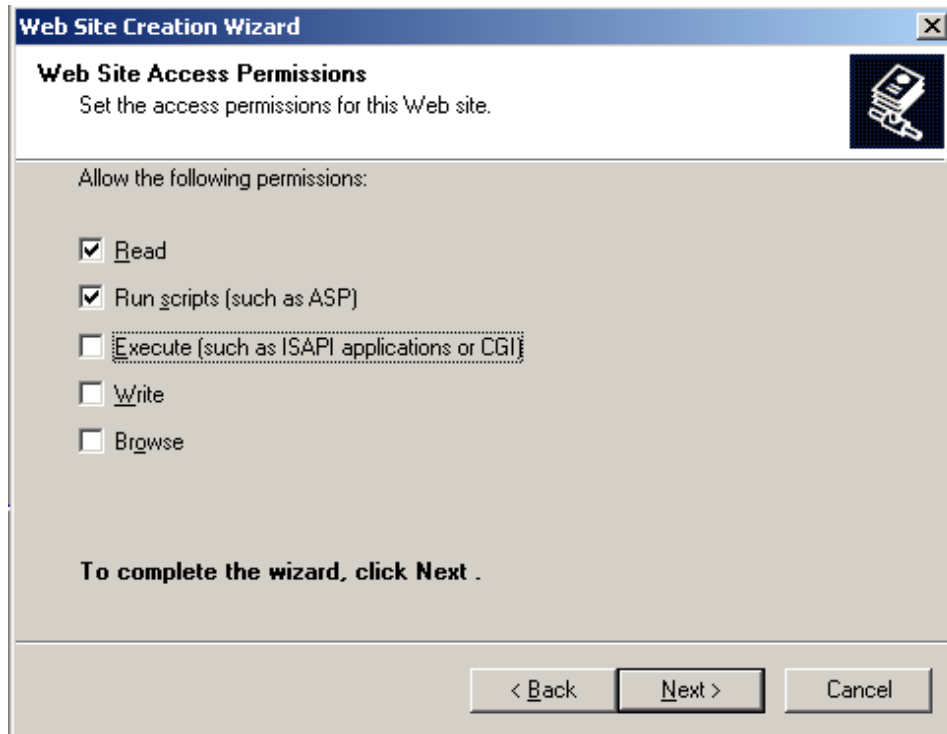
The screenshot shows a window titled "Web Site Creation Wizard" with a close button in the top right corner. The main heading is "IP Address and Port Settings" and the instruction is "Specify an IP address, port setting, and host header for the new Web site." Below this, it says "Enter the IP address to use for this Web site:" followed by a dropdown menu. Then, it says "TCP port this Web site should use (Default: 80):" followed by a text input field containing the number "80". Below that, it says "Host header for this Web site (Default: None):" followed by a text input field. At the bottom of the window, there are three buttons: "< Back", "Next >", and "Cancel".

9. The **TCP port this Web site should use (default: 80)** typically will be left as the default value, 80. This port value can be changed if your organization uses a different port for web access.
10. For the **Host Header for this Web site (Default: None)**, leave blank to default to the IP address. Entering a host header name will restrict access to the site to that name – users will not be able to access the site via IP address. See Microsoft IIS documentation for more information.
11. Click **Next**.
12. To enter the **Path**, browse to the directory where the SmartMsg Citizen/Campus Alerting web files reside. (Recall the path used in step 2, where SmartMsg web files were unzipped and extracted into the website folder.)



13. Click **Next**.

14. Check Read and Run scripts (such as ASP).
15. Click Next.



16. Click **Finish**.
17. In the left tree list, expand the contents (click the plus sign next to the name) until you can see the server you are installing to. Expand to see the website just created (or the default web site, if that is site being used.)
18. Right click the site and choose "Properties".
19. Click the "Home Directory" tab.
20. Under "Application Settings", change "Execute Permissions" to: "Scripts and Executables".
21. Click "Apply" button.
22. Click "OK" button.

