



miSecureMessages

MSM Administrator Guide

All rights reserved. © October 2016



American Tel-A-Systems Inc.
4800 Curtin Drive, McFarland, Wisconsin USA 53558-9424
www.amtelco.com

Confidentiality Agreement

This document and the information contained herein are proprietary to American Tel-A-Systems, Inc. It is provided and accepted in confidence only for use in the installation, training, operation, maintenance, and repair of Amtelco equipment by the original owner. It also may be used for evaluation purposes if submitted with the prospect of purchase of equipment.

This document is not transferable. No part of this document may be reproduced in whole or in part by any means, including chemical, electronic, digital, xerographic, facsimile, recording, or other method, without the expressed, written, permission of American Tel-A-Systems, Inc.

Trademarks and Copyrights

The product or products described in this document are covered and protected by one or more of the following United States patents: 4,916,726; 5,113,429; 5,259,024; 5,469,491; 6,141,413; 7,359,918; 7,593,962; and 7,831,546. Other patents, both foreign and domestic, are pending.

Amtelco and PC-MX-Infinity are federally registered trademarks of American Tel-A-Systems, Inc.

The following statement is made in lieu of using a trademark symbol with every occurrence of registered, trademarked and copyrighted names:

Registered, trademarked and copyrighted names are used in this document only in an editorial fashion, and to the benefit of the registration, trademark or copyright owner with no intention, expressed or implied, of infringement of the registration, trademark or copyright.



American Tel-A-Systems Inc.
4800 Curtin Drive, McFarland, Wisconsin USA 53558-9424

Visit Amtelco on the World Wide Web at <http://www.amtelco.com>

Index

To navigate to a topic, click the topic below.

To return to this index page, click the [Index](#) hyperlink located at the end of each section.

MSM Administrator Guide	1
Logging into MSM Administrator	2
Navigating in MSM Administrator	4
Configuration	5
Licenses	9
Connections	12
System Responses	17
Contacts	19
Contact Settings	21
Devices.....	27
Groups.....	29
Circles	36
Reports	39
Attachment Usage Report	42
Billing Report.....	43
Device List Report	44
Message Log Report	46
Events.....	48
Event Viewer	49
Notification Settings	51
Messages.....	57

[Confidentiality Agreement](#)

[Trademarks and Copyrights](#)



<https://miamtelcocloud.com>

MSM Administrator Guide

All rights reserved © October 2016

The screenshot displays the MSM Administrator Application interface. At the top, there is a navigation bar with the 'miSecure Messages' logo and the title 'Administration'. The server version is 6.4.5974.17679 and the site version is 6.4.5882.6. A 'Help' icon and 'Logout' link are also present. Below the navigation bar, there are tabs for 'Configuration', 'Licenses', 'Connections', 'System Responses', 'Contacts', 'Devices', 'Groups', 'Circles', 'Reports', 'Events', and 'Messages'. The 'Configuration' tab is active, showing two main sections: 'Database Details' and 'System Settings'.

Database Details

Database Limit	Archive Limit	Database Size	Unallocated Database Size	Maintenance Time	IS Version
Unlimited	Unlimited	681.81MB	266.57MB	1:00	Is44

System Settings

System Name
miSecureMessages

[Change Administrator Access](#)

Session Timeout
60 Seconds

Archive Mode
Local Storage

Archive Threshold
10 Days

Notification Attempts
10

Notification Interval
0 hrs 2 min 00 sec

Allow Device To Device Messaging

IS Status Update URL
https://infinity.amtelco.com/isweb/mobile/default.aspx

The MSM Administrator Application is used to administer miSecureMessages. Administrators can use the MSM Administrator Application to configure system settings, monitor licenses, configure connections, edit the list of quick responses available to users, manage contacts, view device information, set up license groups, set up Contact Circles, and run reports. This document covers all of the functions of the MSM Administrator Application.

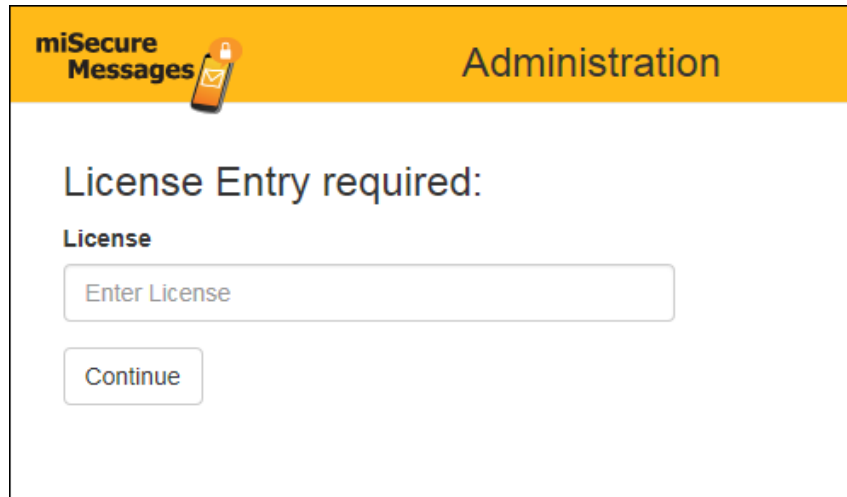
[Logging into MSM Administrator](#)

[Index](#)

Logging into MSM Administrator

The MSM Administrator Application can be accessed through a web browser or through a link in the miSecureMessages cloud application.

If you are logging in through a web browser using a shared web site, the License Entry Required page is displayed.



The screenshot shows the 'miSecure Messages Administration' interface. At the top, there is a yellow header with the 'miSecure Messages' logo on the left and the word 'Administration' on the right. Below the header, the main content area has a white background. It features the heading 'License Entry required:' in a large, dark font. Underneath this heading is the label 'License' in a smaller, bold font. Below the label is a text input field with the placeholder text 'Enter License'. At the bottom of the form is a button labeled 'Continue'.

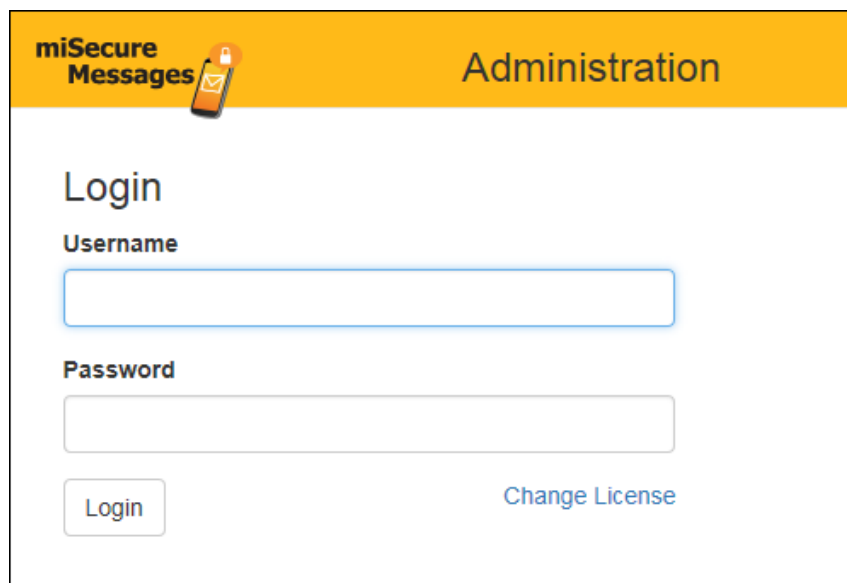
License

Your license key is provided by Amtelco.

If the License field is displayed, enter your miSecureMessages license key.

Click the Continue button.

If you are launching the MSM Administrator from a link in the miSecureMessages cloud application and have not yet changed the username and password, you are automatically logged into the MSM Administrator application. Otherwise, the MSM Administrator Login screen is displayed.



The screenshot shows the 'miSecure Messages Administration' interface. At the top, there is a yellow header with the 'miSecure Messages' logo on the left and the word 'Administration' on the right. Below the header, the main content area has a white background. It features the heading 'Login' in a large, dark font. Underneath this heading is the label 'Username' in a smaller, bold font. Below the label is a text input field. Below the input field is the label 'Password' in a smaller, bold font. Below the label is another text input field. At the bottom left of the form is a button labeled 'Login'. At the bottom right of the form is a link labeled 'Change License' in blue text.

Username

Enter your MSM Administrator username.

By default, your username is *system*. After you have logged in, you can change your username on the Configuration page.

Password

Enter your MSM Administrator Password.

By default, your Password is *password*. After you have logged in, you can change your Password using the Change Administrator Access hyperlink on the Configuration page.

System Setup Access

When the MSM Administrator Application is first installed or accessed, the **system** username allows you to log in. One of the first tasks you must perform after installing or logging into the MSM Administrator Application is to change the username and assign a confidential password to prevent subsequent unauthorized use.

Note: If you need to switch to a different license, click the Change License hyperlink to navigate to the License Entry Required screen. Enter a license key and then click the Continue button to return to the Login screen.

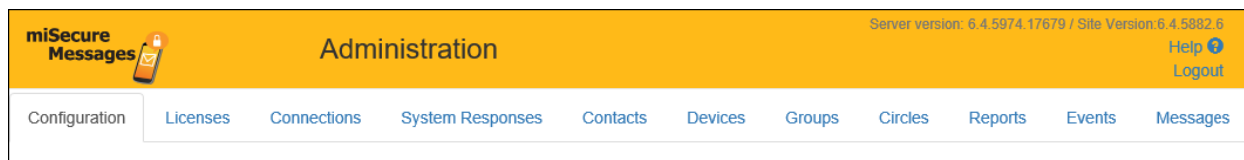
Click the Login button.

The MSM Administrator banner and tabs for each of the MSM Administrator pages are displayed.


[Navigating in MSM Administrator](#)

[Index](#)

Navigating in MSM Administrator



The hyperlinks displayed in the upper right corner of the MSM Administrator Application are used to refresh the display and to log out of the application.

- To access online help files, click the **Help** icon. 
- To log out of the MSM Administrator Application, click the **Logout** hyperlink.

The MSM Administrator Application features are accessed on a series of tabbed pages.

Click a tab to display the corresponding page of the MSM Administrator Application.

The following tabbed pages are available.

Tab	Description
Configuration	The Configuration page is used to view database information and to configure miSecureMessages system settings.
Licenses	The Licenses page is used to set the location of the MSM Web Service and displays information about your purchased licenses, group licenses, and purchase history.
Connections	The Connections page is used to establish connections between the MSM Administrator Application and the other servers and services that may be present in the system configuration.
System Responses	The System Responses page is used to customize the list of quick responses that are available to secure message recipients.
Contacts	The Contacts page is used to view, edit, and delete miSecureMessages contacts. The Contacts page also can be used to configure contacts before registration to make the registration process simpler for clients.
Devices	The Devices page is used to view a list of the devices registered for miSecureMessages.
Groups	The Groups page is used to create, edit, and delete miSecureMessages groups and to change which contacts are registered for each group.
Circles	The Circles page is used to create, edit, and delete miSecureMessages Contact Circles.
Reports	The Reports page is used to run reports on the miSecureMessages data.
Events	The Events page is used to monitor the miSecureMessages system event log and to configure e-mail notifications for specific events.
Messages	The Messages page is to view secure messages by contact and group.

[Index](#)

Configuration

Click the **Configuration** tab to access the **Configuration** page.

The Configuration page is used to view database information and to configure miSecureMessages system settings.

miSecure Messages Administration

Server version: 6.4.5974.17679 / Site Version: 6.4.5882.6

Help Logout

Configuration Licenses Connections System Responses Contacts Devices Groups Circles Reports Events Messages

Database Details

Database Limit	Archive Limit	Database Size	Unallocated Database Size	Maintenance Time	IS Version
Unlimited	Unlimited	681.81MB	266.57MB	1:00	Is44

System Settings

System Name
miSecureMessages

[Change Administrator Access](#)

Session Timeout
60 Seconds

Archive Mode
Local Storage

Archive Threshold
10 Days

Notification Attempts
10

Notification Interval
0 hrs 2 min 00 sec

Allow Device To Device Messaging

IS Status Update URL
https://infinity.amtelco.com/isweb/mobile/default.aspx

Update

Database Details

The Database Details section of the Configuration page displays information about the miSecureMessages database.

