Amtelco Secure Messages

Admin Web User Guide

All rights reserved. © September 2025

R&D Software Department
4800 Curtin Drive, McFarland, WI USA 53558
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 may not be reproduced in whole or in part for any other purposes without the express 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; 7,831,546; 10,917.524; and 11,032,416. 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.

Index

Index

To navigate to a topic, click the topic below.

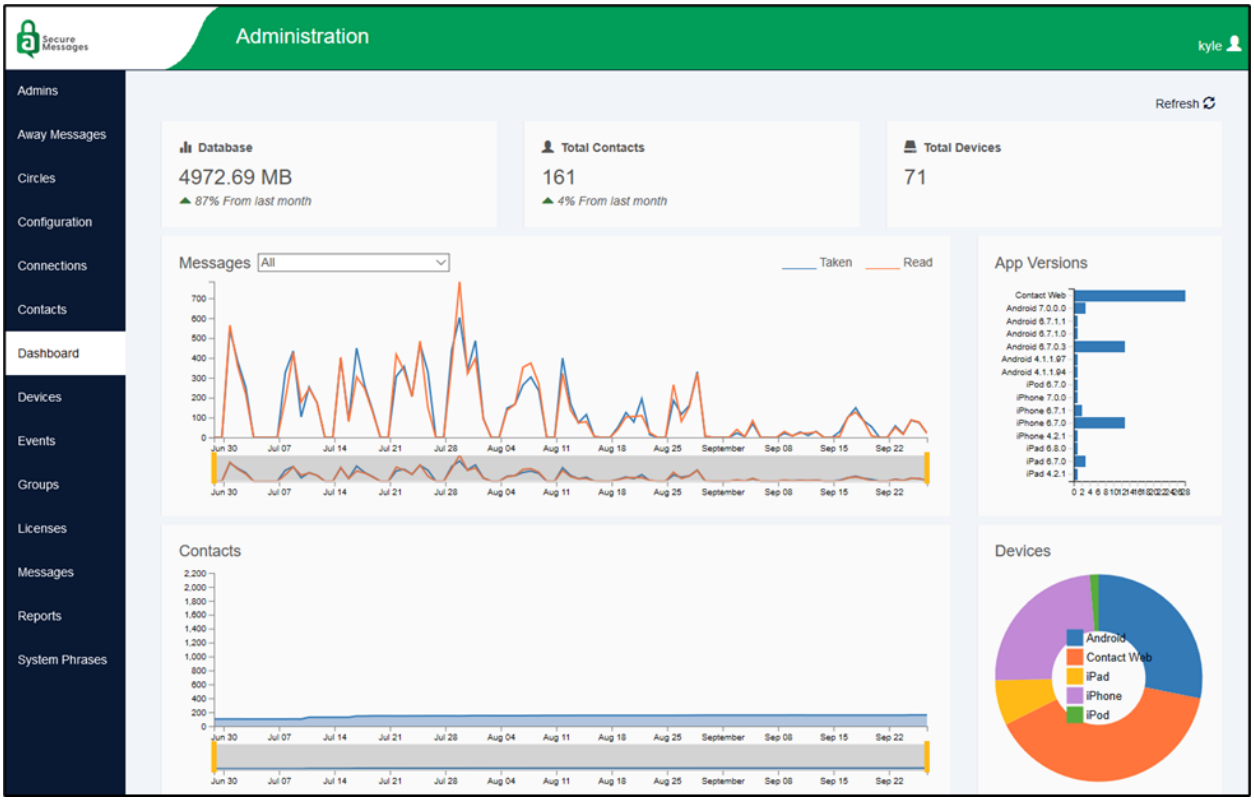
To return to this index page, click the Return to Index hyperlink located at the end of each section.

Amtelco Secure Messages Admin Web User Guide 1
Logging into Amtelco Secure Messages Admin Web 2
Navigating in Amtelco Secure Messages Admin Web 4
Admin Settings 6
Adding and Editing Amtelco Secure Messages Admin Web Administrators 8
Resetting an Administrator Password 12
System Away Messages 13
Circles 16
System Configuration 20
Database Details 21
System Settings 22
Authentication Settings 24
Admin Password Settings 25
High Availability Servers 26
eMail Registration Settings 28
Connections 31
Contacts 37
Contact Importer 40
Contact Settings 50
Contact Group Settings 62
Dashboard 66
Devices 69
System Events 73
Groups 85
General 88
Password/Passcode 97
Contacts 101
Device Menu 103
Permissions 106
Phrases 114
Roles 118
Email Messages 121
Licenses 129
Message Information 132
Reports 134
Attachment Usage Report 139
Audit Report 140
Contact List Report 142
Contacts Without Devices Report 144
Database Size Report 145
Device List Report 146

Device Versions Report 147
Event Log Report 148
Group Audit Report 149
Group Contact List Report 151
Group Device List Report 153
Group Device Versions Report 154
Group Message Counts Report 155
Group Message Details Report 156
Group Messages - Formatted Report 158
Group Messages Report 159
Message Counts Report 162
Message Details Report 163
Messages - Formatted Report 165
Messages Report 166
Notifications Report 169
Orphaned Contacts Report 170
System Phrases 171
Appendixes 174
Actions 175
Message Menus and Toolbars 194

Return to Confidentiality Agreement
Return to Trademarks and Copyrights

Amtelco Secure Messages Admin Web User Guide



The Amtelco Secure Messages Admin Web is used to administer the Amtelco Secure Messages secure mobile device messaging solution. Administrators can use the Amtelco Secure Messages Admin Web to configure system settings, monitor licenses, configure connections, edit the Quick Phrases available to users, manage contacts, view device information, set up groups, set up Contact Circles, and run reports. This document covers all of the functions of the Amtelco Secure Messages Admin Web.

[Logging into Amtelco Secure Messages Admin Web]

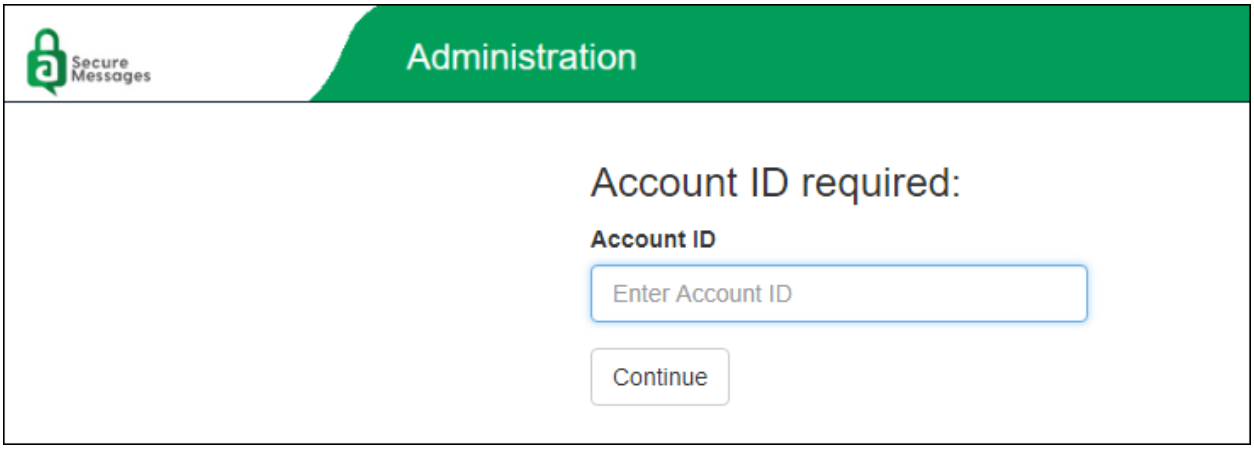
[Navigating in Amtelco Secure Messages Admin Web]

[Return to Index]

Logging into Amtelco Secure Messages Admin Web

Amtelco Secure Messages Admin Web can be accessed through a web browser.

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



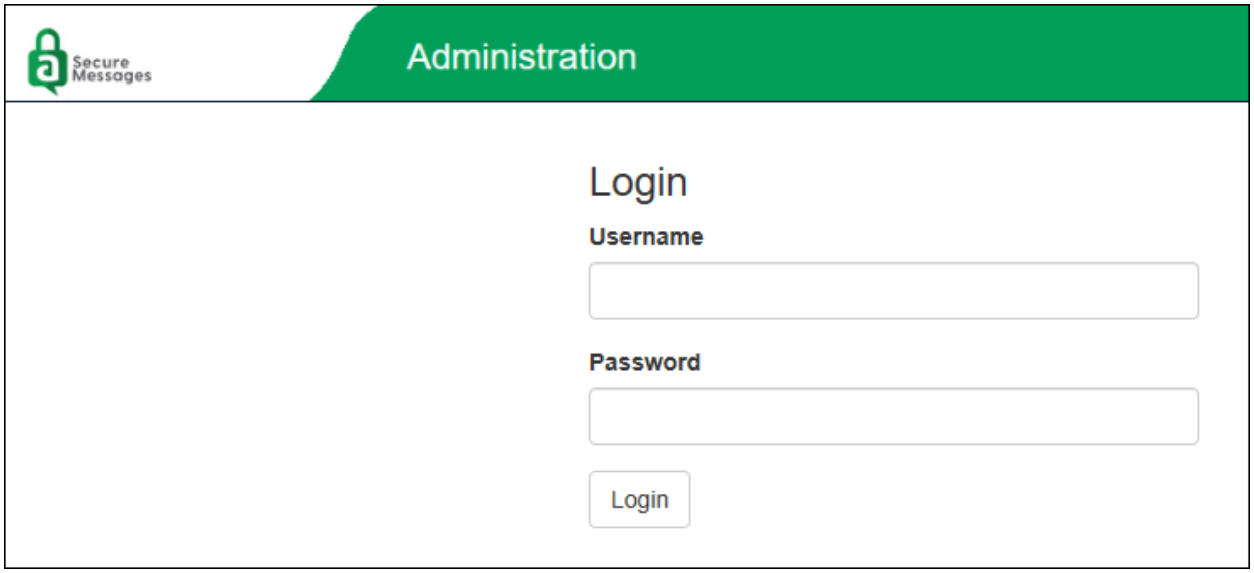
Account ID

Your Account ID is provided by Amtelco.

If the Account ID field is displayed, enter your Amtelco Secure Messages Account ID.

Click the Continue button.

The Amtelco Secure Messages Admin Web Login screen is displayed.



Username

Enter your Amtelco Secure Messages Admin Web username.

By default, your username is *system*.

Note: The *system* username cannot be changed, but additional usernames can be created by clicking the New icon ✚ on the Admin Settings page.

Password

Enter your Amtelco Secure Messages Admin Web password.

By default, your password is *password*. After you have logged in, you can change your password using the Edit command on the Admin Settings page.

System Setup Access

> When the Amtelco Secure Messages Admin Web is first installed, the *system* username allows you to log in. One of the first tasks you must perform after installing the Amtelco Secure Messages Admin Web is to change the system password to prevent subsequent unauthorized use.

Note: If you need to switch to a different account, click the Change Account hyperlink below the Password field to navigate to the Account ID Required screen. Enter an Account ID and then click the Continue button to return to the Login screen.

The Change Account hyperlink is only available if Amtelco hosts the Amtelco Secure Messages server.

Click the Login button.

The Dashboard page is displayed. The Amtelco Secure Messages Admin Web banner is displayed at the top of the page, and the Amtelco Secure Messages Admin Web Navigation Menu is displayed on the left side of the page.

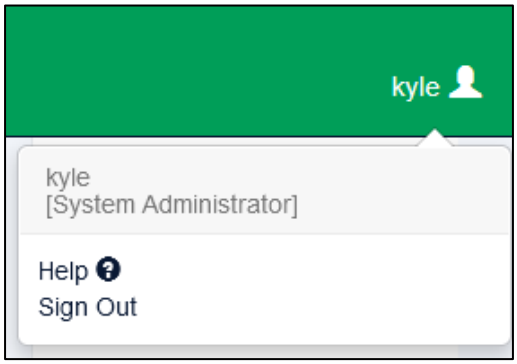
Return to Index

Navigating in Amtelco Secure Messages Admin Web

Your username is displayed in the upper right corner of the Amtelco Secure Messages Admin Web banner. The username is hyperlinked and is used to access the Help and Sign Out hyperlinks.

To access the Help and Sign Out hyperlinks, click the username hyperlink.

A pop-up window displays your username, your Amtelco Secure Messages Admin Web access type in brackets, the Help hyperlink, and the Sign Out hyperlink.

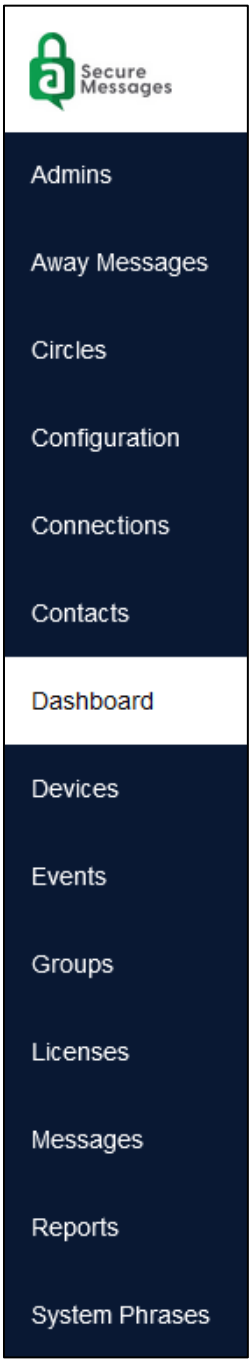


- **To access online help files, click the Help icon or the Help hyperlink.**
- **To log out of the Amtelco Secure Messages Admin Web, click the Sign Out hyperlink.**
- **To hide the pop-up window, click the username hyperlink again.**

Amtelco Secure Messages Admin Web Navigation Menu

The Amtelco Secure Messages Admin Web pages are accessed using the navigation menu displayed on the left side of the screen.

Click a command on the navigation menu to display the corresponding page of the Amtelco Secure Messages Admin Web.



- The **Admins** command opens the Admin Settings page, which is used to add, edit, and delete Amtelco Secure Messages Admin Web administrators.
- The **Away Messages** command opens the System Away Messages page, which is used to add, edit, and delete system away messages.
- The **Circles** command opens the Circles page, which is used to create, edit, and delete Amtelco Secure Messages Contact Circles.
- The **Configuration** command opens the System Configuration page, which is used to view database information and to configure Amtelco Secure Messages system settings.

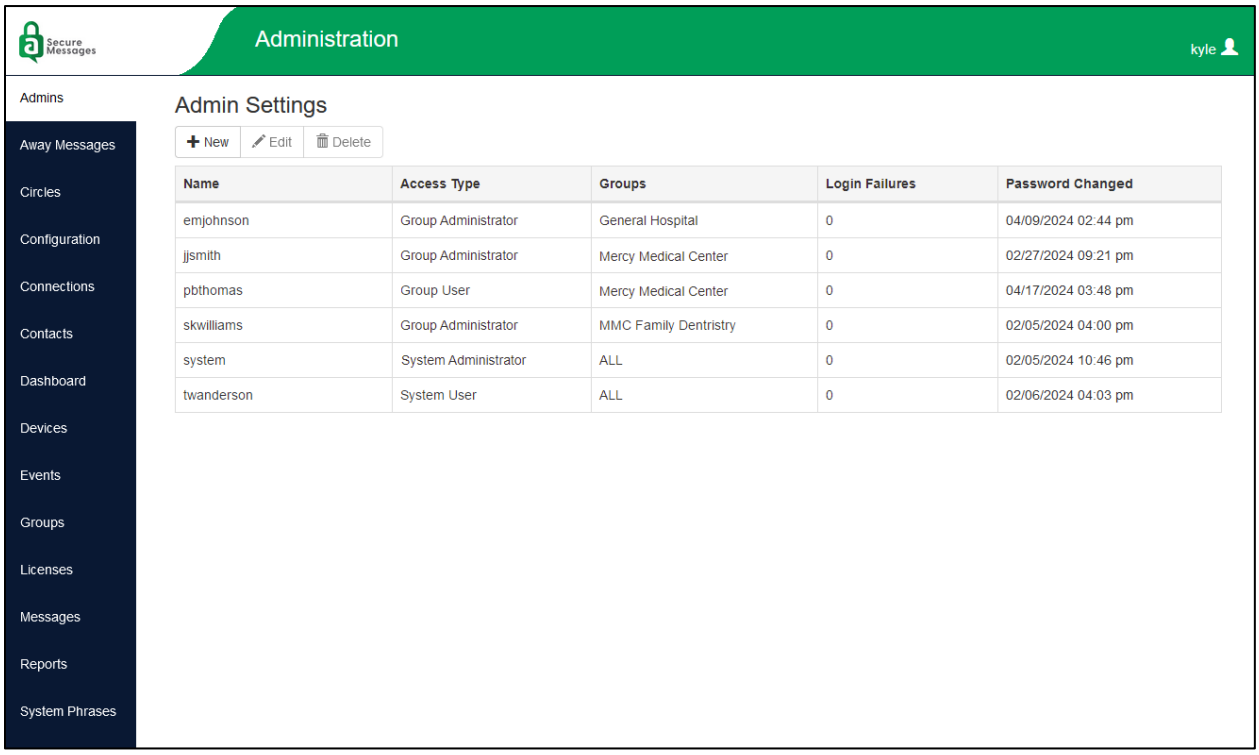
- The **Connections** command opens the Connections page, which is used to establish connections between the Amtelco Secure Messages Admin Web and the other servers and services that may be present in the system configuration.
- The **Contacts** command opens the Contacts page, which is used to view, edit, and delete Amtelco Secure Messages contacts.
- The **Dashboard** command opens the Dashboard page, which is used to monitor Amtelco Secure Messages system, contact, and device information and activity.
- The **Devices** command opens the Devices page, which is used to view a list of the devices registered for Amtelco Secure Messages.
- The **Events** command opens the System Events page, which is used to configure e-mail notifications for specific Amtelco Secure Messages system events.
- The **Groups** command opens the Groups page, which is used to create, edit, and delete Amtelco Secure Messages groups, change which contacts are registered for each group, configure permission settings for each group, and create, edit, and delete group phrases and roles.
- The **Licenses** command opens the Licenses page, which is used to set the location of the Amtelco Secure Messages Web Service and displays information about your licenses, group licenses, and purchase history.
- The **Messages** command opens the Message Information page, which is used to view secure messages that were transmitted.
- The **Reports** command opens the Reports page, which is used to run reports on the Amtelco Secure Messages data.
- The **System Phrases** command opens the System Phrases page, which is used to customize system Quick Phrases.

Return to Index

Admin Settings

The Admin Settings page is used to add, edit, and delete Amtelco Secure Messages Admin Web administrators. Amtelco Secure Messages Admin Web administrators are users that are able to log in to the Amtelco Secure Messages Admin Web and view or edit various Amtelco Secure Messages settings based upon the administrator's access type.

Click the Admins command on the navigation menu to access the Admin Settings page.



The Admin Settings page displays a table of all existing Amtelco Secure Messages Admin Web administrators in alphabetical order by username.

Column	Description
Name	The Name column displays the username of each Amtelco Secure Messages Admin Web administrator. If the username is locked, the words "Locked Out" are displayed in red text to the right of the username. If a username is locked, contact the person authorized to use that username and find out if that person had trouble logging in or forgot the password. A locked username could be an indication that an unauthorized person was trying to access the system using someone else's username. If you verify that the correct person was having trouble logging in, you can reset the user's password by following the instructions provided under the topic Resetting an Administrator Password.
Access Type	The Access Type column displays the type of permissions granted to the Amtelco Secure Messages Admin Web administrator.

Column	Description
Groups	The Groups column displays the names of the groups to which the Amtelco Secure Messages Admin Web administrator has access. Amtelco Secure Messages Admin Web administrators that have been granted System User or System Administration permissions have access to all groups, so the word “ALL” is displayed in the Groups column for these administrators.
Login Failures	The Login Failures column displays the number of times the username was used in a failed login attempt. If the number of failed login attempts reaches the Retries Till Lockout value programmed in the Administration Settings pane of the System Configuration screen, the account is locked out. The number of login failures is reset to 0 (zero) when the username is used to log in successfully or the user’s password is reset.
Password Changed	The date and time that the user’s password was most recently changed.

Admin Toolbar

The Admin Toolbar is displayed near the top of the Admin Settings page. The Admin Toolbar is used to add and delete Amtelco Secure Messages Admin Web accounts, and to edit individual Amtelco Secure Messages Admin Web administrator settings such as password, access type, and group membership.

Icon	Description
✚	Click the **New** icon to add a new Amtelco Secure Messages Admin Web administrator.
✎	Click the **Edit** icon to edit settings or reset the password for the selected Amtelco Secure Messages Admin Web administrator.
🗑	Click the **Delete** icon to delete the selected Amtelco Secure Messages Admin Web administrator.

Adding and Editing Amtelco Secure Messages Admin Web Administrators
Resetting an Administrator Password
Return to Navigating in Amtelco Secure Messages Admin Web
Return to Logging into Amtelco Secure Messages Admin Web
Return to Index

Adding and Editing Amtelco Secure Messages Admin Web Administrators

- **To add a new Amtelco Secure Messages Admin Web administrator, click the New icon.** ➕

  The Admin Settings window is displayed.

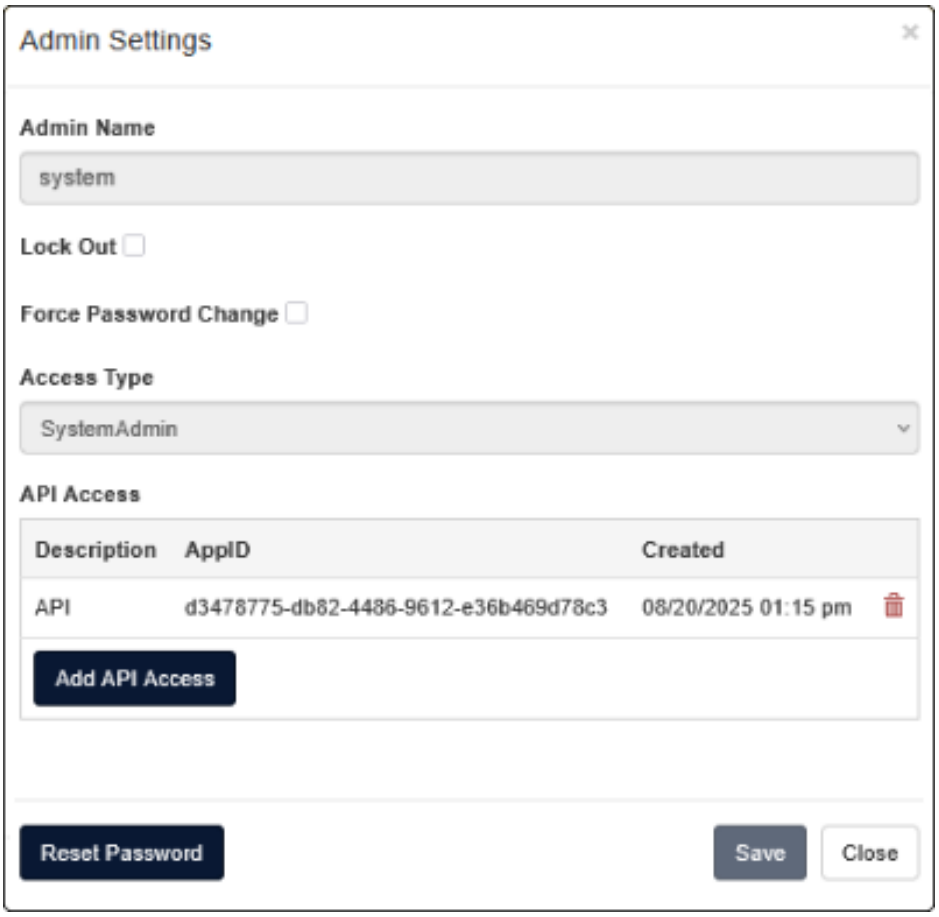
- **To edit settings for an existing Amtelco Secure Messages Admin Web administrator, select the administrator and then click the Edit icon.** ✎

  The Admin Settings window displays the settings for the selected administrator.

Note: Creating an Amtelco Secure Messages Admin Web account only gives an administrator access to the Amtelco Secure Messages Admin Web, and not to the Amtelco Secure Messages Apple, Android, or Contact Web applications. If an Amtelco Secure Messages Admin Web administrator wishes to access and send messages using one of these applications, a separate Amtelco Secure Messages user account must be created for the administrator on the Contacts page.

Admin Settings Window

The Admin Settings window is displayed when adding or editing an administrator. The fields and buttons displayed in the Admin Settings window vary depending on whether the New icon ➕ or the Edit icon ✎ was clicked.



Admin Name

The Admin Name field contains the Amtelco Secure Messages Admin Web account username. The administrator uses this username to log in to the Amtelco Secure Messages Admin Web.

Type a username for the administrator.

Password

The Password field is displayed when adding an administrator. The Password field specifies the password the administrator will use to log into the Amtelco Secure Messages Admin Web application.

Type a password for the administrator.

Re-Type Password

The Re-Type Password field is displayed when adding an administrator. The Re-Type Password field is used to verify the password entered in the Password field.

Type the same password.

☑ Lock Out

The "Lock Out" setting is used to lock an administrator out of the Amtelco Secure Messages Admin Web without deleting the username.

Select this check box to lock this username and prevent it from being used to log into the Amtelco Secure Messages Admin Web.

☑ Force Password Change

The "Force Password Change" setting is used to require a user to change his or her password the next time the user logs into the Amtelco Secure Messages Admin Web.

Select this check box to require this user to change his or her password the next time the user logs into the Amtelco Secure Messages Admin Web.

Access Type

Access Type is the type of permissions granted to the administrator.

Access Type	Description
GroupAdmin	The Group Admin access type enables an Amtelco Secure Messages Admin Web administrator to view and edit the settings for the groups to which they have been granted access. The settings that each Group Admin is able to edit will vary depending upon the Group Administrator Permissions set for each group.
GroupUser	The Group User access type enables an Amtelco Secure Messages Admin Web administrator to view the settings for the groups to which they have been granted access. The settings that each Group User is able to view will vary depending upon the Group User Permissions set for each group.

Access Type	Description
SystemAdmin	The System Admin access type is the highest level of access type and enables an Amtelco Secure Messages Admin Web administrator to view and edit all pages and settings available in the Amtelco Secure Messages Admin Web. System Admins can view and edit settings for all groups and Contact Circles, add and edit Amtelco Secure Messages Admin Web administrators and Amtelco Secure Messages contacts, add and remove connections, edit system configuration settings, add and edit system phrases, configure notification properties, run reports, and more.
SystemUser	The System User access type enables an Amtelco Secure Messages Admin Web administrator to view all pages of the Amtelco Secure Messages Admin Web except the Admin Settings page and the Contact Importer page. A System User is also able to run reports if the Allow System User Report Access setting is enabled on the System Configuration page.

Click the Access Type menu and select the appropriate access type for this administrator.

Groups

The Groups field is displayed when Access Type is set to "GroupAdmin" or "GroupUser." The Groups field contains a list of all available groups.

- **Select the check box to the left of each group to which you want to grant this Group Admin or Group User access.**

  If the group you are looking for is not listed, you can create a new group on the Groups page of the Amtelco Secure Messages Admin Web.

- **To select all groups, click the Select All hyperlink.**
- **To deselect all groups, click the Select None hyperlink.**

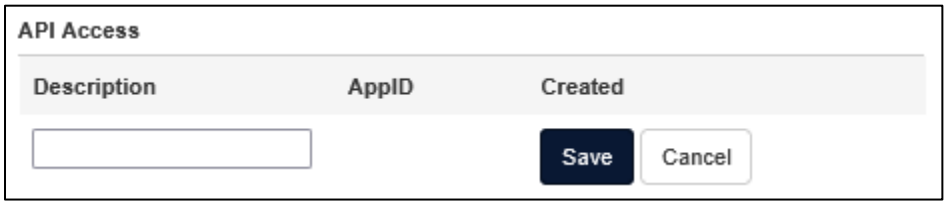
To Save the Admin Settings for the user, click the Save button.
OR
To discard your changes and close the Admin Settings window, click the Close button.

API Access

The API Access section is displayed when editing an administrator. The API Access section is used to generate an App ID and Secret to enable this administrator to access an application programming interface (API).

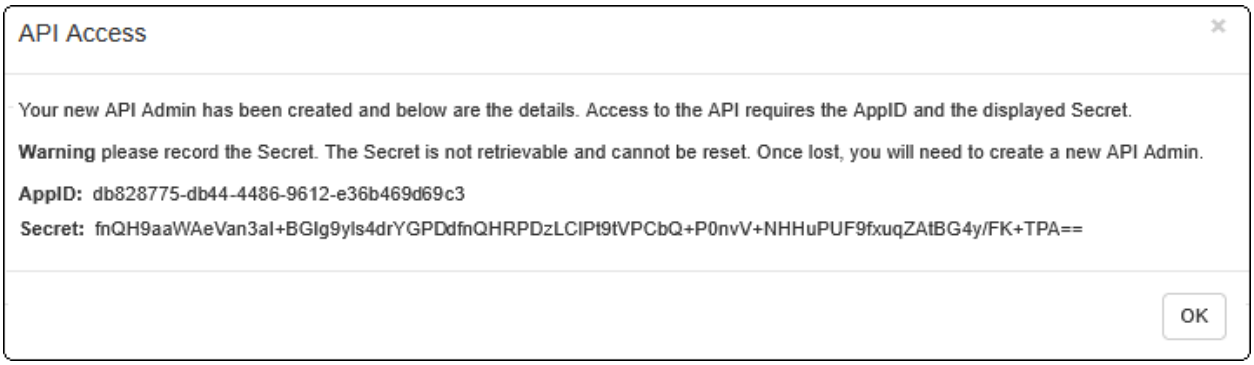
- **To generate an App ID to enable access to an API for the administrator, click the Add API Access button.**

  The Description field is displayed.



Enter a description for this API, then click the Save button.

A dialog box is displayed that shows the App ID and Secret. The Secret is not retrievable and cannot be reset, so be sure to record it.

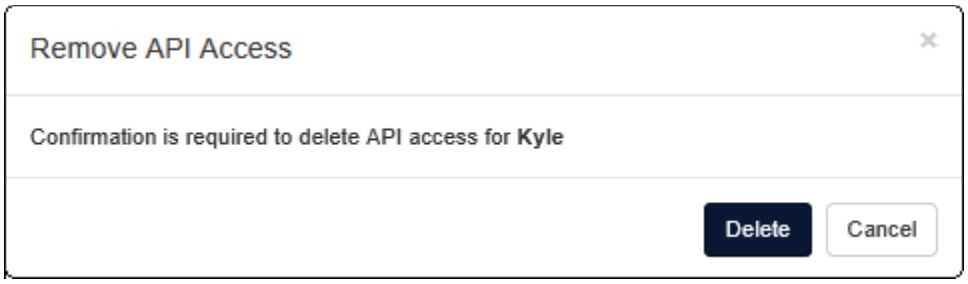


Click the OK button.

The API is displayed in the list.

- **To delete an App ID to remove access to an API for this administrator, click the Delete icon.**

  A confirmation dialog box is displayed.



To cancel the delete request, click the Cancel button.

OR

If you are sure you want to remove API access, click the Delete button.

If you clicked the Delete button, the App ID is removed from the list.

Return to Admin Settings
Return to Index

Resetting an Administrator Password

If an administrator forgets his or her password or is locked out of the Amtelco Secure Messages Admin Web, you can reset the administrator's password.

To reset an administrator's password, select the administrator in the Admin Settings table and then click the Edit icon.

The Admin Settings window is displayed.

Reset Password

The Reset Password button is displayed in the Admin Settings window when you are editing an administrator.

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

The Change Password window is displayed.

Password

Type a new password for the administrator.

Re-Type Password

Type the same password.