Modifying the Settings File

23. Open a Windows Explorer window and navigate to the web application folder (folder where you unzipped to in step 2).

24. Navigate to the "include" directory, and open up settings.asp with Notepad.

25. In settings.asp change the following variable names:

Const SM_SERVER_HOST = "localhost" to:

Const SM_SERVER_HOST = "{your smartmsg server ip address}"

Const SITE_TITLE = "Customer County or School name"

Place appropriate name in the quotation marks.

Const URL_SITE_HOME = "./"

URL_SITE_HOME is for the left image in the header - when clicked browser redirects to this URL.

Const URL_SITE_HOME2 = "http://www.CustomerCounty.com/"

URL_SITE_HOME2 is for the right image in the header - when clicked browser redirects to this URL.

Use the value "./", to set the browser to simply be directed to the main page of this Citizen/Campus Alerting website when clicking the left image.

Normally, if a customer's logo is used in one of the 2 above locations, the browser redirect would be defined for the customer's official website.

Example:

Stevens Institute of Technology logo would be defined with
<http://www.stevens.edu>

26. In the IIS management console: Stop and Start the website, by right clicking and selecting **Stop** and then right clicking and selecting **Start**.

27. Bring up the new website in a browser to verify that the basic website is working. (The site will not be fully functional until SmartMsg is configured as well.) If you are testing from the actual IIS computer, you should be able to type in <http://localhost/WebSiteName> where **WebSiteName** is the name of the site you created in earlier steps. IF you used the Default WebSite, the link will simply be <http://localhost>

XML Documents

The Citizen/Campus Alerting website will be populated with data from 3 XML files. The import will take place within the Mass Dial Module. But first, the XML files need to be created and saved in the proper format for import.

Alerts XML File

The Alerts XML File is used to import alert types into SmartMsg. These are the alerts that Citizen/Campus Alerting users may subscribe to. The format for the document is as follows, for a simple list of alerts:

```
<alerts>
  <alert name="alertname" />
</alerts>
```

"alertname" will be replaced with the name of the alert you decide upon. The `<alert name="alertname" />` line can be repeated for as many alerts as you wish to import.

An example Alerts XML File might look like this:

```
<alerts>
  <alert name="All Campus Community Members" />
  <alert name="Graduate Students" />
  <alert name="Other" />
  <alert name="Undergraduate Students" />
</alerts>
```

The example above would provide the user with a simple list of alerts they may subscribe to in the Alert Manager portion of the Citizen/Campus Alerting website. The Alert Manager would have a checkbox for the alerts, like this:

- All Campus Community Members
- Graduate Students
- Other
- Undergraduate Students

A simple list of alerts, as shown in the example above, may be all you need. In some cases, an extensive list of alerts may suit your needs better. When there are multiple alerts involved, alert groups may be necessary. Alert groups can be imported into the system to organize the alerts more efficiently. For example, you might have a group of alerts called "Road Alerts" containing multiple highway/freeway alerts. At the same time, you could have a group of alerts called "Weather Alerts" containing alerts relating to different weather conditions. The format for the document is as follows, for an import containing alert groups:

```
<alerts>
  <alertgroup name ="AlertGroupName" >
    <heading> Text for Heading </heading>
    <alert name ="AlertName" />
  </alertgroup >
</alerts>
```

```
</alertgroup>
</alerts>
```

Where “*AlertGroupName*” is the title you decide upon for the group of alerts, *Text for Heading* is the text appearing above the list of alerts, and “*AlertName*” is the title for the single alert. The `<alert name =”AlertName” />` line can be repeated for as many single alerts you wish to import. The lines of code below may also be repeated for as many alert groups you wish to import:

```
<alertgroup name =”AlertGroupName” >
  <heading> Text for Heading </heading>
  <alert name =”AlertName” />
</alertgroup>
```

You may also put an alert group within another alert group. In this case, the code might look like this:

```
<alerts>
  <alertgroup name =”AlertGroupName” >
    <heading> Text for Heading </heading>
    <alertgroup name =”AlertGroupName” />
      <heading> Text for Heading </heading>
      <alert name=”AlertName” />
    </alertgroup>
  </alertgroup>
</alerts>
```