Column	Description
Database Limit	The Database Limit specifies the maximum size that the miSecureMessages database is allowed to reach. For on-site miSecureMessages installations, the Database Limit can be configured in the MSM Server Configuration application.

Configuration

Column	Description
Archive Limit	The Archive Limit specifies the maximum total allowed storage space size for all miSecureMessages archive files. For on-site miSecureMessages installations, the Archive Limit can be configured in the MSM Server Configuration application.
Database Size	The Database Size is the current size of the miSecureMessages database.
Unallocated Database Size	The Unallocated Database Size is the amount of disk space within the miSecureMessages database that is no longer in use.
Maintenance Time	The Maintenance Time is the time, in 24-hour military format, when the miSecureMessages archive task is performed each day. For on-site miSecureMessages installations, the Maintenance Time can be configured in the MSM Server Configuration application.
IS Version	The IS Version is a code representing the version of IS Server software that is in use on your system. The version is represented by the letters “is” and the first two digits of the version number.

System Settings

System settings are settings that apply to your miSecureMessages system.

System Name

The System Name is no longer used within the miSecureMessages App. It has been replaced by the group names configured on the Groups page.

You can use the System Name field to provide as a descriptive name for your system.

Type a descriptive name for your miSecureMessages system.

Change Administrator Access

To change your MSM Administrator username and password, click “Change Administrator Access.”

The Administrator Access window is displayed.

Username

The MSM Administrator username is used to log into the MSM Administrator Application.

To change your MSM Administrator username, type the username you want to use to access the MSM Administrator Application.

Password

Password is your MSM Administrator password.

To change your MSM Administrator password, enter a password that you will remember.

Re-Type Password

Type the password again.

Note: It is important to keep your MSM Administrator password a secret to prevent unauthorized access to your MSM Administrator settings.

Click the Save button to save the new MSM Administrator username and password.

or

To return to the Configuration page without saving your changes, click the Close button.

Session Timeout

This Session Timeout setting is a security setting that limits the number of seconds a miSecureMessages session can remain idle before the session key expires. This setting does not produce a visible effect for miSecureMessages users because a new session key is generated automatically the next time the user interacts with the miSecureMessages App or the Contact Web. This setting does have an effect on performance and server resources.

The Session Timeout should approximate the amount of time it takes most users to compose and send a message. Shorter Session Timeouts result in extra web service calls that affect performance; longer Session Timeouts increase the amount of server resources used to track sessions that may no longer be needed.

Type the number of seconds of inactivity to allow within a miSecureMessages session before expiring the session key.

Archive Mode

The Archive Mode determines how messages are archived.

- **Select “None” to keep all messages until they are manually deleted.**
- **Select “Purge Only” to purge messages older than the Archive Threshold without saving them to an archive file.**
- **Select “Local Storage” to archive messages older than the Archive Threshold to a local drive specified in the miSecureMessages Server Configuration.**

This option requires the purchase of the Archive feature.

- **Select “AmazonS3” to archive messages older than the Archive Threshold to the Amazon Simple Storage Service (S3).**

This option requires the purchase of the Archive feature. It may also require the purchase of additional storage space depending on your needs.

Archive Threshold

The Archive Threshold determines the minimum age of the threads that will be archived daily. The age of the thread is determined by the last time that anyone modified the thread.

Select the number of days to keep a thread before it is archived.

Notification Attempts

The Attempts setting specifies the maximum number of notifications to send for one secure message using the Persistent Alert feature. Message notifications are sent until the message is read by the recipient or the specified number of Notification Attempts has been reached. This setting can be overridden by the Max Notifications setting in the Contact Settings for each contact.

Configuration

Enter the maximum number of notifications that miSecureMessages should send when waiting for a recipient to read a secure message.

If this number is reached without receiving a read receipt from the device, the notification will not be resent but the message still will be displayed when the user checks the device.

Notification Interval

The Interval setting determines the default amount of time to wait between notifications when waiting for a secure message to be read by the recipient. This setting can be overridden by the Interval setting in the Contact Settings for each contact.

Enter the number of hours, minutes, and seconds to wait between notification attempts.

Allow Device To Device Messaging

This setting determines whether miSecureMessages users can send secure messages to each other from their mobile devices and the miSecureMessages Contact Web or if they can only receive and reply to messages sent from IS, Infinity, and the miSecureMessages cloud application.

- **Select this check box to allow miSecureMessages users to send secure messages to each other from their mobile devices and the miSecureMessages Contact Web.**
- **Clear this check box to allow miSecureMessages users to only receive and reply to messages sent from IS, Infinity and the miSecureMessages cloud application.**

In both cases, secure messages can be initiated from IS, Infinity, and the miSecureMessages cloud application.

IS Status Update URL

IS Status Update is an optional feature that allows miSecureMessages users to update their status from the miSecureMessages app. IS Status Update requires an IS Server and the IS Web Application.

If you are using IS Status Update, enter the following URL (Uniform Resource Locator):

ISWebAddress/mobile/status.aspx

Replace *ISWebAddress* with the web address of your IS Web Application.

Saving Your Configuration Settings

When you have finished entering the configuration settings, click the Update button to update the settings.

[Navigating in MSM Administrator](#)

[Index](#)

Licenses

Click the Licenses tab to access the Licenses page.

The Licenses page is used to set the location of the MSM Web Service and displays information about your purchased licenses, group licenses, and purchase history.

The screenshot shows the 'miSecure Messages Administration' interface. At the top, there's a navigation bar with tabs for Configuration, Licenses, Connections, System Responses, Contacts, Devices, Groups, Circles, Reports, Events, and Messages. The 'Licenses' tab is active. Below the navigation bar, there's a section for 'miSecureMessages Licensing Web Service Url' with a text input field containing 'https://domain/msmwebs/MSM_0022/service.asmx' and a 'Refresh Licenses' button. Below this are three tables: 'Purchased Licenses', 'Group Licenses', and 'Purchase History'.

License Type	Total	Allocated to Groups	Available	Licensed Devices	Un-Licensed Devices
Device	1000	400	185	215	0
Attachment	Unlimited	400	Unlimited	146	0

License	Account/ID	Name	Allocated	Attachment Size	Licensed Devices	Un-Licensed Devices
000.00.0000	0	General Hospital		1 MB	84	0
111.11.1111	1	Mercy Medical Center	300	10 MB	131	0
222.22.2222	2	MMC Family Dentistry	100	10 MB	0	0

License	Total	Inception	Expiration
Device	1000	2/20/2015 6:34:14 PM	2/20/2017 6:34:16 PM
Attachment	Unlimited		12/31/2016 6:00:00 PM
Archive	N/A		12/31/2016 6:00:00 PM

miSecureMessages Licensing Web Service URL

This setting indicates the Uniform Resource Locator (URL) of the Amtelco Licensing Web Service. This URL is provided by Amtelco.

If you have purchased new licenses or have renewed licenses, click the Refresh Licenses button to update the Licenses page.

The MSM Administrator Application connects to the Amtelco Licensing Web Service to retrieve the updated license information. The updated information is displayed on the Licenses page.

Purchased Licenses

The Purchased Licenses table displays information about the miSecureMessages licenses that have been purchased for your miSecureMessages account and are not expired.

Column	Description
License Type	There are two types of licenses. <ul style="list-style-type: none">• Each Device license allows one device to use the miSecureMessages App or one user to log into the Contact Web.• Each Attachment license allows one user to use miSecureMessages attachments.
Total	Total indicates the total number of licenses that have been purchased and are not expired.
Allocated to Groups	Allocated to Groups indicates the number of licenses that have been allocated to miSecureMessages groups. If this number is greater than the Total number of licenses, not all groups will be allowed to reach their maximum number of allocated licenses. The licenses are distributed on a first come first serve basis to devices and Contact Web users until the number of Available licenses is zero.
Available	Available indicates the number of licenses that are available for new devices or new users.
Licensed Devices	Licensed Devices indicates the number of devices (Android, iPhone, iPad, and iPod Touch) and Contact Web users that are registered for licenses.
Un-Licensed Devices	Un-Licensed Devices indicates the number of devices and Contact Web users that attempted to register for miSecureMessages but were unable to obtain a license because none were available.

Group Licenses

The Group Licenses table displays information about the miSecureMessages groups that have been created for your miSecureMessages account. By default, a group named “Group 0” is created for your main license key. This group can be renamed on the Groups page of the MSM Administrator Application

Groups can be used to separate miSecureMessages users into different Contact Lists. Each group is assigned a separate license key. Devices that register the miSecureMessages app using a group license will have a Contact List that only shows devices that have been registered with that same group license. Users can register a device for more than one license and can switch between them by selecting an Account Name in the miSecureMessages App.

Groups are configured on the Groups page of the MSM Administrator Application.

Column	Description
License	License indicates the license key used to register a device for the group.
Account/ID	Account/ID indicates the unique Group ID.
Name	Name indicates the name assigned to the group. The group name is displayed in the miSecureMessages Apps as the Account Name when users register using a group license key other than the main license key. When users register using the main license key, the System Name is displayed as the Account Name. Users select an Account Name to switch from one license to another.
Allocated	Allocated indicates the maximum number of devices and Contact Web users that are allowed to register for the group. This number limits the number of devices and Contact Web users that can register for the group.
Attachment Size	Attachment Size is the maximum size of each attachment. If a user attaches a file that is larger than the maximum size, the attachment will be reduced to the maximum size or the user will be prompted to select a smaller file.
Licensed Devices	License Devices indicates the number of devices (Android, iPhone, iPad, and iPod Touch) and Contact Web users that are registered for the group
Un-Licensed Devices	Un-Licensed Devices indicates the number of devices and Contact Web users that attempted to register for the group but were unable to obtain a group license because none were available.

Purchase History

The Purchase History table displays a history of the purchases made for your miSecureMessages account.

Column	Description
License	License indicates the type of licenses purchased.
Total	Total indicates the number of licenses purchased.
Inception	Inception indicates the date and time that the licenses were activated.
Expiration	Expiration indicates the date and time that the licenses will expire. Expired licenses need to be renewed in order to continue to be used.

[Navigating in MSM Administrator](#)

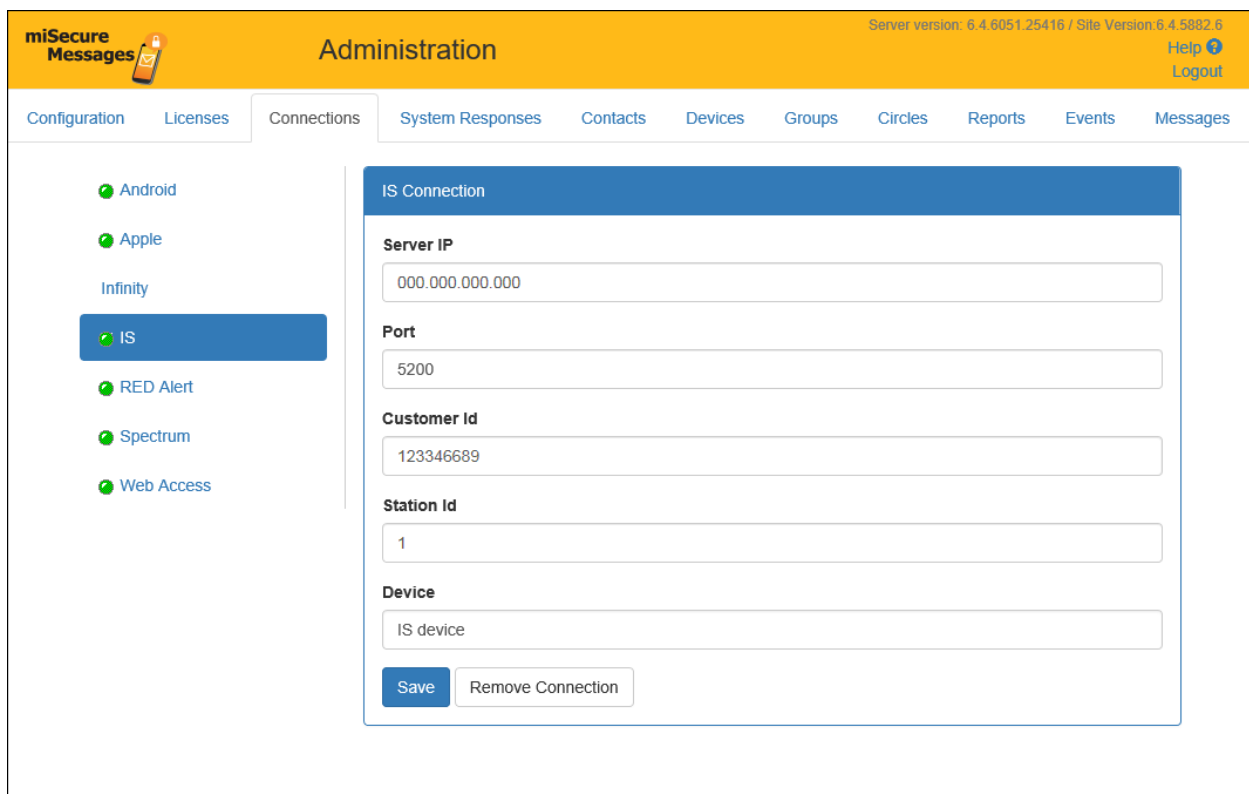
[Index](#)

Connections

Click the **Connections** tab to access the **Connections** page.