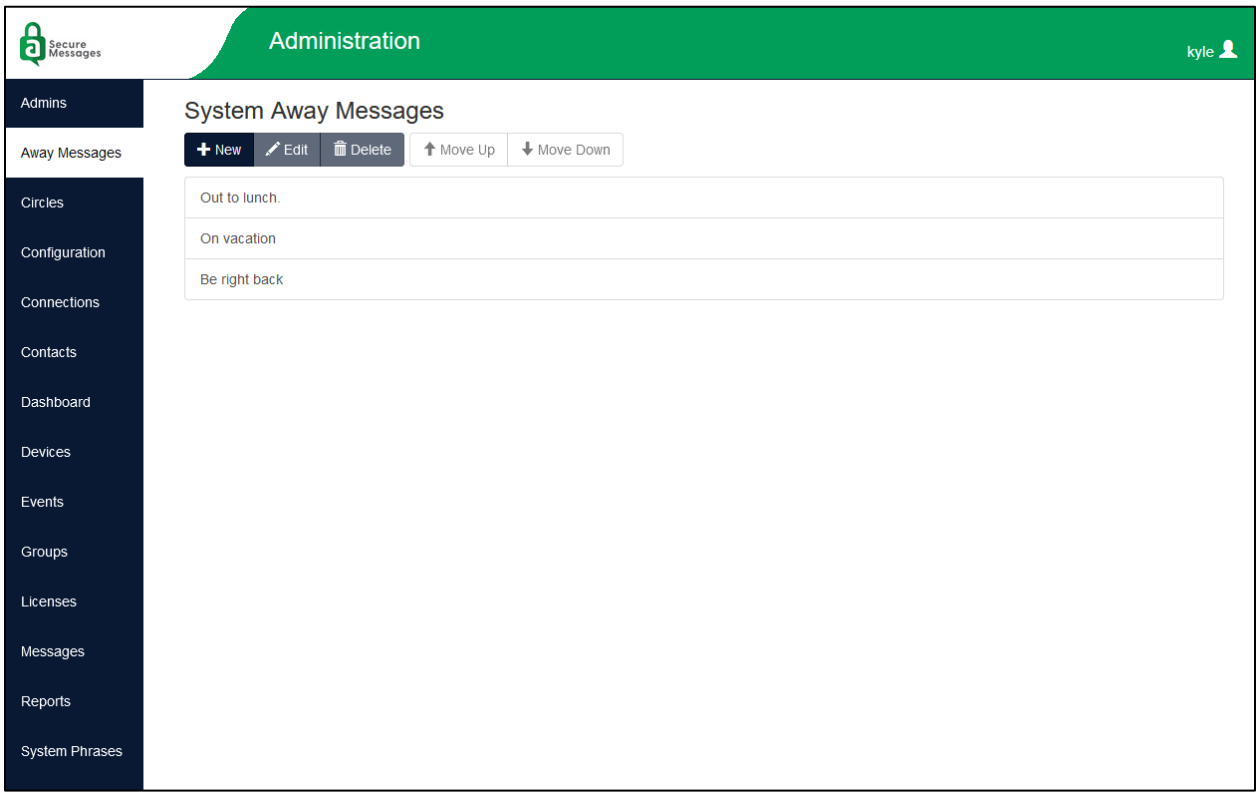
Click the Save button to save your changes.

Return to Admin Settings
Return to Index

System Away Messages

The System Away Messages page is used to customize the system away messages that are available to any group that is enabled for system away messages. When an Amtelco Secure Messages user turns off Amtelco Secure Messages notifications, the user can select one of these away messages, select one of the group away messages, or type a custom away message.

Click the Away Messages command on the navigation menu to access the System Away Messages page.



Away Messages Toolbar

The Away Messages Toolbar is displayed near the top of the System Away Messages page. The Away Messages Toolbar is used to make changes to the system away messages that are available to Amtelco Secure Messages users when turning off Amtelco Secure Messages notifications.

Icon	Description
	Click the **New** icon to add a new system away message.
	Click the **Edit** icon to edit the selected system away message.
	Click the **Delete** icon to delete the selected system away message.
	Click the **Move Up** icon to move the selected system away message closer to the top of the list.

Icon	Description
	Click the **Move Down** icon to move the selected system away message closer to the bottom of the list.

Adding and Editing Away Messages

- **To add a system away message, click the New icon.**

  The Away Message window is displayed with a blank text field.

- **To edit a system away message, click the away message that you want to edit and then click the Edit icon.**

  The Away Message window displays the selected away message in a text field.

Message

Type the away message that you want to add, or edit the existing away message.

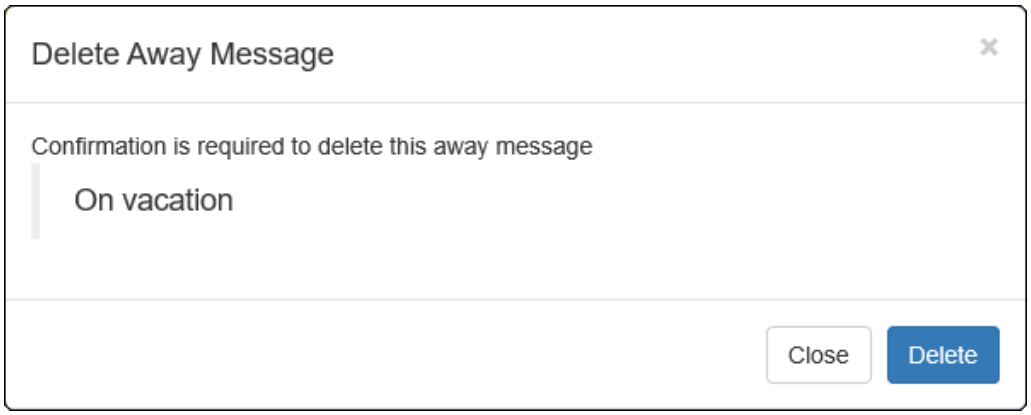
Click the Save Changes button.

The new or edited message is displayed in the list.

Deleting an Away Message

To remove a system away message, click the message 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 message, click the Delete button.

If you clicked the Delete button, the message is removed from the list.

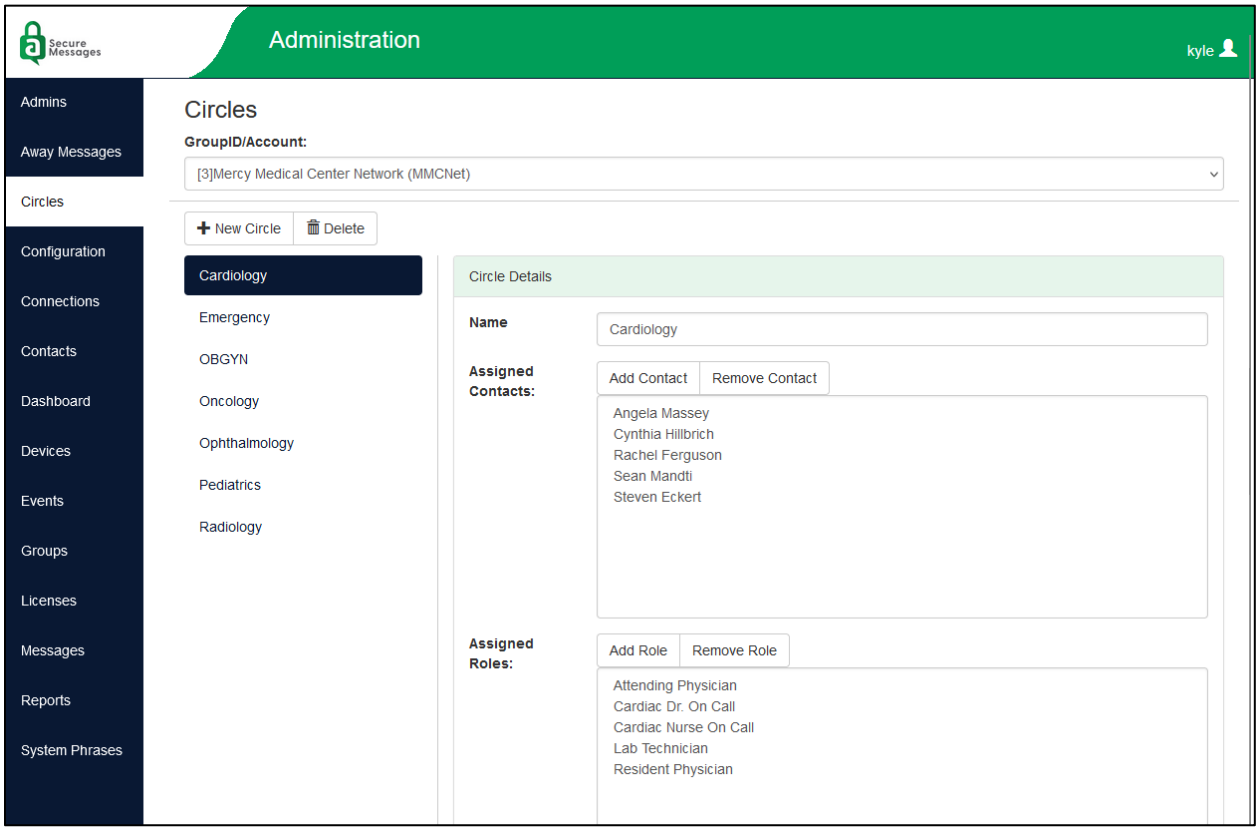
Return to Navigating in Amtelco Secure Messages Admin Web

Return to Index

Circles

The Circles page is used to create, edit, and delete Amtelco Secure Messages Contact Circles.

Click the Circles command on the navigation menu to access the Circles page.



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

Note: Adding roles to Contact Circles and sending messages to roles requires the optional Role-Based Messaging feature.

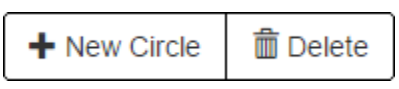
Group ID/Account

Contact Circles are organized within Amtelco Secure Messages groups.

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

A list of all the Contact Circles that have been created for the selected group is displayed 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
➕	Click the **New Circle** icon to add a new Contact Circle.
🗑	Click the **Delete** icon to delete the selected Contact Circle.

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 Amtelco Secure Messages app and the Amtelco Secure Messages 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.

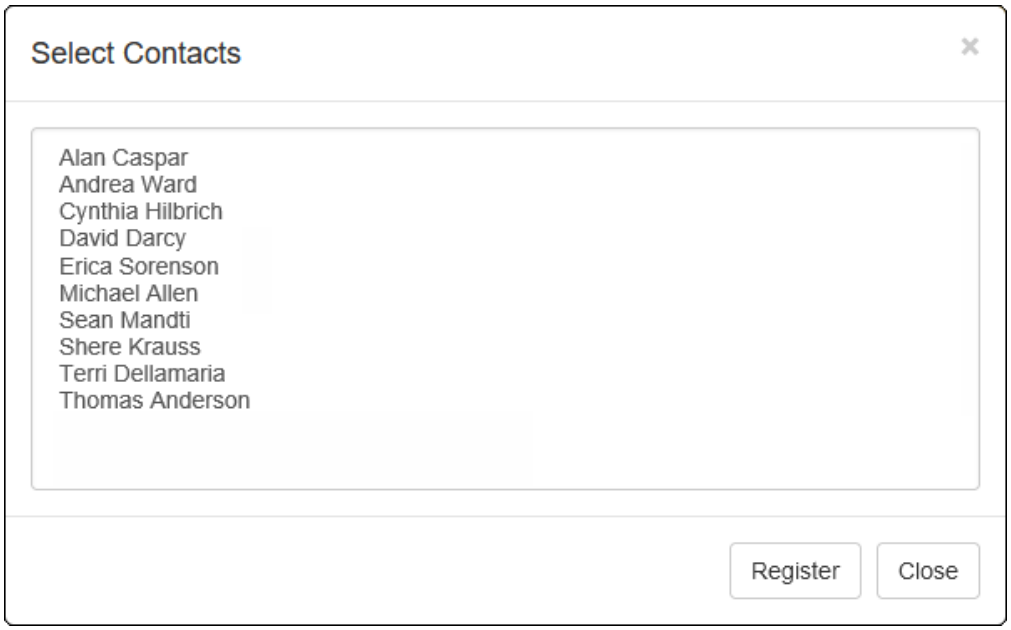
Type a name that indicates the purpose of this Contact Circle.

Assigned Contacts

Contacts added to a Circle will be displayed as members of the Circle in the Contacts page of the Amtelco Secure Messages app and the Amtelco Secure Messages Contact Web.

To add contacts to a Circle, click the Add Contact button.

The Select Contacts window is displayed.



Select the name of the contact that you want to add in the Select Contacts window.

- **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 Assigned Contacts menu.

To remove contacts from a Circle, select the name of the contact that you want to remove in the Assigned 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 Remove Contact button.

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

Assigned Roles

The Assigned Roles section is used with the optional Role-Based Messaging feature. When a role is added to a Circle, messages sent to the Circle will be sent to the people who are on-call for the role.

To add roles to a Circle, click the Add Role button.

The Select Roles window is displayed.

Select the name of the role that you want to add in the Select Roles window.

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

Click the Continue button.

The selected roles are displayed in the Assigned Roles menu.

To remove roles from a Circle, select the name of the role that you want to remove in the Assigned Roles menu.

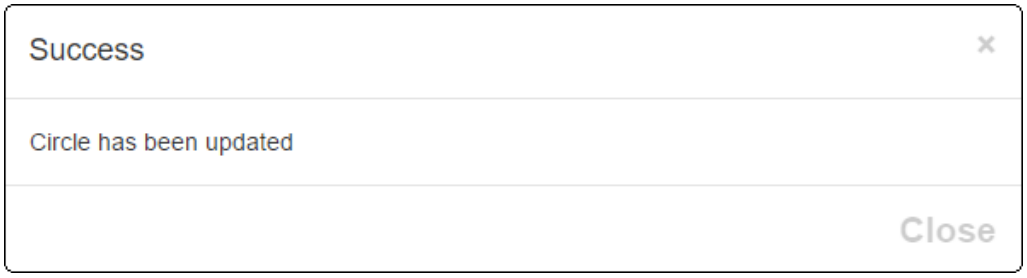
- **You can hold down the CTRL key to select multiple roles.**
- **You can hold down the SHIFT key to select a range of roles.**

Click the Remove Role button.

The selected roles are removed from the Assigned Roles menu.

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

A dialog box is displayed to confirm the changes were saved successfully.



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.

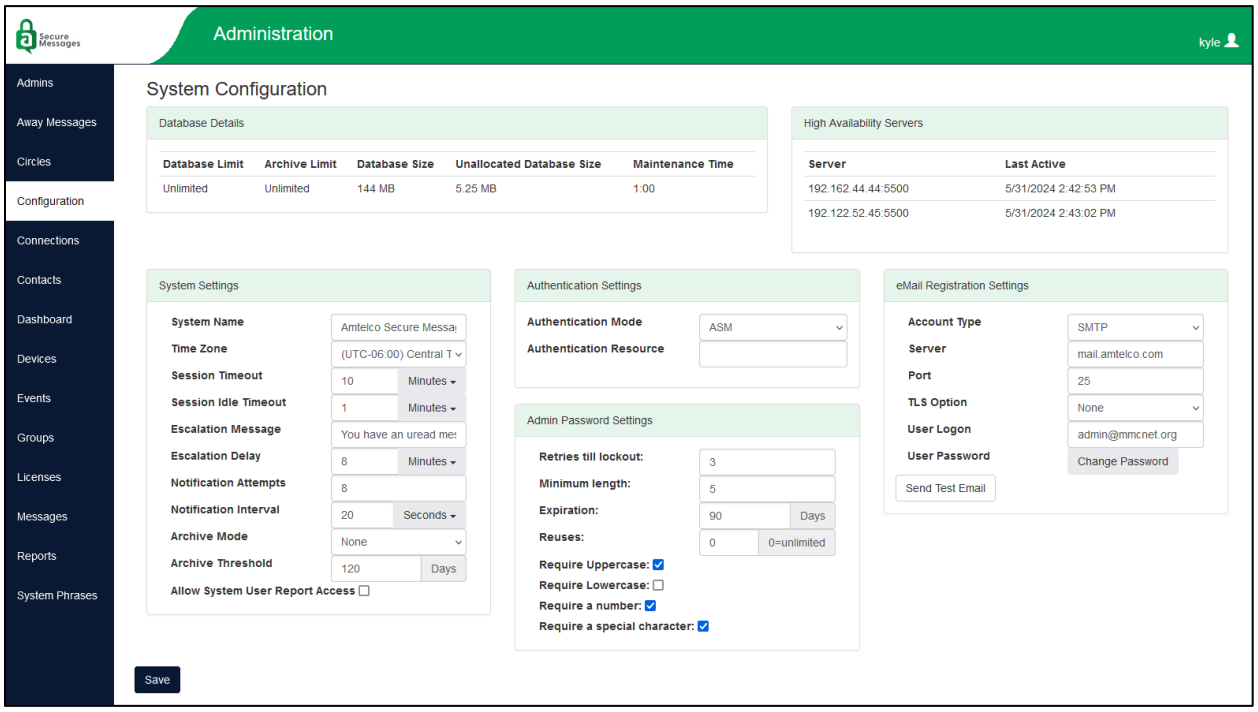
If you clicked the Delete button, the Circle is removed from the list.

Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

System Configuration

The System Configuration page is used to view database information and to configure Amtelco Secure Messages system settings.

Click the Configuration command on the navigation menu to access the System Configuration page.



Database Details
System Settings
Authentication Settings
Admin Password Settings
High Availability Servers
eMail Registration Settings
Return to Adding and Editing Amtelco Secure Messages Admin Web Administrators
Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

Database Details

The Database Details section of the System Configuration page displays information about the Amtelco Secure Messages database.

Column	Description
Database Limit	The Database Limit specifies the maximum size that the Amtelco Secure Messages database is allowed to reach. For on-site Amtelco Secure Messages installations, the Database Limit can be configured in the Amtelco Secure Messages Server Configuration application.
Archive Limit	The Archive Limit specifies the maximum total allowed storage space size for all Amtelco Secure Messages archive files. For on-site Amtelco Secure Messages installations, the Archive Limit can be configured in the Amtelco Secure Messages Server Configuration application.
Database Size	The Database Size is the current size of the Amtelco Secure Messages database.
Unallocated Database Size	The Unallocated Database Size is the amount of disk space within the Amtelco Secure Messages database that is no longer in use.
Maintenance Time	The Maintenance Time is the time, in 24-hour military format, when the Amtelco Secure Messages archive task is performed each day. For on-site Amtelco Secure Messages installations, the Maintenance Time can be configured in the Amtelco Secure Messages Server Configuration application.

Return to System Configuration
Return to Index

System Settings

System Settings are settings that apply to your Amtelco Secure Messages system.

System Name

The System Name is no longer used within the Amtelco Secure Messages 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 Amtelco Secure Messages system.

TimeZone

The Time Zone setting is used to specify the time zone of your Amtelco Secure Messages system. All reports for this Amtelco Secure Messages system will be run in this time zone.

Click the Time Zone field and select a time zone from the menu.

Session Timeout

The Session Timeout setting is a security setting that limits the amount of time an Amtelco Secure Messages session can continue (either active or idle) before the session key expires. This setting does not produce a visible effect for Amtelco Secure Messages users because a new session key is generated automatically. This setting does have an effect on performance and server resources.

Enter the number of hours, minutes, or seconds to allow an Amtelco Secure Messages session to continue before expiring the session key, and then select the appropriate unit of measurement from the menu.

Session Idle Timeout

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

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

Enter the number of hours, minutes, or seconds of inactivity to allow within an Amtelco Secure Messages session before expiring the session key, and then select the appropriate unit of measurement from the menu.

Escalation Message

The Escalation Message is a text message that is sent to the contact phone number of an Amtelco Secure Messages contact if that contact is sent a secure message and does not read it within the time specified by the Escalation Delay setting. The message should inform the contact that there is an unread secure message. This setting specifies the default Escalation Message for newly created groups.

Note: This feature only functions for contacts that have a phone number specified in Contact Settings.

Enter a message to text to contacts who do not read a secure message before the Escalation Delay elapses.

Escalation Delay

The Escalation Delay setting is the amount of time to wait for a contact to read a secure message before texting the Escalation Message to the contact's phone number. This setting specifies the default Escalation Delay for newly created groups.

Enter the number of hours, minutes, or seconds to wait for a contact to read a secure message before texting the Escalation Message, and then select the appropriate unit of measurement from the menu.

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 Notification Attempts setting under the General tab in Group Properties and in the Contact Settings for each contact.

Enter the maximum number of notifications that Amtelco Secure Messages 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 Notification Interval setting under the General tab in Group Properties and in the Contact Settings for each contact.

Enter the number of hours, minutes, or seconds to wait between notification attempts, and then select the appropriate unit of measurement from the menu.

Archive Mode

The Archive Mode determines how messages are archived.

- **Select "None" to keep all messages until they are manually deleted.**

  The None option does not archive any message threads.

- **Select "Purge Only" to purge messages older than the Archive Threshold without saving them to an archive file.**

  The Purge Only option does not archive any message threads and automatically deletes threads older than the Archive Threshold.

- **Select "Local Storage" to archive messages older than the Archive Threshold to a local drive specified in the Amtelco Secure Messages Server Configuration.**

  The Local Storage option is only available for on-site Amtelco Secure Messages installations. When selecting the Local Storage option, make sure that your Amtelco

Secure Messages Server Configuration specifies a Thread Archive Path to a secure location that is protected by appropriate access restrictions to prevent unauthorized access to message content and attachments.

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).**

  The Amazon S3 option is available on both hosted Amtelco Secure Messages subscriptions and on-site Amtelco Secure Messages installations and requires a customer-provided Amazon S3 account. When selecting the Amazon S3 option, make sure that your Amazon S3 account is configured with the appropriate access restrictions to prevent unauthorized access to message content and attachments.

  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.

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

☑ Allow System User Report Access

The "Allow System User Report Access" setting allows Amtelco Secure Messages Admin Web administrators with System User access type to access the Reports page and run reports.

- **Select this check box to enable System Users to access the Reports page and run reports.**
- **Clear this check box to make the Reports page unavailable to System Users.**

Authentication Settings

The Authentication Settings are settings that determine how administrators are able to log into the Amtelco Secure Messages Admin Web.

Authentication Mode

Amtelco Secure Messages Admin Web administrator login names can be configured for one of two authentication modes: ASM (Amtelco Secure Messages) and SSO (Single Sign-On). SSO authentication requires a certificate from an SSO Identity Provider and the installation and configuration of the Amtelco Secure Messages Assertion Consumer Web. This feature has been tested with the following SSO Identity Providers: Active Directory Federation Services (ADFS) and Azure Active Directory (AD).

Note: The SSO option requires a certificate from a Single Sign-On Identity Provider.

- **Select "ASM" to use the Amtelco Secure Messages server to keep track of passwords and perform authentication.**
- **Select "SSO" to use a Single Sign-On Identity Provider to keep track of passwords and perform authentication.**

Authentication Resource

The Authentication Resource setting is used to specify the Uniform Resource Locator (URL) of your Single Sign-On Provider when the Authentication Mode is set to "SSO."

If you are using SSO authentication, enter the URL specified by your Single Sign-On Identity Provider.

Admin Password Settings

The Admin Password Settings are used to set parameters for administrator passwords used to login into the Amtelco Secure Messages Admin Web.

Retries till lockout

This setting controls how many times someone can attempt to log into the Amtelco Secure Messages Admin Web with a valid administrator name and an incorrect password before that administrator name is locked. When an administrator name is locked, it cannot be used to access Amtelco Secure Messages until the password is reset in the Admin Settings for that administrator.

If Retries till lockout is set to zero (0), administrator names are never locked due to failed login attempts.

Enter a number of failed login attempts to allow before locking an administrator name.
OR
Enter zero (0) to prevent lockouts.

Minimum length

This setting enforces a minimum length for passwords.

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

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

Expiration

Expiration indicates the number of days an administrator's password can be in effect before it expires. Expired passwords need to be changed in order to continue using Amtelco Secure Messages.

Enter the number of days that passwords are valid before expiring.

Reuses

The Reuses setting determines the number of unique passwords that must be set for an administrator before the administrator can reuse an old password.

Enter the number of unique passwords that must be set before an administrator can reuse an old password.
OR
Enter zero (0) to always allow administrators to reuse old passwords.

☑ Require Uppercase

The "Require Uppercase" option requires passwords to contain at least one upper case letter.

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

☑ Require Lowercase

The "Require Lowercase" option requires passwords to contain at least one lower case letter.

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

☑ Require a number

The "Require a number" option requires passwords to contain at least one digit.

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

☑ Require a special character

The "Require a special character" option requires passwords to contain at least one of the following special characters:

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

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

Saving Your Configuration Settings

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

Return to System Configuration
Return to Index

High Availability Servers

The optional High Availability feature allows the Amtelco Secure Messages solution to be configured for multiple servers, with automated failover from one server to another when the primary server goes down. One step in configuring Amtelco Secure Messages for High Availability is adding servers to the Servers key in the Amtelco Secure Messages Admin Web's web.config file. The High Availability Servers pane displays information about the servers added to the Servers key in the Amtelco Secure Messages Admin Web's web.config file.

Note: Having servers listed in the High Availability Servers pane does not guarantee that your system is configured for automated failover. Contact Amtelco for more information about configuring your Amtelco Secure Messages system for High Availability.

Column	Description
Server	The Server column displays the IP address and port number of each server listed in the Servers key of the web.config file. The IP address and port number are separated by a colon (:).
Last Active	The Last Active column displays the date and time that Amtelco Secure Messages last received confirmation that the server was active. The Last Activate information is updated every minute. The Server Inactive event is triggered when the Last Active date and time for an Amtelco Secure Messages server is more than 10 minutes old, provided there is another Amtelco Secure Messages server still active to send the event notification.

Return to System Configuration

Return to Index

eMail Registration Settings

The eMail Registration Settings are settings that apply to the Amtelco Secure Messages Email Registration feature. These settings are also used for password reset e-mail messages.

Account Type

The Account Type setting is used to specify the type of e-mail protocol that is used for Email Registration. The following e-mail protocols may be used: Simple Mail Transfer Protocol (SMTP), Google Workspace, and Microsoft (MS) Graph Send.

Select the desired e-mail protocol to be used for Email Registration.

The settings for the selected Account Type are displayed.

SMTP Settings

When SMTP is selected as the Account Type, the following settings are displayed.

Server
The value in the Server field is used as the mail server for registration and password reset e-mail messages.

Type the name of your mail server.

Port
The value in the Port field indicates the port to use for registration and password reset e-mail messages. Port 25 is typically used.

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

TLS Option
The TLS Option setting is used to configure Transport Layer Security (TLS) or Secure Sockets Layer (SSL) protocol for sending registration and password reset e-mail messages.

- **Select "None" to disable the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) encryption.**

  If "None" is selected, the connection is not encrypted.

- **Select "Auto" to have the e-mail service decide if SSL or TLS protocol is used or no encryption is used.**

  If "Auto" is selected and the server does not support SSL or TLS, the connection continues without any encryption.

- **Select "SslOnConnect" to use the SSL or TLS encryption.**

  The "SslOnConnect" option uses SSL or TLS encryption. If the server does not support SSL or TLS, the connection fails.

- **Select "StartTls" to use TLS encryption only.**

  The "StartTls" option uses the STARTTLS extension to take an existing, insecure connection between the e-mail client and the e-mail server and turn it into a secure connection. This is done after the STARTTLS extension reads the greeting and the capabilities of the server. If the server does not support STARTTLS, the connection fails and a "NotSupportedException" error is thrown.

- **Select "StartTlsWhenAvailable" to use TLS encryption if available but otherwise use no encryption.**

  The "StartTlsWhenAvailable" option uses the STARTTLS extension to take an insecure connection between the e-mail client and the e-mail server and turn it into a secure connection. This is done after the STARTTLS extension reads the greeting and the capabilities of the server. If the server does not support STARTTLS, the connection continues but is not encrypted.

User Logon
The value in the User Logon field is used as the login for connecting to the mail server.

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

User Password
The value in the User Password field is used as the password for connecting to the mail server.

Click the Change Password button.

The User Password field is displayed.

Enter the password associated with the login name if the mail server requires a password, then click the Close icon ✖ to hide the field.

Google Workspace Settings

When Google Workspace is selected as the Account Type, the following settings are displayed.

Service Account
The Service Account field determines the e-mail address of a Google Workspace service account.

Enter the e-mail address found on the Details page of your Google Workspace service account.

Cert Thumbprint
The Cert Thumbprint setting is used to specify the Google Workspace service account key.

Enter a key found on the Keys page of your Google Workspace service account.

User Name
The User Name field is used to specify the principal.

Enter the Principal found on the Principals tab on the Permissions page of your Google Workspace service account.

MS Graph Send Settings

When MS Graph Send is selected as the Account Type, the following settings are displayed.

Client ID
The Client ID setting is used to specify the Application (client) ID of your Microsoft account.

Enter the Application (client) ID found on the App Registrations, App Properties screen of your Microsoft account.

Tenant ID
The Tenant ID setting is used to specify the Directory (tenant) ID of your Microsoft account.

Enter the Directory (tenant) ID found on the App Registrations, App Properties screen of your Microsoft account.

Client Secret
The Client Secret field is used to specify the value of the secrets record.

Click the Change Secret button.

The Client Secret field is displayed.

Enter the Value found on the Certificates & Secrets page of your Microsoft account, then click the Close icon ✖ to hide the field.

User Name
The User Name field is used to specify the username of an Azure Active Directory user who has been added to the allowed User and Groups of the Enterprise Application.

Enter the username of the Azure Active Directory user.

☑ *Save To Sent Items*
The Save To Sent Items option is used to save sent e-mail messages to the Microsoft account's Sent Items folder.

Select this check box to save sent e-mail messages to the Microsoft account's Sent Items folder.
OR
Clear this check box to disable saving sent e-mail addresses to the Microsoft account's Sent Items folder.

Send Test Email

When you have finished configuring the Email Registration Settings, click the Send Test Email button to test the settings.

If the test was successful, an e-mail message is sent via the specified e-mail protocol. The body of the e-mail message contains the text "Amtelco Secure Messages Registration test message."

Saving Your Configuration Settings

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

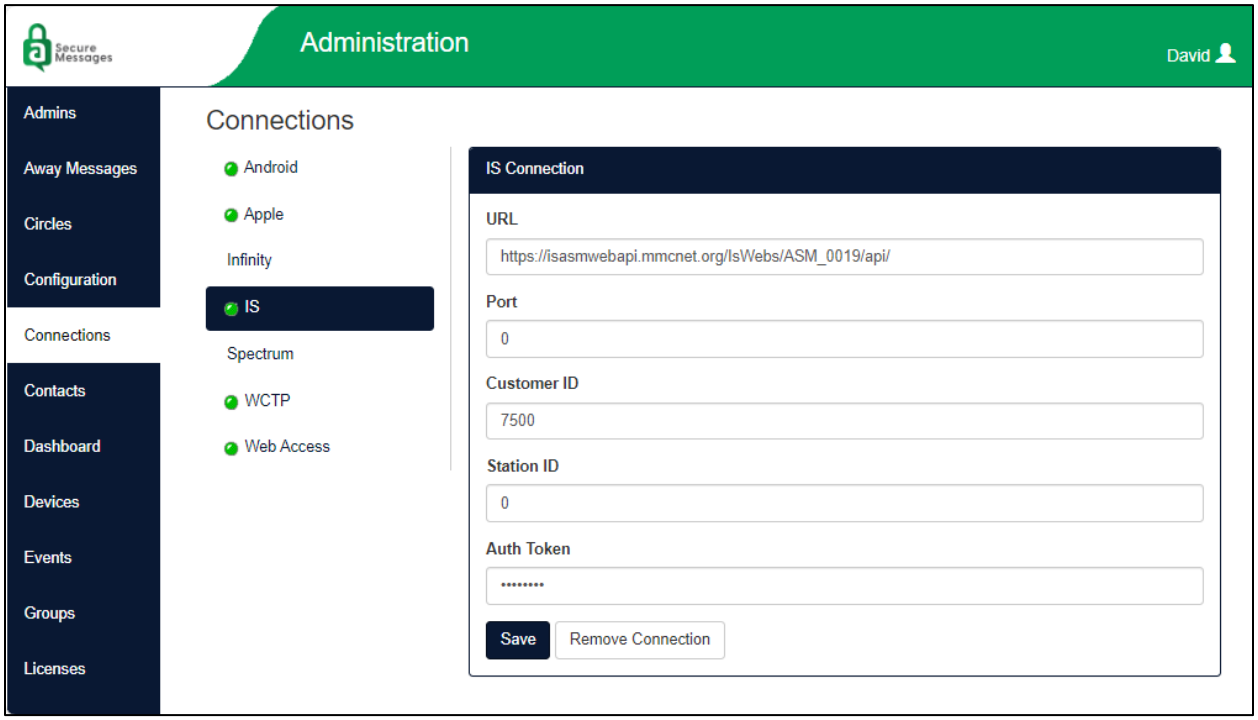
Return to System Configuration
Return to Index

Connections

The Connections page is used to establish connections between the Amtelco Secure Messages Admin Web 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
- Spectrum Server
- Wireless Communications Transfer Protocol (WCTP)
- Web Access for Amtelco Secure Messages customers

Click the Connections command on the navigation menu to access the Connections page.



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

A red icon is displayed next to the name of each connection that has been started but is experiencing issues and is not currently working.

No icon is displayed next to the name of each connection that has not been set up or enabled.