Here is an example of an XML file containing alert groups:

```
<alerts>
  <alertgroup name="Road Alerts">
    <heading>Choose the road alerts you would like to receive</heading>
    <alert name="Hwy 72" />
    <alert name="Hwy 28" />
  </alertgroup>
  <alertgroup name="Weather Alerts">
    <heading>Choose the weather alerts you would like to receive</heading>
    <alert name="Tornado Warning" />
    <alert name="Flood Warning" />
  </alertgroup>
  <alertgroup name="School Alerts">
    <heading>Choose the schools you would like to receive alerts on</heading>
    <alert name="Jefferson High School" />
    <alert name="Washington Middle School" />
    <alert name="Lincoln Elementary School" />
  </alertgroup>
</alerts>
```

The website configuration pertaining to the XML file above would have radio buttons for each alert group type on the first page, like this:

Choose an alert type

/ Main

- Road Alerts
- Weather Alerts
- School Alerts

If the user chose Road Alerts, they would see:

Choose the road alerts you would like to receive

/ **Main** / Road Alerts

- Hwy 72
- Hwy 28

If the user chose School Alerts, they would see:

Choose the schools you would like to receive alerts on

/ **Main** / School Alerts

- Jefferson High School
- Washington Middle School
- Lincoln Elementary School

And if the user chose Weather Alerts, they would see the alerts pertaining to weather conditions.

Important Note: When you have finished configuring your xml file, save it and take note of the location you save the file to. You will need to recall the path to the file in a subsequent step of this process.

Communities XML File

The Communities XML file is used to import city and zip code information into SmartMsg. The format for the document is as follows:

```
<commzips>  
  <commzip comm="CityName" zip="ZipCode" />  
</commzips>
```

“*CityName*” will be replaced with the name of the city you are importing into the system and “*ZipCode*” will be replaced with the city’s corresponding zip code. The <comm="CityName" zip=ZipCode" /> line can be repeated for as many cities and zip codes you wish to import.

An example Communities XML file might look like this:

```
<commzips>  
  <commzip comm="Birmingham" zip="48009" />  
  <commzip comm="Walled Lake" zip="48390" />  
  <commzip comm="Wolverine Lake" zip="48390" />  
  <commzip comm="Detroit" zip="48201" />  
  <commzip comm="Detroit" zip="48202" />  
  <commzip comm="Detroit" zip="48203" />  
</commzips>
```

Important Note: Save the xml file, and take note of the location you save the file to. You will need to recall the path to the file in a subsequent step of this process.

Association Groups XML File

The Association Groups XML file is used to link groups of users to alerts. For example, you might create an association group for “Students” that is tied to the alert “All Students”. Users in the “Students” group would then be automatically subscribed to the “All Students” alert.

The format for the document is as follows:

```
<association_groups>
  <role name=RoleName>
    <group name=AssociationGroupTitle alert=AlertName/>
  </role>
</association_groups>
```

The “*RoleName*” is one of the existing roles within the CITIZEN/CAMPUS ALERTING system. Roles define profiles that determine whether or not a user will be able to see certain fields on the CITIZEN/CAMPUS ALERTING website. The roles within the CITIZEN/CAMPUS ALERTING system currently are: All, Citizen, Student, and Ext_Auth.

“*AssociationGroupTitle*” is what you will name the Association Group.

“*AlertName*” is the name of the alert that will be linked to this association group.

Here is an example of an Association Group XML File:

```
<association_groups>
  <role name="Student">
    <group name="All Students" alert="All Students" />
  </role>
</association_groups>
```

Now, a user could be imported into the SmartMsg/CITIZEN/CAMPUS ALERTING system and assigned to the “All Students” Association Group. This would mean that they will have a website role of “Student”, and they will be automatically subscribed to the “All Students” alert.

SmartMsg Configuration

A Standard Install of SmartMsg Server does not include all the necessary server modules for a Citizen/Campus Alerting system. The Mass Dial module and the XML modules should be obtained via SmartMsg Auto Update.