The Connections page is used to establish connections between the MSM Administrator Application and the other servers and services that may be present in the system configuration:

- Google Cloud Messaging (GCM) for Android devices
- Apple Push Notification Service
- Infinity Server
- Intelligent Series (IS) Server
- RED Alert Server
- Spectrum Server
- Web Access for miSecureMessages customers



A green icon  is displayed next to the name of each connection that has been started.

To display the settings for a connection, click the name of the connection.

The settings for the selected connection are displayed.

Android

An Android Server connection is required if secure messages will be viewed on Android devices.

URL

Enter the URL (Uniform Resource Locator) of the Google Cloud Messaging (GCM) notification service.

Click the Save button to save the new connection information and to start the connection.

A green icon  is displayed next to Android Server.


Apple

An Apple Server connection is required if secure messages will be viewed on Apple devices.

APNS Server

Enter the web address of the Apple Push Notification Service (APNS).

Click the Save button to save the new connection information and to start the connection.

A green icon  is displayed next to Apple Server.

Infinity

The miSecureMessages solution can be integrated with Amtelco's Infinity automated call distribution and unified messaging system.

Server IP

Enter the IP address of the Infinity Server.

Port

Enter 50 followed by the two-digit station number of an unused port on the Infinity Server.

For example, if 23 were an unused station number, the Port would be 5023.

Login

Enter with a unique Infinity login that has been granted access to the "Secure Messages" station type in the Infinity Supervisor Application.

This login should be a login that is not used by any operators nor any other Infinity features.

Instructions for creating a miSecureMessages login are provided in the *miSecureMessages Partnership Guide* and the *miSecureMessages On-Site System Guide*.

Password

Enter the password associated with the unique Infinity miSecureMessages login.

Route

Enter a route number that is not already in use on your Infinity system.

This route number is inserted into dial strings to route messages to the miSecureMessages Web Server. The standard route is 25.

Enter a route number that is not already in use on your Infinity system.

More information about Infinity dial strings is provided in the *miSecureMessages Partnership Guide* and the *miSecureMessages On-Site System Guide*.

Device

After the Infinity Connection is started, the Device field displays the Device Name used by the Infinity Server.

Click the Save button to save the new connection information and to start the connection.

A green icon  is displayed next to Infinity.

Connections

IS

The miSecureMessages solution can be integrated with the Intelligent Series (IS) suite of applications.

Server IP

Enter the IP address of the IS Server.

Port

Enter the port number of the IS Server.

Customer ID

Enter your unique customer ID provided by Amtelco.

Station ID

The Station ID is used to differentiate between MSM Web Service to use on systems that have more than one MSM Web Service. This Station ID is used when programming IS Directory Contact Methods to indicate which MSM Web Service to use to send messages to and from Intelligent Series applications.


If you are using more than one MSM Web Service to communicate with your IS Server, each MSM Web Service should have a different Station ID.

Do not change the Station ID unless instructed to do so by Amtelco Field Engineering.

Device

After the IS Connection is started, the Device field displays the Device Name used by the IS Server.

Click the Save button to save the new connection information and to start the connection.

A green icon  is displayed next to IS.

RED Alert

The miSecureMessages solution can be integrated with Amtelco's RED Alert rapid emergency deployment and notification application.

Server IP

Enter the IP address of the RED Alert Server.

Port

Enter the port number of the RED Alert Server.

License

Enter your RED Alert license key.

Impersonation Level

Select the Impersonation Level to use when communicating with the RED ALERT Server.

Domain

Enter the Domain on which the RED Alert Server resides.

User

If the MSM Server and the RED Alert Server are on different domains, it may be necessary to supply MSM with the username and password of a sufficiently privileged account on the machine running RED Alert or the domain on which it resides.

Enter with a user name with privileges to access RED Alert on the RED Alert Server.

Password

Enter the password associated with the user name.

Device

After the RED Alert Connection is started, the Device field displays the Device Name used by the RED Alert application.

Click the Save button to save the new connection information and to start the connection.

A green icon  is displayed next to RED Alert.

Spectrum

The miSecureMessages solution can be integrated with Telescan's Spectrum application.

Device

After the Spectrum Connection is started, the Device field displays the Device Name used by the Spectrum application.

To activate the connection to the Spectrum application, click the "Create Connection" button.

A green icon  is displayed next to Spectrum.

Web Access

The miSecureMessages solution features a Contact Web application that your customers can use to send secure messages and view secure messages through a web browser. Starting Web Access enables the Contact Web feature.

Note: Each user that logs into the Contact Web application will have a Web Device added to their contact. Each of these Web Devices consumes one miSecureMessages license out of your purchased licenses.

To activate the connection to the Contact Web application, click the "Create Connection" button.

A green icon  is displayed next to Web Access.

Removing a Connection

To delete a connection to a server or service, click the name of the connection.

The settings for the selected connection are displayed.

Click the "Remove Connection" button.

A confirmation dialog box is displayed.

If you are sure you want to delete the connection, click the OK button.

or

Click the Cancel button to keep the connection.

Connections

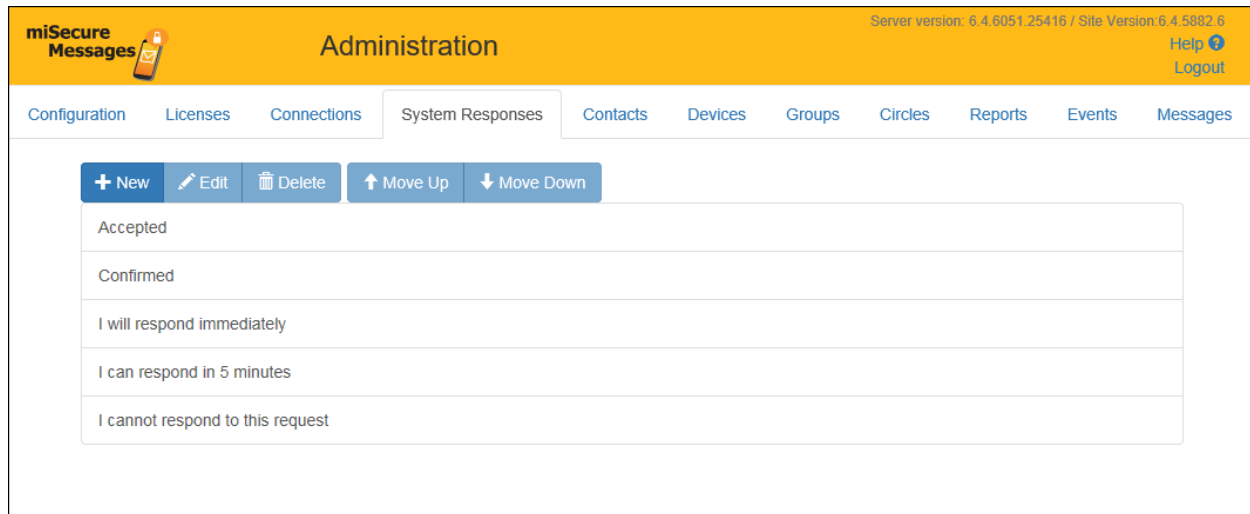
[Navigating in MSM Administrator](#)

[Index](#)

System Responses

Click the **System Responses** tab to access the **System Responses** page.

The System Response page is used to customize the list of quick responses that are available to secure message recipients. When a user views a secure message, the user can select one of these quick responses or can type a custom response.



Response Phrases Toolbar

The Response Phrases Toolbar is displayed near the top of the System Responses page. Use the Response Phrases Toolbar to make changes to the list of quick responses that are available to your miSecureMessages users when replying to a secure message.

Icon	Description
	To add a new response phrase, click the New icon.
	To edit a response phrase, click the desired phrase to select it and then click the Edit icon.
	To delete a response phrase, click the desired phrase to select it and then click the Delete icon.
	To move a phrase closer to the top of the list, click the desired phrase to select it and then click the Move Up icon.
	To move a phrase closer to the bottom of the list, click the desired phrase to select it and then click the Move Down icon.

Adding a Response Phrase

To add a response phrase, click the **New** icon.

The Response Editor window is displayed.



Response Phrase

Type the phrase that you want to add.


Click the **Save Changes** button.

System Responses

The new phrase is displayed at the bottom of the list.

To reposition the phrase, click the phrase to select it and then use the Move Up  and Move Down  icons to move the phrase to a new position in the list.


Editing a Response Phrase

To edit a response phrase, click the phrase that you want to edit and then click the Edit icon. 

The Response Editor window is displayed.

Make changes to the response phrase and then click the Save Changes button to save your changes.

Deleting a Response Phrase

To remove a response phrase, click the phrase that you want to remove and then click the Delete icon. 

A dialog box is displayed to confirm the delete request.

To cancel the delete request, click the Close button.

or

If you are sure you want to delete the phrase, click the Delete button.

The phrase is removed from the list.

[Navigating in MSM Administrator](#)

[Index](#)

Contacts

Click the **Contacts** tab to access the **Contacts** page.

The **Contacts** page is used to view, edit, and delete **miSecureMessages** contacts. The **Contacts** page also can be used to configure contacts before registration to make the registration process simpler for clients.

When users register the **miSecureMessages** app on their mobile device, their name and username are automatically saved on the **miSecureMessages** Server. This information is displayed on the **Contacts** page.

The screenshot shows the 'miSecureMessages Administration' interface. At the top, there's a navigation menu with tabs: Configuration, Licenses, Connections, System Responses, **Contacts**, Devices, Groups, Circles, Reports, Events, Messages. Below the menu, there's a 'Create User' button and a 'Refresh' icon. A 'Show' dropdown is set to '10' entries, and there's a search field. The main content is a table with the following data:

Name	User Name		
Allan Thompson	athompson	Edit	Delete
Amanda Foege	afoege	Edit	Delete
Andrea Ward	award	Edit	Delete
April Ziegler	aziegler	Edit	Delete
Brianna Sura	bsura	Edit	Delete
Christine Coburn	ccoburn	Edit	Delete
Cynthia Hilbrich	chilbrich	Edit	Delete
Daniel Anderson	danderson	Edit	Delete
David Darcy	ddarcy	Edit	Delete
DeAnn Womson	dwomson	Edit	Delete

At the bottom, it says 'Showing 1 to 10 of 1,423 entries' and has a pagination bar with 'Previous', '1', '2', '3', '4', '5', '...', '143', and 'Next'.