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

The settings for the selected connection are displayed on the right side of the screen.

Android

An Android Server connection is required if secure messages will be viewed on Android devices. The Android connection is set up in the Amtelco Secure Messages server.

Apple

An Apple Server connection is required if secure messages will be viewed on Apple devices. The Apple connection is set up in the Amtelco Secure Messages server.

Infinity

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

Infinity Connection

The following Infinity Connection settings are displayed when the Infinity connection is selected.

Server IP

The Server IP field is used to enter the Internet Protocol (IP) address of the Infinity Server.

Enter the IP address of the Infinity Server.

Port

The Port field is used to designate which port to use to communicate with the Infinity Server.

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

The Login field is used to specify a dedicated Infinity login to use to send messages from Infinity to Amtelco Secure Messages.

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 an Amtelco Secure Messages login are provided in the *Amtelco Secure Messages Partnership Guide* and the *Amtelco Secure Messages On-Site System Guide*.

Password

The Password is used with the login specified in the Login field to authenticate to the Infinity Server.

Enter the password associated with the unique Infinity Amtelco Secure Messages login.

Route

The route number is inserted into dial strings to route messages to the Amtelco Secure Messages 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 *Amtelco Secure Messages Partnership Guide* and the *Amtelco Secure Messages On-Site System Guide*.

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

A green icon is displayed next to Infinity.

IS

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

IS Connection

The following IS Connection settings are displayed when the IS connection is selected.

URL

The URL field is used to specify the Uniform Resource Locator (URL) of the ASM Web Service in order to connect to Intelligent Series version 5.7 and later. To connect to an older version of Intelligent Series, the URL field is used to specify the Internet Protocol (IP) address of the IS Server.

If you are connecting to IS version 5.7 or later, enter the URL of the ASM Web Service.

OR

If you are connecting to an older version of IS, enter the IP address of the IS Server.If the system is configured for High Availability, multiple IP addresses can be added.

Note: Connecting multiple IS server IP addresses requires Intelligent Series (IS) Server version 5.6 or later.

To enter multiple IP addresses, separate each IP address with a comma.

For example, if the IP address of Server A is 000.000.000.000 and the IP address of Server B is 111.111.111.111, enter “000.000.000.000,111.111.111.111” in the Server IP field.

You can include the port number with each IP address in the Server IP field by adding a colon and the port number to the end of each IP address, or if the servers are using the same port number, you can enter the port number in the Port field.

Port

The Port field is not used when connecting Amtelco Secure Messages 7.0 or later to IS 5.7 or later.

When connecting to older version of Intelligent Series, the Port field is used to designate which port to use to communicate with the IS Server.

Note: If you are connecting to Intelligent Series version 5.7 or later, this field should be set to “0” (zero) or left blank. For older version of Intelligent Series, if you included the port numbers with the IP addresses in the Server IP field, the Port field should be set to “0” or left blank.

If you are connecting to IS version 5.7 or later, or if you included the port numbers in the Server IP field, set Port to “0” (zero) or leave it blank.

OR

If you are connected to an older version of IS and did not include port numbers in the Server IP field, enter the port number of the IS Server.

Customer ID

The Customer ID field is used to specify your unique IS customer ID provided by Amtelco.

Enter your unique IS customer ID provided by Amtelco.

Station ID

The Station ID is used to differentiate between ASM Web Services on systems that have more than one ASM Web Service. This Station ID is used when programming IS Directory Contact Methods to indicate which ASM Web Service to use to send messages from Intelligent Series applications. If you are using more than one ASM Web Service to communicate with your IS Server, each ASM Web Service should have a different Station ID.

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

Auth Token

The Auth Token field is used with Intelligent Series version 5.7 and later to store a password that secures the publicly-facing ASM Web Service. This password is compared to the password stored in the Password field of the matching MSM Connection configured in the System Setup pages of IS Supervisor in order to authenticate to the IS Server.

Enter the password to use to authenticate between the ASM Web Service and the IS Server.

Note: The password entered in the Auth Token field must match the password entered in the Password field of the MSM Connection created in the following instructions.

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

A green icon is displayed next to IS.

Spectrum

The Amtelco Secure Messages solution can be integrated with the Spectrum application.

Spectrum Connection

The following Spectrum Connection settings are displayed when the Spectrum connection is selected.

Server IP

The Server IP field is used to enter the Internet Protocol (IP) address of the Spectrum Server.

Enter the IP address of the Spectrum Server.

Port

The Port field is used to designate which port to use to communicate with the Spectrum Server.

Enter the port number of the Spectrum Server.

User

The User field is used to specify a Spectrum user name to use to send messages from Spectrum to Amtelco Secure Messages.

Enter the Spectrum user name to be used to connect to the Spectrum system.

Password

The Password is used with the user name specified in the User field to authenticate to the Spectrum Server.

Enter the password associated with the Spectrum user name.

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

A green icon is displayed next to Spectrum.

WCTP

The Escalation Message feature can be used to send a text message to the contact phone number of a Amtelco Secure Messages contact if that contact is sent a secure message and does not read it within the Escalation Delay specified on the Configuration page. The Wireless Communications Transfer Protocol (WCTP) connection is used to connect Amtelco Secure Messages to the SMS aggregator used to send the escalation text messages.

WCTP Connection

The following WCTP Connection settings are displayed when the WCTP connection is selected.

URL

The URL field is used to specify the Uniform Resource Locator (URL) of the WCTP provider used to send escalation text messages.

Type the URL of the WCTP provider.

Auth ID

Auth ID is the Authorization ID provided by Infinite Convergence to use their SMS service.

If you are using Infinite Convergence's SMS service, enter the Authorization ID provided by Infinite Convergence.

Auth Code

Auth Code is the Authorization Code provided by Infinite Convergence to use their SMS service.

If you are using Infinite Convergence's SMS service, enter the security code provided by Infinite Convergence.

User

The User field is used to specify username to use to send messages to the WCTP provider.

Enter the username required by the WCTP provider, if any.

Password

The Password is used with the username specified in the User field to authenticate to the WCTP provider.

Enter the password associated with the username, if any.

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

A green icon is displayed next to WCTP.

Web Access

The Amtelco Secure Messages 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 Amtelco Secure Messages 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.

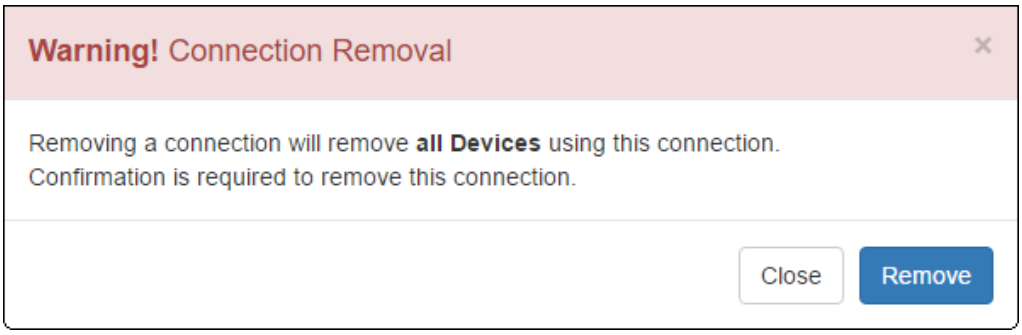
Removing a Connection

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 remove the connection, click the Remove button.

OR

Click the Close button to keep the connection.

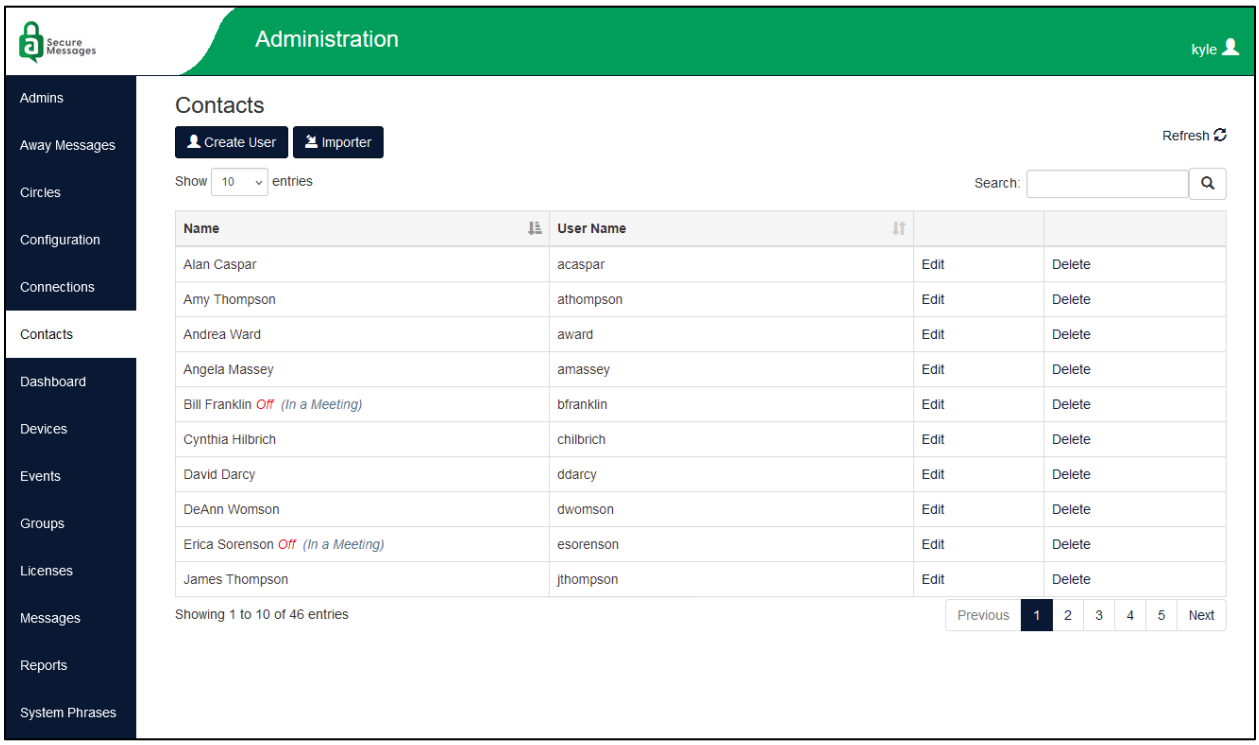
Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

Contacts

The Contacts page is used to view, edit, and delete Amtelco Secure Messages 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 Amtelco Secure Messages app on their mobile device, their name and username are automatically saved on the Amtelco Secure Messages Server. This information is displayed on the Contacts page.

Click the Contacts command on the navigation menu to access the Contacts page.



Column	Description
Name	Name is the contact name that is displayed in the Amtelco Secure Messages Contacts directory and on all messages that the user sends. If the contact's Amtelco Secure Messages notifications are off, the word "Off" is displayed in red text to the right of the contact's name, followed by the contact's away message in parenthesis. If the contact is locked, the words "Locked" are displayed in blue text to the right of the contact's name. If a contact is locked, contact the person authorized to use that contact name and find out if that person had trouble logging in or forgot the password. A locked contact could be an indication that an unauthorized person was trying to access the system using someone else's username. If you verify that the correct person was having trouble logging in, you can unlock the contact by editing the contact and clicking the UnLock User button.

Column	Description
User Name	The username is used to identify the user to the Amtelco Secure Messages 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, type the information that you want to find into the Search and either press the ENTER key or click the Search icon.**
- **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 the Refresh icon.**

Importing Contacts

If the Contact Importer feature is enabled on your system, an Importer button is displayed on the Contacts page. The Contact Importer feature can import contacts from Active Directory, SQL, or a delimited text file. The Contact Importer is only available for on-site implementations.

To import contacts from Active Directory, SQL, or a delimited text file, click the Importer button.

The Contact Importer page is displayed.

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 Amtelco Secure Messages app on a device or logs into the Amtelco Secure Messages 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 pane is 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 in the same row of the table as that contact's information.

The Contact Settings pane is displayed.

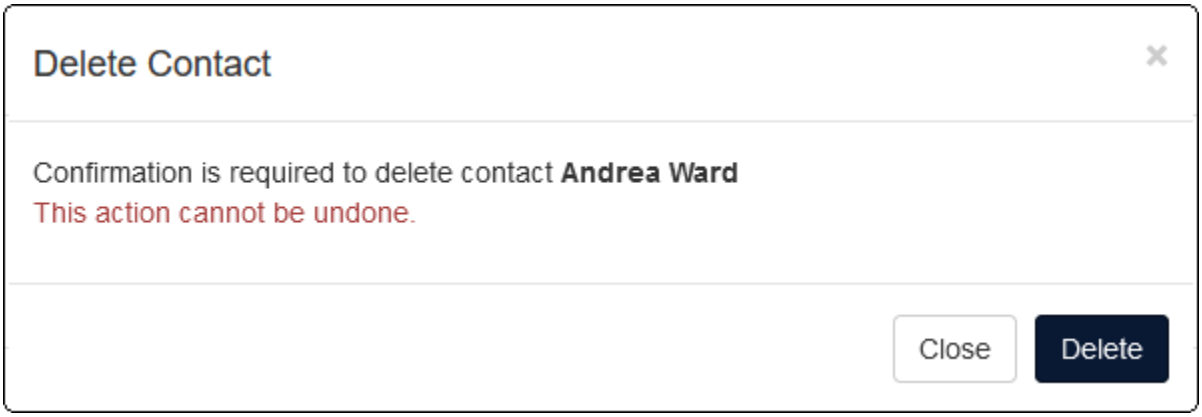
Make changes to the contact settings as desired.

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

Deleting a Contact

To delete a contact, click the Delete hyperlink in the same row of the table as that contact's information.

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



To cancel the delete request, click the Close button.

OR

If you are sure you want to delete the contact, click the Delete button 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 Importer

Contact Settings

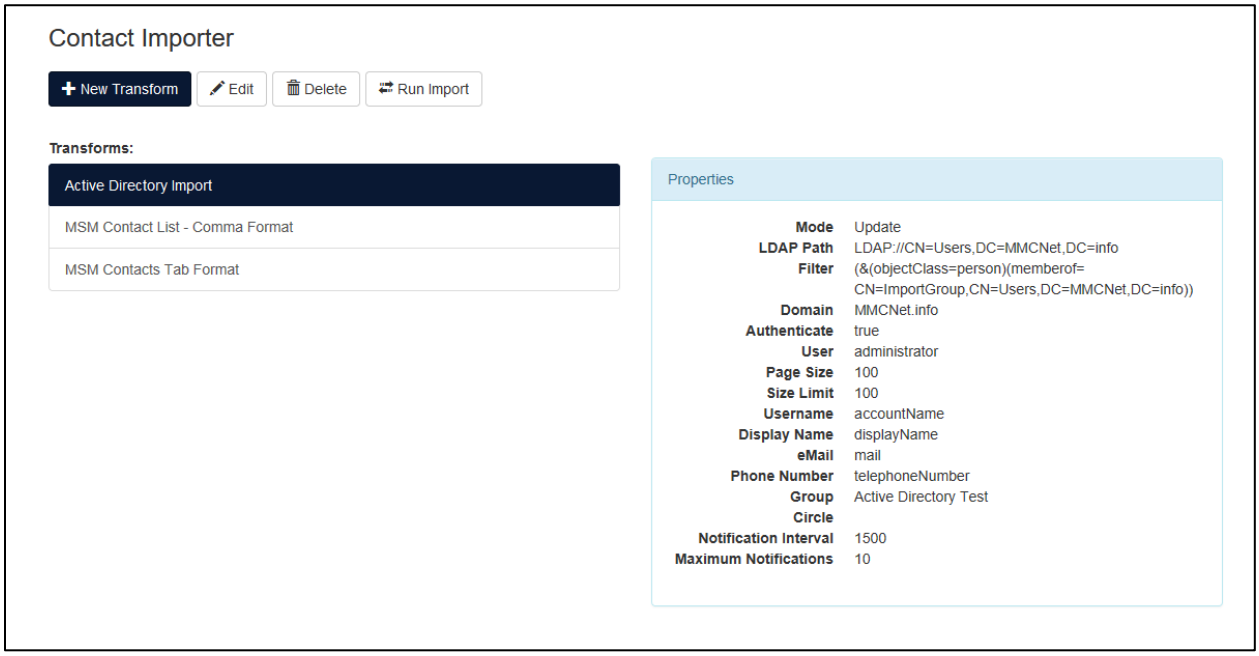
Return to Adding and Editing Amtelco Secure Messages Admin Web Administrators

Return to Navigating in Amtelco Secure Messages Admin Web

Return to Index

Contact Importer

The Contact Importer page is used to import contacts. For on-site implementations, the Contact Importer can import contacts from Active Directory, SQL, a delimited text file, or a Comma-Separated Value (CSV) file. For hosted implementations, contacts can be imported by uploading a delimited text file or a CSV file.



Transforms

The transforms that have been configured are listed in the Transforms menu.

Click the name of a transform to select it.

Properties

The properties of the selected transform are displayed in the Properties pane.

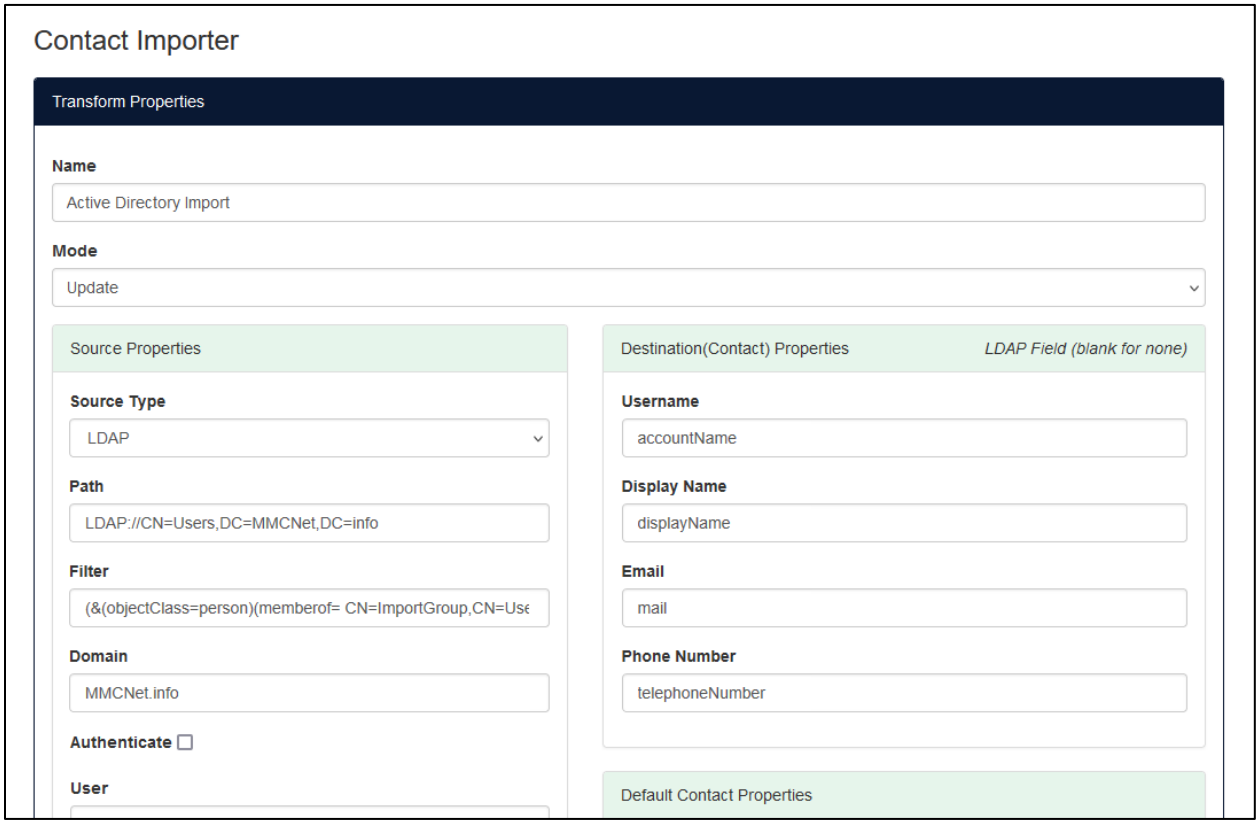
Creating a Transform

The first step in importing contacts is to create a transform.

To add a new transform, click the New Transform button.

The Transform Properties pane is displayed.

Transform Properties



Name

The Name field is used to identify the transform in the Transform menu.

Type a name for the transform.

Mode

The Mode menu is used to select the type of transformation to perform. The modes of transformation are explained in the following table:

Mode	Description
Append	An Append transformation adds new contacts for all of the information contained in the source.
Update	An Update transformation checks the source information for usernames that match the usernames of existing contacts. It updates the contact settings of existing contacts for usernames that are a match and adds new contacts for usernames that are not a match.

Select the mode of transformation to perform.

Source Properties

The Source Properties pane is used to configure the settings for the source of the transformation.

Source Type

The Source Type menu is used to select the source for the transformation. For on-site implementations, the File, CSV File, SQL or LDAP source types can be used. For hosted implementations, the File Upload or CSV File Upload source types can be used.

The Contact Importer accepts the following types of sources:

Source Type	Works With	Description
File	On-site Amtelco Secure Messages	The File source type is used with on-site Amtelco Secure Messages installations. It is used to import contacts from a text (TXT) file in which a specified character is used as a delimiter to separate pieces of information.
File Upload	Hosted Amtelco Secure Messages	The File Upload source type is used with hosted Amtelco Secure Messages installations. It is used to upload and import contacts from a text (TXT) file in which a specified character is used as a delimiter to separate pieces of information.
CSV File	On-site Amtelco Secure Messages	The CSV File source type is used with on-site Amtelco Secure Messages installations. It is used to import contacts from a Comma-Separated Values file.
CSV File Upload	Hosted Amtelco Secure Messages	The CSV File Upload source type is used with hosted Amtelco Secure Messages installations. It is used to upload and import contacts from a Comma-Separated Values file.
SQL	On-Site Amtelco Secure Messages	The SQL source type is used with on-site Amtelco Secure Messages installations. It is used to import contacts from an SQL database.
LDAP	On-Site Amtelco Secure Messages	The LDAP source type is used with on-site Amtelco Secure Messages installations. It is used to import contacts from Active Directory using Lightweight Directory Access Protocol (LDAP).

Select the type of source that you have.

The settings displayed in the Source Properties pane change depending on the type of source selected in the Source Type menu.

File

The File setting is displayed when the Source Type is set to “File” or “CSV File.”

The File setting is used to specify the path to the source file. The source file must be stored in a location that is accessible from the server that is running the Amtelco Secure Messages Admin Web application.

Type the full path from the server running the Amtelco Secure Messages Admin Web to the file, including the drive letter, folders, and file name.

Delimiter

The Delimiter setting is displayed when the Source Type is set to “File” or “File Upload.”

The Delimiter is the character used to separate the pieces of information in the source file. The two options for the delimiter are “Tab” and “Comma.”

Select the character used to separate the source data.

Qualifier

The Qualifier setting is displayed when the Source Type is set to “File” or “File Upload.”

The Qualifier is a character used to group information that contains a line feed or the delimiter but should be considered one piece of data. The string qualifier must be placed at the start and end of the information that is to be grouped. The choices for string qualifier are “None,” “Single Quote,” and “Double Quote.”

Select the character used as a string qualifier in the source file
OR
Select None if no string qualifier was used.

☑ File Has Header

The “File Has Header” check box is displayed when the Source Type is set to “File,” “File Upload,” “CSV File,” or “CSV File Upload.” This check box should be selected when importing a file that contains column headers in the first line of the file. Selecting this check box tells the importer to skip the first line of information when importing contacts from the file.

- **Select this check box if the import file contains column headers in the first row.**
- **Clear this check box if the import file does not contain column headers.**

SQL Connection

The SQL Connection setting is displayed when the Source Type is set to “SQL.”

The SQL Connection specifies the connection string used to connect to the source SQL table.

A typical SQL connection string is in the following format:

User id=*SQL_Login*;Password=*SQL_Password*;Initial catalog=*Database*;data source=*Server*;

Replace *SQL_Login* with the user ID used to access the source SQL table.

Replace *SQL_Password* with the password used to access the source SQL table.

Replace *Database* with the name of the SQL database.

Replace *Server* with the name of the SQL server.

Type the Connection String used to access the SQL database.

SQL Command

The SQL Command setting is displayed when the Source Type is set to “SQL.”

The SQL Command is used to select listings from the source SQL table.

The following is an example of an SQL command that returns all listings in a table:

SELECT * FROM *TableName*

Replace *TableName* with the name of the source SQL table.

Enter the SQL command that will return the contact data that you want to import from the source SQL table.

Path

The Path setting is displayed when the Source Type is set to “LDAP.”

The Path indicates the name or IP address of the LDAP server. It is best to consult with your IT staff to determine the location, address, and actual syntax of the Path setting. You may find it helpful to use an LDAP Browser to view the structure of the LDAP server data store in order to identify the components of the Path and Filter settings. By default, most LDAP directory servers do not include a way to view the LDAP data structure. A number of LDAP Browsers are available via the Internet for free download. Amtelco makes no recommendations concerning choice of LDAP Browser.

Type the local area network (LAN) name or the IP address of the of the LDAP server in the syntax used by the LDAP application.

Filter

The Filter setting is displayed when the Source Type is set to “LDAP.”

The Filter parameter is used to specify one or more LDAP search strings to be executed against the LDAP data store by the Contact Importer, listed in the syntax used by the LDAP application. It is best to consult with your IT staff to determine the actual syntax and scope of the Filter setting.

Type the LDAP search string or strings for the Contact Importer to execute to import the LDAP data.

Domain

The Domain setting is displayed when the Source Type is set to “LDAP.”

This setting determines the domain used for simple authentication.

If simple authentication is enabled, enter the Domain Name of the LDAP server.

☑ Authenticate

The Authenticate check box is displayed when the Source Type is set to “LDAP.”

This setting enables simple authentication of the Contact Importer to access the LDAP server.

- **Select this check box to enable simple authentication.**
- **Clear this check box to use anonymous authentication.**

User

The User setting is displayed when the Source Type is set to “LDAP.”

This setting determines the User Name used for simple authentication.

If simple authentication is enabled, enter the User Name to use for the LDAP import as configured in the access control component of the LDAP server.

Password

The Password setting is displayed when the Source Type is set to “LDAP.”

This setting determines the Password used for simple authentication.

If simple authentication is enabled, enter the Password associated with the User Name as configured in the access control component of the LDAP server.

Page Size

The Page Size setting is displayed when the Source Type is set to "LDAP."

The Page Size controls the number of objects that are returned in a single search result. The typical value is 1,000.

Enter the value of the Max Page Size specified in your LDAP server configuration.

Size Limit

The Size Limit setting is displayed when the Source Type is set to "LDAP."

The Size Limit controls the number of results that a client can retrieve in a single operation.

Enter the value of the Size Limit specified in your LDAP server configuration.

Destination(Contact) Properties

The Destination(Contact) Properties pane is used to match fields of the source with Amtelco Secure Messages contact settings.

Note: When Source Type is set to "File," field indexes starting at zero are used. For example, a value of zero (0) indicates the first field in the file, a value of one (1) indicates the field is located after the first tab or comma in the destination file, and so on.

Username

The Username is used to identify the user to the Amtelco Secure Messages 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. If the group's Registration Type is Self Registration, the user will need to provide the username the first time that the user logs into the Amtelco Secure Messages 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 Amtelco Secure Messages Status and OnCall features, you must provide an IS Agent Login Name for the user in the IS Supervisor application. If the IS Agent Login Name does not match the imported username, the IS Agent Login Name must be specified in the contact's IS Agent Login settings.

If you want to be able to use Infinity dial strings to send secure messages to contacts, the username may not include spaces, accent marks (as used in languages like French and Spanish), nor any of these special characters: " [€ £ ¥ + ,

- **If Source Type is set to "File," "File Upload," "CSV File," or "CSV File Upload," enter the index number of the field in the source file that contains contact usernames.**
- **If the Source Type is set to "SQL" or "LDAP," enter the name of the source field that contains contact usernames.**

Display Name

Display Name is the contact name that is displayed in the Amtelco Secure Messages Contacts directory and on all messages that the user sends. First name and last name are recommended (for example, “John Smith”).

- **If Source Type is set to “File,” “File Upload,” “CSV File,” or “CSV File Upload,” enter the index number of the field in the source file that contains contact display names.**
- **If the Source Type is set to “SQL” or “LDAP,” enter the name of the source field that contains contact display names.**

Email

The Email setting is used with the Email Registration feature to send registration and password reset e-mail messages.

- **If Source Type is set to “File,” “File Upload,” “CSV File,” or “CSV File Upload,” enter the index number of the field in the source file that contains contact e-mail addresses.**
- **If the Source Type is set to “SQL” or “LDAP,” enter the name of the source field that contains contact e-mail addresses.**
- **Leave this setting blank if you do not want to import e-mail addresses.**

Phone Number

The Phone Number setting can be used to place a phone call to a contact from the Amtelco Secure Messages app and to send escalation text messages to a contact.

- **If Source Type is set to “File,” “File Upload,” “CSV File,” or “CSV File Upload,” enter the index number of the field in the source file that contains contact phone numbers.**
- **If the Source Type is set to “SQL” or “LDAP,” enter the name of the source field that contains contact phone numbers.**
- **Leave this setting blank if you do not want to import contact phone numbers.**

Default Contact Properties

The Default Properties pane is used to specify default values to use in the contact settings for imported contacts.

Group

The Group menu contains the names of the Groups that have been configured. The Group setting specifies the account group to which imported contacts are assigned.

Select the Group to which imported contacts should be assigned.

Circle

The Circle menu contains the names of the Contact Circles that have been configured for the selected Group. The Circle setting specifies the Contact Circle to which imported contacts are assigned.

Select the Circle to which imported contacts should be assigned.

Notification Interval

The Notification Interval setting specifies the Notification Interval to apply to imported contacts. The Notification 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, or seconds to wait between notification attempts, and then select the appropriate unit of measurement from the menu.

Maximum Notifications

The Maximum Notifications setting specifies the Notification Attempts to apply to imported contacts. Notification Attempts 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 Notification Attempts setting has been sent.

Enter the maximum number of notifications that Amtelco Secure Messages 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.

Saving Your Changes

When you are finished configuring the Transform Properties, click the Save button to save the settings and return to the Contact Importer page.

OR

To discard your changes and return to the Contact Importer page, click the Cancel button.

If you created a new transform, the transform is added to the Transforms menu.

Editing a Transform

To make changes to an existing transform, click the name of the transform in the Transforms menu.

The properties of the selected transform are displayed in the Properties pane.

Click the Edit button.

The Transform Properties pane is displayed.

Make the desired changes to the Transform Properties.

When you are finished making changes, click the Save button to save your changes and return to the Contact Importer page.

OR

To discard your changes and return to the Contact Importer page, click the Cancel button.

Running a Transform

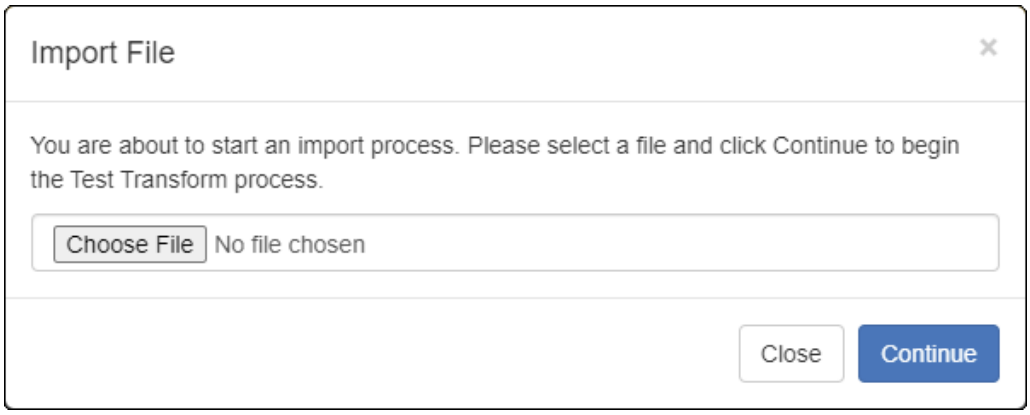
Once a transform has been saved, it can be used to import contacts.

When you are ready to run a transform to import clients, click the name of the transform in the Transforms menu.

The properties of the selected transform are displayed in the Properties pane.

Click the Run Import button.

- If the Source Type property of the transform is set to “File Upload” or “CSV File Upload,” the Import File dialog box is displayed.



Click the Browse button or the Choose File button.

A file browser window is displayed.