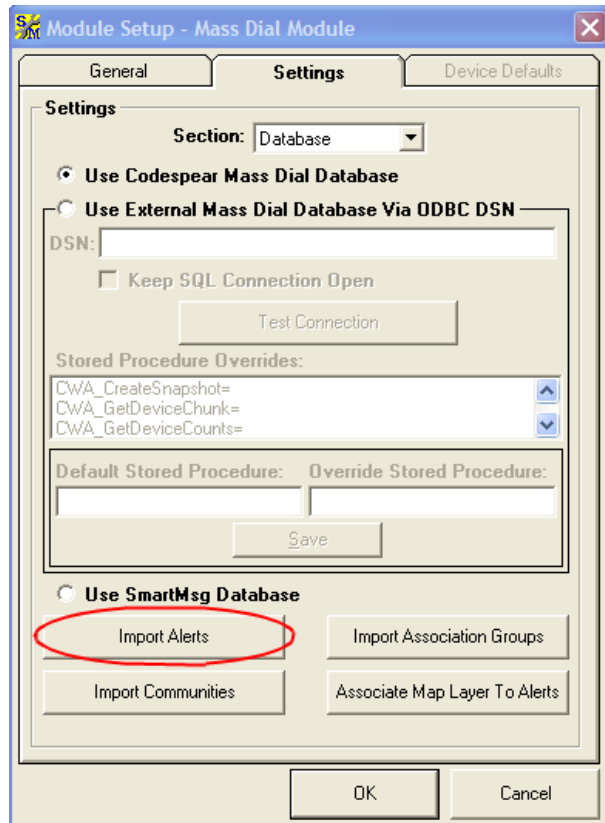
- 1) Run the Auto Update utility (from the SmartMsg Administrator Tool or from an Auto Update Package obtained through Codespear Technical Support) and install the **Mass Dial module** and **XML modules**. Also select updates for any other applicable server modules.
- 2) Restart the SmartMsg Server service after running the Auto Update. (This can be done by restarting the SmartMsg Server Service in Control Panel-> Administrative Tools-> Services or by right clicking the server in the SmartMsg Administrator Tool and clicking the “Restart SmartMsg Server” button.)
- 3) Once the SmartMsg server has been restarted, select **Properties** from the **Global Menu**.
- 4) Click the **Modules** Tab.
- 5) Select **Mass Dial Module** and click the **Setup** button.
- 6) On the General tab, make sure that the **Enable Module for System** option is checked.
- 7) Click the **Settings** Tab.
- 8) Select **Database** from the **Section** dropdown menu.

You then have 3 options for the database that you will use with your Citizen/Campus Alerting system:

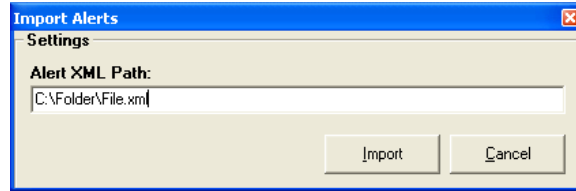
- **Codespear Database** – you may choose to use the Codespear Database structure for your Citizen/Campus Alerting system. Your users will not consume user licenses if you use the Codespear Database. Using the Codespear Database is recommended for systems with under 100,000 users.
- **External Database** – you may choose to use you own SQL database that SmartMsg can access via ODBC. Your users will not consume user licenses if you use an External Database. Using an External Database is recommended for systems with more than 100,000 users.
- **SmartMsg Database** – you may choose to use the SmartMsg Database for your Citizen/Campus alerting system. With this method, every user that logs into your portal will consume a regular SmartMsg user license, but they will have full user profile functionality within SmartMsg. This means that users will have the option to create rules for their devices, whereas the other 2 options do not allow this feature.

1) Select which Database option you will use. If you select the **Use Codespear Mass Dial Database** or the **Use SmartMsg Database** options, you can then go to the next step. If you choose the **Use External Mass Dial Database Via ODBC DSN**, you will then need to enter your **DSN** (Data Source Name) into the text box below it. The **Stored Procedures** are an advanced topic and you may need to contact Codespear Technical Support for assistance.