Column	Description
Name	Name is the contact name that is displayed in the miSecureMessages Contacts directory and on all messages that the user sends.
User Name	The username is used to identify the user to the miSecureMessages Service.

- To sort the **Contacts** table by name or username, click the appropriate column heading.
- To change the number of contacts that are displayed, click the **Show** menu and select the number of contacts to display.
- To search for a contact, click the **Search** field and type the information that you want to find.
- To view the next page of contacts, click **Next**.
- To the previous page of contacts, click **Previous**.

- To view a specific page of contacts, click the page number.
- To refresh the list of contacts, click Refresh.

Creating a New Contact

To add a new contact manually, click the **Create User** button.

A dialog box appears to warn you that creating a user on the Contact page will create a contact for that user but the user will not be able to receive secure messages until the user registers the miSecureMessages App on a device or logs into the miSecureMessages Contact Web application.

If you want to create a contact manually instead of allowing the user to create his or her own contact information, click the **Continue** button.

The [Contact Settings](#) are displayed.

Configure the contact settings for the new contact.

When you have finished, click the **Save** button.

The name and user name of the new contact is displayed in the table on the Contacts page.

Editing Contact Settings

To view or edit **Contact Settings**, click the **Edit** hyperlink to the right of the contact information.

The [Contact Settings](#) are displayed.

Make changes the contact settings as desired

When you have finished, click the **Save** button to save your changes.

Deleting a Contact

To delete a contact, click the **Delete** hyperlink to the right of that contact information.

A dialog box is displayed to verify that you want to delete the contact.

To cancel the delete request, click the **Cancel** button.

or

If you are sure you want to delete the contact, click **OK** to remove the contact from the **Contact** list.

Note: If you have an Intelligent Series (IS) Server, an IS contact is created when the connection to your IS Server is configured. If you have an Infinity Server, an Infinity contact is created when the connection to your Infinity Server is configured. These contacts are required to send messages from your IS and Infinity systems and should not be deleted.

[Contact Settings](#)

[Navigating in MSM Administrator](#)

[Index](#)

Contact Settings

The Contact Settings pane is displayed when adding or editing a contact.

Contact Settings

Name

Username

Phone Number

Reset Password
Reset Passcode
Logout User

Notification Settings

Notification Alert

Interval hrs min sec

Max Notifications

IS Settings

Username

Password

Groups

Select	Account/ID	Name	License	Visible
<input checked="" type="checkbox"/>	0	General Hospital	000.00.0000	<input checked="" type="checkbox"/>
<input checked="" type="checkbox"/>	1	Mercy Medical Center	111.11.1111	<input checked="" type="checkbox"/>
<input type="checkbox"/>	2	MMC Family Dentistry	222.22.2222	<input checked="" type="checkbox"/>

Contact Devices

Name	Type	Licensed	Inception	Sound	
Andrea's iPhone	iPhone	true	02/26/2015 10:12 AM	ringin.wav	Delete
Web app device	WebApp	true	04/29/2015 08:50 AM		Delete

Save
Close

Adding or Changing a Photo

To add a photo or change the contact's photo, click the **Edit icon**.

The Image Loader window is displayed.

Click the Browse button.

The Choose File to Upload window is displayed.

Navigate to the location of the image file.

Select the configuration file and then click the Open button.

The path to the image file is displayed in the Image Loader window.

Click the Save button to load the image.

Contacts

Reset Password

The Reset Password button is displayed when you are editing a user. The Reset Password button can be used to reset the user's password if the user has forgotten it.

To reset the user's password, click the Reset Password button.

The Reset Password window is displayed.

Type a new password in the New Password field and the Re-Enter Password field. Then click the Save button.

Reset Passcode

The Reset Passcode button is displayed when you are editing a user. The Reset Passcode button can be used to reset the user's passcode if the user has forgotten it.

To reset the user's passcode, click the Reset Passcode button.

The Reset Passcode window is displayed.

Type a new passcode in the New Passcode field and the Re-Enter Passcode field. Then click the Save button.

Lockout User

The Lockout User button is displayed when you are editing a user that is not locked out. The Lockout User button can be used to deactivate a user without losing all of the user's contact settings and device registrations. This feature is designed to remove a user from miSecureMessages while making it easier to reactivate the user in case the user returns to the company or organization.

To deactivate a user, click the Lockout User button.

The Lockout User button is replaced with an UnLock User button to indicate that the user is deactivated. An UnLock button is displayed in the Contacts table next to the name of all locked users.

UnLock User

The UnLock User button is displayed when you are editing a locked user. The UnLock User button can be used to reactivate the user.

To reactive a locked user, click the UnLock User button.

The UnLock User window is displayed. The UnLock User window is used to assign a new password to the user.

Type a new password in the New Password field and the Re-Enter Password field. Then click the Save button.

The UnLock User button is replaced with a Lockout User button to indicate that the user is activated.

Name

Name is the contact name that is displayed in the miSecureMessages Contacts directory and on all messages that the user sends. First name and last name are recommended (for example, "John Smith").

Enter the contact name that you want to display in the Contact List.

Username

The Username is used to identify the user to the miSecureMessages Service. Each contact must have a unique username (for example, “jsmith”). Usernames can be up to 50 characters long. The use of spaces in a username is not recommended. The user will need to provide the username the first time that the user logs into the miSecureMessages App. The username is also required to log into the Contact Web application.

If you want the user to be able to access the optional miSecureMessages Status and OnCall features, you must provide an IS Agent Login Name for the user in the IS Supervisor Application. This IS Agent Login Name must either match the username entered here or the username specified in the IS Settings pane.

- **If you are creating a new user, enter a unique username.**
- **If you are editing a user, the username is displayed in read-only format and cannot be edited.**

Phone Number

The Phone Number can be used to place a phone call to a contact from the miSecureMessages App.

If you want miSecureMessages users to be able to call this contact from the miSecureMessages App, enter a phone number to dial when calling this contact.

Password

The Password setting is displayed when you are creating a new user. The Password is used to verify the identity of the user. Passwords can be up to 50 characters long and should be kept a secret.

If you are creating a new user, enter a password for the user.

The user will need to provide the Password the first time that the user logs into the miSecureMessages App. The Password is also required to log into the Contact Web application.

Notification Settings

The Notification Settings can be used to customize how this Contact is notified when a secure message is received. These settings override the Notification Server Settings on the Configuration page.

Notification Alert

This setting can be cleared to disable notifications for testing purposes. In normal use, it should be enabled so that the miSecureMessages user receives secure message notifications.

Leave this check box enabled except in special cases in which it needs to be disabled for testing.

Interval

By default, Interval is set to the Interval specified on the Configuration page. The Interval determines the amount of time to wait between notifications when waiting for a secure message to be read by the recipient.

Enter the number of hours, minutes, and seconds to wait between notification attempts.

Contacts

Max Notifications

By default, Max Notifications is set to the number of Attempts specified on the Configuration page. Max Notifications specifies the maximum number of notifications to send for one secure message using the Persistent Alert feature. Message notifications are sent until the message is read by the recipient or the number of notifications indicated by the Max Notification setting have been sent.

Enter the maximum number of notifications that miSecureMessages should send when waiting for a recipient to read a secure message.

If this number is reached without receiving a read receipt from the device, the notification will not be resent but the message still will be displayed when the user checks the device.

IS Settings

The IS Settings can be used to access the optional miSecureMessages Status and OnCall features for users whose miSecureMessages username and password do not match their IS Agent Login Name and Password.

- The miSecureMessages Status feature requires an IS Server and the IS Directory Contacts feature. The Status feature allows the user to change his or her status using the miSecureMessages App.
- The miSecureMessages OnCall feature requires an IS Server and the IS Directory OnCall feature. The OnCall feature allows the user to send secure messages by selecting resources from IS Directory OnCall schedules that the user has permission to view.

Username

The Username is used to log into the IS Server when a user tries to access the optional miSecureMessages Status and OnCall features.

- **If the contact's miSecureMessages username and password match an IS Agent Login Name and Password on the IS Server, this field can be left blank.**
- **If the contact's miSecureMessages username and password do not match an IS Agent Login Name and Password, type the user's IS Agent Login Name as it is configured in the IS Supervisor Application.**

Password

The Password is used to log into the IS Server when a user tries to access the optional miSecureMessages Status and OnCall features.

- **If the contact's miSecureMessages username and password match an IS Agent Login Name and Password on the IS Server, this field can be left blank.**
- **If the contact's miSecureMessages username and password do not match an IS Agent Login Name and Password, type the user's IS Agent Password as it is configured in the IS Supervisor Application.**

Groups

If you are editing a user, the Groups table displays information about the licenses with which the selected Contact is registered. Contacts can be added to groups on the Groups page of the MSM Administrator Application.

Column	Description
<input checked="" type="checkbox"/> Select	Use the Select check box to assign the contact to groups. <ul style="list-style-type: none"> • To add the contact to a group, select the Select check box. • To remove the contact from a group, clear the Select check box.
Account/ID	The Account/ID is a unique number that identifies the group.
Name	Name indicates the name assigned to the group. The group name is displayed in the miSecureMessages Apps as the Account Name when users register using a group license key other than the main license key. When users register using the main license key, the System Name is displayed as the Account Name.
License	License indicates the license key used to register devices for the group.
<input checked="" type="checkbox"/> Visible	The Visible check box is used to hide contacts from the Contact list in the miSecureMessages Apps. Contacts are visible by default. <ul style="list-style-type: none"> • To hide a contact from the Contact list, clear the Visible check box. • To display a contact in the Contact list, select the Visible check box.

Contact Devices

If you are editing a user, the Contact Devices table displays information about the devices that have been registered for the selected Contact.

No devices are listed in the Contact Devices table until the user registers the miSecureMessages App on a device or logs into the Contact Web application. If you are creating a new user, the user will need the miSecureMessages username and password specified at the top of the Contact Settings pane in order to log into the miSecureMessages App or the Contact Web Application.

Column	Description
Name	Name indicates the name of the device as specified when the miSecureMessages App was registered. For Contact Web access, “Web app device” is displayed.
Type	Type indicates the type of device. Possible device types are Android, Infinity, iPhone, iPad, iPod, IS, and WebApp (for Contact Web access).
Licensed	Licensed is a True or False value indicating whether a valid license is assigned to the device. If “False” is listed, the license has expired and needs to be renewed.
Inception	Inception indicates the date and time that the miSecureMessages App was registered on the device, or for Contact Web access, the date and time that the user logged into the Contact Web for the first time.

Contacts

Column	Description
Sound	Sound indicates the name of the sound file selected for the miSecureMessages Notification Sound on the device. For Contact Web access, no sound file is displayed.

To delete a device, click the Delete hyperlink in the same row of the table as the device information.

When a device is deleted, the miSecureMessages app cannot be used to view or send messages on the deleted device.

When you are finished entering contact settings, click the Save button to save the settings and return to the Contacts list.

If you were creating a new user, the user's name and username are displayed in the Contacts table.

[Contacts](#)

[Navigating in MSM Administrator](#)

[Index](#)

Devices

Click the **Devices** tab to access the **Devices** page.