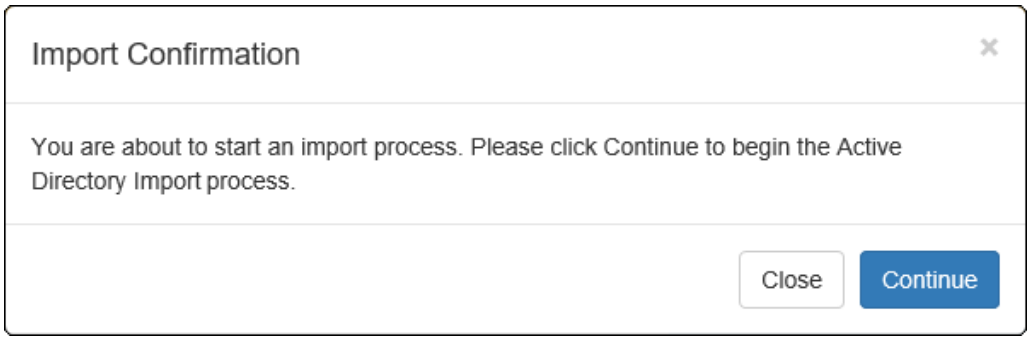
Navigate to the location of the import file.

Select the import file and then click the Open button.

The name of the import file is displayed in the Import File window.

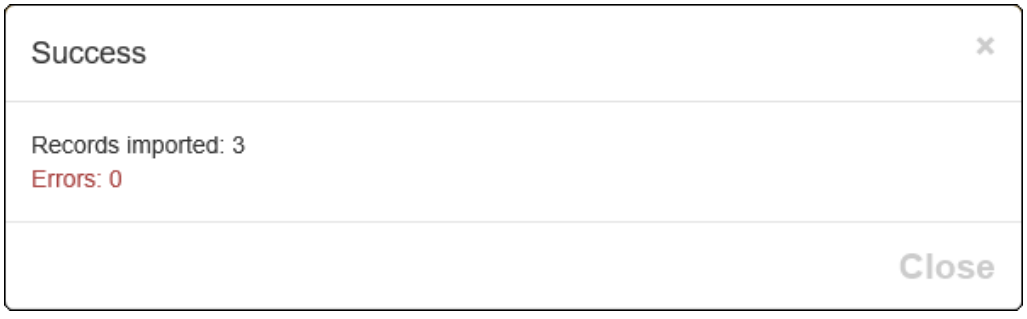
Click the Continue button to start the contact import process.

- If the Source Type property of the transform is set to “File,” “CSV File,” “SQL,” or “LDAP,” the Import Confirmation dialog box is displayed.



Click the Continue button to start the contact import process.

If the transformation finishes successfully, a “Success” message is displayed with information about the number of records imported and the number of errors that occurred during the transformation.



Click the Close button to return to the Contact Importer page.

Deleting a Transform

To delete a transform, click the name of the transform in the Transforms menu.

The properties of the selected transform are displayed in the Properties pane.

Click the Delete button.

A confirmation dialog box is displayed.

To cancel the delete request, click the Close button.

OR

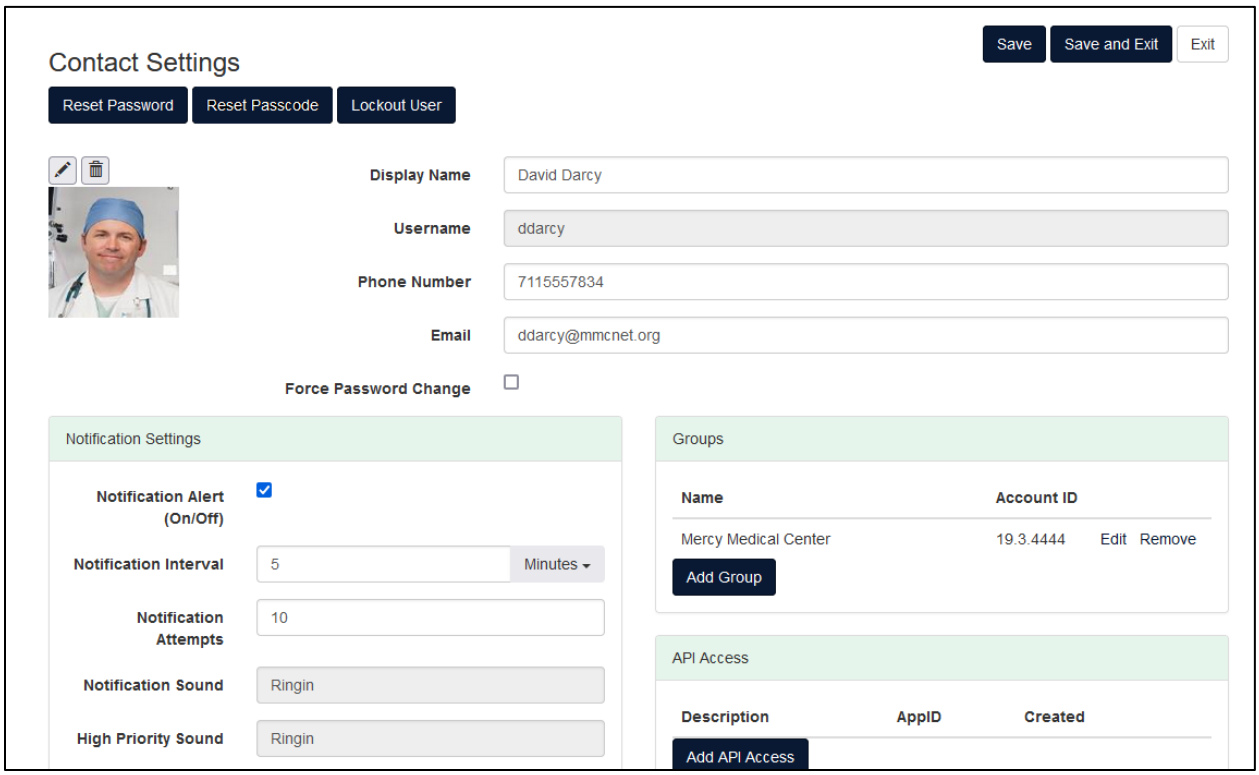
If you are sure you want to delete the transform, click the Delete button.

If you clicked the Delete button, the transform is removed from the list.

Return to Contacts
Return to Index

Contact Settings

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

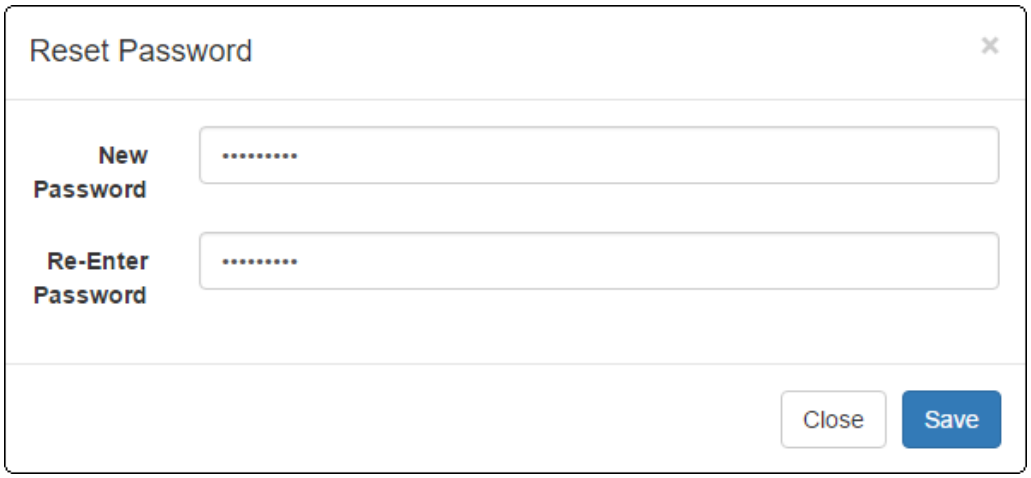


Reset Password

The Reset Password button is displayed when you are editing a user. The Reset Password button is used to reset the user's password if the user has forgotten it. The password is used to log into Amtelco Secure Messages when registering the Amtelco Secure Messages app using Self Registration. The password is also used to log into the Amtelco Secure Messages Contact Web.

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.

OR

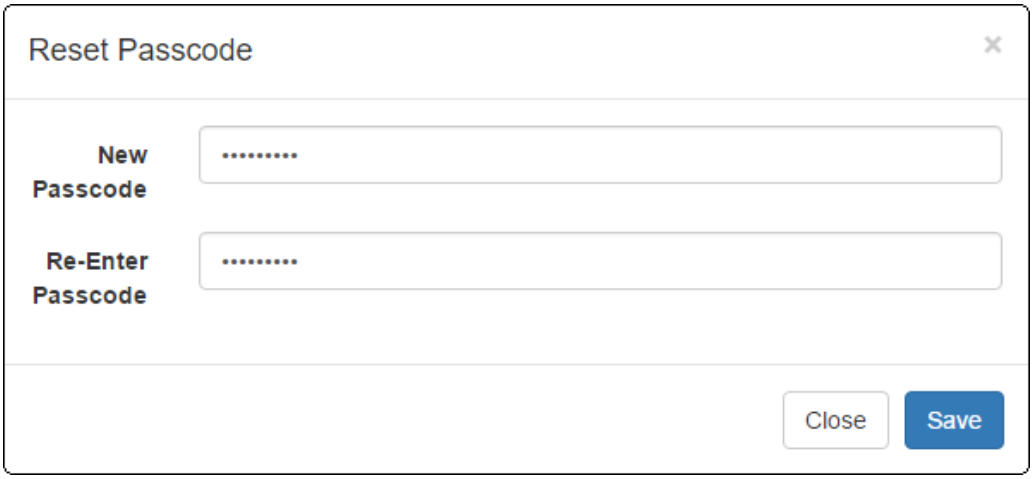
Click the Close button to close the Reset Password window without changing the contact's password.

Reset Passcode

The Reset Passcode button is displayed when you are editing a user. The Reset Passcode button is used to reset the user's passcode if the user has forgotten it. The passcode is the code that the user must enter each time the app is opened on the user's device.

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.

OR

Click the Close button to close the Reset Passcode window without changing the contact's passcode.

Lockout User

The Lockout User button is displayed when you are editing a contact that is not locked out. The Lockout User button is 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 Amtelco Secure Messages 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 contact is deactivated. When a contact is locked, the word "Locked" is displayed in blue italic text next to the user's name on the Contacts page.

UnLock User

The red UnLock User button is displayed when you are editing a locked contact. The UnLock User button is used to reactivate the contact.

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

The Unlock Contact window is displayed.

Type a new password in the New Password field and the Re-Enter Password field, and type a new passcode in the New Passcode field and the Re-Enter Passcode field.

Click the Save button to unlock the contact.

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

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 or the Choose File button.

A file browser window is displayed.

Navigate to the location of the image file.

Select the image file and then click the Open button.

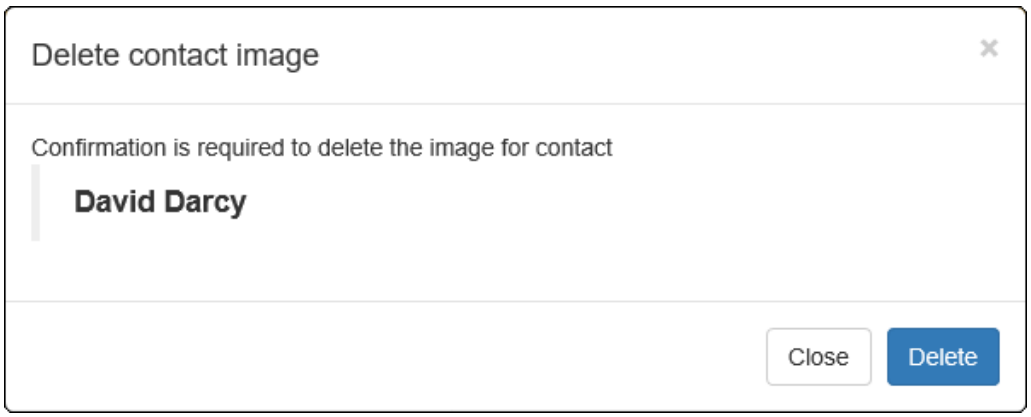
The path to the image file is displayed in the Image Loader window.

Click the Save button to load the image.

Deleting a Photo

To delete the contact's photo, click the Delete icon.

A confirmation dialog box is displayed.



To cancel the delete request, click the Close button.

OR

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

If you clicked the Delete button, the image is removed.

Display Name

Display Name is the contact name that is displayed in the Amtelco Secure Messages 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 Amtelco Secure Messages 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. If the group's Registration Type is Self Registration, the user will need to provide the username the first time that the user logs into the Amtelco Secure Messages 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 Amtelco Secure Messages 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 Agent Login pane.

If you want to be able to use Infinity dial strings to send secure messages to this contact, the username may not include spaces, accent marks (as used in languages like French and Spanish), nor any of these special characters: " [€ £ ¥ + ,

- **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 Amtelco Secure Messages app. The Phone Number setting is also used with the Escalation Message feature to send a text message to the contact if a secure message is sent to the contact and the contact does not read it before the Escalation Delay expires. The Escalation Message and the Escalation Delay are configured on the Configuration Page and on the General Group Properties page of each group.

To enable users to be able to call this contact from the Amtelco Secure Messages app and enable the Amtelco Secure Messages to text an escalation message to this contact, enter the contact's phone number.

Note: The "Hide Phone Number" permission in Group Properties can be used to hide contact phone numbers from Amtelco Secure Messages app users and still allow the phone numbers to be used for escalation messages.

Email

The Email setting is used with the Email Registration feature to send registration and password reset e-mail messages.

If you want to be able to send this user registration and password reset e-mail messages, enter the user's e-mail address.

Password

The Password setting is displayed when you are creating a new contact. 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 when registering for a group using Self Registration. The Password is also required to log into the Contact Web application.

☑ Force Password Change

The "Force Password Change" setting is used to force a contact to change his or her password the next time the contact logs into one of the Amtelco Secure Messages apps or the Amtelco Secure Messages Contact Web. The contact will be prompted with the password requirements and will be required to enter a password that does not match the existing password. When the contact changes his or her password, the "Force Password Change" check box is cleared automatically.

Select this check box to force the contact to change his or her Amtelco Secure Messages password the next time the contact logs in.

Notification Settings

The Notification Settings are used to customize how this Contact is notified when a secure message is received. These settings override the Notification Attempts and Notification Interval settings under the General tab in Group Properties and on the System Configuration page.

☑ Notification Alert (On/Off)

The "Notification Alert (On/Off)" setting determines whether the contact is able to receive secure message notifications. When the Notifications Alert (On/Off) check box is not selected, any users who attempt to send a message to the contact will be notified that this contact is unavailable.

- **Select this check box to enable this contact to receive notifications of secure messages.**
- **Clear this check box to disable Amtelco Secure Messages notifications for this contact.**

  The Away Message window is displayed.

  Follow the instructions for setting an away message.

Notification Interval

By default, Notification Interval is set to the interval specified on the System Configuration page. The Notification 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, or seconds to wait between notification attempts, and then select the appropriate unit of measurement from the menu.

Notification Attempts

By default, Notification Attempts is set to the number of Notification Attempts specified on the System Configuration page. Notification Attempts 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 Notification Attempts setting has been sent.

Enter the maximum number of notifications that Amtelco Secure Messages 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 Sound

The Notification Sound field displays the name of the sound file that plays when the contact receives a normal priority message notification. The Notification Sound can only be edited in the Amtelco Secure Messages Contact Web and in the Amtelco Secure Messages app on the contact's personal device.

High Priority Sound

The High Priority Sound field displays the name of the sound file that plays when the contact receives a high priority message notification. The High Priority Sound can only be edited in the Amtelco Secure Messages Contact Web and in the Amtelco Secure Messages app on the contact's personal device.

Away Message

The Away Message field is displayed when editing a contact. The Away Message field displays the away message that is currently selected for the contact.

Note: The Away Message is only in effect while the Notification Alert (On/Off) setting is not checked. If the Notification Alert (On/Off) setting is checked, Amtelco Secure Messages notifications are turned on for the contact.

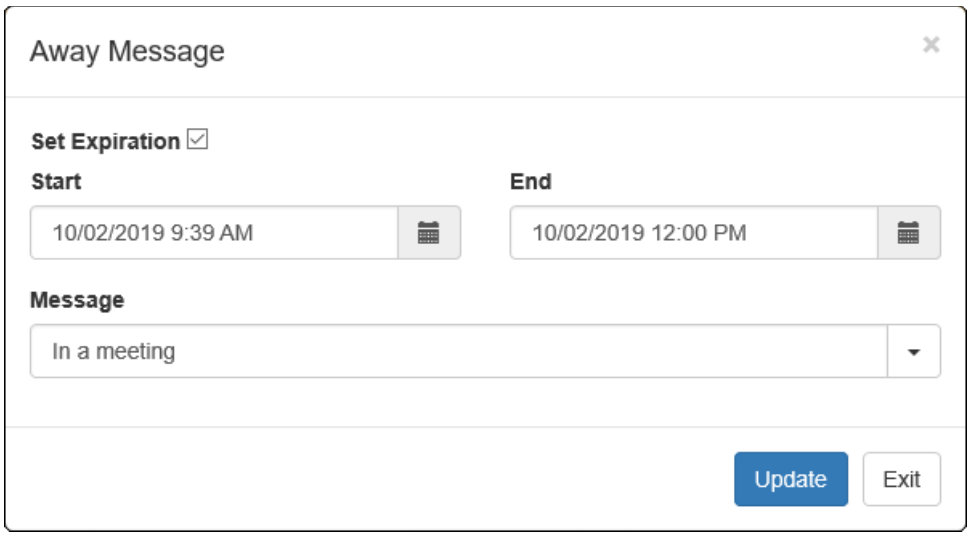
To set an Away Message for this contact, click the Set Message button.

The Away Message window is displayed.

Follow the instructions for setting an away message.

Setting an Away Message

The Away Message window is displayed by clicking the Set Message button or by clearing the Notification Alert (On/Off) check box.



☑ Set Expiration

The "Set Expiration" setting determines whether the away message has a start and end time. If the check box is not selected, the away message will apply from the time it is saved until notifications are turned back on or another away message is set.

- **To set an away message starting immediately with no expiration date and time, leave the "Set Expiration" check box unchecked.**
- **To set an away message with a start date and time and an end time, select the "Set Expiration check box.**

  The Start and End settings are displayed.

Start

The Start field is displayed when the "Set Expiration" check box is selected.

To change the start date and time, click the Calendar icon to the right of the Start field.

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 at the bottom of the calendar.**

  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 field is displayed when the "Set Expiration" check box is selected.

To change the end date and time, click the Calendar icon to the right of the End field.

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.**

Message

The Message is the away message that will be displayed to Amtelco Secure Messages users.

Type an away message into the Message field.

OR

Click the down arrow icon and select an away message.

Click the Update button to apply the away message.

The Notification Alert (On/Off) check box is cleared, and the away message is displayed in the Away Message field. The start date and time and the end date and time, if any, are displayed below the Away Message field.

Groups

The Groups section displays a list of the groups for which the contact is registered.

Column	Description
Name	Name indicates the name of the group. The group name is displayed in the Amtelco Secure Messages apps as the Account Name in the Amtelco Secure Messages apps and the Amtelco Secure Messages Contact Web. Users select an Account Name to switch from one account to another.
Account ID	Account ID indicates the Account ID used to register users for the group.

- **To edit the contact's group settings, click the Edit hyperlink in the same row of the table as that group's information.**

  The Contact Group Settings are displayed.

- **To remove the contact from a group, click the Remove hyperlink to the right of the group's Account ID.**

- **To add the contact to a group, click the Add Group button.**

  A menu and two buttons are displayed.

  Open the menu and select the name of the group to which you want to add this contact.

  Click the Save button to add the contact to the group.
  OR
  Click the Cancel button to cancel adding the contact to a group.

API Access

The API Access section displays a list of the App IDs that are active for the contact to use to access the Amtelco Secure Messages Application Programming Interface (API). The Amtelco Secure Messages API provides access to commands that can be used to interface between Amtelco Secure Messages and other applications.

Column	Description
Description	The description column displays the descriptive text that was entered when adding API access for this contact.
AppID	The AppID column displays the unique App ID generated for this contact in order to provide access to the Amtelco Secure Messages API.
Created	The Created column displays the date and time that the App ID was created.

Granting API Access

In order to use the Amtelco Secure Messages API, a contact must be granted a unique App ID and password.

Note: API Access should only be granted to a contact created for a developer or Information Technology employee who is charged with integration of Amtelco Secure Messages with another application and who has signed your organization's required documentation to ensure data integrity and the security and privacy of protected information.

To grant the contact access to the Amtelco Secure Messages Application Programming Interface (API), click the Add API Access button.

A field and two buttons are displayed. The field is used to provide a description of the API access for future reference.

Type a descriptive of the API access, for example the name of the application that will be interfacing with Amtelco Secure Messages through the API.

Click the Save button to generate the API App ID and password.
OR
Click the Cancel button to return to the Contact Settings screen without granting API access.

If you clicked the Save button, the API Access dialog box is displayed. The API Access dialog box displays a unique App ID and Password that the contact can use to access the Amtelco Secure Messages API.

Note: The App ID will be visible in the API Access table, but the Password will not be shown anywhere but within the API Access dialog box. It is very important to record the Password in a secure location before clicking the OK button. If you don't record the Password, you will have to remove the App ID and generate a new one.

Copy the password and record it in a secure location so that you can provide it to the contact.

When you have copied the password to a secure location, click the OK button.

The description and the unique App ID are added to the API Access table.

Removing API Access

To remove this contact's API access, click the Remove hyperlink to the right of the App ID.

The Remove API Access dialog box is displayed.

To cancel the delete request, click the Close button.

OR

If you are certain you want to delete the App ID, click the Delete button.

If you clicked the Delete button, the App ID is removed from the table.

Devices

The Devices table displays information about the devices that have been registered for the selected contact.

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

Column	Description
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.
OS	OS indicates the operating system running on the device, if available, or the API Level for Android devices.
Secure Messages Version	Secure Messages Version indicates the version number of the Amtelco Secure Messages app that is installed on the device, if available.
Phone	The Phone column displays the phone number assigned to the device, or an Add hyperlink that can be used to add a phone number to the device.
Last Accessed	Last Accessed indicates the date and time that the Amtelco Secure Messages 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.

Adding a Device Phone Number

Device phone numbers can be used with the Shared Device feature to allow Amtelco Secure Messages users to call a contact person who doesn't use the same device every day. The device phone number is displayed in the Amtelco Secure Messages apps on the Contact Info page for the contact who is logged into the Amtelco Secure Messages app on that device.

To add a phone number to a device, click the Add hyperlink in the same row of the table as that device's information.

The Device Phone Number dialog box is displayed.

Type the device's phone number into the Phone Number field.

Click the Save button to save your changes.
OR
Click the Cancel button to discard your changes.

If you clicked Save, the phone number is displayed as a hyperlink in the Devices table.

Editing or Removing a Device Phone Number

To edit or remove a device's phone number, click the phone number hyperlink.

The Device Phone Number dialog box is displayed.

Edit or delete the phone number in the Phone Number field.

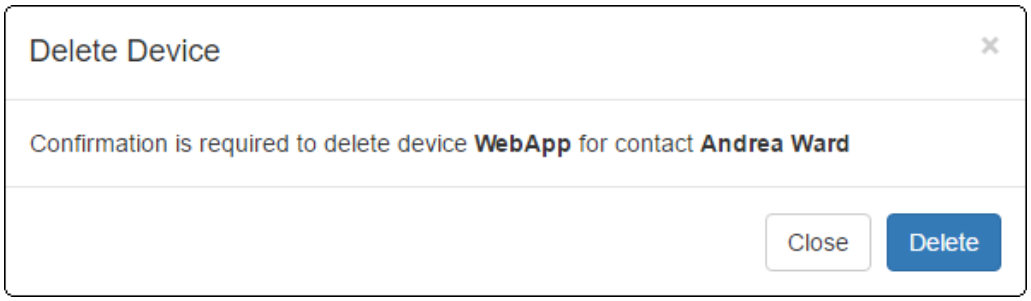
Click the Save button to save your changes.
OR
Click the Cancel button to discard your changes.

Deleting a Device

When a device is no longer being used by the contact, it can be deleted from the Devices table. If a device is given to another Amtelco Secure Messages user and is not configured as a Shared Device, you will need to delete the device from the Contact Settings for the previous user before the new user will be able to log into Amtelco Secure Messages on the device.

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

A confirmation dialog box is displayed.



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

To cancel the delete request, click the Close button.

OR

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

If you clicked the Delete button, the device is removed.

Saving Your Changes

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

OR

To save your settings and remain on the Contact Settings screen, click the Save button.

OR

To discard your changes and return to the Contacts list, click the Exit button.

If you created a new user, the user's name and username are added to the Contacts table.

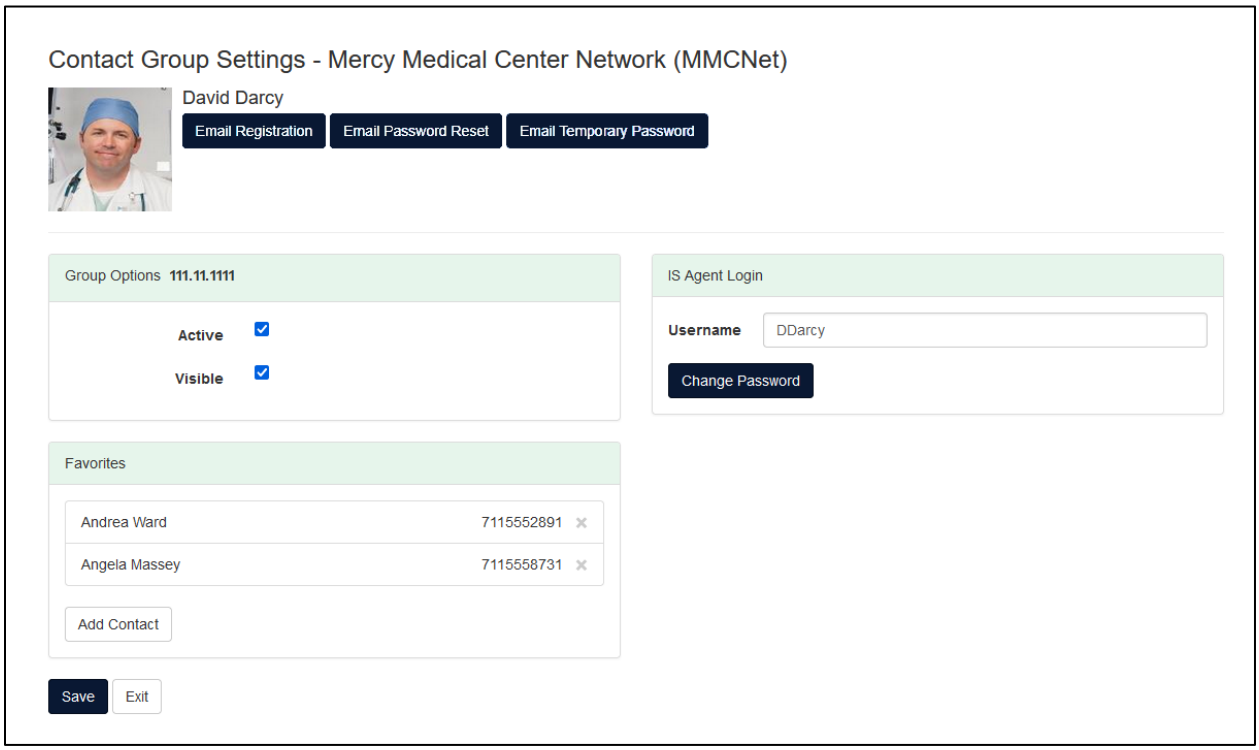
Contact Group Settings

Return to Contacts

Return to Index

Contact Group Settings

The Contact Group Settings pane is displayed when editing groups within a user's Contact Settings.



Email Registration

The Email Registration button is displayed if the Registration Type for this group is set to "Email Registration" and there is an e-mail address specified in the contact's Email setting.

The Email Registration button is used to send an e-mail message that contains a hyperlink that the contact can use to register for Amtelco Secure Messages. The registration e-mail is configured under the Initial Registration tab and the Multiple Device Registration tab in the Email Messages Group Properties.

To send a registration e-mail to this contact, click the Email Registration button.

Email Password Reset

The Email Password Reset button is displayed if the Registration Type for this group is set to "Email Registration" and there is an e-mail address specified in the contact's Email setting.

For groups using Email Registration, the Email Password Reset button is used to send an e-mail message that contains a hyperlink that the contact can use to create a new Amtelco Secure Messages password and passcode from one of the Amtelco Secure Messages apps. If you need to reset the password for an Amtelco Secure Messages Contact Web user, use the Email Temporary Password button instead.

The password reset e-mail is configured under the Reset Password tab in the Email Messages Group Properties.

To e-mail a password reset hyperlink to this contact to enable the contact to reset his or her password in the Amtelco Secure Messages apps, click the Email Password Reset button.

If the Amtelco Secure Messages App user clicks on the hyperlink in the e-mail message before it expires, the user will be prompted to choose a new password and passcode.

Email Temporary Password

The Email Temporary Password button is displayed if there is an e-mail address specified in the contact's Email setting.

The Email Temporary Password button is used to send an e-mail message that contains a temporary password that is generated by Amtelco Secure Messages to be used to log into Amtelco Secure Messages from the Amtelco Secure Messages Contact Web or from one of the Amtelco Secure Messages apps. After logging in with the temporary password, the user will be prompted to choose a new password.

The temporary password e-mail is configured under the Reset Temporary Password tab in the Email Messages Group Properties.

To e-mail a temporary Amtelco Secure Messages password to enable the contact to login in to the Amtelco Secure Messages Contact Web or the Amtelco Secure Messages apps and change his or her password, click the Email Temporary Password button.

In order to log into Amtelco Secure Messages, the contact will be required to enter the temporary password. After entering the temporary password, the contact will be prompted to choose a new password.

Group Options

☑ Active

The "Active" check box is used to activate or block a contact from logging into this group. Contacts are inactive until they register using an Email Registration hyperlink or an Account ID.

- **To prevent this contact from logging into this group, clear the Active check box.**
- **To allow this contact to log into this group, select the Active check box.**

☑ Visible

The "Visible" check box is used to show or hide the contact in the Contact list in the Amtelco Secure Messages apps. Contacts are visible by default.

- **To hide this contact from the Contact list, clear the Visible check box.**
- **To display this contact in the Contact list, select the Visible check box.**

IS Agent Login

The IS Agent Login is used to access the optional Amtelco Secure Messages Status and OnCall features for users whose Amtelco Secure Messages username and password do not match their IS Agent Login Name and Password.

- The Amtelco Secure Messages Status feature requires an IS Server and the IS Directory Contacts feature. The Status feature enables the user to change his or her status using the Amtelco Secure Messages app.

- The Amtelco Secure Messages OnCall feature requires an IS Server and the IS Directory OnCall feature. The OnCall feature enables 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 Amtelco Secure Messages Status and OnCall features.

- **If the contact's Amtelco Secure Messages 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 Amtelco Secure Messages 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.**

Change Password

The Change Password button is used to change the password used to log into the IS Server when a user tries to access the optional Amtelco Secure Messages Status and OnCall features.

If the contact's Amtelco Secure Messages username and password do not match an IS Agent Login Name and Password, click the Change Password button.

The Password field and ReType Password fields are displayed.

Password

Type the user's IS Agent Password as it is configured in the IS Supervisor application.

Confirm Password

Type the same password.

Personal Circle Settings

The Personal Circle Settings are used to edit this contact's Personal Circle. Personal Circles can be named under the General tab in Group Properties.

The Personal Circle Settings pane is labeled with the name of the Personal Circle as specified under the General tab in Group Properties

The names and phone numbers of the contacts in this contact's Personal Circle are displayed.

- **To add contacts and roles to the Personal Circle, click the Add Contact button.**

  The Contacts window is displayed.

  #### Contacts

  The Contacts window displays the names of contacts that have been registered for the selected group and roles for that group.

  Select the check boxes next to the names of the contacts and roles that you want to add.

  Clear the check box next to the names of the contact and roles you want to remove.

  When you have finished selecting contacts and roles, click the Save button.

  The selected contacts' names and roles are displayed in the Personal Circle Settings pane.

- **To remove a contact from the Personal Circle, click the X next to the contact's name or role.**

Saving Your Changes

Contact Group Settings are saved separately from the Contact Settings.

To save your changes to the Contact Group Settings and return to the Contact Settings page, click the Save button.

OR

To return to the Contacts Settings page without saving your Contact Group Settings changes, click the Exit button.