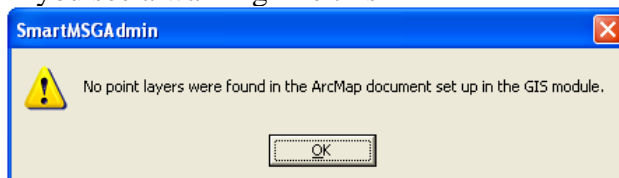
2) Click the **Import Alerts** button.



- 3) Enter the path and file name of the xml file containing alert information.

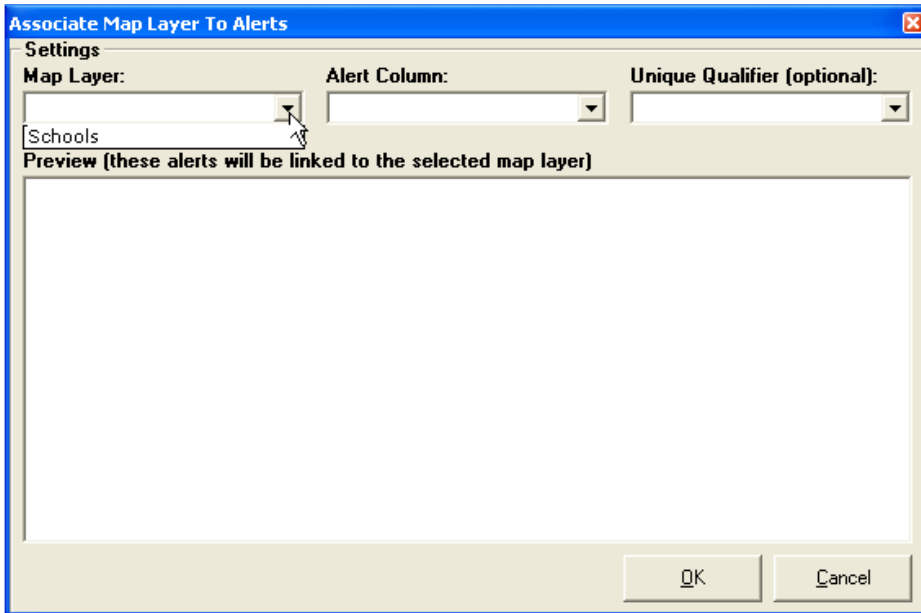


- 4) Click the **Import** button.
- 5) Click the **Import Association Groups** button.
- 6) Enter the path and file name of the xml file containing association group information.
- 7) Click **Import**.
- 8) Click the **Import Communities** button.
- 9) Enter the path and filename of the xml file that contains city and zip code data.
- 10) Click **Import**.
- 11) (OPTIONAL) Click the **Associate Map Layer to Alerts** button. *Note: This step has a prerequisite – the GIS Console module must be configured before this step can be completed. Please refer to GIS Console documentation for instructions.*
If you see a warning like this –