The **Devices** page is used to view a list of the devices registered for miSecureMessages.

miSecure Messages Administration

Server version: 6.4.6051.25416 / Site Version: 6.4.5882.6

Help Logout

Configuration Licenses Connections System Responses Contacts **Devices** Groups Circles Reports Events Messages

Show 10 entries Search: Refresh

Contact	Device	Type	Model	Version	OS	Inception	Accessed
Alan Caspar	Alan's Phone	Android	"GT-P5210 (santos10wifi)"	"4.1.1.22"	"19"	8/23/2016 10:18:29 AM	8/26/2016 1:27:46 PM
Andrea Ward	Andrea's iPad	iPad	iPad	"4.1.3"	"8.4.1"	9/15/2015 11:39:31 AM	8/17/2016 2:31:43 PM
Andrea Ward	Web app device	WebApp				8/24/2016 4:11:49 PM	9/13/2016 1:27:56 PM
Angela Massey	Angela's Phone	Android	"SCH-I545(jfftevw)"	"4.1.1.19"	"21"	9/16/2016 9:08:29 AM	9/16/2016 9:08:30 AM
David Darcy	Web app device	WebApp				8/23/2016 10:40:49 AM	8/29/2016 10:19:56 AM
David Darcy	David's iPhone	iPhone	iPhone	"4.1.1.19"	"10.0.1"	12/14/2015 2:41:12 PM	9/16/2016 9:39:01 AM
IS	IS device	IS				8/23/2016 10:17:26 AM	8/31/2016 11:55:21 AM
Michael Allen	Web app device	WebApp				9/16/2016 9:13:49 AM	9/16/2016 9:33:28 AM
Michael Allen	Michael's iOS Device	iPhone	iPhone	"4.1.1.19"	"10.0.1"	8/23/2016 9:04:08 AM	9/1/2016 10:04:07 AM
Rachel Ferguson	Web app device	WebApp				2/10/2016 1:54:17 PM	8/17/2016 11:08:12 AM

Showing 1 to 10 of 964 entries



Previous 1 2 3 4 5 ... 97 Next

The device information is displayed in a read-only table. Devices can only be removed by editing a contact on the **Contacts** page.

Column	Description
Contact	Contact indicates the display name of the contact as registered in the device's miSecureMessages App settings or programmed in the MSM Administrator Application Contact Settings.
Device	Device indicates the name of the device as specified when the miSecureMessages App was registered. For Contact Web access, "Web app device" is displayed.
Type	Type indicates the type of device. Possible device types are Android, Infinity, iPhone, iPad, iPod, IS, and WebApp (for Contact Web access).

Devices

Column	Description
Model	Model indicates the model of the device, if available.
Version	Version indicates the version number of the miSecureMessages App that is installed on the device, if available.
OS	OS indicates the operating system running on the device, if available, or the API Level for Android devices.
Inception	Inception indicates the date and time that the miSecureMessages App was registered on the device, or for Contact Web access, the date and time that the user logged into the Contact Web for the first time.
Accessed	Accessed indicates the date and time that the miSecureMessages App was last accessed on the device, or for Contact Web access, the date and time that the user most recently logged into the Contact Web.

- To sort the **Devices** table by contact name, device name, type, model, app version, operating system, license state, inception date and time, or accessed date and time, click the appropriate column heading.
- To change the number of devices that are displayed, click the **Show** menu and select the number of devices to display.
- To search for a device, click the **Search** field and type the information that you want to find.
- To view the next page of devices, click **Next**.
- To the previous page of devices, click **Previous**.
- To view a specific page of devices, click the page number.
- To refresh the list of devices, click **Refresh**.
- To view the details pane, click the **Expand** icon. 
- To hide detail pane, click the **Collapse** icon. 

[Navigating in MSM Administrator](#)

[Index](#)

Groups

Click the **Groups** tab to access the **Groups** page.

The Groups page is used to create, edit, and delete miSecureMessages groups, referred to as “Accounts” in the miSecureMessages Apps.

The screenshot displays the miSecureMessages Administration interface. At the top, there's a navigation bar with tabs for Configuration, Licenses, Connections, System Responses, Contacts, Devices, Groups, Circles, Reports, Events, and Messages. The 'Groups' tab is selected. Below the navigation bar, there's a toolbar with '+ New Group' and 'Delete' buttons. On the left, a list of groups is shown: '0 General Hospital', '1 Mercy Medical Center' (highlighted), and '2 MMC Family Dentistry'. The main area shows the details for '1 Mercy Medical Center'. Fields include: Account/ID: 1, Name: Mercy Medical Center, Licenses: 300, License: 111.11.1111, Default Circle: Staff, Registration Password: Change Password, Allow Self Registration: checked, Attachment Size: 10 MB, and Contact Web: https://miamtelccloud.com/Home/default?id=ABcdefgHij. At the bottom, there are sections for Password Settings (Retries till lockout: 3, Minimum length: 7) and Passcode Settings (Retries till lockout: 0, Minimum length: 0).



Groups can be used to separate miSecureMessages users into different Contact Lists. Each group is assigned a separate license key. Devices that register the miSecureMessages app using a group license will have a Contact List that only shows devices that have been registered with that same group license. Users can register a device for more than one license and can switch between them by selecting an Account Name in the miSecureMessages App.

The miSecureMessages groups that have been created for your account are displayed in a menu on the left side of the Groups page. By default, a group named “Group 0” is created for your main license key. This group can be renamed.

Groups Toolbar


The Groups Toolbar is displayed near the top of the Groups page. Use the Groups Toolbar to create groups and to delete groups.

Groups

Icon	Description
	To add a new group, click the New Group icon.
	To delete a group, click the desired group to select it and then click the Delete icon.

Details

The Details pane is used to configure the settings for a selected group and to configure the settings for a new group.

- **To add a group, click the New Group icon.** 
The settings on the Details pane are reset to the default values for a new group.
- **To edit a group, click the group that you want to edit.**
The Details pane displays the settings for the selected group.

Account/ID

The Account/ID is a unique number that identifies the group.

Name

Name indicates the name assigned to the group. The group name is displayed in the miSecureMessages Apps as the Account Name when users register using this group's license key. Users select an Account Name to switch from one license to another.

Enter the Account Name that you want to display for this group.

Licenses

The Licenses setting determines the maximum number of devices and Contact Web users that can register for miSecureMessages app using this group license. The number of devices and Contact Web users allowed to register for each group license cannot exceed the total licenses that you have purchased.

Enter the number of devices and Contact Web users that you want to allow to register for this group.

The licenses setting is not displayed when Group 0 is selected because Group 0 uses all available licenses by default.

License

License indicates the license key used to register devices for the group.

Default Circle

The Default Circle setting is used to change the name of the default Contact Circle that contains the names of all users that register for this group. If the Default Circle setting is left blank, the default Contact Circle is labeled "Global Contacts."

Contact Circles provide a way to organize contacts. App users can select a Circle to send messages to all members of that Circle, or can select individual contacts to send a message to those individuals.

To change the name of the default Circle from "Global Contacts" to something else, type the text that you want to display as the name of the default Circle.

Registration Password

The Registration Password is a password that ensures that only administrators who know the password can register a device. The Registration Password provides Two Factor Authentication, but requires an administrator to have physical access to each device in order to register the miSecureMessages App.

- **If you want users to be able to register their own devices without entering the Registration Password, do not set a Registration Password.**
- **To add a Registration Password, or to change the Registration Password, click Change Password.**

The Registration Password window is displayed.

Password

Type the password that you want to require for registering devices.

Re-Type Password

Type the same password.

Note: In order to provide Two Factor Authentication, the Registration Password should be kept secret from everyone except the administrators who are allowed to register devices.

Click the Save button to save your changes.

or

To discard your changes, click the Close button.

Allow Self Registration

This option allows new users to self-register the miSecureMessages app by creating their own username and password.

If this option is enabled, users can self-register the miSecureMessages app on a device by entering a miSecureMessages license key and creating their own username and password. This method requires the least amount of setup work in the MSM Administrator Application but requires the user to enter the most registration information.

- **If you want to allow users to create their own username and password, select the “Allow Self Registration” check box.**

If this option is disabled, usernames and passwords must be created in the MSM Administrator Application. Then users can register the miSecureMessages app on a device by entering a miSecureMessages license key and logging into the miSecureMessages application using the username and password that has been assigned to them. This method makes the self-registration process easier for the end user, but requires more setup work in the MSM Administrator Application.

- **If you want to allow users to log in only using previously configured usernames and passwords, clear the “Allow Self Registration” check box.**

Attachment Size

The Attachment Size setting is used to enable the Attachments feature for this group and to limit the maximum size of attachments.

Groups

Note: Attachments can only be enabled on groups that do not have more licenses than the number of Attachment licenses available.

- **To disable attachments for this group, set Attachment Size to 0 (zero).**
- **To enable attachments for this group, enter the maximum attachment size, in megabits, that you want to allow.**

If a user selects an attachment that is larger than the maximum size, the attachment will be reduced to the maximum size or the user will be prompted to select a smaller file.

Contact Web

Contact Web indicates the URL (Uniform Resource Locator) that customers can use to log into the Contact Web Application as a member of this group.

Password Settings

Passwords are used to log into miSecureMessages when registering the miSecureMessages App on a device. Passwords are also used to log into the miSecureMessages Contact Web. The Password Settings are used to set parameters for miSecureMessages passwords and allow administrators to enforce complex password requirements.

Retries till lockout

This setting controls how many times someone can attempt to log in with a valid username and an incorrect password before that username is locked. When a username is locked, it cannot be used to access miSecureMessages until it is reset in the Contact Settings for that user.

If Retries till Lockout is set to 0 (zero), usernames are never locked due to failed login attempts.

Enter the number of failed login attempts to allow before locking a username.

or

Enter 0 (zero) to prevent lockouts.

Minimum Length

This setting enforces a minimum length for passwords.

If Minimum Length is set to 0 (zero), no minimum is enforced.

Enter the minimum length required for passwords. If no minimum is required, enter 0 (zero).

Require Uppercase

Select this check box to require passwords to contain at least one uppercase letter.

Require Lowercase

Select this check box to require passwords to contain at least one lowercase letter.

Require a number

Select this check box to require passwords to contain at least one digit.

Require a special character

Select this check box to require passwords to contain at least one of the following special characters:

` ~ ! @ # \$ % ^ & * () - _ + = { [] } | \ : ; " ' < , > . ? /

Passcode Settings

The passcode is an optional security feature that requires a code to be entered each time the miSecureMessages App is opened on a device. The Passcode Settings are used to set parameters for miSecureMessages passcodes and allow administrators to enforce complex passcode requirements.

Retries till lockout

This setting controls how many times someone can enter an incorrect passcode before the username associated with the device is locked. When a username is locked, it cannot be used to access miSecureMessages until it is reset in the Contact Settings for that user.

If Retries till Lockout is set to 0 (zero), usernames are never locked due to failed passcode attempts.

Enter the number of failed passcode attempts to allow before locking a username.

or

Enter 0 (zero) to prevent lockouts.

Minimum Length

This setting enforces a minimum length for passcodes.

If Minimum Length is set to 0 (zero), no minimum is enforced.

Enter the minimum length required for passcodes. If no minimum is required, enter 0 (zero).

Require Uppercase

Select this check box to require passcodes to contain at least one uppercase letter.

Require Lowercase

Select this check box to require passcodes to contain at least one lowercase letter.

Require a number

Select this check box to require passcodes to contain at least one digit.

Require a special character

Select this check box to require passcodes to contain at least one of the following special characters:

` ~ ! @ # \$ % ^ & * () - _ + = { [] | \ : ; " ' < , > . ? /

When you have finished making changes to the Details settings, click the Update button to save your changes.

The name of the new group is displayed in the list along the left side of the Groups window.

Contacts

The Contacts pane is used to register contacts for a group and to un-register contacts from a group.

To change which contacts are registered for a group, click the group to select it.

Click the Contacts tab.

The Contacts pane is displayed.

Groups

License

License indicates the license key used to register devices for the group.

Allocated Licenses

Allocated Licenses indicates the maximum number of devices and Contact Web users that can register for miSecureMessages app using this group license. The number of devices and Contact Web users allowed to register for each group license cannot exceed the total licenses that you have purchased.

The Allocated Licenses is not displayed when Group 0 is selected because Group 0 uses all available licenses by default.

Registered Devices

Registered Devices indicates the number of devices (Android, iPhone, iPad, and iPod Touch) and Contact Web users that are registered for the group.

UnRegistered Devices

UnRegistered Devices indicates the number of devices and Contact Web users that attempted to register for the group but were unable to obtain a group license because none were available.

Available Contacts

The Available Contacts menu displays the names and device types of contacts that have been created but are not registered for the selected group.

- **To add contacts to the group, select the check boxes next to the names of the contacts that you want to add.**
- **To exclude a contact, clear the check box next to the name of the contact.**

When you have finished selecting contacts, click the Register button.

The selected contacts' names are removed from the Available Contacts menu and are displayed in the Registered to Group menu.