The Contact Settings page is displayed.

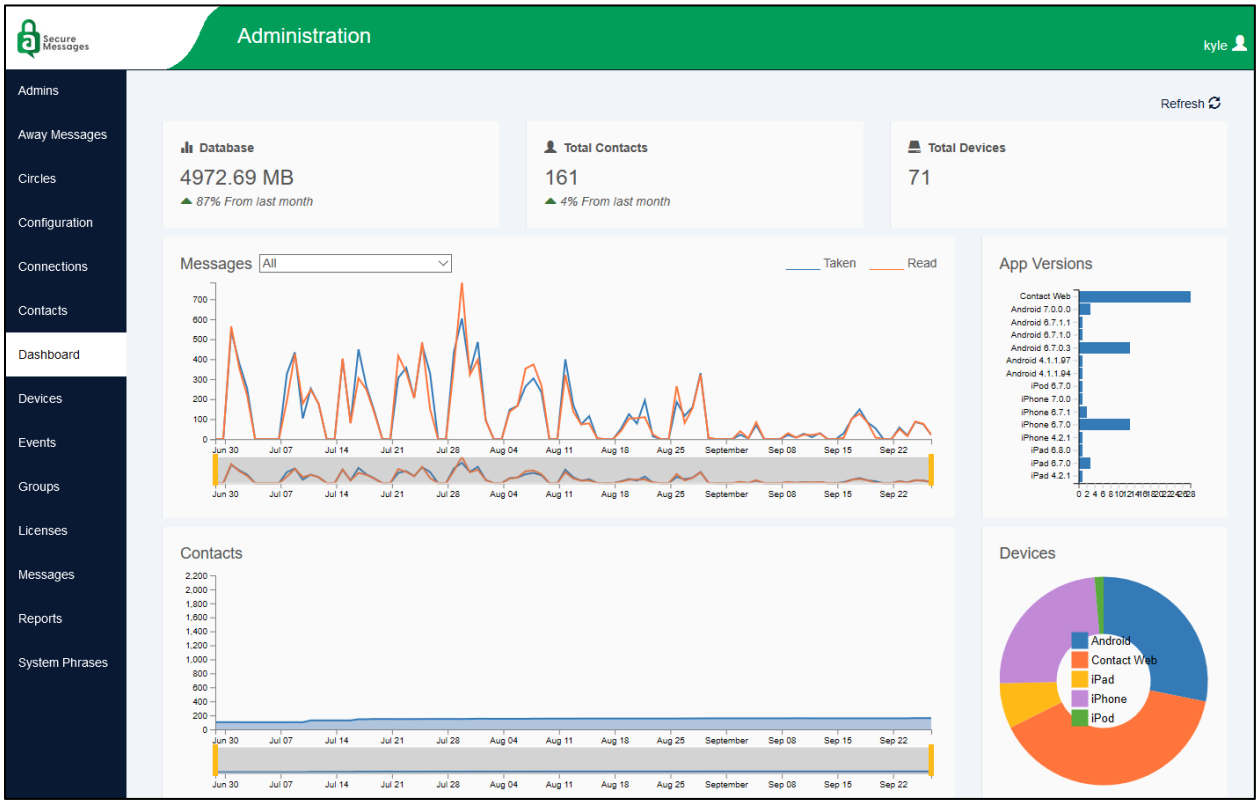
Return to Contact Settings

Return to Index

Dashboard

The Dashboard page is used to monitor Amtelco Secure Messages system, contact, and device information and activity.

Click the Dashboard command on the navigation menu to access the Dashboard page.



Refreshing the Dashboard

The Refresh icon in the top-right corner of the screen is used to refresh the Dashboard.

To refresh the Dashboard, click the Refresh icon.

Database

The Database pane monitors how much space is available in the database.

A green up arrow icon is displayed if the available space in the database has increased from the previous month.

A red down arrow icon is displayed if the available space in the database has decreased from the previous month.

Note: When Amtelco Secure Messages users are added into the database, the database availability will decrease.

Total Contacts

The Total Contacts pane indicates the total number of contacts in the Amtelco Secure Messages database.

A green up arrow icon is displayed if the total contacts registered in the database increased from the previous month.

A red down arrow icon is displayed if the total number of contacts registered in the database decreased from the previous month.

Total Devices

The Total Devices pane indicates the total number of devices registered in the Amtelco Secure Messages database.

Messages

The Messages pane indicates the relationship between taken messages and read messages. The message data is displayed in a line graph.

The menu is used to filter the data by group.

Select "All" to display data for all groups.

OR

Select a group name to display the data for that group only.

"Taken" indicates the number of secure messages in the Amtelco Secure Messages database that have been sent. Taken messages are marked by a blue line on the line graph.

"Read" indicates the number of secure messages in the Amtelco Secure Messages database that have been read. Read messages are marked by an orange line on the line graph.

The yellow slider bars are used to adjust the date range that is displayed on the graph.

- **Click and drag the slider bar on the left to set the start date.**
- **Click and drag the slider bar on the right to set the end date.**

App Versions

The App Versions pane indicates the version numbers of the Amtelco Secure Messages app that are installed on devices. The number of devices using each version is displayed in a bar graph.

Click a bar of the graph to display the type of device, version number, and number of devices indicated by that bar.

Contacts

The Contacts pane indicates the number of registered contacts in the Amtelco Secure Messages database over a period of time. The registered contact data is displayed in a line graph.

The yellow slider bars are used to adjust the date range that is displayed on the graph.

- **Click and drag the slider bar on the left to set the start date.**
- **Click and drag the slider bar on the right to set the end date.**

Devices

The Devices pane indicates the count of each type of device registered in the Amtelco Secure Messages database. Possible device types include Android, Contact Web, iPhone, iPad, and iPod. The device data is displayed in a pie chart.

Point to a section of the pie chart to display the device type, the number of devices of that type, and the percentage of all registered devices represented by that section of the pie chart.

Messages By Group

The Messages By Group table displays message information about Amtelco Secure Messages groups.

Column	Description
Group	Group indicates the Amtelco Secure Messages group name.
Taken	Taken messages indicate the number of secure messages in the Amtelco Secure Messages group database that have been sent.
%Change	%Change indicates the percent change of taken messages from the previous month. A green up arrow icon ▲ is displayed if the group taken messages in the database increased from the previous month. A red down arrow icon ▼ is displayed when the group taken messages in the database decreased from the previous month.
Read	Read indicates the number of secure messages in the Amtelco Secure Messages group database that have been read.
%Change	%Change indicates the percent change of taken messages from the previous month. A green up arrow icon ▲ is displayed if the group read messages in the database increased from the previous month. A red down arrow icon ▼ is displayed when the group read messages in the database decreased from the previous month.

Event Log

The Event Log table displays message information about Amtelco Secure Messages events.

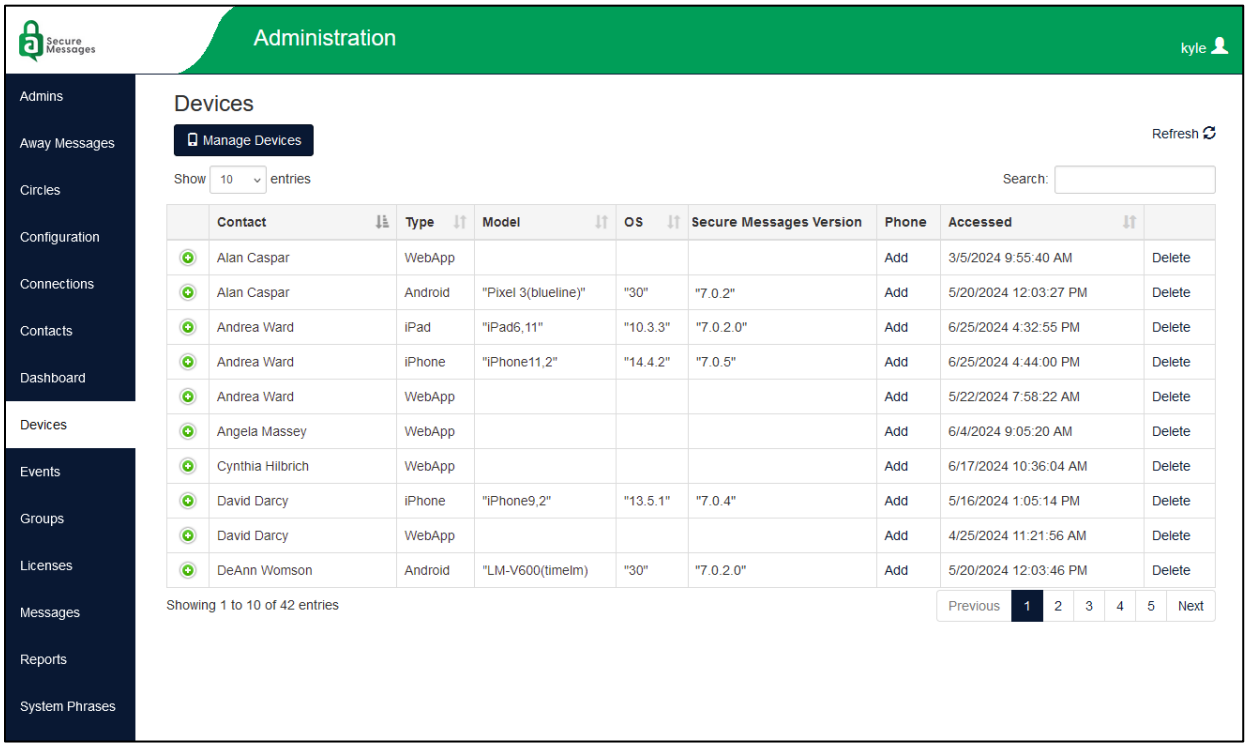
Column	Description
Time	Time indicates the date and time the event occurred.
Event	Event indicates a description of the event.

Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

Devices

The Devices page is used to view a list of the devices registered for Amtelco Secure Messages.

Click the Devices command on the navigation menu to access the Devices page.



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 Amtelco Secure Messages app settings or programmed in the Amtelco Secure Messages Admin Web Contact Settings.
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.
OS	OS indicates the operating system running on the device, if available, or the API Level for Android devices.
Secure Messages Version	Secure Messages Version indicates the version number of the Amtelco Secure Messages app that is installed on the device, if available.

Column	Description
Phone	The Phone column displays the phone number assigned to the device, or an Add hyperlink that can be used to add a phone number to the device. The phone number assigned to a device is displayed in the Amtelco Secure Messages apps in place of the contact phone number when the contact is logged into a Shared Device. This allows Amtelco Secure Messages users to call a contact person who doesn't use the same device every day.
Accessed	Accessed indicates the date and time that the Amtelco Secure Messages 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, type, model, app version, operating system, 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 the Refresh icon**
- **To view the details pane, click the Expand icon.**
- **To hide the details pane, click the Collapse icon.**

Adding a Device Phone Number

Device phone numbers can be used with the Shared Device feature to allow Amtelco Secure Messages users to call a contact person who doesn't use the same device every day. The device phone number is displayed in the Amtelco Secure Messages apps on the Contact Info page for the contact who is logged into the Amtelco Secure Messages app on that device.

To add a phone number to a device, click the Add hyperlink in the same row of the table as that device's information.

The Device Phone Number dialog box is displayed.

Type the device's phone number into the Phone Number field.

Click the Save button to save your changes.
OR
Click the Cancel button to discard your changes.

If you clicked Save, the phone number is displayed as a hyperlink in the Devices table.

Editing or Removing a Device Phone Number

To edit or remove a device's phone number, click the phone number hyperlink.

The Device Phone Number dialog box is displayed.

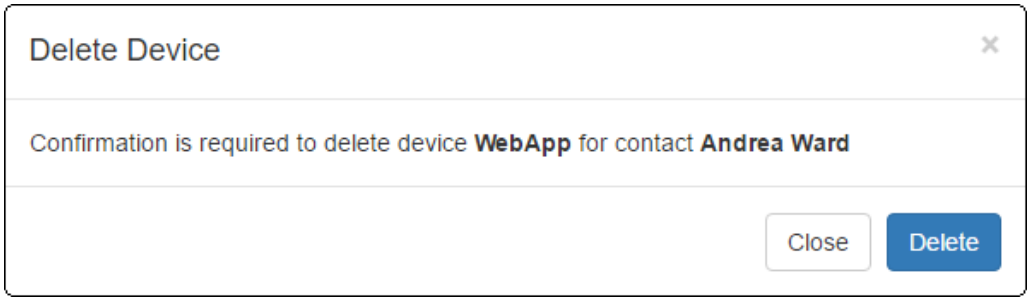
Edit or delete the phone number in the Phone Number field.

Click the Save button to save your changes.
OR
Click the Cancel button to discard your changes.

Deleting a Device

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

A confirmation dialog box is displayed.



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

To cancel the delete request, click the Close button.
OR
If you are sure you want to delete the device, click the Delete button.

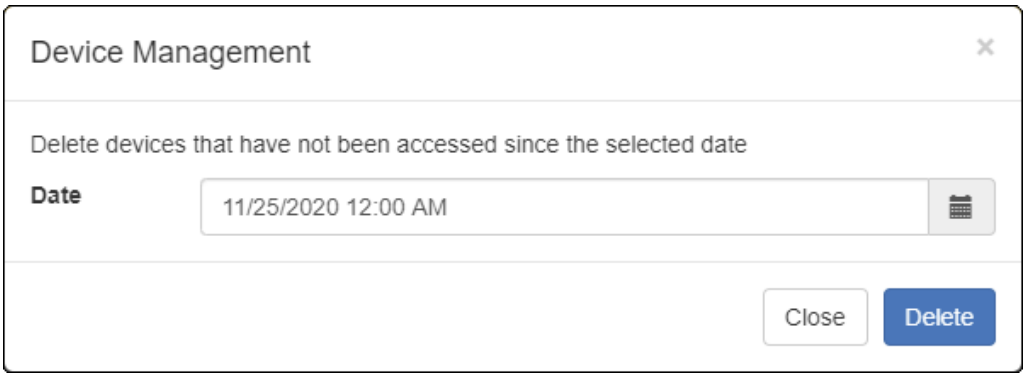
If you clicked the Delete button, the device is removed.

Managing Devices

The Manage Devices button provides the ability to mass delete devices that have not been accessed since a customizable date and time.

To remove unused devices, click the Manage Devices button.

The Device Management dialog box is displayed.



Date

The Date field is used to specify a date and time to compare to the accessed date for devices to determine which devices to delete. Any devices that have not been accessed since the date and time specified can be deleted by clicking the Delete button.

To change the 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 at the bottom of the calendar.**

  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 selected a date and time, click the Delete button.

A dialog box is displayed to verify that you want to delete all devices that have not been accessed since the specified date and time.

To cancel your delete request, click the No button.

OR

If you are certain you want to delete all devices that have not been accessed since the specified date and time, click the Yes button.

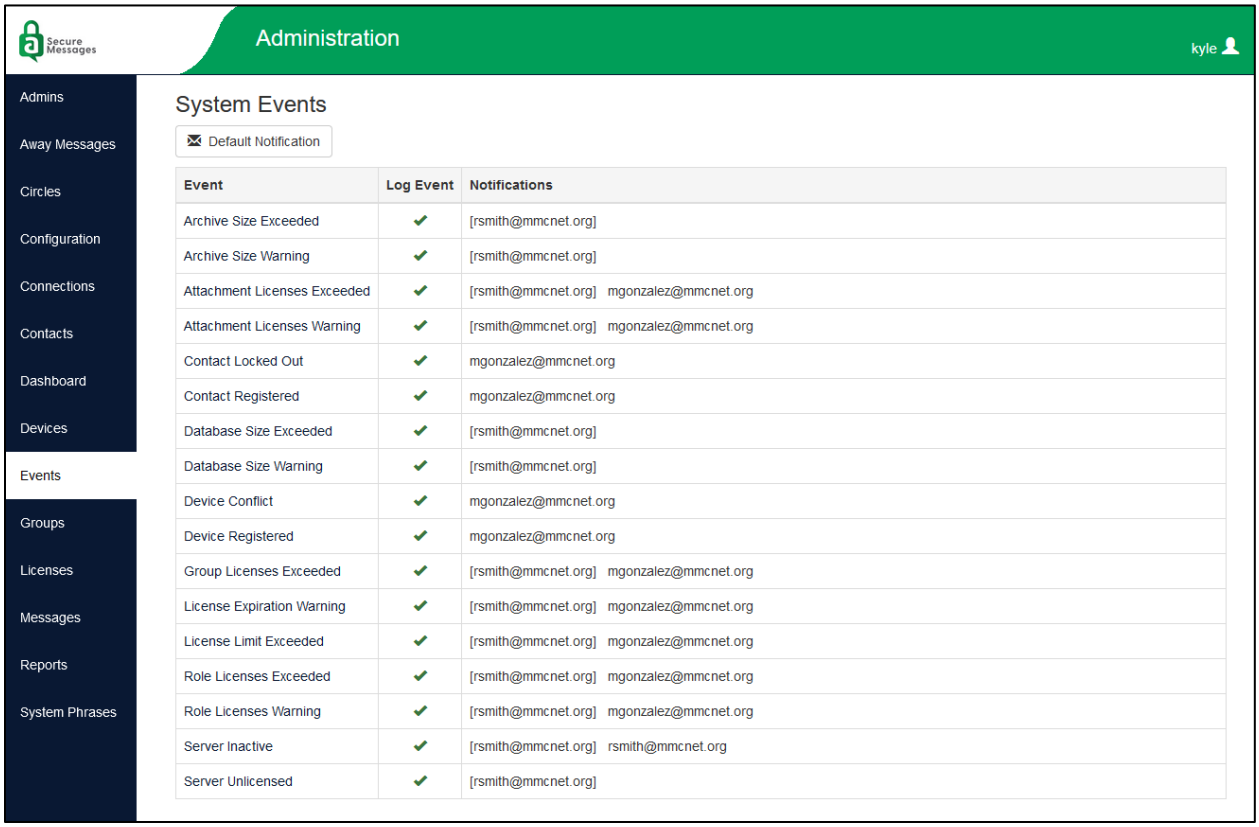
If you clicked the Yes button, all of the devices that have not been accessed since the date and time specified in the Device Management dialog box are deleted from the Amtelco Secure Messages database and are removed from the Devices table.

Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

System Events

The System Events page is used to configure e-mail notifications for specific Amtelco Secure Messages system events.

Click the Events command on the navigation menu to access the System Events page.



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

Column	Description
Event	The name of each event is displayed. Click the event name to configure the notification settings for that event.
Log Event	A green check mark in this column indicates notifications of this event type are logged whenever the event occurs and can be viewed in the Event Log Report.
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.

System Events

Event	Description
Archive Size Exceeded	The Archive Size Exceeded event sends a notification when an action attempts to exceed the disk space allotted for archives.
Archive Size Warning	The Archive Size Warning event sends a notification when the archive size reaches a specified threshold.
Attachment Licenses Exceeded	The Attachment Licenses Exceeded event sends a notification when a user registration attempts to exceed the number of attachment licenses purchased.
Attachment Licenses Warning	The Attachment Licenses Warning event sends a notification seven days before attachment licenses are due to expire.
Database Size Exceeded	The Database Size Exceeded event sends a notification when an action attempts to exceed the disk space allocated for the Amtelco Secure Messages database.
Database Size Warning	The Database Size Warning event sends a notification when the database size reaches a specified threshold.
Device Conflict	The Device Conflict event sends a notification when someone tries to register a device that is registered to another user.
Device Registered	The Device Registered event sends a notification whenever Amtelco Secure Messages is registered on a device.
Group Licenses Exceeded	The Group Licenses Exceeded event sends a notification when a user registration attempts to exceed the number of licenses allocated to a group.
License Expiration Warning	The License Expiration Warning event sends a notification seven days before Amtelco Secure Messages licenses are due to expire.
License Limit Exceeded	The License Limit Exceeded event sends a notification when a user registration attempts to exceed the number of Amtelco Secure Messages licenses purchased.
Role Licenses Exceeded	The Role Licenses Exceeded event sends a notification when a user registration attempts to exceed the number of role licenses purchased.
Role Licenses Warning	The Role Licenses Warning event sends a notification seven days before role licenses are due to expire.

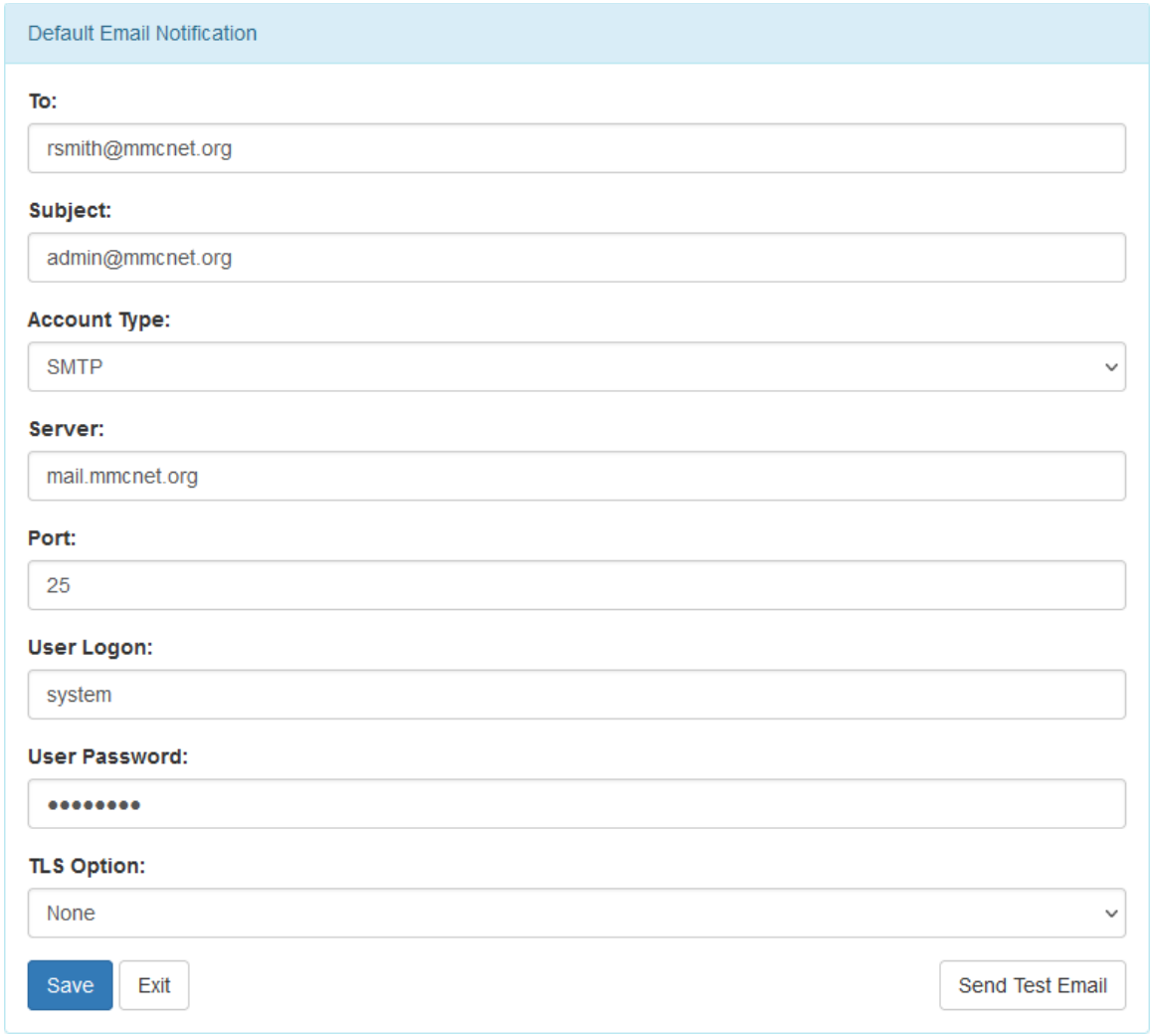
Event	Description
Server Inactive	The Server Inactive event is used with the optional High Availability feature. The Server Inactive event sends a notification when the Last Active date and time for an Amtelco Secure Messages server is more than 10 minutes old, provided there is another Amtelco Secure Messages server still active to send the notification. If both servers are down, or if the High Availability Feature is not configured, the Server Inactive event will not be able to send a notification.
Server Unlicensed	The Server Unlicensed event is used with the optional High Availability feature. The Server Unlicensed event sends a notification when an Amtelco Secure Messages Server is started up and there are not enough High Availability licenses available. The unlicensed server will run in Degraded Mode, meaning it won't process requests from the Amtelco Secure Messages apps.
User Locked Out	The User Locked Out event sends a notification when a user is locked out of Amtelco Secure Messages.
User Registered	The User Registered event sends a notification when a user registers for Amtelco Secure Messages.

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.

Subject

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

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

Account Type

The Account Type setting is used to specify the type of e-mail protocol that is used for event notifications. The following e-mail protocols may be used: Simple Mail Transfer Protocol (SMTP), Google Workspace, and Microsoft (MS) Graph Send.

Select the desired e-mail protocol to be used for event notifications.

The settings for the selected Account Type are displayed.

SMTP Account Settings

When SMTP is selected as the Account Type, the following settings are displayed.

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

Type the name of your mail server.

Port
The value in the Port 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.

User Logon
The value in the User Logon 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.

User Password
The value in the User Password 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.

TLS Option
The TLS Option setting is used to configure Transport Layer Security (TLS) and Secure Sockets Layer (SSL) protocol for event notifications.

- **Select "None" to disable the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) encryption.**

  If "None" is selected, the connection is not encrypted.

- **Select "Auto" to have the e-mail service decide if SSL or TLS protocol is used or no encryption is used.**

  If "Auto" is selected and the server does not support SSL or TLS, the connection continues without any encryption.

- **Select "SslOnConnect" to use the SSL or TLS encryption.**

  The "SslOnConnect" option uses SSL or TLS encryption. If the server does not support SSL or TLS, the connection fails.

- **Select "StartTls" to use TLS encryption only.**

  The "StartTls" option uses the STARTTLS extension to take an existing, insecure connection between the e-mail client and the e-mail server and turn it into a secure connection. This is done after the STARTTLS extension reads the greeting and the

capabilities of the server. If the server does not support STARTTLS, the connection fails and a "NotSupportedException" error is thrown.

- **Select "StartTlsWhenAvailable" to use TLS encryption if available but otherwise use no encryption.**

  The "StartTlsWhenAvailable" option uses the STARTTLS extension to take an insecure connection between the e-mail client and the e-mail server and turn it into a secure connection. This is done after the STARTTLS extension reads the greeting and the capabilities of the server. If the server does not support STARTTLS, the connection continues but is not encrypted.

Google Workspace Settings

When Google Workspace is selected as the Account Type, the following settings are displayed.

Service Account
The Service Account field determines the e-mail address of a Google Workspace service account.

Enter the e-mail address found on the Details page of your Google Workspace service account.

Cert Thumbprint
The Cert Thumbprint setting is used to specify the Google Workspace service account key.

Enter a key found on the Keys page of your Google Workspace service account.

User Name
The User Name field is used to specify the principal.

Enter the Principal found on the Principals tab on the Permissions page of your Google Workspace service account.

MS Graph Send Settings

When MSGraph Send is selected as the Account Type, the following settings are displayed.

Client id
The "Client id" setting is used to specify the Application (client) ID of your Microsoft account.

Enter the Application (client) ID found on the App Registrations, App Properties screen of your Microsoft account.

Tenant id
The "Tenant id" setting is used to specify the Directory (tenant) ID of your Microsoft account.

Enter the Directory (tenant) ID found on the App Registrations, App Properties screen of your Microsoft account.

Client Secret
The Client Secret field is used to specify the value of the secrets record.

Enter the Value found on the Certificates & Secrets page of your Microsoft account.

User Name
The User Name field is used to specify the username of an Azure Active Directory user who has been added to the allowed User and Groups of the Enterprise Application.

Enter the username of the Azure Active Directory user.

☑ *Save To Sent Items*

The Save To Sent Items option is used to save sent e-mail messages to the Microsoft account's Sent Items folder.

Select this check box to save sent e-mail messages to the Microsoft account's Sent Items folder.

OR

Clear this check box to disable saving sent e-mail addresses to the Microsoft account's Sent Items folder.

Send Test Email

When you have finished configuring the Email Notification Entries, click the Send Test Email button to test the default 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 the Save button to save your settings and return to the System Events page.

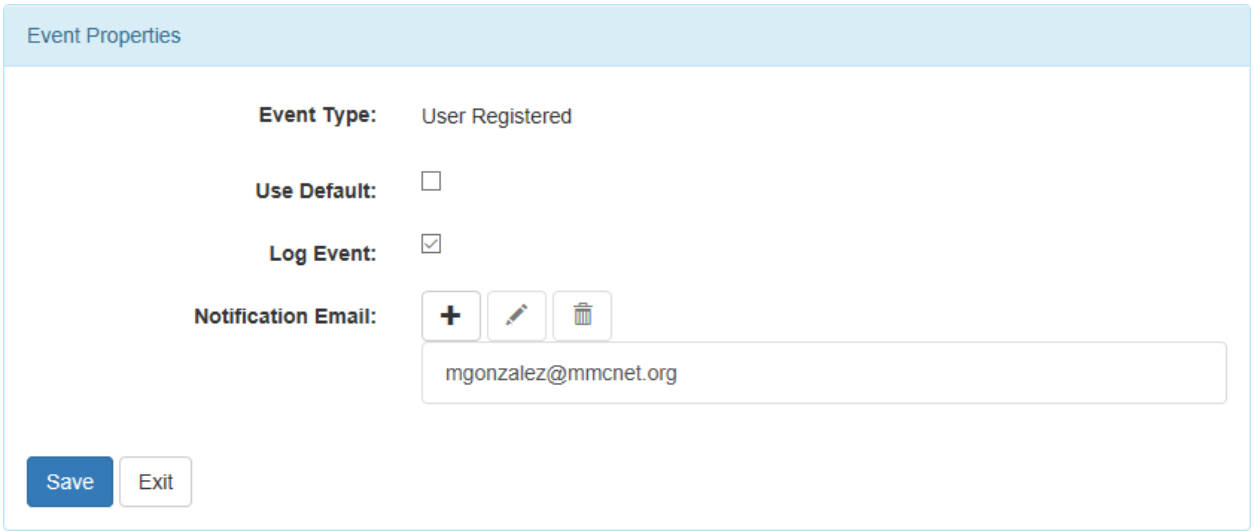
OR

To discard your changes, click the Exit button.

Configuring Event Notifications

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

The Event Properties pane is displayed.



Event Type

The name of the event is displayed.

☑ Use Default

If the Use Default 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.

Select the Use Default check box to use the Default Email Notification settings.

☑ Log Event

If the Log Event check box is selected, notifications of this event type are logged whenever the event occurs and can be viewed in the Event Log Report.