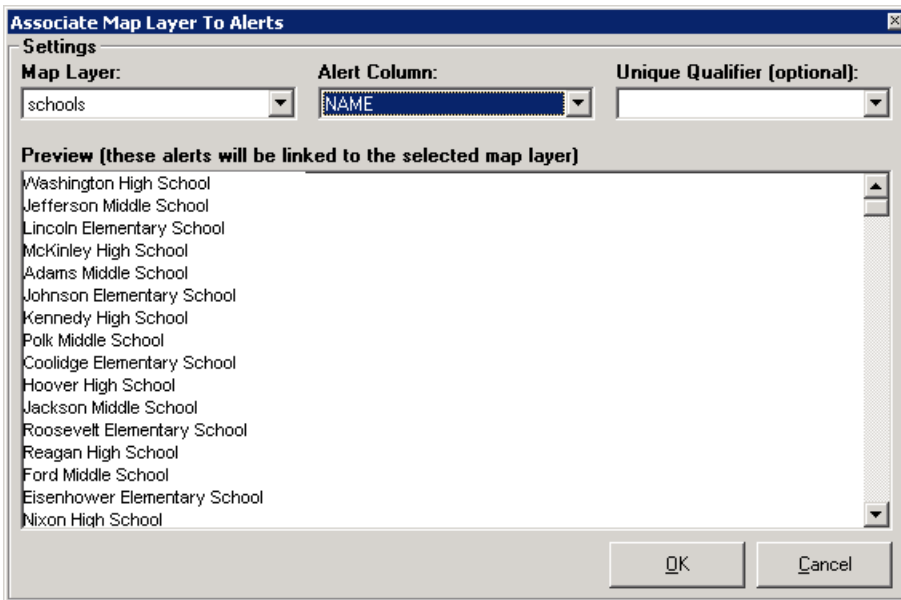


This means that the map document you associated with the GIS module doesn't contain point layers OR you have not set up the GIS Console module correctly.

- 12) Choose the **Map Layer** (Point layer) you want to associate to an alert from the dropdown list. In the example below, the map layer we are choosing is "Schools".

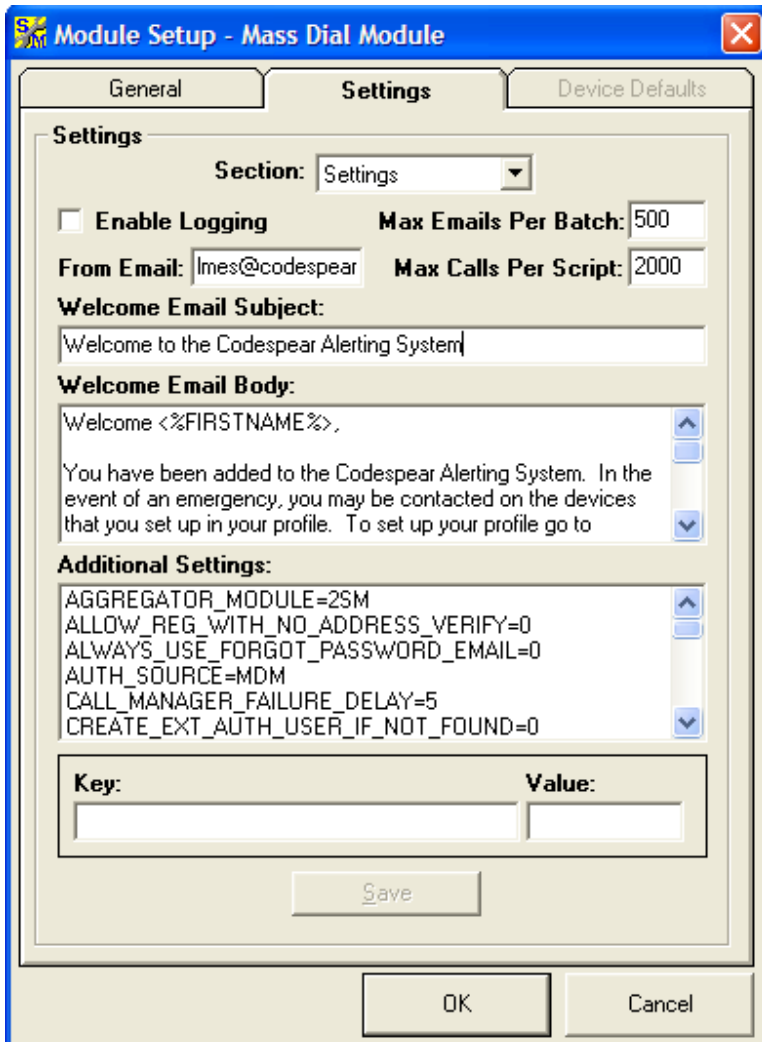


- 13) Then, choose an **Alert Column**. This will be the column in the data that identifies each point on the map. In our Schools example below, the Alert Column is “NAME”. For your map data, it may be something different. You can view the Preview window to check to be sure that you have chosen the right alert column.



- 14) The last field on this screen should be used if any of the data in the Alert Column is the same. A unique qualifier can be chosen to identify the point. For example, if there were 2 schools called “Adams Middle School” in your map data, you could choose a Unique Qualifier, like the “City” to uniquely identify the point.

- 15) Click **OK**.