Registered to Group

The Registered to Group menu displays the names and device types of contacts that are registered for the selected group.

- **To remove contacts from the group, select the check boxes next to the names of the contacts that you want to remove.**
- **To keep a contact, clear the check box next to the name of the contact.**

When you have finished selecting contacts, click the UnRegister button.

The selected contacts' names are removed from the Registered to Group menu and are displayed in the Available Contacts menu.

Note: When you remove a contact from a group, that contact will have to reregister using a different miSecureMessages license key if not already registered for a different group.

Deleting a Group

To remove a group, click the group that you want to remove and then click the Delete icon. 

A dialog box is displayed to confirm the delete request.

To cancel the delete request, click the Close button.

or

If you are sure you want to delete the group, click the Delete button.

The group is removed from the list.

Note: When you delete a group, any devices that were registered for the miSecureMessages App using that group's license key will have to be reregistered using a different miSecureMessages license key if not already registered for a different license.

[Navigating in MSM Administrator](#)

[Index](#)

Circles

Click the **Circles** tab to access the **Circles** page.

The Circles page is used to create, edit, and delete miSecureMessages Contact Circles.

The screenshot displays the miSecureMessages Administration interface. At the top, the 'miSecure Messages' logo is on the left, and 'Administration' is centered. The right side shows 'Server version: 6.4.6051.25416 / Site Version: 6.4.5882.6', 'Help', and 'Logout'. A navigation bar includes 'Configuration', 'Licenses', 'Connections', 'System Responses', 'Contacts', 'Devices', 'Groups', 'Circles', 'Reports', 'Events', and 'Messages'. The 'Circles' tab is active. Below the navigation, a 'GroupID/Account:' dropdown is set to '[1]Mercy Medical Center'. To the left, a menu lists 'Cardiology', 'Emergency', 'Pediatrics', and 'Radiology', with 'Cardiology' selected. The main content area is titled 'Circle Details' and shows a 'Name' field with 'Cardiology'. Under 'Contact Registration', there are two columns: 'Available Contacts' (listing Cynthia Hilbrich, David Darcy, Rachel Ferguson, Ryan Sauter, Sean Mandt, Shere Krauss, Steven Eckert, Terri Dellamaria, and Thomas Anderson) and 'Registered Contacts' (listing Andrea Ward, Angela Massey, and Michael Allen). Buttons for 'Register', 'UnRegister', and 'Update' are visible.

Contact Circles provide a way to organize contacts. The Circles that are created in on the Circles page appear on the Contacts page of the miSecureMessages app. App users can select a Circle to send messages to all members of that Circle, or can select individual contacts to send a message to those individuals.

Group ID/Account



Contact Circles are organized within miSecureMessages groups.

Select a group from the Group ID/Account menu to display the circles settings for that group.

The Contact Circles that have been created for the selected group are displayed in a menu on the left side of the Circles page.


Circles Toolbar

The Circles Toolbar is used to create, edit, and delete Contact Circles for the group selected in the Group ID/Account menu.

Icon	Description
	To add a new Contact Circle, click the New Circle icon.
	To delete a Contact Circle, click the name of the Circle to select it and then click the Delete icon.

Circle Details

The Circle Details pane is used to configure a Contact Circle.

- **To add a Contact Circle, click the New Circle icon  and then make changes to the Circle Details settings.**
- **To edit a Contact Circle, click the Circle that you want to edit and then make changes to the Circle Details settings.**

Name

The Circle Name will be displayed on the Contacts page of the miSecureMessages App and the MSM Contact Web. App and Web users can select a Circle to send messages to all members of that Circle, or can select individual contacts to send a message to those individuals.

Type a name that indicates the purpose of this Contact Circle.

Contact Registration

Contacts added to a Circle will be displayed as members of the Circle in the Contacts page of the miSecureMessages App and the MSM Contact Web.

To add contacts to a Circle, select the name of the contact that you want to add in the Available Contacts menu.

- **You can hold down the CTRL key to select multiple contacts.**
- **You can hold down the SHIFT key to select a range of contacts.**

Click the Register button.

The selected contacts' names are displayed in the Registered Contacts menu.

To remove contacts from a Circle, select the name of the contact that you want to remove in the Registered Contacts menu.


- **You can hold down the CTRL key to select multiple contacts.**
- **You can hold down the SHIFT key to select a range of contacts.**

Click the UnRegister button.

The selected contacts' names are removed from the Registered Contacts menu.

When you are finished editing the Circle Name and adding and removing contacts, click the Update button to save your changes.

Deleting a Circle

To remove a Contact Circle, click the Circle that you want to remove and then click the Delete icon. 

A dialog box is displayed to confirm the delete request.

To cancel the delete request, click the Close button.

or

If you are sure you want to delete the Circle, click the Delete button.

The Circle is removed from the list.

[Navigating in MSM Administrator](#)

[Index](#)

Reports

Click the Reports tab to access the Reports page.

The Reports page is used to run reports on the miSecureMessages data.

The screenshot shows the 'miSecureMessages Administration' interface. At the top right, it displays 'Server version: 6.4.6051.25416 / Site Version 6.4.5882.6' and 'Help Logout' links. The navigation menu includes 'Configuration', 'Licenses', 'Connections', 'System Responses', 'Contacts', 'Devices', 'Groups', 'Circles', 'Reports', 'Events', and 'Messages'. The 'Reports' tab is active. The 'Report Selection' form contains the following elements:

- Report name:** A dropdown menu with 'MessageLog' selected.
- Start:** A date and time field set to '09/16/2016 12:00 AM'.
- End:** A date and time field set to '09/17/2016 12:00 AM'.
- Contacts:** A list of contacts with checkboxes: Alan Caspar, Andrea Ward, Angela Massey, David Darcy, IS, and Michael Allen. There are 'Select All' and 'Clear Selections' links and a search box.
- Groups:** A list of groups with checkboxes: General Hospital, Mercy Medical Center, and MMC Family Dentistry. There are 'Select All' and 'Clear Selections' links.
- Report Type:** A dropdown menu with 'Excel' selected.
- Run Report:** A blue button at the bottom left.

Report Name

Click the drop list and select the name of the report that you want to run.

Report	Description
Attachment Usage	The Attachment Usage Report displays the amount of disk space being used to store attachments for each miSecureMessages group.
Billing	The Billing Report displays counts of all secure messages sent by each contact within the date and time range specified. The counts are listed by contact name according the contact who sent the message.

Reports


Report	Description
Device List	The Device List Report displays a list of devices registered for miSecureMessages. The devices are listed by contact name.
Message Log	The Message Log Report displays information about secure messages sent and received by the contacts within the date and time range specified. The report is divided into separate pages for each contact name.

Start


The Start parameter is displayed when the Billing Report or Message Log Report is selected. The Start parameter is used to indicate the start of the date and time range to include in the report.

To change the start date and time, click the Calendar icon. 

A calendar is displayed.

- **To select a date, click the date on the calendar.**
- **To select a date from the previous month, click the left arrow.**
- **To select a date from the next month, click the right arrow.**
- **To display a calendar of months, click the month and year at the top of the calendar.**
- **To change the time, click the Clock icon.** 

The time settings are displayed.


- **Use the up and down arrows to select a time.**
- **Click AM or PM to change the time of day.**
- **To return to the calendar, click the Calendar icon.** 

End


The End parameter is displayed when the Billing Report or Message Log Report is selected. The End parameter is used to indicate the end of the date and time range to include in the report.

To change the end date and time, click the Calendar icon. 

A calendar is displayed.

- **To select a date, click the date on the calendar.**
- **To select a date from the previous month, click the left arrow.**
- **To select a date from the next month, click the right arrow.**
- **To display a calendar of months, click the month and year at the top of the calendar.**
- **To change the time, click the Clock icon.** 

The time settings are displayed.

- **Use the up and down arrows to select a time.**
- **Click AM or PM to change the time of day.**
- **To return to the calendar, click the Calendar icon.** 

Contacts

The Contacts parameter is displayed when the Billing Report, Device List Report, or Message Log Report is selected. The Contacts parameter is used to indicate which contacts' data should be included in the report.

- To add a contact, select the check box next to the name of the contact.
- To exclude a contact, clear the check box next to the name of the contact.
- To select all contacts, click "Select All."
- To clear all selections, click "Clear Selections."
- To search for a contact, click the Search field and type all or part of the contact name.

Groups

The Groups parameter is displayed when the Billing Report, Device List Report, or Message Log Report is selected. The Groups parameter is used to indicate which groups' data should be included in the report.

- To add a group, select the check box next to the name of the group.
- To exclude a group, clear the check box next to the name of the group.
- To select all groups, click "Select All."
- To clear all selections, click "Clear Selections."
- To search for a group, click the Search field and type all or part of the group name.

Report Type

Click the drop list and select the format that you want to use for the report.

When you have finished setting the parameters for the report, click the Run Report button.

The report is displayed in a new browser window.

[Attachment Usage Report](#)

[Billing Report](#)

[Device List Report](#)

[Message Log Report](#)

[Navigating in MSM Administrator](#)

[Index](#)

Attachment Usage Report

The Attachment Usage Report displays the amount of disk space being used to store attachments for each miSecureMessages group.

Attachment Usage	
Group	Size
General Hospital	121472784
Mercy Medical Center	66646522
MMC Family Dentistry	80947874

Column	Description
Group	Group indicates the name of each group that has been allocated space for storing attachments.
Size	Size indicates the amount of disk space, in bytes, that is currently being used to store attachments.

[Reports](#)

[Navigating in MSM Administrator](#)

[Index](#)

Billing Report

The Billing Report displays counts of all secure messages sent by each contact within the date and time range specified. The counts are listed by contact name according to the contact who sent the message.

Billing				
Name	Taken	Completed	Read	Deleted
Alan Thompson	50	1	50	50
Amanda Foege	64	6	64	64
Alan Caspar	82	6	82	82
Andrea Ward	51	1	51	51
April Ziegler	8	0	8	8
Briana Sura	5	0	5	5
Christine Coburn	32	2	32	32
Cynthia Hilbrich	121	2	121	121
Daniel Anderson	22	1	22	22
David Darcy	15	0	15	15
DeAnn Womson	0	0	0	0
IS	40	3	40	40
Jami Deschner	27	0	27	27
Laura Ledger	10	0	10	10
Luis Salinas	6	0	6	6
Maren Gonzalez	2	0	2	2
Michael Allen	4	0	4	4
Michael Caspar	5	0	5	5
Steven Eckert	6	2	6	6
Terri Dellamaria	1	0	1	1
Yao Ling	1	0	1	1

Column	Description
Name	Name indicates the name of each contact included in the report parameters.
Taken	Taken indicates the number of secure messages that this contact sent.
Completed	Completed indicates the number of secure messages that this contact marked "Completed."
Read	Read indicates the number of secure messages that this contact read.
Deleted	Deleted indicates the number of secure messages that this contact deleted.

[Reports](#)

[Navigating in MSM Administrator](#)

[Index](#)

Device List Report

The Device List Report displays a list of devices registered for miSecureMessages. The devices are listed by contact name.