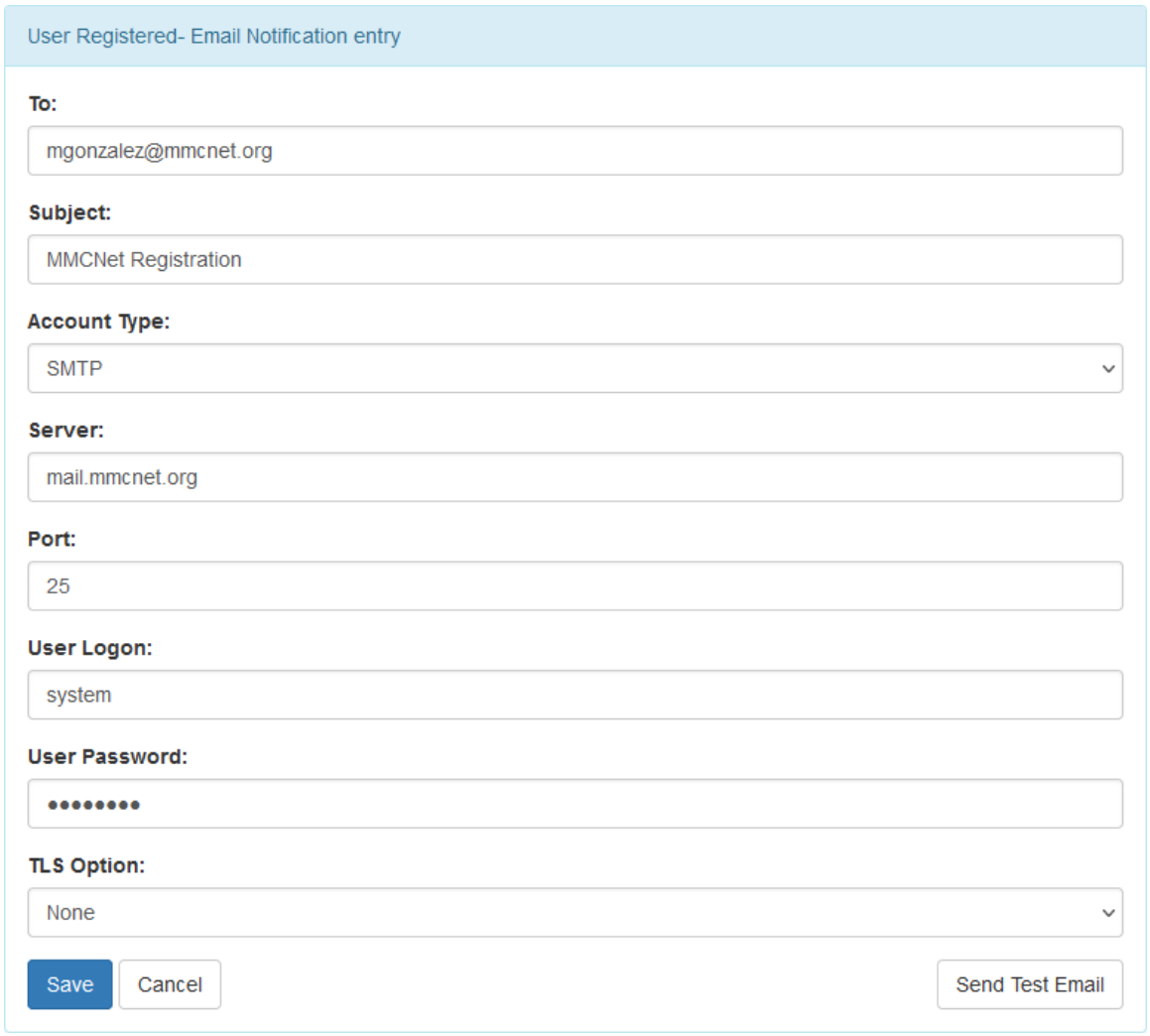
- **Select the Log Event check box to save this type of event notification in the event log.**
- **Clear the Log Event check box to exclude this type of event notification from the event log.**

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 the From 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 the Subject 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.

Account Type

The Account Type setting is used to specify the type of e-mail protocol that is used for event notifications. The following e-mail protocols may be used: Simple Mail Transfer Protocol (SMTP), Google Workspace, and Microsoft (MS) Graph Send.

Select the desired e-mail protocol to be used for event notifications.

The settings for the selected Account Type are displayed.

SMTP Account Settings

When SMTP is selected as the Account Type, the following settings are displayed.

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

Type the name of your mail server.

Port
The value in the Port 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.

User Logon
The value in the User Logon 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.

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

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

TLS Option
The TLS Option setting is used to configure Transport Layer Security (TLS) for event notifications.

- **Select "None" to disable the Transport Layer Security (TLS) and Secure Sockets Layer (SSL) encryption.**

  If "None" is selected, the connection is not encrypted.

- **Select "Auto" to have the e-mail service decide if SSL or TLS protocol is used or no encryption is used.**

  If "Auto" is selected and the server does not support SSL or TLS, the connection continues without any encryption.

- **Select "SslOnConnect" to use the SSL or TLS encryption.**

  The "SslOnConnect" option uses SSL or TLS encryption. If the server does not support SSL or TLS, the connection fails.

- **Select "StartTls" to use TLS encryption only.**

  The "StartTls" option uses the STARTTLS extension to take an existing, insecure connection between the e-mail client and the e-mail server and turn it into a secure connection. This is done after the STARTTLS extension reads the greeting and the capabilities of the server. If the server does not support STARTTLS, the connection fails and a "NotSupportedException" error is thrown.

- **Select "StartTlsWhenAvailable" to use TLS encryption if available but otherwise use no encryption.**

  The "StartTlsWhenAvailable" option uses the STARTTLS extension to take an insecure connection between the e-mail client and the e-mail server and turn it into a secure

connection. This is done after the STARTTLS extension reads the greeting and the capabilities of the server. If the server does not support STARTTLS, the connection continues but is not encrypted.

Google Workspace Settings

When Google Workspace is selected as the Account Type, the following settings are displayed.

Service Account
The Service Account field determines the e-mail address of a Google Workspace service account.

Enter the e-mail address found on the Details page of your Google Workspace service account.

Cert Thumbprint
The Cert Thumbprint setting is used to specify the Google Workspace service account key.

Enter a key found on the Keys page of your Google Workspace service account.

User Name
The User Name field is used to specify the principal.

Enter the Principal found on the Principals tab on the Permissions page of your Google Workspace service account.

MS Graph Send Settings

When MS Graph Send is selected as the Account Type, the following settings are displayed.

Client ID
The Client ID setting is used to specify the Application (client) ID of your Microsoft account.

Enter the Application (client) ID found on the App Registrations, App Properties screen of your Microsoft account.

Tenant ID
The Tenant ID setting is used to specify the Directory (tenant) ID of your Microsoft account.

Enter the Directory (tenant) ID found on the App Registrations, App Properties screen of your Microsoft account.

Client Secret
The Client Secret field is used to specify the value of the secrets record.

Enter the Value found on the Certificates & Secrets page of your Microsoft account.

User Name
The User Name field is used to specify the username of an Azure Active Directory user who has been added to the allowed User and Groups of the Enterprise Application.

Enter the username of the Azure Active Directory user.

☑ *Save To Sent Items*
The Save To Sent Items option is used to save sent e-mail messages to the Microsoft account's Sent Items folder.

Select this check box to save sent e-mail messages to the Microsoft account's Sent Items folder.
OR
Clear this check box to disable saving sent e-mail addresses to the Microsoft account's Sent Items folder.

Send Test Email

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 Save button to save your Notification Email settings and return to the Event Properties pane.

OR

To discard your Notification Email changes, click the Cancel button.

When you have finished configuring the Event Properties, click the Save button to save your Use Default and Log Event settings and return to the System Events page.

OR

To discard your changes to the Use Default and Log Event settings, click the Exit button.

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

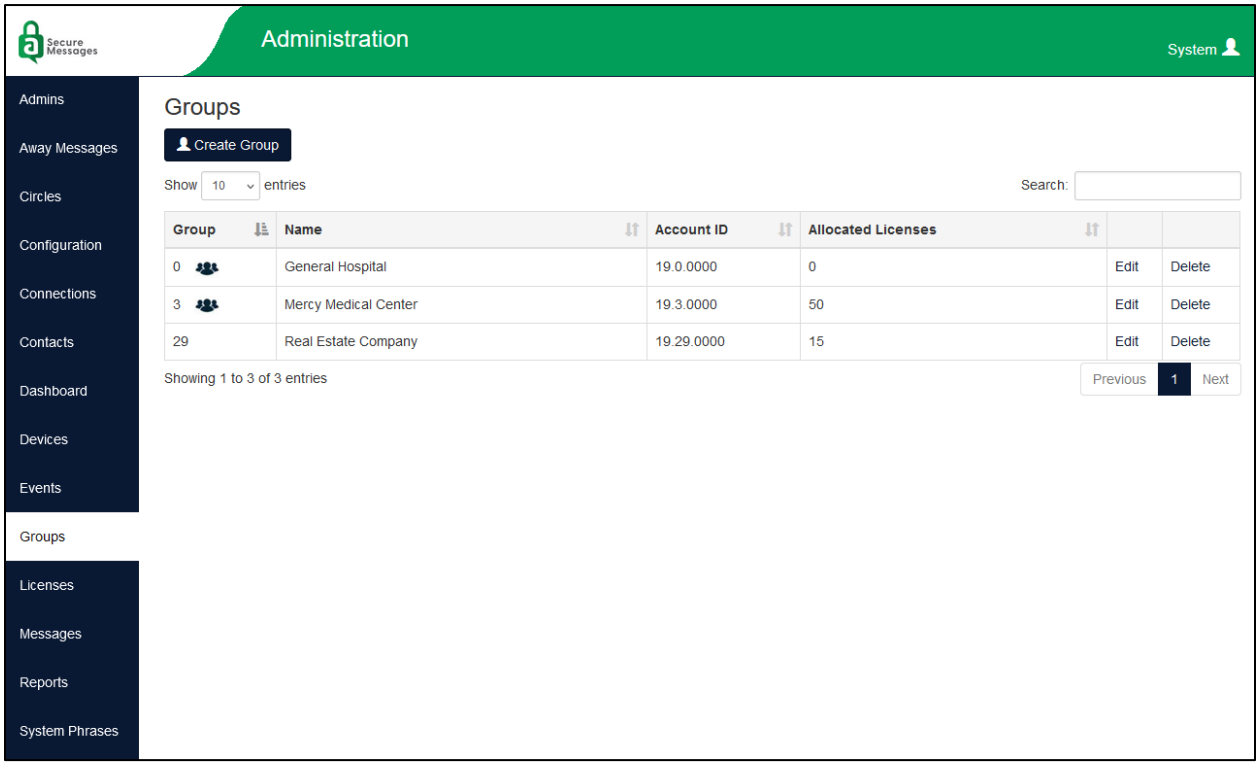
Return to Navigating in Amtelco Secure Messages Admin Web

Return to Index

Groups

The Groups page is used to create, edit, and delete Amtelco Secure Messages groups, referred to as “Accounts” in the Amtelco Secure Messages apps. The Groups page is also used to change which contacts are registered for each group, configure permission settings for each group, and create, edit, and delete group phrases.

Click the Groups command on the navigation menu to access the Groups page.



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

The Amtelco Secure Messages groups that have been created for your account are displayed in a table on the Groups page. By default, a group named “Group 0” is created for your main license. This group can be renamed.

Groups

Column	Description
Group	The Group column displays the unique number that identifies the group. The roles icon is displayed for groups with the optional Role-Based Messaging feature enabled.
Name	Name indicates the name of the group. The group name is displayed as the Account Name in the Amtelco Secure Messages apps and the Amtelco Secure Messages Contact Web. Users select an Account Name to switch from one account to another.
Account ID	The Account ID column displays the Account ID number used to register devices for the group.
Allocated Licenses	Allocated Licenses is the maximum number of devices and Contact Web users that can register for Amtelco Secure Messages app using this Account ID. A value of 0 (zero) is displayed for Group 0 because Group 0 uses all available licenses.

- **To sort the Groups table by group number, name, Account ID, or maximum number of licenses, click the appropriate column heading.**
- **To change the number of groups that are displayed, click the Show menu and select the number of groups to display.**
- **To search for a group, click the Search field and type the information that you want to find.**
- **To view the next page of groups, click Next.**
- **To the previous page of groups, click Previous.**
- **To view a specific page of groups, click the page number.**

Adding and Editing Groups

- **To add a group, click the Create Group button.**

  The General Group Properties for the new group are displayed.

- **To view or edit a group's Group Properties, click the Edit hyperlink in the same row of the table as that group's information.**

  The Group Properties for the selected group are displayed. For each group, the properties are divided into tabs: General, Password/Passcode, Contacts, Device Menu, Permissions, Phrases, Roles and Email Messages.

When you are finished editing Group Properties, click Exit to return to the Groups table.

Deleting a Group

To remove a group, click the Delete hyperlink in the same row of the table as that group's information.

A dialog box is displayed to confirm the delete request.

To cancel the delete request, click the Cancel button.

OR

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

If you clicked the Delete button, the group is removed from the table.

Note: When you delete a group, any devices that were registered for the Amtelco Secure Messages app using that group's Account ID will have to be reregistered using a different Account ID if not already registered for a different group.

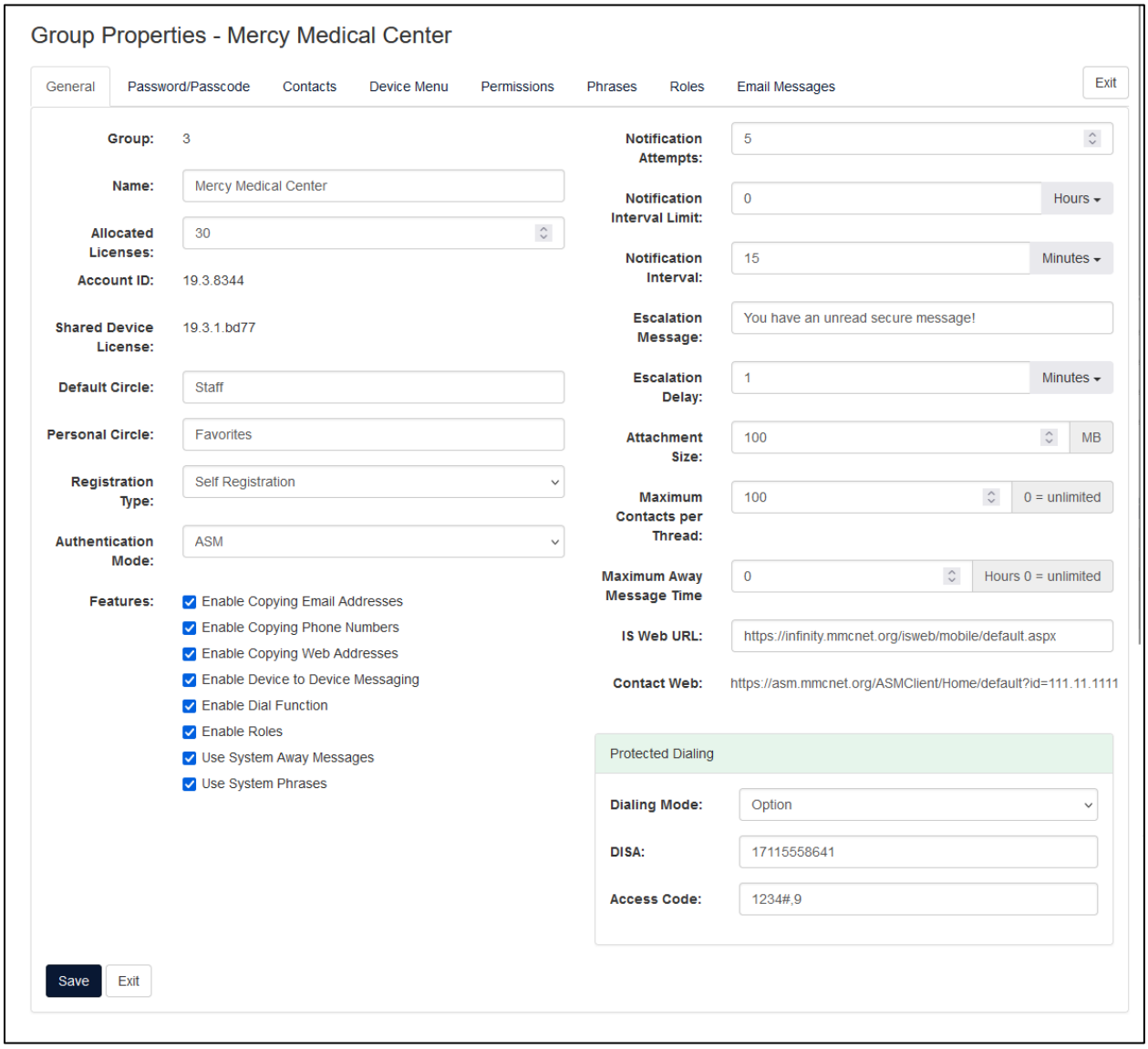
General
Password/Passcode
Contacts
Device Menu
Permissions
Phrases
Roles
Email Messages

Return to Adding and Editing Amtelco Secure Messages Admin Web Administrators
Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

General

The settings under the General tab are used to edit general Group Properties.

If the General Group Properties are not displayed, click the General tab.



Group

The Group is a unique number that identifies the group.

Name

Name indicates the name of the group. The group name is displayed as the Account Name in the Amtelco Secure Messages apps and the Amtelco Secure Messages Contact Web. Users select an Account Name to switch from one account to another.

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

Allocated Licenses

The Allocated Licenses setting determines the maximum number of devices and Contact Web users that can register for Amtelco Secure Messages app using this Account ID. The number of devices and Contact Web users allowed to register for each group 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 Allocated Licenses setting is not displayed when Group 0 is selected because Group 0 uses all available licenses by default.

Account ID

Account ID indicates the Account ID number used to register devices for the group.

Shared Device License

Shared Device License indicates the Account ID number used to register Shared Devices for the group.

Shared Device Account ID numbers allow devices to be registered for use by multiple Amtelco Secure Messages users. An Amtelco Secure Messages Admin Web administrator username and password with SystemAdmin access is required to add a Shared Device Account ID to a device. Once the device has been registered as a Shared Device, users are prompted with a Login screen that asks for their Amtelco Secure Messages username and password.

Users are able to log into a device at the start of their shift and log out of it at the end of their shift, allowing another person to use the device. This feature enables healthcare organizations to provide their employees with a pool of devices to use at work and keep personal devices off of the network.

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.

Personal Circle

The Personal Circle setting is used to create a Personal Circle that will be displayed in the Contacts List for this group. The Personal Circle acts as a favorites area to which each user can add their own favorite contacts and roles. If this setting is left blank, the Personal Circle feature will not be displayed.

- **To make a Personal Circle available for this group, type the text that you want to display as the name of the Personal Circle.**

  Example: “Favorites,” “My Favorites,” or “My Personal Circle.”

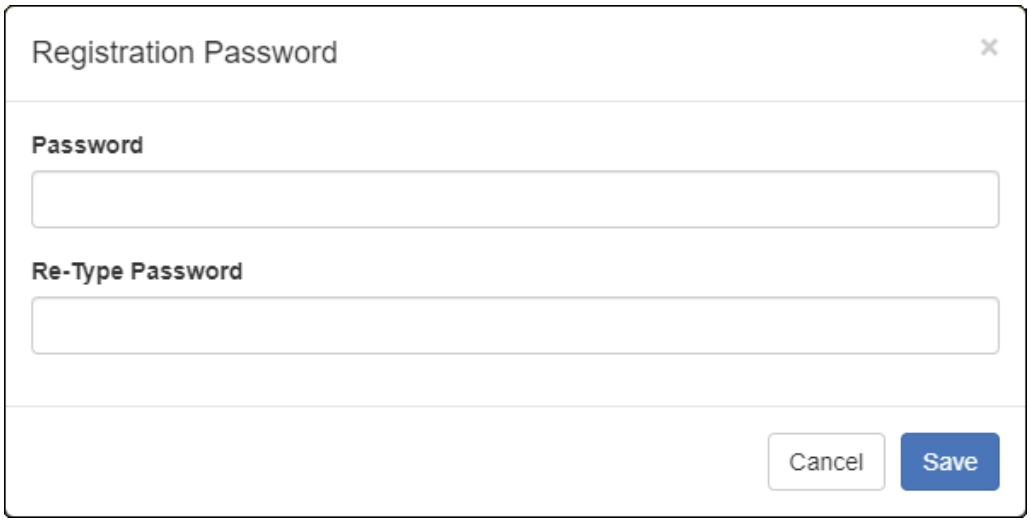
- **To disable the Personal Circle feature for this group, leave this field blank.**

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 Amtelco Secure Messages 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 to a new group, type the password into the Registration Password field.**
- **To add a Registration Password or change the Registration Password for an existing group, 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.

Click the Save button to save your changes.
OR
To discard your changes, click the Close button.

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.

Registration Type

The Registration Type menu is used to select a registration method for the group's users. The options are Self Registration, Admin Registration, and Email Registration.

Select the type of registration that you want to use.

Registration Type	Description
Self Registration	This Self Registration option enables new users to self-register the Amtelco Secure Messages app by creating their own username and password. If this option is selected, users can self-register the Amtelco Secure Messages app on a device by entering an Amtelco Secure Messages Account ID and creating their own username and password. This method requires the least amount of setup work in the Amtelco Secure Messages Administrator application but requires the user to enter the most registration information.
Admin Registration	The Admin Registration option requires a registration password to register the device. The contact will need to be created by an administrator who knows the password. If the Admin Registration option is selected, usernames and passwords must be created in the Amtelco Secure Messages Administrator application. An administrator must register the devices by entering a Amtelco Secure Messages Account ID, the registration password, and the user's username and password in the Amtelco Secure Messages app on the device.
Email Registration	The Email Registration option sends an e-mail message to the user's e-mail address when the Email Registration button is clicked in the user's Contact Group Settings or the Send Email Registration button on the group's Contacts properties. The e-mail message contains a hyperlink that the contact can use to register for Amtelco Secure Messages. The registration e-mail is configured under the Initial Registration tab and the Multiple Device Registration tab in the Email Messages Group Properties. **Note:** The minimum operating system requirement for Email Registration on iOS devices is iOS 9.0.

Email Registration/Reset Timeout

This setting is used if Email Registration is chosen as the registration type. The Email Registration/Reset Timeout is the duration of time the hyperlink in the registration e-mail invitation is active after the invitation is sent.

Enter the time in hours, minutes, or seconds that the Amtelco Secure Messages Email Registration hyperlink should be active, and then select the appropriate unit of measurement from the menu.

Authentication Mode

The Authentication Mode setting determines how contacts in this group are able to log into Amtelco Secure Messages apps and the Contact Web. Each Amtelco Secure Messages group can be configured for one of two authentication modes: ASM (Amtelco Secure Messages) and SSO (Single Sign-On). SSO authentication requires a certificate from an SSO Identity Provider and the installation and configuration of the Amtelco Secure Messages Assertion Consumer Web. This feature has been tested with the following SSO Identity Providers: Active Directory Federation Services (ADFS) and Azure Active Directory (AD).

Note: The SSO option requires a certificate from a Single Sign-On Identity Provider. Contacts are identified by username, not e-mail address.

- **Select "ASM" to use the Amtelco Secure Messages server to keep track of passwords and perform authentication.**
- **Select "SSO" to use a Single Sign-On Identity Provider to keep track of passwords and perform authentication.**

Authentication Resource

The Authentication Resource setting is used to specify the Uniform Resource Locator (URL) of your Single Sign-On Provider when the Authentication Mode is set to "SSO."

If you are using SSO authentication, enter the URL specified by your Single Sign-On Identity Provider.

Features

The Features check boxes are used to enable or disable several Group Properties.

☑ *Allow Copying Email Addresses*
The "Allow Copying Email Addresses" setting allows contacts in this group to copy e-mail addresses in the Amtelco Secure Messages app.

Select this check box to enable contacts in this group to copy e-mail addresses in the Amtelco Secure Messages app.
OR
Clear this check box if you don't want contacts in this group to copy e-mail addresses in the Amtelco Secure Messages app.

☑ *Allow Copying Phone Numbers*
The "Allow Copying Phone Numbers" setting allows contacts in this group to copy phone numbers in the Amtelco Secure Messages app.

Select this check box to enable contacts in this group to copy phone numbers in the Amtelco Secure Messages app.
OR
Clear this check box if you don't want contacts in this group to copy phone numbers in the Amtelco Secure Messages app.

☑ *Allow Copying Web Address*
The "Allow Copying Web Address" setting allows contacts in this group to copy web addresses in the Amtelco Secure Messages app.

Select this check box to enable contacts in this group to copy web addresses in the Amtelco Secure Messages app.
OR
Clear this check box if you don't want contacts in this group to copy web addresses in the Amtelco Secure Messages app.

☑ *Enable Device to Device Messaging*
The "Enable Device to Device Messaging" setting allows contacts in this group to send secure messages to each other from their mobile devices and the Amtelco Secure Messages Contact Web. If this setting is not selected, Amtelco Secure Messages users can only receive and reply to messages sent from IS and Infinity.

Select this check box to enable contacts in this group to send secure messages to each other from their mobile devices and the Amtelco Secure Messages Contact Web.

OR

Clear this check box to enable contacts in this group to only receive and reply to messages sent from IS and Infinity.

In both cases, secure messages can be initiated from IS and Infinity.

☑ *Enable Dial Function*

The "Enable Dial Function" setting allows contacts in this group to use the phone dial function on the Phone Dialer page in the Amtelco Secure Messages app. If this setting is not selected, the Phone Dialer page will be hidden for contacts in this group.

Select this check box to enable contacts in this group to use the phone dial function on the Phone Dialer page.

OR

Clear this check box if you don't want contacts in this group to use the phone dial function on the Phone Dialer page.

☑ *Enable Roles*

The "Enable Roles" setting enables the optional Role-Based Messaging feature for this group. The available roles for this group can be configured under the Roles tab in Group Properties.

Select this check box to enable Role-Based Messaging for this group.

OR

Clear this check box to disable Role-Based Messaging for this group.

☑ *Use System Away Messages*

The "Use System Away Messages" setting allows contacts in this group to access the system away messages defined on the Away Message page.

Select this check box to enable contacts in this group to select system away messages.

OR

Clear this check box if you don't want contacts in this group to use the system away messages.

☑ *Use System Phrases*

The "Use System Phrases" setting allows contacts in this group to access the system Quick Phrases defined on the System Phrases page.

Select this check box to enable contacts in this group to select system Quick Phrases.

OR

Clear this check box if you don't want contacts in this group to use the system Quick Phrases.

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 Notification Attempts setting in the Contact Settings for each contact.

Enter the maximum number of notifications that Amtelco Secure Messages 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 Limit

The Notification Interval Limit setting specifies the maximum number of hours, minutes, or seconds to which contacts can set their Notification Interval in the Contact Settings.

Enter the maximum number of hours, minutes, or seconds to allow contacts to select as their Notification Interval, and then select the appropriate unit of measurement from the menu.

Notification Interval

The Notification 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 Notification Interval setting in the Contact Settings for each contact.

Enter the number of hours, minutes, or seconds to wait between notification attempts, and then select the appropriate unit of measurement from the menu.

Escalation Message

The Escalation Message is a text message that is sent to the phone number of an Amtelco Secure Messages contact if that contact is sent a secure message and does not read it within the time specified by the Escalation Delay setting. The message should inform the contact that there is an unread secure message.

Note: This feature only functions for contacts that have a phone number specified in Contact Settings.

Enter a message to text to contacts who do not read a secure message before the Escalation Delay elapses.

Escalation Delay

The Escalation Delay setting is the amount of time to wait for a contact to read a secure message before texting the Escalation Message to the contact's phone number.

Enter the number of hours, minutes, or seconds to wait for a contact to read a secure message before texting the Escalation Message, and then select the appropriate unit of measurement from the menu.

Attachment Size

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

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

To enable attachments for this group, enter the maximum attachment size, in megabits, that you want to allow.

OR

To disable attachments for this group, set Attachment Size to zero (0).

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.

Maximum Away Message Time

The "Maximum Away Message Time" setting determines the maximum number of hours to which contacts can set their Away Message before it expires in the Amtelco Secure Messages app Notification Settings.

Enter the maximum number of hours to allow contacts to select as the duration of their Away Message.

Maximum Contacts Per Thread

The Maximum Contacts Per Thread setting specifies the maximum number of contacts that can be included when sending a message.

Enter the maximum number of contacts that Amtelco Secure Messages should allow when sending a secure message.

OR

Enter 0 (zero) to allow an unlimited number of contacts to be included when sending a secure message.

IS Web URL

The IS Web URL setting is used to specify the website for the mobile version of IS OnCall and Status that is displayed in the app when a user selects OnCall or Status in the app menu.

Enter the URL for the mobile version of the website for IS OnCall and Status.

Contact Web

Contact Web indicates the URL that customers can use to log into the Contact Web application as a member of this group.

Protected Dialing

Protected Dialing settings allow phone calls placed from the Amtelco Secure Messages App to be routed through Genesis, enabling users to keep their personal device's phone number private and to display their call center or organization's phone number.

Note: Genesis Protected Dialing requires Intelligent Series (IS) Server version 5.5 or later, Genesis 5.7 or later, the Protected Dialing feature, and the Auto Attendant feature.

(It is possible to use the Infinity DISA/RISA function to route phone calls through Infinity if you have the Internal PBX feature. For more information about Protected Dialing through Infinity, please contact Amtelco Field Service.)

Dialing Mode

Dialing Mode setting provides three options for dialing phone numbers from within the Amtelco Secure Messages apps.

Select Dialing Mode that you want to use.

Mode	Description
Phone	In Phone mode, phone numbers are dialed directly from the user's device, displaying the device's phone number.
DISA	DISA (Direct Inward System Access) mode uses a Genesis Direct Inward Dialing (DID) Phone Number and a Protected Dialing Passcode to create an overdial,

Mode	Description
	displaying the organization or call center's phone number rather than the device's phone number.
Option	In Option mode, each time the user places a call from the Amtelco Secure Messages App, the user can choose between "Dial direct" to dial directly from the device or "Mask my phone number" to use DISA to dial through Genesis.

DISA

The DISA field is used with the DISA and Option dialing modes to specify the Direct Inward Dialing (DID) phone number to the IS Client configured for the Protected Dialing behavior. The number should be followed by a pound sign (#). Commas can be added after the pound sign to pause the dialer for 2 seconds per comma if needed.

If using the DISA or Option Dialing Mode, enter the DID phone number assigned to your Protected Dialing Client, followed by the pound sign (#).

Add a comma (,) to the end if you need the dialer to pause before dialing the Access Code.

Access Code

The Access Code is an access code used with the DISA and Option dialing modes to provide access to Genesis dialing and to determine which IS Client is billed for the call. The Access Code must match the Protected Dialing Passcode configured on an IS Client, plus a pound sign (#) and any characters that are needed to dial out.

If using the DISA or Option Dialing Mode, enter the Protected Dialing Passcode for the desired IS Client, followed by the pound sign (#) and any characters needed to dial out.

Example: If the DID phone number assigned to your Protected Dialing Client was 17115551212, the Protected Dialing Passcode for the IS Client that you wanted to bill was 1234, the system needed a two-second pause between numbers, and your system required a 9 to dial out, you would use the following settings.

Dialing Mode: DISA

DISA: 17115551212#,

Access Code: 1234#9

When you have finished configuring General settings for the group, click the Save button to save your changes.

If you are creating a new group, the Password/Passcode, Contacts, Device Menu, Permissions, Phrases, Roles and Email Messages tabs for the group become available after you click the Save button.

Return to Groups

Return to Contact Group Settings

Return to Index

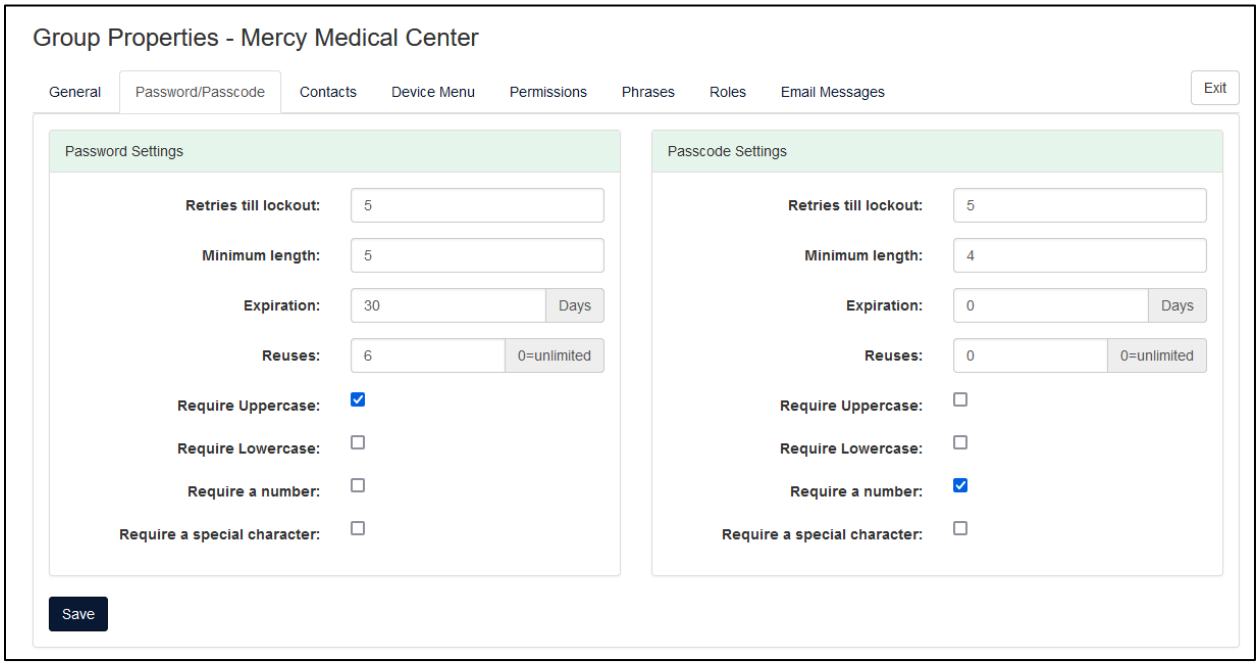
Password/Passcode

The settings under the Password/Passcode tab are used to set parameters for Amtelco Secure Messages passwords and passcodes for the group.