16) Select **Settings** from the Section dropdown menu.

17) Choose whether or not you would like to **Enable Logging**. This enables the logging debug information. The log created is named **MDMdate.log**, where the *date* is in the format of **yymmdd**. For example the Mass Dial Module log file for January 17, 2008 would be called "MDM080117.log".

18) Enter a From **Email** address. This allows Global Administrators to designate a From Email Address that alert recipients on

SMS and Email Devices will see as the alert originator.

19) Enter a number of **Max Emails Per Batch**. When a batch is sent, SmartMsg will wait until it has received some kind of response (failed, received, etc.) from half of the emails, and then will begin sending out the next batch. So, if you set your batch size to 500 and send out an alert to 1000 email recipients – SmartMsg will send out 500 emails, wait for 250 responses and then send out 500 more.

20) Enter a number of **Max Calls Per Script**. This designates the maximum number of calls that will be sent to the dialer at a time.

21) (Optional) Modify the **Welcome Email Subject**, as desired. During a user import, one of the options (located in Additional Settings) is to send the users an email, welcoming them to the Citizen/Campus Alerting system. The text for the subject of the email is defined in this field.

22) (Optional) Modify the **Welcome Email Body**, as desired. During a user import, one of the options (located in Additional Settings) is to send the users an email, welcoming them to the Citizen/Campus Alerting system. The text for the body of the email is defined in this window. Available variables you may include in the email are:

<%FIRSTNAME%> - which will insert the first name of the user receiving the welcome email.

<%LASTNAME%> - which will insert the last name of the user receiving the welcome email.

<%USERID%> - which will insert the User ID that the user will use to log into the Citizen/Campus Alerting website.

<%PASSWORD%> - which will insert the Password that the user will enter to log into the Citizen/Campus Alerting website.

23) Define values for each of the options in **Additional Settings**. Click on a setting in this window and it will fill itself in the **Key** field. The value for the setting can be modified in the **Value** setting. Click Save after each setting you modify. **If you make changes to any of these settings, make sure to use the Save button to save your changes.**

AGGREGATOR_MODULE = If you are using an SMS Aggregator to send out SMS messages (SMS Text Messages or Text Pages), you will use this field to choose from the 2 Aggregator options that we offer. To use the 2SMS Aggregator module, enter 2SM. To use the Air 2 Web Aggregator, enter A2W.

Leave the field blank if you do not plan to use an Aggregator for SMS messages.

ALLOW_REG_WITH_NO_ADDRESS_VERIFY = users must enter an address with a zip code and it must verify with the GIS locator file OR the zip code must be in the zip code layer in the map file. 1 = an address is not required to register.

ALWAYS_USE_FORGOT_PASSWORD_EMAIL = upon clicking the forgot password link on the Citizen/Campus Alerting website login page, a user will be sent an email to the email address they entered when they signed up for the site. 1 = upon clicking the forgot password link on the Citizen/Campus Alerting website login page, an email is sent to the address identified in the FORGOT_PASSWORD_EMAIL field.

AUTH_SOURCE - when the user authenticates (verifies username and password), this field defines what source to authenticate against. MDM = Mass Dial Module (SmartMsg Database), LDAP = LDAP module (external to SmartMsg), and WebAuth = Web Authentication Module (external to SmartMsg) are the available options.

CALL_MANAGER_FAILURE_DELAY – enter the number of minutes you want the system to wait before resending a failed batch of phone calls to the dialer.

CREATE_EXT_AUTH_USER_IF_NOT_FOUND - this option will only be used if you are using an authentication source that is external to SmartMsg (LDAP or WebAuth). 0=a user that authenticates but is not in the mass dial database will not be able to log in. 1=a user that authenticates but is not in the mass dial database will be created in the database.

DEFAULT_ASSOCIATION_GROUP - if you would like to put users into a default group when they sign up, the default group will need to be defined here.

If nothing is entered into this area, users will not be assigned to default association groups and will need to subscribe to any alerts they wish to receive.