Devices								
Contact	Username	Device	Type	Model	Version	OS	Licensed	Inception
Alan Caspar	acaspar	Alan's Phone	Android	"GT-N8013(p4note wifi)"	"4.1.1.10"	"16"	Yes	9/15/2015 11:39:31 AM
Andrea Ward	award	Andrea's iPad	iPad	iPad	"4.1.15"	"9.2"	Yes	12/14/2015 2:41:12 PM
		Web app device	WebApp				Yes	4/6/2016 9:57:40 AM
Angela Massey	amassey	Angela's Phone	Android	"SCH-I545(jfttevwz)"	"4.1.1.10"	"21"	Yes	2/10/2016 1:54:17 PM
David Darcy	ddarcy	Web app device	WebApp				Yes	2/9/2016 11:33:03 AM
		David's iPhone	iPhone	iPhone	"4.1.09.26"	"8.4"	Yes	2/9/2016 11:40:47 AM
IS	IS	IS device	IS				Yes	2/20/2015 12:56:25 PM
Michael Allen	michaelallen	Web app device	WebApp				Yes	2/23/2015 3:50:01 PM
		Michael's iOS Device	iPhone	iPhone	"4.0.9.3"	"8.4"	Yes	7/31/2015 10:34:12 AM
Rachel Ferguson	rferguson	Web app device	WebApp				Yes	2/23/2015 3:52:00 PM
Sean Mandti	smandti	Sean's Phone	Android	"PC36100(supersonic)"	"4.1.0.28"	"10"	Yes	7/28/2015 3:10:48 PM
Shere Krauss	skrauss	Web app device	WebApp				Yes	2/23/2015 3:31:35 PM
Steven Eckert	seckert	Steven's Phone	Android	"Nexus 5X(bullhead)"	"4.1.1.9"	"23"	Yes	2/23/2015 3:30:47 PM
Terri Dellamaria	tdellamaria	Terri's Phone	Android	"8742(thor_6dq)"	"4.1.1.10"	"19"	Yes	2/23/2015 3:30:01 PM
Thomas Anderson	tanderson	Thomas's iPhone	iPhone	iPhone	"4.1.02.84"	"9.3.1"	Yes	2/23/2015 3:50:39 PM

Column	Description
--------	-------------

Contact Contact indicates the display name of the contact as registered in the device's miSecureMessages App settings or programmed in the MSM Administrator Application Contact Settings. If the contact is registered for more than one device, the display name is listed once, followed by gray fields in the additional rows.

Username Username indicates the username of the contact. If the contact is registered for more than one device, the username is listed once, followed by gray fields in the additional rows.

Device Device indicates the name of the device as specified when the miSecureMessages App was registered. For Contact Web access, "Web app device" is displayed.

Type Type indicates the type of device. Possible device types are Android, Infinity, iPhone, iPad, iPod, IS, and WebApp (for Contact Web access).

Model Model indicates the model of the device, if available.

Version Version indicates the version number of the miSecureMessages App that is installed on the device, if available.

Column	Description
OS	OS indicates the operating system running on the device, if available, or the API Level for Android devices.
Licensed	Licensed is a Yes or No value that indicates whether a valid license is assigned to the device. If “No” is listed, the license has expired and needs to be renewed.
Inception	Inception indicates the date and time that the miSecureMessages App was registered on the device, or for Contact Web access, the date and time that the user logged into the Contact Web for the first time.

[Reports](#)

[Navigating in MSM Administrator](#)

[Index](#)

Message Log Report

The Message Log Report displays information about secure messages sent and received by the contacts within the date and time range specified. The report is divided into separate pages for each contact name. The contact name is displayed at the top of the page. A table displays the following columns of information about all messages sent and received by that contact.

Message Log									
Andrea Ward									
Message	From	To	Taken	Read	Completed	Delivered	Subject	Message	Attachmen
4683									
	David Darcy	Andrea Ward	9/20/2016 9:39:15 AM	9/20/2016 9:39:21 AM		9/20/2016 9:39:21 AM	Consult needed	I need your opinion regarding a change in medication for patient John Smith. I spoke with Dr. Michael Allen and he said I should contact you.	0
	Andrea Ward	David Darcy	9/20/2016 9:41:25 AM	9/20/2016 9:41:33 AM		9/20/2016 9:41:33 AM	Consult needed	I spoke with Dr. Allen about the patient and he has the information he needs to proceed.	0
4684									
	Sean Mandti	Andrea Ward	9/20/2016 9:40:28 AM	9/20/2016 9:40:41 AM		9/20/2016 9:40:41 AM	MR 234567	The lab results are ready	4749820
4685									
	Andrea Ward	Ryan Sauter	9/20/2016 9:47:56 AM	9/20/2016 9:48:09 AM	9/20/2016 9:52:36 AM	9/20/2016 9:48:09 AM	Kidney Transplant	Prep OR2 for kidney transplant.	0
	Ryan Sauter	Andrea Ward	9/20/2016 9:48:51 AM	9/20/2016 9:48:59 AM		9/20/2016 9:48:59 AM	Kidney Transplant	Prepping now. What is your ETA?	0
	Andrea Ward	Ryan Sauter	9/20/2016 9:49:05 AM	9/20/2016 9:49:07 AM	9/20/2016 9:52:36 AM	9/20/2016 9:49:07 AM	Kidney Transplant	5 minutes	0

Column	Description
Message ID	Message ID indicates the ID number of each message thread. Each message thread contains one new secure message and all of the replies to that secure message.
From	From indicates the contact name of the person who sent the message.
To	To indicates the contact name of the person to whom the message was addressed.
Taken	Taken indicates the date and time that the message was sent.
Read	Read indicates the date and time that the message was read by the recipient.
Completed	Completed indicates the date and time that the message was marked "Completed."
Delivered	Delivered indicates the date and time that the message was delivered.
Subject	Subject indicates the subject of the message.

Column	Description
Message	Message indicates the content of the message.
Attachment Size (Bytes)	Attachment Size indicates the size in bytes of any attachments sent with the message.

[Reports](#)

[Navigating in MSM Administrator](#)

[Index](#)

Events

Click the **Events** tab to access the Events page.

The Events page is used to monitor the miSecureMessages system event log and to configure e-mail addresses to be notified of specific events.

The screenshot shows the miSecureMessages Administration interface. At the top, there is a navigation bar with tabs for Configuration, Licenses, Connections, System Responses, Contacts, Devices, Groups, Circles, Reports, Events, and Messages. The 'Events' tab is selected. Below the navigation bar, there are two buttons: 'Event Viewer' (which is highlighted) and 'Notification Settings'. A date range selector is set to '08/01/2016 12:00 AM - 08/31/2016 12:00 AM'. The main content area displays a table of events:

Event Id	Date/Time	User	Event
2588	08/29/2016 04:49:20 PM	acaspar	LoginFailure
2587	08/29/2016 04:48:59 PM	acaspar	LoginFailure
2586	08/29/2016 04:48:47 PM	acaspar	LoginFailure
2585	08/26/2016 02:20:51 PM	ddarcy	LoginFailure
2584	08/26/2016 02:20:11 PM	ddarcy	LoginFailure
2583	08/26/2016 02:19:12 PM	ddarcy	LoginFailure
2582	08/26/2016 01:52:11 PM	award	LoginFailure
2581	08/26/2016 01:05:09 PM	esorenson	LoginFailure
2580	08/25/2016 12:57:47 PM	rsauter	LockedOut
2579	08/25/2016 12:57:40 PM	rsauter	LockedOut
2578	08/25/2016 12:57:35 PM	rsauter	LockedOut
2577	08/25/2016 12:56:56 PM	rsauter	PasscodeFailure
2576	08/25/2016 12:56:15 PM	rsauter	PasscodeFailure
2575	08/25/2016 12:54:54 PM	rsauter	PasscodeFailure
2574	08/25/2016 12:53:36 PM	rsauter	PasscodeFailure

The [Event Viewer](#) is displayed by default.

- To configure event notification settings, click **Notification Settings**.

The [Notification Settings](#) page is displayed.

- To return to the Event Viewer, click **Event Viewer**.

[Event Viewer](#)

[Notification Settings](#)

[Navigating in MSM Administrator](#)

[Index](#)

Event Viewer

The Event Viewer is used to monitor the miSecureMessages system events.

To display the Event Viewer, click the Events tab if it is not already selected. If the Notification Settings page is displayed, click Event Viewer.

Event Viewer		Notification Settings	
Select Date Range		08/01/2016 12:00 AM - 08/31/2016 12:00 AM	
Event Id	Date/Time	User	Event
2588	08/29/2016 04:49:20 PM	acaspar	LoginFailure
2587	08/29/2016 04:48:59 PM	acaspar	LoginFailure
2586	08/29/2016 04:48:47 PM	acaspar	LoginFailure
2585	08/26/2016 02:20:51 PM	ddarcy	LoginFailure
2584	08/26/2016 02:20:11 PM	ddarcy	LoginFailure
2583	08/26/2016 02:19:12 PM	ddarcy	LoginFailure
2582	08/26/2016 01:52:11 PM	award	LoginFailure
2581	08/26/2016 01:05:09 PM	esorenson	LoginFailure
2580	08/25/2016 12:57:47 PM	rsauter	LockedOut
2579	08/25/2016 12:57:40 PM	rsauter	LockedOut
2578	08/25/2016 12:57:35 PM	rsauter	LockedOut
2577	08/25/2016 12:56:56 PM	rsauter	PasscodeFailure
2576	08/25/2016 12:56:15 PM	rsauter	PasscodeFailure
2575	08/25/2016 12:54:54 PM	rsauter	PasscodeFailure
2574	08/25/2016 12:53:36 PM	rsauter	PasscodeFailure

The following event information is displayed:

Column	Description
Event ID	The Event ID is a unique identification number assigned to each event.
Date/Time	Date/Time is the date and time that the event occurred.
User	User is the miSecureMessages username of the user that triggered the event.
Event	The Event column indicates the kind of event that occurred.

To change the date range displayed, click the Select Date Range button.

The Date Range window is displayed.

Start

The Start parameter indicates the start of the date and time range to include in the report.

To change the start date and time, click the Calendar icon. 

A calendar is displayed.

Events

- To select a date, click the date on the calendar.
- To select a date from the previous month, click the left arrow.
- To select a date from the next month, click the right arrow.
- To display a calendar of months, click the month and year at the top of the calendar.
- To change the time, click the Clock icon. 🕒

The time settings are displayed.

- Use the up and down arrows to select a time.
- Click AM or PM to change the time of day.
- To return to the calendar, click the Calendar icon. 📅

End

The End parameter indicates the end of the date and time range to include in the report.

To change the end date and time, click the Calendar icon. 📅

A calendar is displayed.

- To select a date, click the date on the calendar.
- To select a date from the previous month, click the left arrow.
- To select a date from the next month, click the right arrow.
- To display a calendar of months, click the month and year at the top of the calendar.
- To change the time, click the Clock icon. 🕒

The time settings are displayed.

- Use the up and down arrows to select a time.
- Click AM or PM to change the time of day.
- To return to the calendar, click the Calendar icon. 📅

When you have finished selecting a date range, click the Update button.

The Events table is updated to show events within the time range specified.

[Events](#)

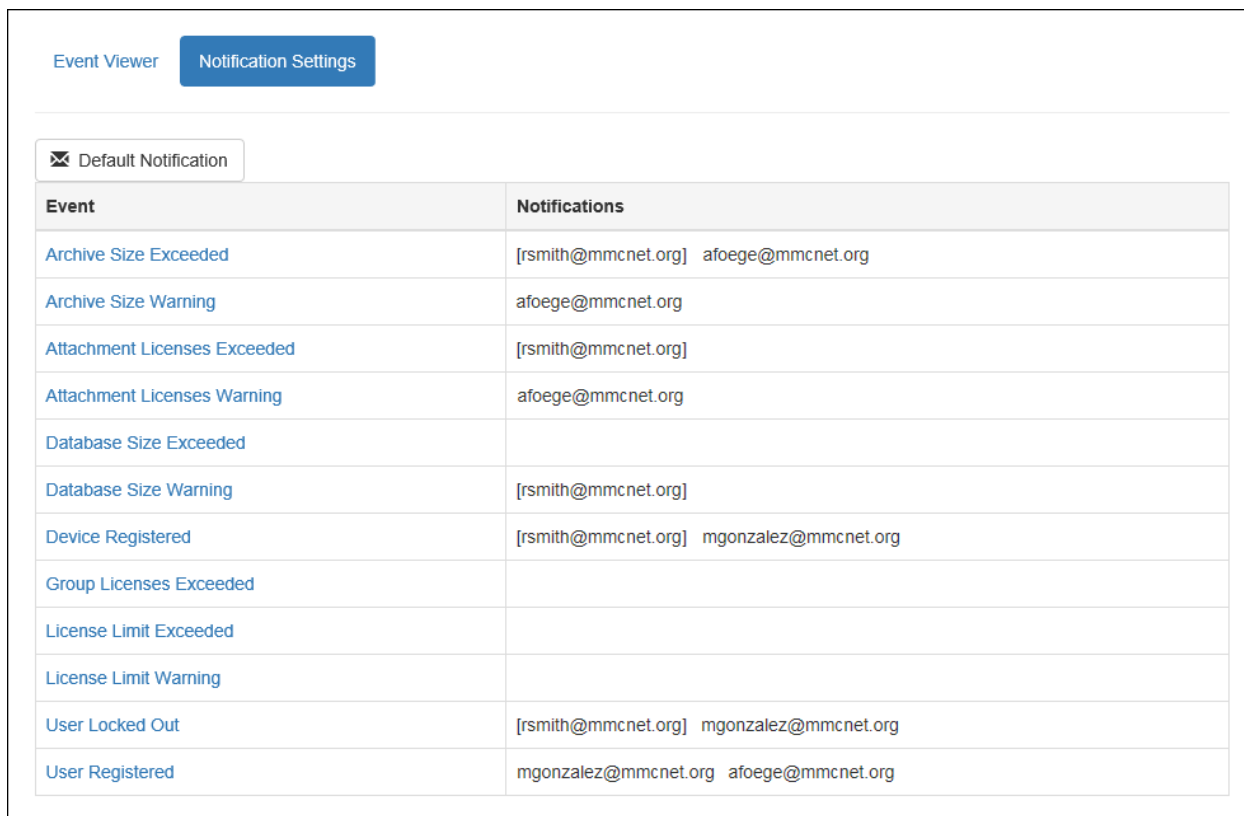
[Navigating in MSM Administrator](#)

[Index](#)

Notification Settings

The Notification Settings page is used to configure e-mail notifications for specific events.