Note: When a group's Authentication Mode is set to "SSO," the Password/Passcode tab is replaced with a Passcode tab that contains the Passcode Settings but no Password Settings. With the SSO, a Single Sign-On Provider maintains passwords.

To edit password and passcode settings for a group, click the Password/Passcode tab.

The Password Settings and Passcode Settings panes are displayed.



Password Settings

Passwords are used to log into Amtelco Secure Messages when registering the Amtelco Secure Messages app on a device. Passwords are also used to log into the Amtelco Secure Messages Contact Web. The Password Settings are used to set parameters for Amtelco Secure Messages passwords and enable administrators to enforce complex password requirements.

Note: When a group's Authentication Mode is set to "SSO," the Password Settings are not displayed. With the SSO, a Single Sign-On Provider maintains passwords.

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 Amtelco Secure Messages until it is reset in the Contact Settings for that user.

Note: This setting should be set to greater than 4 to prevent connection issues.

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

Enter a number (greater than 4) of failed login attempts to allow before locking a username.
OR
Enter zero (0) to prevent lockouts.

Minimum Length

This setting enforces a minimum length for passwords.

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

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

Expiration

Expiration indicates the number of days a contact's password can be in effect before it expires. Expired passwords need to be changed in order to continue using Amtelco Secure Messages.

Enter the number of days that passwords are valid before expiring.

Reuses

The Reuses setting determines the number of unique passwords that must be set for a contact before the contact can reuse an old password.

Enter the number of unique passwords that must be set before a contact can reuse an old password.
OR
Enter zero (0) to always allow contacts to reuse old passwords.

☑ Require Uppercase

The "Require Uppercase" option requires passwords to contain at least one upper case letter.

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

☑ Require Lowercase

The "Require Lowercase" option requires passwords to contain at least one lower case letter.

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

☑ Require a number

The "Require a number" option requires passwords to contain at least one digit.

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

☑ Require a special character

The "Require a special character" option requires passwords to contain at least one of the following special characters:

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

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

Passcode Settings

The passcode is an optional security feature that requires a code to be entered each time the Amtelco Secure Messages app is opened on a device. The Passcode Settings are used to set

parameters for Amtelco Secure Messages passcodes and enable 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 Amtelco Secure Messages until it is reset in the Contact Settings for that user.

Note: This setting should be set to greater than 4 to prevent connection issues.

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

Enter a number (greater than 4) of failed passcode attempts to allow before locking a username.
OR
Enter zero (0) to prevent lockouts.

Minimum Length

This setting enforces a minimum length for passcodes.

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

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

Reuses

The Reuses setting determines the number of unique passcodes that must be set for a contact before the contact can reuse an old passcode.

Enter the number of unique passcodes that must be set before a contact can reuse an old passcode.
OR
Enter zero (0) to always allow contacts to reuse old passcodes.

☑ Require Uppercase

The “Require Uppercase” option requires passcodes to contain at least one upper case letter.

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

☑ Require Lowercase

The “Require Lowercase” option requires passcodes to contain at least one lower case letter.

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

☑ Require a number

The “Require a number” option requires passcodes to contain at least one digit.

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

☑ Require a special character

The “Require a special character” option requires passcodes to contain at least one of the following special characters:

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

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

When you have finished configuring Password Setting and Passcode Setting for the group, click the Save button to save your changes.

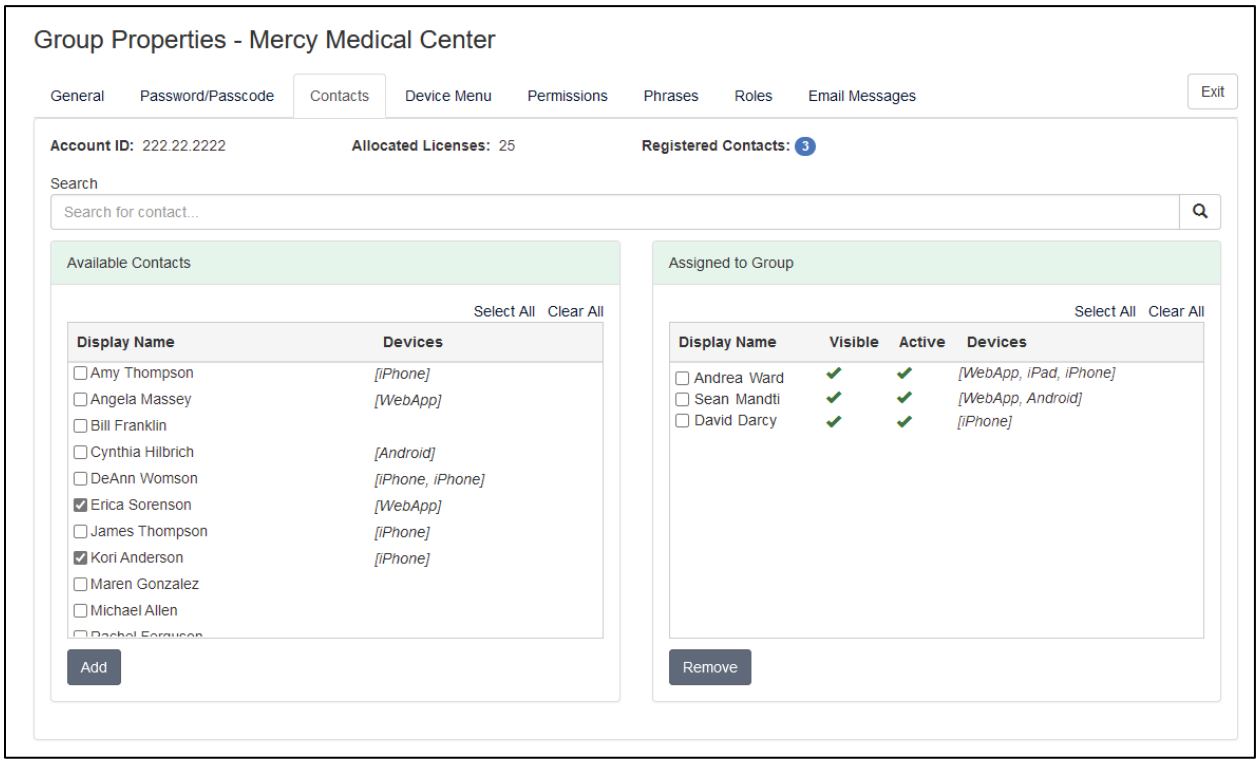
Return to General
Return to Groups
Return to Index

Contacts

The settings under the Contacts tab are used to register contacts for a group and to un-register contacts from a group.

To edit Contacts settings for a group, click the Contacts tab.

The Contacts Group Properties are displayed.



Account ID

Account ID indicates the Account ID 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 Amtelco Secure Messages app using this Account ID. The number of devices and Contact Web users allowed to register for each group 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.

Licensed Contacts

Licensed Contacts indicates the number of contacts that are registered for the group.

Search

The Search field is used to filter the Available Contacts menu and the Assigned to Group menu.

To search for contacts, type the information that you want to find into the Search field and either press the ENTER key or click the Search icon.

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.**
- **To select all contacts, click the Select All hyperlink.**
- **To deselect all contacts, click the Clear All hyperlink.**

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

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

Assigned to Group

The Assigned to Group menu displays the names and device types of contacts that are registered for the selected group. A Check Mark icon ✔ is displayed under the Visible column if the contact is marked visible for this group. A Check Mark icon ✔ is displayed under the Active column if the contact is marked active for this group. A contact's Visible and Active settings can be configured in the Contact Group Properties.

- **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 in the group, clear the check box next to the name of the contact.**
- **To select all contacts, click the Select All hyperlink.**
- **To deselect all contacts, click the Clear All hyperlink.**

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

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

Send Email Registration

The Send Email Registration button is displayed if the Registration Type under the General tab is set to "Email Registration" and one or more contacts are selected in the Assigned to Group menu.

To send a registration e-mail to the contacts selected in the Assigned to Group menu, click the Send Email Registration button.

The e-mail message contains a hyperlink that the contact can use to register for Amtelco Secure Messages. The registration e-mail is configured under the Initial Registration tab and the Multiple Device Registration tab in the Email Messages Group Properties.

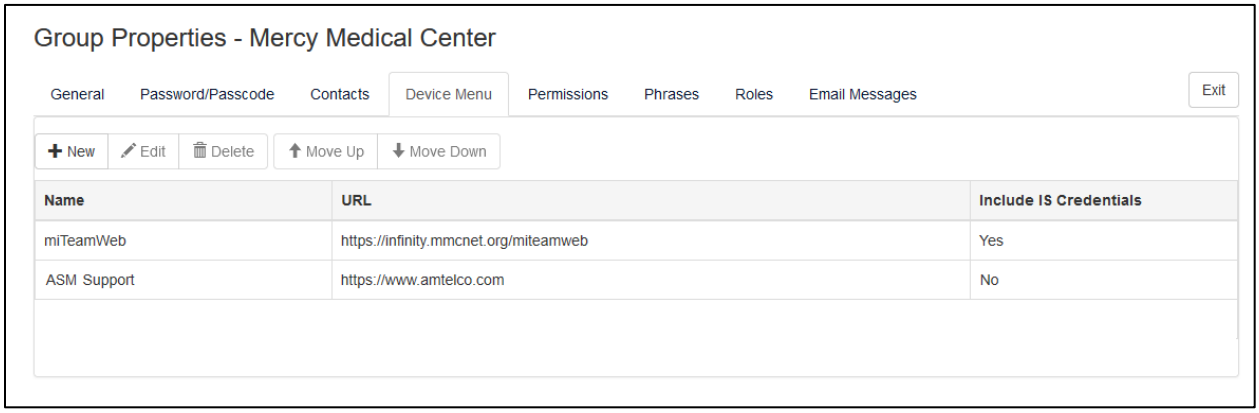
Return to General
Return to Groups
Return to Index

Device Menu

The settings under the Device Menu tab are used to add hyperlinks to internal or external websites to the app menu for this group. The hyperlinks will be displayed in the Links drop-down menu in the app menu.

To add app menu hyperlinks to a group, click the Device Menu tab.

The Device Menu Group Properties are displayed.



Device Menu Toolbar

The Device Menu Toolbar is displayed under the Device Menu tab. The Device Menu Toolbar is used to make changes to the hyperlinks that are displayed in the Amtelco Secure Messages app menu on devices of users registered to this group.

Icon	Description
	Click the **New** icon to add a new hyperlink.
	Click the **Edit** icon to edit the selected hyperlink.
	Click the **Delete** icon to delete the selected hyperlink.
	Click the **Move Up** icon to move the selected hyperlink closer to the top of the list.
	Click the **Move Down** icon to move the selected hyperlink closer to the bottom of the list.

Adding and Editing Device Menu Hyperlinks

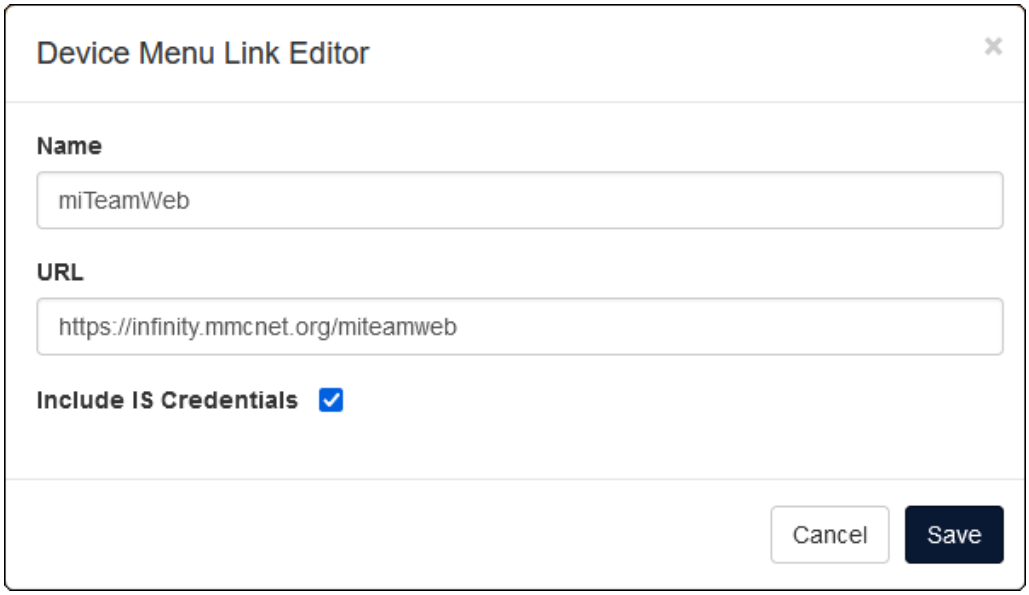
- **To add a hyperlink, click the New icon.**

  The Device Menu Link Editor window is displayed with blank properties.

- **To edit a hyperlink, click the hyperlink that you want to edit and then click the Edit icon.**

  The Device Menu Link Editor window displays the selected hyperlink properties.

Device Menu Link Editor



Name

The Name setting determines the text that will be displayed in the app menu for this hyperlink.

Type the display name for the hyperlink.

URL

The URL field specifies the Uniform Resource Locator (URL) that is launched when the hyperlink is touched, tapped, or clicked by the user.

Enter the URL of the website.

☑ Include IS Credentials

The "Include IS Credentials" check box is used to send a device user's IS Username and Password to the URL.

- **Select this check box if you want the device opening this webpage to send the device user's IS Username and Password to the URL.**

  Note: This setting only works when the URL is for the miTeamWeb application.
- **Clear this check box if you don't want to send the device user's IS Username and Password to the URL.**

Click the Save button.

The new or edited hyperlink is displayed in the table.

Repositioning a Hyperlink

To reposition a hyperlink, click the hyperlink to select it and then use the Move Up ↑ and Move Down ↓ icons to move the hyperlink to a new position in the table.

Deleting a Hyperlink

To remove a hyperlink, click the hyperlink 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 Cancel button.

OR

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

If you clicked the Delete button, the hyperlink is removed.

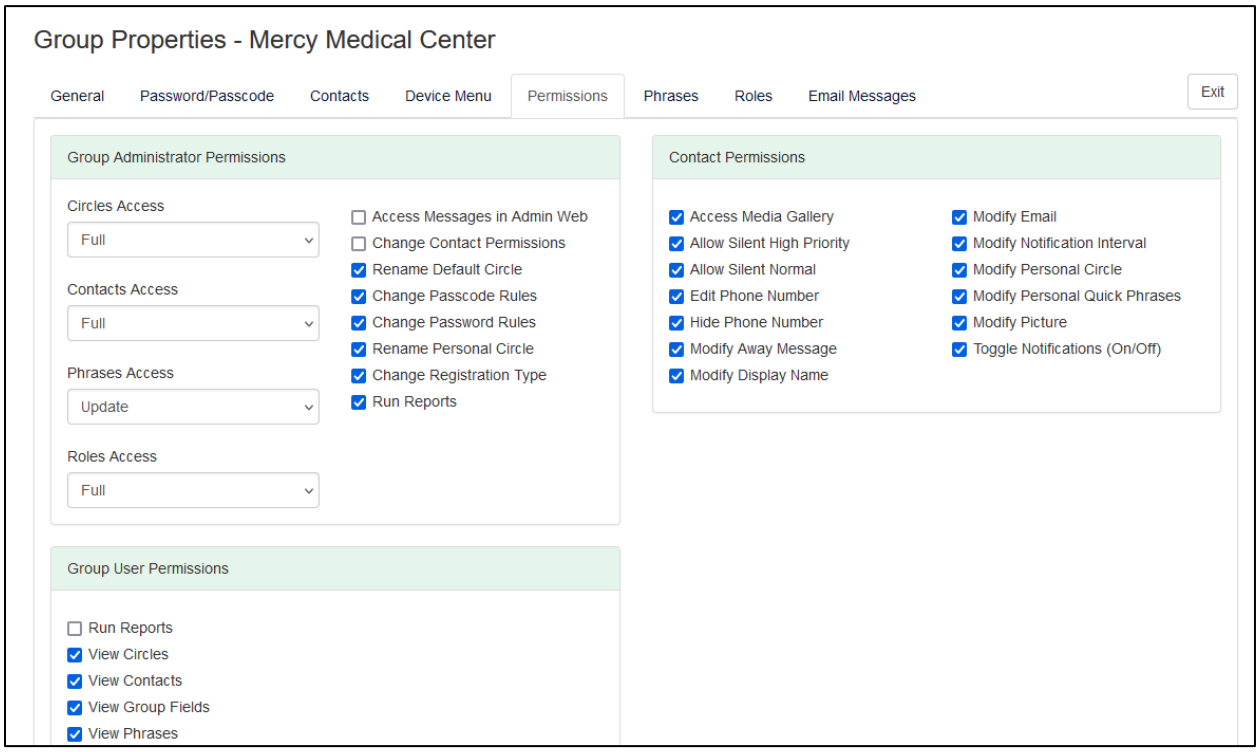
Return to General
Return to Groups
Return to Index

Permissions

The settings under the Permissions tab are used to edit permission settings for Group Administrators, Group Users, and contacts who have been registered to the group.

To edit Permissions settings for a group, click the Permissions tab.

The Permissions Group Properties are displayed.



Group Administrator Permissions

Group Administrator Permissions are used to configure permission settings for Amtelco Secure Messages Admin Web administrators whose access type is set to Group Administrator. All changes made to Group Administrator Permissions apply only to the group that is selected.

Circles Access

The Circles Access setting determines the information group administrators can view and edit on the Circles page of the Amtelco Secure Messages Admin Web. There are four levels of Circles Access.

Access Level	Description
None	When Circles Access is set to None, group administrators are unable to view Circles for this group.
View	When Circles Access is set to View, group administrators are able to view all Circles and Circle Details for this group.
Update	When Circles Access is set to Update, group administrators are able to view all Circles and Circle Details, and can update the Name setting for all Circles.

Access Level	Description
Full	When Circles Access is set to Full, group administrators are able to view Circles, update Circles, add contacts to Circles, remove contacts from Circles, and create and delete Circles.

Click the Circles Access field and select the appropriate access level for group administrators.

Contacts Access

The Contacts Access setting determines the information group administrators can view and edit on the Contacts page of the Amtelco Secure Messages Admin Web and under the Contacts tab in Group Properties. There are four levels of Contacts Access.

Access Level	Description
None	When Contacts Access is set to None, group administrators are unable to view the contacts registered to this group on the Contacts page. Additionally, the Contacts tab is not displayed in the Group Properties for this group.
View	When Contacts Access is set to View, group administrators are able to view the Contact Settings for all contacts registered to this group as well as the Contacts tab in the Group Properties for this group.
Update	When Contacts Access is set to Update, group administrators are able to view licensed contacts on the Contacts page and under the Contacts tab in the Group Properties as well as to update Contact Settings including the Name, Phone Number, Contact Photo, Notification, and IS settings for existing contacts. **Note:** If a contact belongs to multiple groups, the Group Administrator can update that contact's properties only if the Group Administrator has Update or Full permissions in all of that contact's groups.
Full	When Contacts Access is set to Full, group administrators are able to view and update Contact Settings for existing contacts as well as to create and delete contacts within this group. **Note:** If a contact belongs to multiple groups, the Group Administrator can update that contact's properties only if the Group Administrator has Update or Full permissions in all of that contact's groups and can delete that contact only if the Group Administrator has Full permission in all of that contact's groups.

Click the Contacts Access field and select the appropriate access level for group administrators.

Phrases Access

The Phrases Access setting determines the information group administrators can view and edit under the Phrases tab in Group Properties. There are four levels of Phrases Access.

Access Level	Description
None	When Phrases Access is set to None, the Phrases tab is not displayed in the Group Properties when accessed by group administrators.

Access Level	Description
View	When Phrases Access is set to View, group administrators are able to view existing group phrases under the Phrases tab in Group Properties.
Update	When Phrases Access is set to Update, group administrators are able to view, edit, and reorder all existing group phrases.
Full	When Phrases Access is set to Full, group administrators are able to view, edit, reorder, create, and delete group phrases.

Click the Phrases Access field and select the appropriate access level for group administrators.

Roles Access

The Roles Access setting determines the information group administrators can view and edit under the Roles tab in Group Properties. There are four levels of Roles Access.

Access Level	Description
None	When Roles Access is set to None, the Roles tab is not displayed in the Group Properties when accessed by group administrators.
View	When Roles Access is set to View, group administrators are able to view existing group roles under the Roles tab in Group Properties.
Update	When Roles Access is set to Update, group administrators are able to view and edit all existing group roles.
Full	When Roles Access is set to Full, group administrators are able to view, edit, create, and delete group roles.

Click the Roles Access field and select the appropriate access level for group administrators.

☑ Access Messages in Admin Web

The "Access Messages in Admin Web" setting allows group administrators to view messages for this group on the Message Information page.

Select this check box to enable group administrators to view messages for this group.
OR
Clear this check box if you don't want group administrators to view messages for this group.

☑ Change Contact Permissions

The "Change Contact Permissions" setting allows group administrators to edit the Contact Permissions settings under the Permissions tab in the Group Properties for this group.

Select this check box to enable group administrators to edit Contact Permissions for this group.
OR
Clear this check box if you don't want group administrators to edit Contact Permissions.

☑ Rename Default Circle

The "Rename Default Circle" setting allows group administrators to edit the Default Circle setting under the General tab in the Group Properties for this group.

Select this check box to enable group administrators to change the default Circle for this group.
OR
Clear this check box if you don't want group administrators to change the default Circle for this group.

☑ Change Passcode Rules

The "Change Passcode Rules" setting allows group administrators to view and edit the Passcode Settings under the General tab in the Group Properties for this group.

Select this check box to enable group administrators to view and edit Passcode Settings for this group.
OR
Clear this check box to prevent group administrators from viewing and editing Passcode Settings.

☑ Change Password Rules

The "Change Password Rules" setting allows group administrators to view and edit the Password Settings under the General tab in the Group Properties for this group.

Select this check box to enable group administrators to view and edit Password Settings for this group.
OR
Clear this check box to prevent group administrators from viewing and editing Password Settings.

☑ Rename Personal Circle

The "Rename Personal Circle" setting allows group administrators to change the name of the Personal Circle under the General tab in the Group Properties for this group.

Select this check box to enable group administrators to edit the Personal Circle name for this group.
OR
Clear this check box if you don't want group administrators to edit the Personal Circle name

☑ Change Registration Type

The "Change Registration Type" setting allows group administrators to edit the Registration Type under the General tab in the Group Properties for this group.

Select this check box to enable group administrators to edit the Registration Type setting for this group.
OR
Clear this check box if you don't want group administrators to edit the Registration Type setting.

☑ Run Reports

The "Run Reports" setting allows group administrators to run reports for this group.

Select this check box to enable group administrators to run reports for this group.
OR
Clear this check box if you don't want group administrators to run reports for this group.

Group User Permissions

Group User Permissions are used to configure permission settings for Amtelco Secure Messages Admin Web administrators whose access type is set to Group User. All changes made to Group User Permissions apply only to the group that is selected.

☑ Run Reports

The "View Reports" setting allows group users to run reports for this group.

Select this check box to enable group users to run reports for this group.
OR
Clear this check box if you don't want group users to run reports for this group.

☑ View Circles

The "View Circles" setting allows group users to view all Circles created for this group on the Circles page.

Select this check box to enable group users to view Circles for this group.
OR
Clear this check box if you don't want group users to view Circles for this group.

☑ View Contacts

The "View Contacts" setting allows group users are able to view the Contacts tab in Group Properties and view the Contact Settings for contacts registered for this group.

Select this check box to enable group users to view contacts and Contact Settings for this group.
OR
Clear this check box if you don't want group users to view contacts and Contact Settings for this group.

☑ View Group Fields

The "View Group Fields" setting allows group users to view the General tab in the Group Properties for this group.

Note: Password and Passcode Settings are available only to system administrators and group administrators when the Change Password Rules and Change Passcode Rules settings are enabled. Group users are unable to view Password Settings and Passcode Settings.

Select this check box to enable group users to view the General tab in the Group Properties for this group.
OR
Clear this check box to make the General tab unavailable to group users.

☑ View Phrases

The "View Phrases" setting allows group users to view the Phrases tab in the Group Properties for this group.

Select this check box to enable group users to view the Phrases tab in the Group Properties for this group.
OR
Clear this check box to make the Phrases tab unavailable to group users.

Contact Permissions

Contact Permissions are used to configure permission settings for contacts registered to this group.

☑ Access Media Gallery

The “Access Media Gallery” setting allows contacts in this group to access their device’s Photo Gallery from the Amtelco Secure Messages app to attach photos and videos to an Amtelco Secure Messages message. Disabling this feature forces users to take a photo or record a video from the Amtelco Secure Messages app in order to attach it.

Select this check box to enable contacts in this group to attach a photo or video from their device’s Photo Gallery to Amtelco Secure Messages messages.

OR

Clear this check box if you want contacts in this group to only be allowed to attach photos and videos taken from the Amtelco Secure Messages app.

☑ Allow Silent High Priority

The “Allow Silent High Priority” setting determines whether contacts in this group can disable notification sounds for high priority secure messages in the Amtelco Secure Messages apps by selecting “Silent” in the Notification Settings.

Select this check box to enable contacts in this group to set the notification sound for high priority messages to “Silent.”

OR

Clear this check box if you don’t want contacts in this group to set the notification sound for high priority messages to “Silent.”

☑ Allow Silent Normal

The “Allow Silent Normal” setting determines whether contacts in this group can disable notification sounds for normal priority secure messages in the Amtelco Secure Messages apps by selecting “Silent” in the Notification Settings.

Select this check box to enable contacts in this group to set the notification sound for normal priority messages to “Silent.”

OR

Clear this check box if you don’t want contacts in this group to set the notification sound for normal priority messages to “Silent.”

☑ Edit Phone Number

The “Edit Phone Number” setting allows contacts in this group to edit their own contact phone number.

Select this check box to enable contacts in this group to edit their own contact phone number.

OR

Clear this check box if you don’t want contacts in this group to edit their own contact phone number.

☑ Hide Phone Number

The “Hide Phone Number” setting determines whether contacts in this group can view other contact phone numbers in the Amtelco Secure Messages apps and in the Amtelco Secure Messages Contact Web.

Note: This setting is used to hide contact phone numbers, but does not hide device phone numbers.

Select this check box to hide contact phone numbers when displaying Contact Info to contacts in this group in the Amtelco Secure Messages apps or the Amtelco Secure Messages Contact Web.

OR

Clear this check box to show contact phone numbers when displaying Contact Info to contacts in this group in the Amtelco Secure Messages apps or the Amtelco Secure Messages Contact Web.

☑ Modify Away Message

The "Modify Away Message" setting allows contacts in this group to create custom away messages.

Select this check box to enable contacts to enter their own custom away message.

OR

Clear this check box if you don't want contacts to be able to create custom away messages.

☑ Modify Display Name

The "Modify Display Name" setting allows contacts in this group to edit their own display name.

Select this check box to enable contacts to edit their own display name.

OR

Clear this check box if you don't want contacts to edit their own display name.

☑ Modify Email

The "Modify Email" setting allows contacts in this group to edit their own e-mail address.

Select this check box to enable contacts in this group to edit their own e-mail address.

OR

Clear this check box if you don't want contacts in this group to edit their own e-mail address.

☑ Modify Notification Interval

The "Modify Notification Interval" setting allows contacts in this group to edit their own notification interval.

Select this check box to enable contacts in this group to edit their own notification interval.

OR

Clear this check box if you don't want contacts in this group to edit their own notification interval.

☑ Modify Personal Circle

The "Modify Personal Circle" setting allows contacts in this group to add contacts and roles to their Personal Circle and remove contacts and roles from their Personal Circle.

Select this check box to enable contacts in this group to choose which contacts and roles are members of their Personal Circle.

OR

Clear this check box if you don't want contacts in this group to choose which contacts and roles are members of their Personal Circle.

☑ Modify Personal Quick Phrases

The "Modify Personal Quick Phrases" setting allows contacts in this group to create their own personal Quick Phrases.

Select this check box to enable contacts in this group to create their own personal Quick Phrases.

OR

Clear this check box if you don't want contacts in this group to be able to create personal Quick Phrases.

☑ Modify Picture

The “Modify Picture” setting allows contacts in this group to change their own contact photo.

Select this check box to enable contacts in this group to change their own contact photo.

OR

Clear this check box if you don’t want contacts in this group to change their own contact photo.

☑ Toggle Notifications (On/Off)

The “Toggle Notifications (On/Off)” setting allows contacts in this group to disable and enable message notifications for their devices using the Notification Alert (On/Off) setting.

Select this check box to enable contacts in this group to disable and enable their own message notifications.

OR

Clear this check box to prevent contacts in this group from enabling and disabling their own message notifications.

When you have finished configuring Permissions settings for the group, click the Save button to save your changes.

Return to General

Return to Groups

Return to Adding and Editing Amtelco Secure Messages Admin Web Administrators

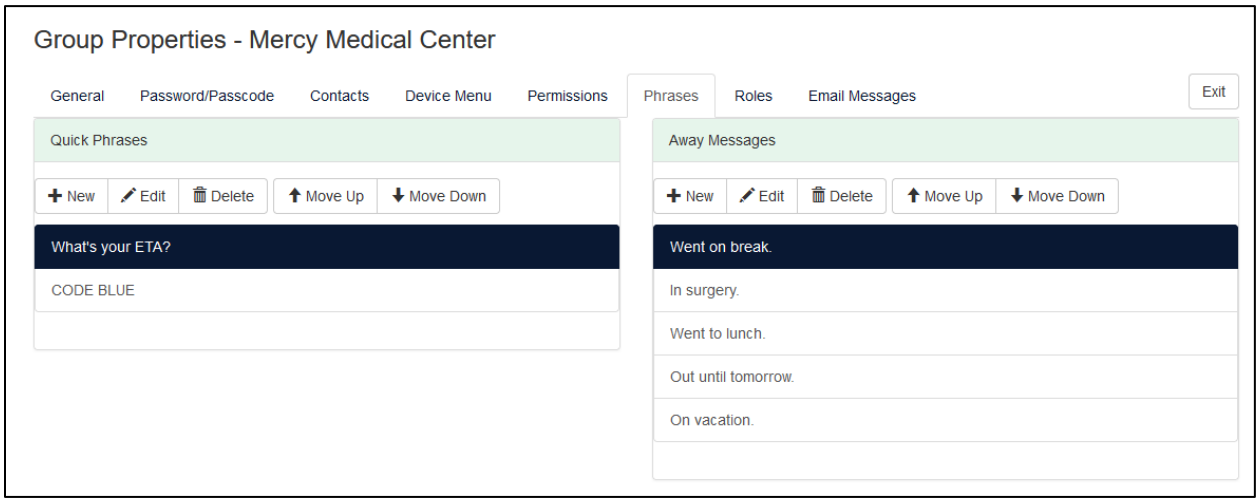
Return to Index

Phrases

The settings under the Phrases tab are used to create and edit Quick Phrases and away messages that are available to users registered to the group.

To edit Quick Phrases and away messages for a group, click the Phrases tab.

The Phrases Group Properties are displayed.



Quick Phrases

When a contact composes or replies to a secure message, the user can select one of the Quick Phrases listed in the Quick Phrases pane.

Phrases Toolbar

The Phrases Toolbar is displayed at the top of the Quick Phrases pane. The Phrases Toolbar is used to make changes to the Quick Phrases that are available to Amtelco Secure Messages users registered to this group when composing or replying to a secure message.

Icon	Description
	Click the **New** icon to add a new phrase.
	Click the **Edit** icon to edit the selected phrase.
	Click the **Delete** icon to delete the selected phrase.
	Click the **Move Up** icon to move the selected phrase closer to the top of the list.
	Click the **Move Down** icon to move the selected phrase closer to the bottom of the list.

Adding and Editing Phrases

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

  The Quick Phrase window is displayed with a blank text field.

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

The Quick Phrase window displays the selected phrase in a text field.

Phrase

Type the phrase that you want to add, or edit the existing phrase.

Click the Save Changes button.

The new or edited phrase is displayed in the list.

Repositioning a Phrase

To reposition a 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.

Deleting a Phrase

To remove a 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 Cancel button.

OR

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

If you clicked the Delete button, the phrase is removed from the list.

Away Messages

When a contact sets Amtelco Secure Messages notifications to Off, the user can select one of the away messages listed in the Away Messages pane.

Away Messages Toolbar

The Away Messages Toolbar is displayed at the top of the Away Messages pane. The Away Messages Toolbar is used to make changes to the away messages that are available to Amtelco Secure Messages users registered to this group when turning Amtelco Secure Messages notifications off.