EMAIL_REQ - defines whether or not an email address is required when users sign up for the website. 0=an email address is not required. 1=an email address is required

FORGOT_PASSWORD_EMAIL - when the ALWAYS_USE_FORGOT_PASSWORD_EMAIL=1, the forgotten user information will be sent to the email address identified in this field.

LOG_ALERT_SUBSCRIPTION_CHANGES - logs changes in alert subscriptions to the SmartMsg database Transactions table. 0=changes are not logged. 1=changes are logged.

LOG_DEVICE_CHANGES - logs changes in the total number of devices to the SmartMsg database Transactions table. 0=changes are not logged. 1=changes are logged.

LOG_GEN_PWD_TO_FILE_DURING_IMPORT - if you will be importing Mass Dial Users with the SmartMsg Data Import Export Tool, one of the options is to generate random passwords for each new user. This setting will determine whether to log the passwords, along with the username and email address, to a comma delimited file. The file will be located in the Program Files> Codespear> SmartMsg> Server folder and will be called "MDM_GeneratedPasswords.csv".

Then, after the import is complete, you can use the information in the comma delimited file to email usernames and passwords to the users you imported. You could also give this information to a Call Center, for when/if users have problems logging in. 0=do not create the *.csv file. 1= create the log *.csv file.

LOG_USER_CHANGES - logs changes in user profile information to the SmartMsg database Transactions table. 0=changes are not logged. 1=changes are logged.

MAX_ALERTS_PER_USER - defines a maximum number of alerts users may subscribe to. An blank entry means that there is no limit to the number of alerts users may subscribe to.

MAX_DEVICES_PER_USER - defines a maximum number of devices users may enter. An blank entry means that there is no limit to the number of devices users may enter.

MAX_EMAIL_PER_USER - defines a maximum number of email devices users may enter. An blank entry means that there is no limit to the number of email devices users may enter.

MAX_PHONE_PER_USER - defines a maximum number of phone devices users may enter. An blank entry means that there is no limit to the number of phone devices users may enter.

MAX_PHONE_RETRIES - defines a maximum number of times the system will retry a phone number after a call fails.

MAX_SMSCELL_PER_USER - defines a maximum number of SMS cell phone devices users may enter. An blank entry means that there is no limit to the number of SMS cell phone devices users may enter.

MAX_SMSPAGER_PER_USER - defines a maximum number of SMS pager devices users may enter. An blank entry means that there is no limit to the number of SMS pager devices users may enter.

MINUTES_BETWEEN_PHONE_RETRIES – failed calls are put in a queue. SmartMsg will retry to send the calls in the queue after the amount of time you specify here.

NAME_REQ - defines whether or not the first name and last name are required when a user signs up for the system. 0=a name is not required. 1=a name is required.

SEND_WELCOME_EMAIL - defines whether or not an email is sent to new users when they imported to the SmartMsg system via the Data Import Export Tool. The email properties are defined in the **Welcome Email Subject** and **Welcome Email Body** fields. 0=a welcome email is not sent. 1=a welcome email is sent.

TEST_TEMPLATE – In the web portal there is a Test Device button where users can send test alerts to their devices to verify that they have created them correctly. The alert that is sent out by clicking the Test Device button is determined by the template you enter here. You will first have to create a template in SmartMsg, and then enter it's name here.

TOKEN_LIFETIME - when a user forgets his password, a token is randomly created for them so they may log into the system. This field defines how long the token is valid for, in minutes.

USE_AGGREGATOR – determines whether or not you will be using an SMS Aggregator to send out SMS messages 1= use an Aggregator, 0= do not use an aggregator. If this is sent to 1, the Aggregator defined in the AGGREGATOR_MODULE setting will be used.

VERBOSE_LOGIN_ERRORS - defines the information given to users when their login fails. 0=the only thing users see is "invalid login". 1=specific information about why their login failed is stated to the user. (This option is less secure.)

24) When you are done configuring the Settings on this tab, click the **OK** button.

25) The next step in the process is to Import Users and Devices via the SmartMsg Data Import Export Tool. So, you can leave or minimize the SmartMsg Administrator Tool. From here, please see the additional document on *Importing Mass Dial Users and Devices*.