To display the Notification Settings page, click Notification Settings on the Events page.



Event	Notifications
Archive Size Exceeded	[rsmith@mmcnet.org] afoege@mmcnet.org
Archive Size Warning	afoege@mmcnet.org
Attachment Licenses Exceeded	[rsmith@mmcnet.org]
Attachment Licenses Warning	afoege@mmcnet.org
Database Size Exceeded	
Database Size Warning	[rsmith@mmcnet.org]
Device Registered	[rsmith@mmcnet.org] mgonzalez@mmcnet.org
Group Licenses Exceeded	
License Limit Exceeded	
License Limit Warning	
User Locked Out	[rsmith@mmcnet.org] mgonzalez@mmcnet.org
User Registered	mgonzalez@mmcnet.org afoege@mmcnet.org

The Notification Settings page displays a table of events and the e-mail addresses that are configured to be notified of the events.

Column	Description
Event	The name of each event is displayed. Click the event name to configure the notification settings for that event.
Notifications	The e-mail addresses that are configured to be notified of the event are displayed. E-mail addresses configured in the Default Email Notification settings are displayed in brackets.

The following event notifications can be configured.

Event	Description
Archive Size Exceeded	Sends a notification when an action attempts to exceed the disk space allotted for archives
Archive Size Warning	Sends a notification when the archive size reaches a specified threshold
Attachment Licenses Exceeded	Sends a notification when a user registration attempts to exceed the number of attachment licenses purchased

Events

Event	Description
Attachment Licenses Warning	Sends a notification seven days before attachment licenses are due to expire
Database Size Exceeded	Sends a notification when an action attempts to exceed the disk space allocated for the miSecureMessages database
Database Size Warning	Sends a notification when the database size reaches a specified threshold
Device Registered	Sends a notification whenever miSecureMessages is registered on a device
Group Licenses Exceeded	Sends a notification when a user registration attempts to exceed the number of group licenses allocated to a group
License Limit Exceeded	Sends a notification when a user registration attempts to exceed the number of miSecureMessages licenses purchased.
License Limit Warning	Sends a notification seven days before miSecureMessages licenses are due to expire
User Locked Out	Sends a notification when a user is locked out of miSecureMessages
User Registered	Sends a notification when a user registers for miSecureMessages

Configuring the Default Notification

Before configuring notifications for individual events, you should first configure the Default Email Notification settings.

To configure the Default Email Notification settings, click the Default Notification icon. 

The Default Email Notification pane is displayed.

To

The To field is used to indicate an e-mail address to which event notifications should be sent by default.

Enter the e-mail address that should receive most event notifications.

From

The value in this field is used as the default From Address for event notifications.

Enter the e-mail address to use as the From Address for most event notifications.

Subject

The text in this field is used as the default Subject for event notifications.

Enter the text to use as the default subject for event notifications.

Server

The value in this field is used as the default mail server for event notifications.

Type the name of your mail server.

Port

The value in this field is used as the default port for event notifications. Port 25 is typically used.

Enter the IP Port number as configured on the e-mail server.

Login

The value in this field is used as the default Login for event notifications.

Enter the login name to access the e-mail account on the mail server if the mail server requires a login.

Password

The value in this field is used as the default Password for event notifications.

Enter the password associated with the login name if the mail server requires a password.

Use TLS

The value in this field determines whether Transport Layer Security (TLS) is used by default to send event notifications.

- **Select this check box to use TLS to send event notifications between MSM and the e-mail server.**
- **Clear this check box to disable TLS.**

Encrypted

The value in this field determines whether encryption is used by default to send event notifications.

- **Select this check box to enable e-mail encryption by default.**
- **Clear this check box to disable e-mail encryption by default.**

E-mail encryption requires a Public Key Certificate and an enterprise e-mail server.

When e-mail encryption is enabled, the MSM E-mail Service communicates with the enterprise e-mail server. When an event notification e-mail is generated by MSM, the MSM E-mail Service uses your Public Key Certificate to encrypt the message. The MSM E-mail Service then sends the encrypted message to the enterprise e-mail server. The enterprise e-mail server is responsible for sending the message to the recipient via the Internet or your intranet. When the e-mail message is received by the recipient, the recipient's Public Key Certificate is verified with the Certified Authority. If it is valid, the recipient can access the e-mail message.

When you have finished configuring the Default Email Notification settings, click the Save button to save your settings and return to the Notification Settings page.

or

To discard your changes, click the Exit button.

Configuring Event Notifications

To configure notifications for an event, click the name of the event.

Events

The Event Properties pane is displayed.

Event Type

The name of the event is displayed.




Use Default

If this check box is selected, notifications of this event type are sent to the e-mail address that has been configured in the Default Email Notification settings whenever the event occurs.

To use the Default Email Notification settings, select the Use Default check box.

Notification Email

Any e-mail addresses (other than the default) that have been configured to receive this type of event notifications are listed.

- **To add a new notification e-mail address, click the New icon.** 
- **To edit a notification e-mail address, click the desired e-mail address to select it and then click the Edit icon.** 
- **To delete a notification e-mail address, click the desired e-mail address to select it and then click the Delete icon.** 

When adding or editing a notification e-mail address, the Email Notification Entry pane is displayed.

To

The To field is used to indicate an e-mail address to which the event notifications should be sent.

Enter the e-mail address that should receive this type of event notification.

From

The value in this field is used as the From Address when an event notification is sent.

Enter the e-mail address to use as the From Address for this type of event notification.

Subject

The text in this field is used as the Subject when an event notification is sent.

Enter the text to use as the subject for this type of event notification.

Threshold

The Threshold setting is displayed when adding a Notification Email to the Archive Size Warning or the Database Size Warning. The warning notification is sent when the archive or database size reaches the Threshold.

Enter the threshold size, in megabytes, that will trigger the warning notification.

Server

The value in this field is used as the mail server value for event notifications.

Type the name of your mail server.

Port

The value in this field indicates the port to use for event notifications. Port 25 is typically used.

Enter the IP Port number as configured on the e-mail server.

Login

The value in this field is used as the Login for event notifications.

Enter the login name to access the e-mail account on the mail server if the mail server requires a login.

Password

The value in this field is used as the Password for event notifications.

Enter the password associated with the login name if the mail server requires a password.

Use TLS

The value in this field determines whether Transport Layer Security (TLS) is used to send event notifications.

- **Select this check box to use TLS to send event notifications between MSM and the e-mail server.**
- **Clear this check box to disable TLS.**

Encrypted

The value in this field determines whether encryption is used to send event notifications.

- **Select this check box to enable e-mail encryption.**
- **Clear this check box to disable e-mail encryption.**

E-mail encryption requires a Public Key Certificate and an enterprise e-mail server.

When e-mail encryption is enabled, the MSM E-mail Service communicates with the enterprise e-mail server. When an event notification e-mail is generated by MSM, the MSM E-mail Service uses your Public Key Certificate to encrypt the message. The MSM E-mail Service then sends the encrypted message to the enterprise e-mail server. The enterprise e-mail server is responsible for sending the message to the recipient via the Internet or your intranet. When the e-mail message is received by the recipient, the recipient's Public Key Certificate is verified with the Certified Authority. If it is valid, the recipient can access the e-mail message.

When you have finished configuring the Email Notification Entries, click the Send Test Email button to test the notification settings.

If the test was successful, an e-mail message is sent to the e-mail address specified in the To field. The body of the e-mail message contains the text "This is a test message."

Click Update button to save your settings and return to the Event Properties pane.

or

To discard your changes, click the Cancel button.

When you have finished configuring the Event Properties, click the Save button to save your settings and return to the Notification Settings page.

or

To discard your changes, click the Exit button.

The e-mail addresses that were configured to be notified of the event are displayed in the Notifications column.

Events

[Events](#)

[Navigating in MSM Administrator](#)

[Index](#)

Messages

The Messages page is used to view miSecureMessages messages that were transmitted. The messages can be viewed by contact and by group.

To display the Messages page, click the Messages tab.

The screenshot shows the miSecure Messages Administration interface. At the top, there is a navigation menu with tabs: Configuration, Licenses, Connections, System Responses, Contacts, Devices, Groups, Circles, Reports, Events, and Messages. The Messages tab is selected. Below the navigation menu, there is a 'Message Information' section with two dropdown menus: 'Contact' (set to Andrea Ward) and 'Group' (set to Mercy Medical Center). A list of messages is displayed on the left, with the message '09/20/2016 9:41:25 am Consult needed' selected. The detailed view of this message shows the following information:

09/20/2016 9:41:25 am

From: Andrea Ward
To: David Darcy
Priority: Normal
Read: Yes
Completed: No
Attachments:

I spoke with Dr. Allen about the patient and he has the information he needs to proceed.

Below the message content, there is a list of status notifications:

- 09/20/2016 9:41:25 am **Taken** Andrea Ward
- 09/20/2016 9:41:25 am **Read** Andrea Ward
- 09/20/2016 9:41:25 am **Delivered** Andrea Ward
- 09/20/2016 9:41:25 am **NewMessage[Notification]** ddarcy on device: David's iPhone [iPhone]
- 09/20/2016 9:41:33 am **Delivered** David Darcy
- 09/20/2016 9:41:33 am **Read** David Darcy
- 09/20/2016 9:41:33 am **MessageDelivery[Notification]** award on device: Andrea's iPad [iPad]
- 09/20/2016 9:41:33 am **MessageRead[Notification]** award on device: Andrea's iPad [iPad]

Below this list, there is another message header:

09/20/2016 9:39:15 am

From: David Darcy
To: Andrea Ward

Contact

The Contact menu is used to search for messages sent or received by a specific miSecureMessages user.

Select the name of the contact whose messages you want to view.

Group

The Group menu is used to search for messages transmitted using a specific miSecureMessages group.


Select the name of the group used to transmit the messages you want to view.

Messages

The date, time, and subject of the secure messages for the selected contact and group are displayed in a menu on the left side of the screen.

To display the contents and history of a message, click a message in the message list.

On the right side of the screen, the date, time, sender, receiver, priority, read status, completed status, file name and size in bytes of any attachments, message, and message history of the selected message are displayed.

To refresh the list of messages, click the Refresh icon. 

[Navigating in MSM Administrator](#)

[Index](#)



American Tel-A-Systems Inc., 4800 Curtin Drive, McFarland, Wisconsin USA 53558-9424