Icon	Description
	Click the **New** icon to add a new away message.
	Click the **Edit** icon to edit the selected away message.
	Click the **Delete** icon to delete the selected away message.
	Click the **Move Up** icon to move the selected away message closer to the top of the list.
	Click the **Move Down** icon to move the selected away message closer to the bottom of the list.

Adding and Editing Away Messages

- **To add an away message, click the New icon.**

  The Away Message window is displayed with a blank text field.

- **To edit an away message, click the away message that you want to edit and then click the Edit icon.**

  The Away Message window displays the selected away message in a text field.

Message

Type the away message that you want to add, or edit the existing away message.

Click the Save Changes button.

The new or edited away message is displayed in the list.

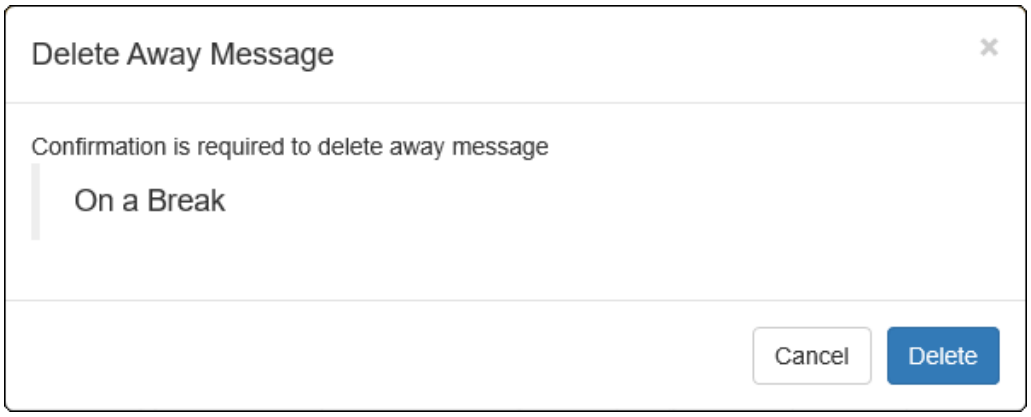
Repositioning an Away Message

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

Deleting an Away Message

To remove an away message, click the message 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 Cancel button.

OR

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

If you clicked the Delete button, the message is removed from the list.

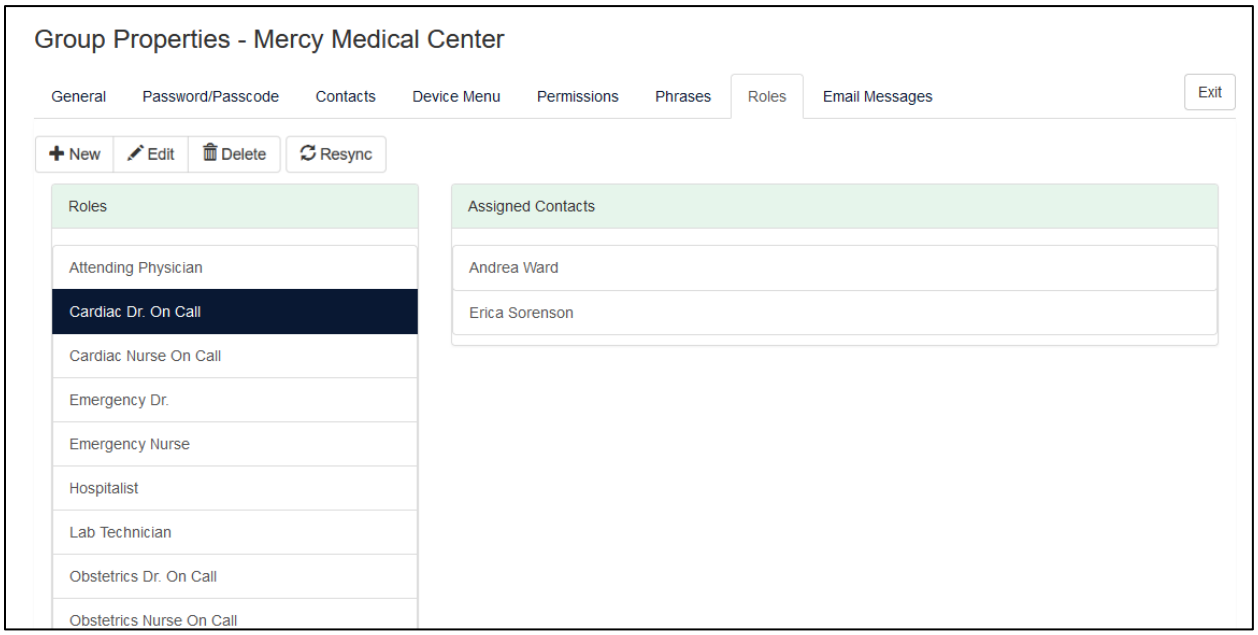
Return to General
Return to Groups
Return to Index

Roles

The settings under the Roles tab are used to create, edit, and delete roles that are used for the optional Role-Based Messaging feature for the group.

To edit roles for a group, click the Roles tab.

The Roles Group Properties are displayed.



Roles Toolbar

The Roles Toolbar is displayed under the Roles tab. The Roles Toolbar is used to make changes to the roles that are used for Role-Based Messaging for the group.

Icon	Description
✚	Click the **New** icon to add a new role.
✎	Click the **Edit** icon to edit the selected role.
🗑	Click the **Delete** icon to delete the selected role.
↻	Click the **Resync** icon to refresh the list of roles in the Roles pane and contacts in the Assigned Contacts pane.

Adding and Editing Roles

- **To add a role, click the New icon.** ✚

  The Role window is displayed with a blank Name field.

- **To edit a role, click the role that you want to edit and then click the Edit icon.** ✎

  The Role window is displayed.

Role Name

Type the name of the role that you want to add or edit.

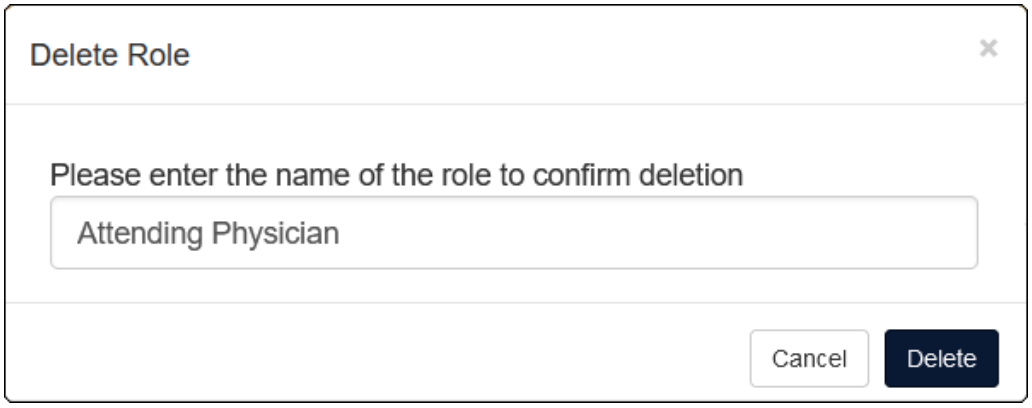
Click the Save Changes button.

The new or edited role is displayed in the list.

Deleting a Role

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

A dialog box is displayed to confirm the delete request.



Enter the full role name in the field, including the correct capitalization, spacing, and punctuation.

To cancel the delete request, click the Cancel button.

OR

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

If you clicked the Delete button, the role is removed from the list.

Contacts

The Contacts pane displays the names of the contacts that are assigned to the role selected in the Roles list.

In order for contacts to be assigned to a role, the role must be assigned to an on-call shift in one of the Intelligent Series (IS) applications, and contacts must be assigned to the shift. More information about on-call scheduling is provided in the “Directory OnCall Scheduling” section of the *Web Supervisor Reference Guide* and the *Intelligent Series Supervisor Reference Guide*.

To view all of the contacts assigned to a role, select the role from the list.

The contacts that belong to the selected role are displayed in the Assigned Contacts pane.

Return to General
Return to Groups
Return to Index

Email Messages

The settings under the Email Messages tab are used to create and edit automatic e-mail messages for initial registration, multiple device registration, and resetting a user's password and passcode.

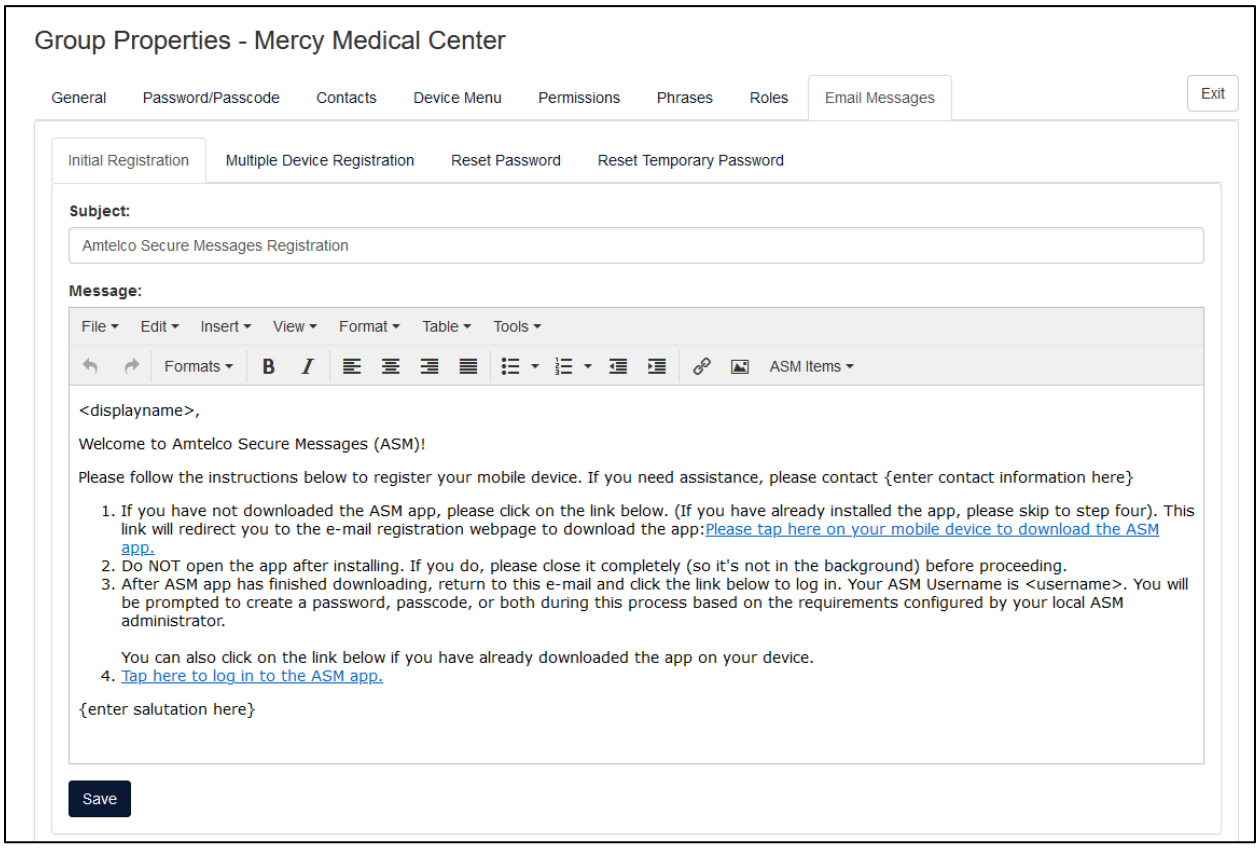
To edit the e-mail message settings for a group, click the Email Messages tab.

The e-mail message settings are divided into tabs.

- **Click the Initial Registration tab to configure the e-mail message that is sent to contacts to allow them to register the Amtelco Secure Messages app on a device.**
- **Click the Multiple Device Registration tab to configure the e-mail message that is sent to contacts to allow them to register Amtelco Secure Messages on multiple devices.**
- **Click the Reset Password tab to configure the e-mail message that is sent to contacts that need to reset their password or passcode for Amtelco Secure Messages.**
- **Click the Reset Temporary Password tab to configure the e-mail message that is sent to contacts that need to reset their password for the Amtelco Secure Messages Contact Web.**

Initial Registration

The settings under the Initial Registration tab are used to create an e-mail message that can be sent to a contact to allow that person to register the Amtelco Secure Messages app on a device.



Subject

The text in the Subject field is used as the subject for the initial registration e-mail.

Enter the text to use as the subject for initial registration e-mail.

Message

The text and formatting in the Message field is used as the body of the initial registration e-mail. The template saved in Group 0 will be used as the default template when new groups are created.

Edit the template as desired to create the message for initial registration e-mail.

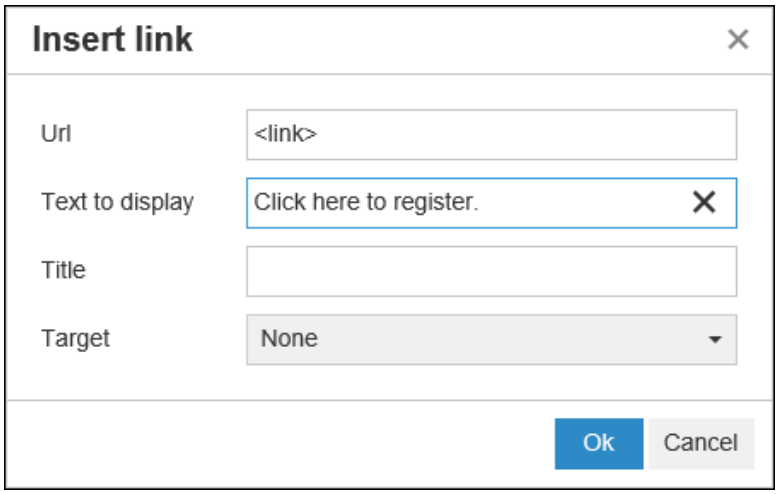
A Registration URL link is required for initial e-mail registration.

To insert the Registration URL link that is required for initial e-mail registration, click the position in the template where you want to insert the hyperlink. Then open the ASM Items menu and click the Registration URL command.

A Click here to register hyperlink is inserted into the template. This hyperlink is mapped to a URL value of <link>. Each time an Initial Registration e-mail message is sent, the <link> value is replaced with a unique e-mail registration URL that identifies a new Amtelco Secure Messages user and allows that person to register Amtelco Secure Messages on a device.

To edit the hyperlink, right-click the hyperlink to display the context menu and then click the Link command.

The Insert Link window is displayed.



Url

The Url property must be set to <link> in order for e-mail registration to function. This will be replaced with a unique e-mail registration URL each time that an Initial Registration e-mail message is sent.

Do not change the Url value.

Text to display

The value in the “Text to display” property is displayed as a hyperlink in the e-mail message.

Type the text that you want to display as the hyperlink in the e-mail message.

Click the Ok button to save your changes to the hyperlink properties and return to the Initial Registration settings.

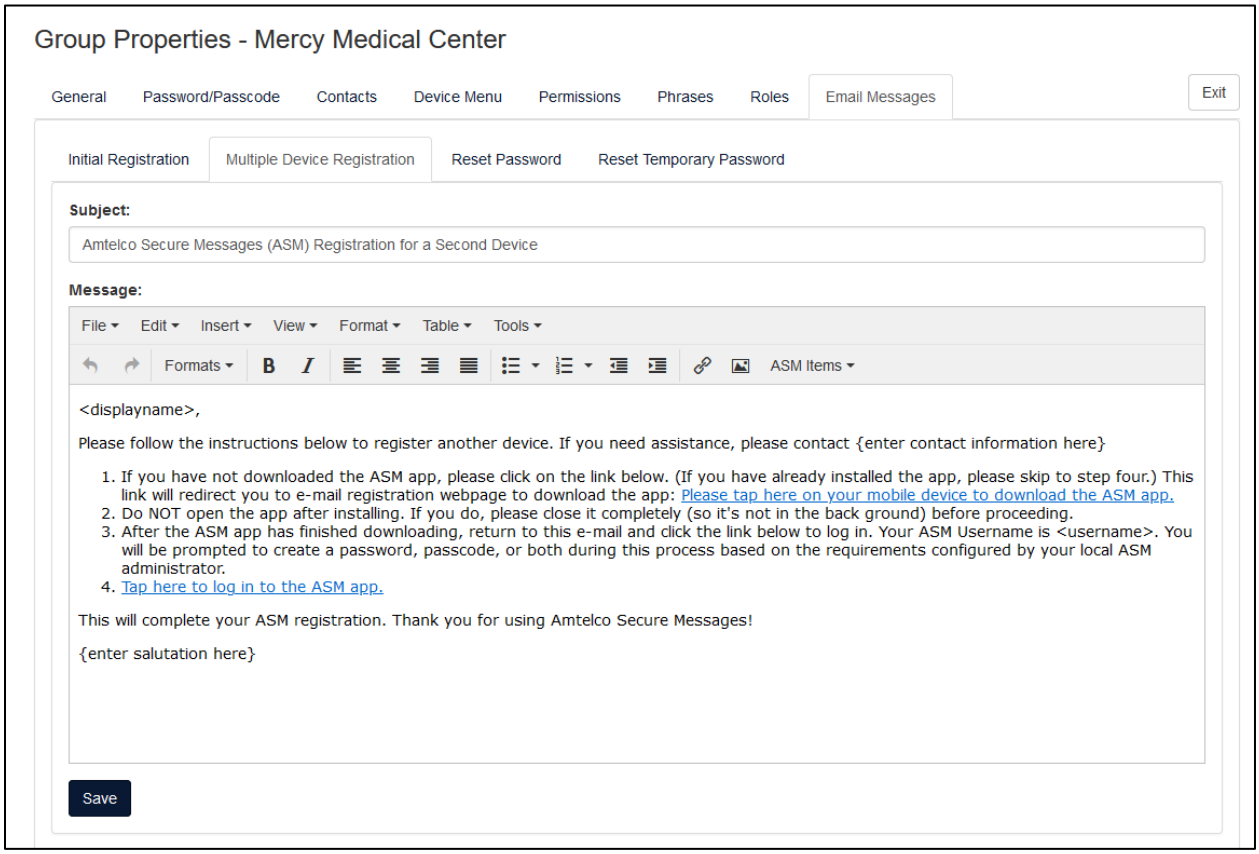
When you are finished editing the Initial Registration e-mail subject and message, click the Save button to save your changes.

A dialog box is displayed to confirm the changes were saved successfully.

For more information regarding the different icons and commands available in the Messages menus and toolbars, refer to the Message Menus and Toolbars table in the appendixes of this document.

Multiple Device Registration

The settings under the Multiple Device Registration tab are used to create an automatic e-mail message that can be sent to a contact to allow that person to register Amtelco Secure Messages on an additional device. In this scenario, the contact is already registered for Amtelco Secure Messages on an initial device.



Subject

The text in the Subject field is used as the subject for the multiple device registration e-mail.

Enter the text to use as the subject for multiple device registration e-mail.

Message

The text and formatting in the Message field is used as the body of the multiple device registration e-mail. The template saved in Group 0 will be used as the default template when new groups are created.

Edit the template as desired to create the message for multiple device registration e-mail.

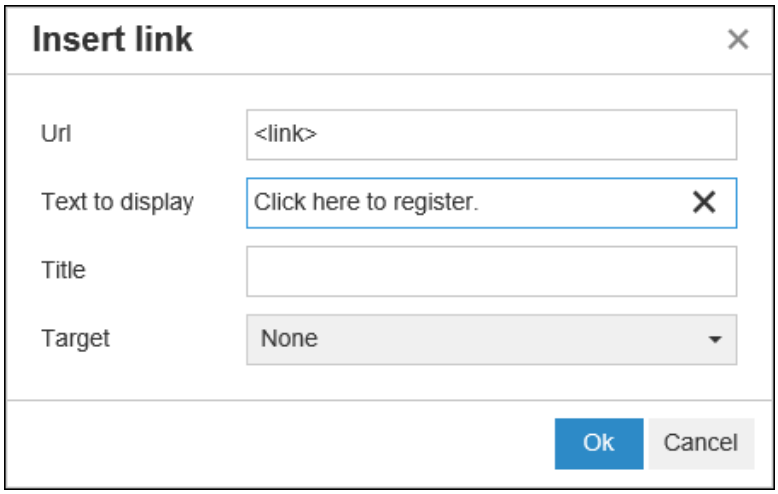
A Registration URL link is required for multiple device e-mail registration.

To insert the Registration URL link that is required for multiple device e-mail registration, click the position in the template where you want to insert the hyperlink. Then open the ASM Items menu and click the Registration URL command.

A Click here to register hyperlink is inserted into the template. This hyperlink is mapped to a URL value of <link>. Each time a Multiple Device Registration e-mail message is sent, the <link> value is replaced with a unique e-mail registration URL that identifies the Amtelco Secure Messages user and allows that person to register Amtelco Secure Messages on an additional device.

To edit the hyperlink, right-click the hyperlink to display the context menu and then click the Link command.

The Insert Link window is displayed.



Url

The Url property must be set to <link> in order for e-mail registration to function. This will be replaced with a unique e-mail registration URL each time that a Multiple Device Registration e-mail message is sent.

Do not change the Url value.

Text to display

The value in the "Text to display" property is displayed as a hyperlink in the e-mail message.

Type the text that you want to display as the hyperlink in the e-mail message.

Click the Ok button to save your changes to the hyperlink properties and return to the Multiple Device Registration settings.

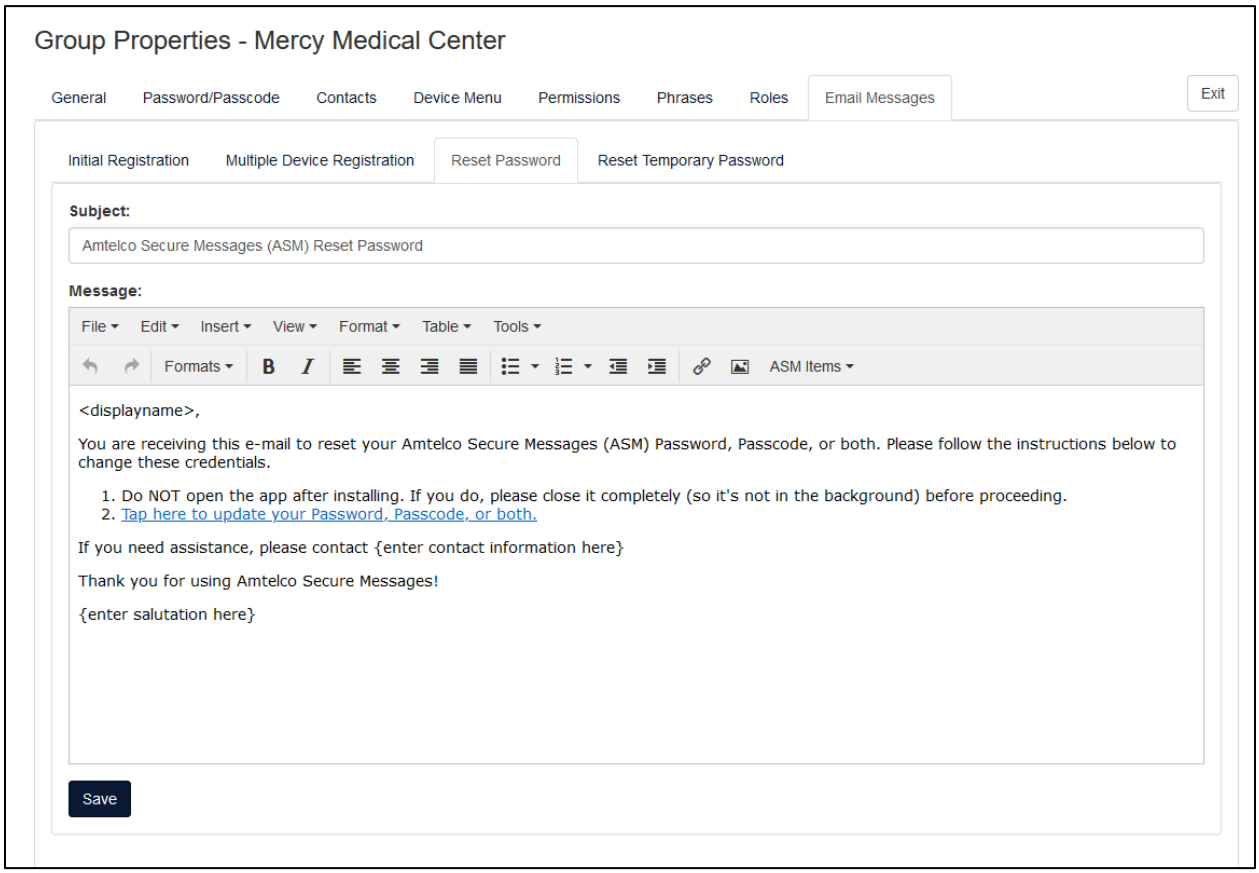
When you are finished editing the Multiple Device Registration e-mail subject and message, click the Save button to save your changes.

A dialog box is displayed to confirm the changes were saved successfully.

For more information regarding the different icons and commands available in the Messages menus and toolbars, refer to the Message Menus and Toolbars table in the appendixes of this document.

Reset Password

The settings under the Reset Password tab are used to create an e-mail message that will be sent to contacts that need to reset their password and passcode for the Amtelco Secure Messages apps. The e-mail message is sent using the Email Password Reset button in Contact Group Settings.



Subject

The text in the Subject field is used as the default Subject for the reset password e-mail.

Enter the text to use as the subject for reset password e-mail.

Message

The text and formatting in the Message field is used as the body of the reset password e-mail. The template saved in Group 0 will be used as the default template when new groups are created.

Edit the template as desired to create the message for reset password e-mail.

A Registration URL link is required for resetting passwords and passcodes.

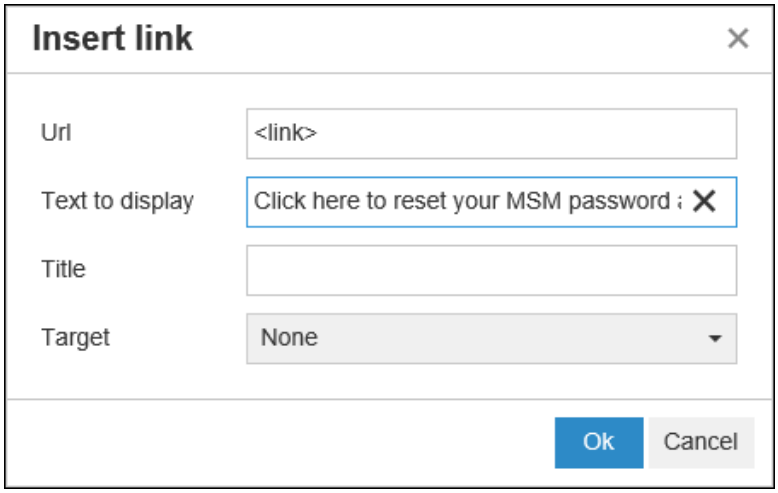
To insert the Registration URL link that is required for resetting passwords and passcodes, click the position in the template where you want to insert the hyperlink. Then open the ASM Items menu and click the Registration URL command.

A Click here to register hyperlink is inserted into the template. This hyperlink is mapped to a URL value of <link>. Each time a Reset Password e-mail message is sent, the <link> value is

replaced with a unique password reset URL that allows the Amtelco Secure Messages user to reset his or her Amtelco Secure Messages password and passcode.

To edit the hyperlink, right-click the hyperlink to display the context menu and then click the Link command.

The Insert Link window is displayed.



Url

The Url property must be set to <link> in order for resetting passwords and passcodes to function. This will be replaced with a unique e-mail registration URL each time that a Reset Password e-mail message is sent.

Do not change the Url value.

Text to display

The value in the "Text to display" property is displayed as a hyperlink in the e-mail message.

Type the text that you want to display as the hyperlink in the e-mail message.

Click the Ok button to save your changes to the hyperlink properties and return to the Reset Password settings.

When you are finished editing the Reset Password e-mail subject and message, click the Save button to save your changes.

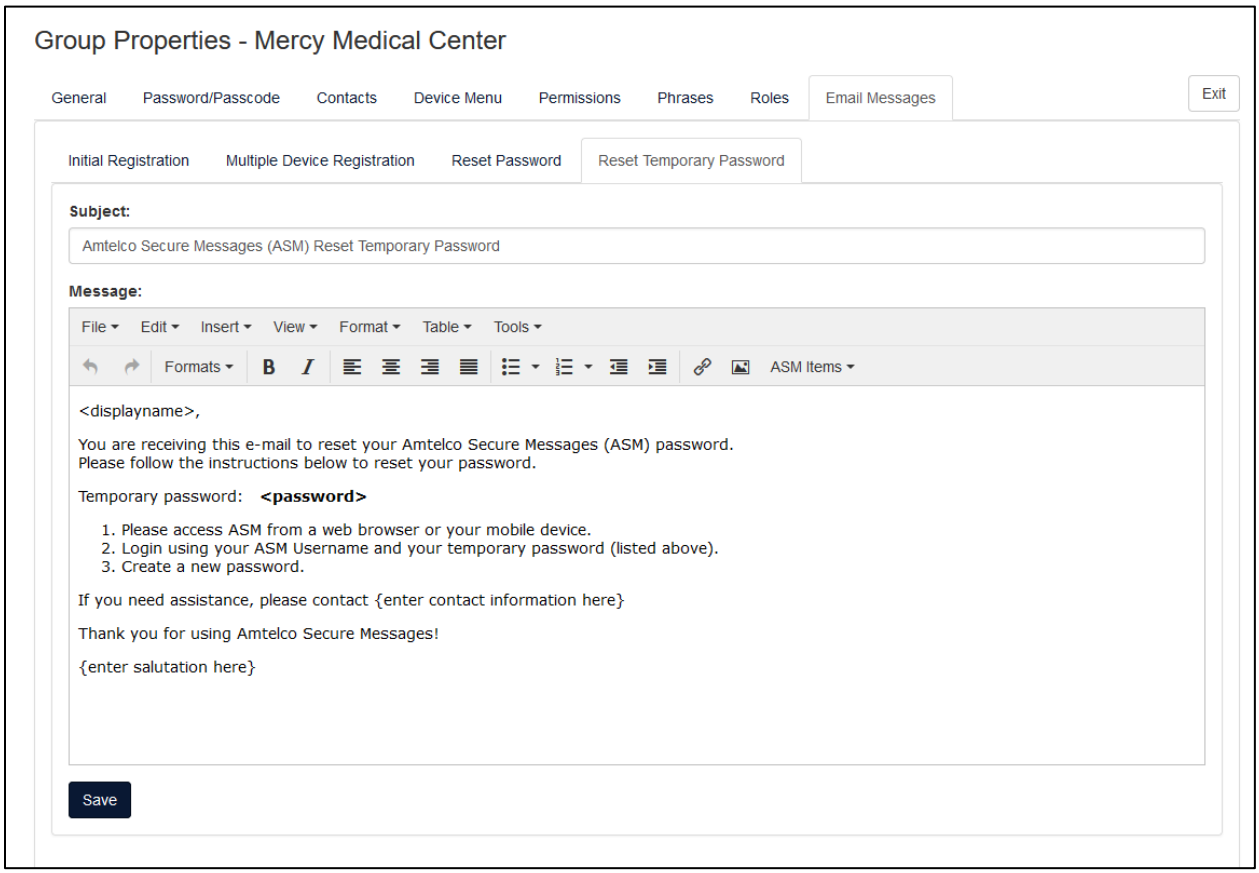
A dialog box is displayed to confirm the changes were saved successfully.

For more information regarding the different icons and commands available in the Messages menus and toolbars, refer to the Message Menus and Toolbars table in the appendixes of this document.

Reset Temporary Password

The settings under the Reset Temporary Password tab are used to create an e-mail message that will be sent to contacts that need to reset their password for the Amtelco Secure Messages

Contact Web. The e-mail message is sent using the Email Temporary Password button in Contact Group Settings.



Subject

The text in the Subject field is used as the default Subject for the reset temporary password e-mail.

Enter the text to use as the subject for reset temporary password e-mail.

Message

The text and formatting in the Message field is used as the body of the reset temporary password e-mail. The template saved in Group 0 will be used as the default template when new groups are created.

Edit the template as desired to create the message for reset temporary password e-mail.

A password field is required for resetting passwords and passcodes.

To insert the password field that is required for sending temporary passwords, click the position in the template where you want to insert the field. Then open the ASM Items menu and click the "Temporary password" command.

The text "<password>" is inserted into the template. Each time a Reset Temporary Password e-mail message is sent, the <password> value is replaced with a temporary password that the contact must enter to reset his or her Amtelco Secure Messages Contact Web password.

When you are finished editing the Reset Temporary Password e-mail subject and message, click the Save button to save your changes.

A dialog box is displayed to confirm the changes were saved successfully.

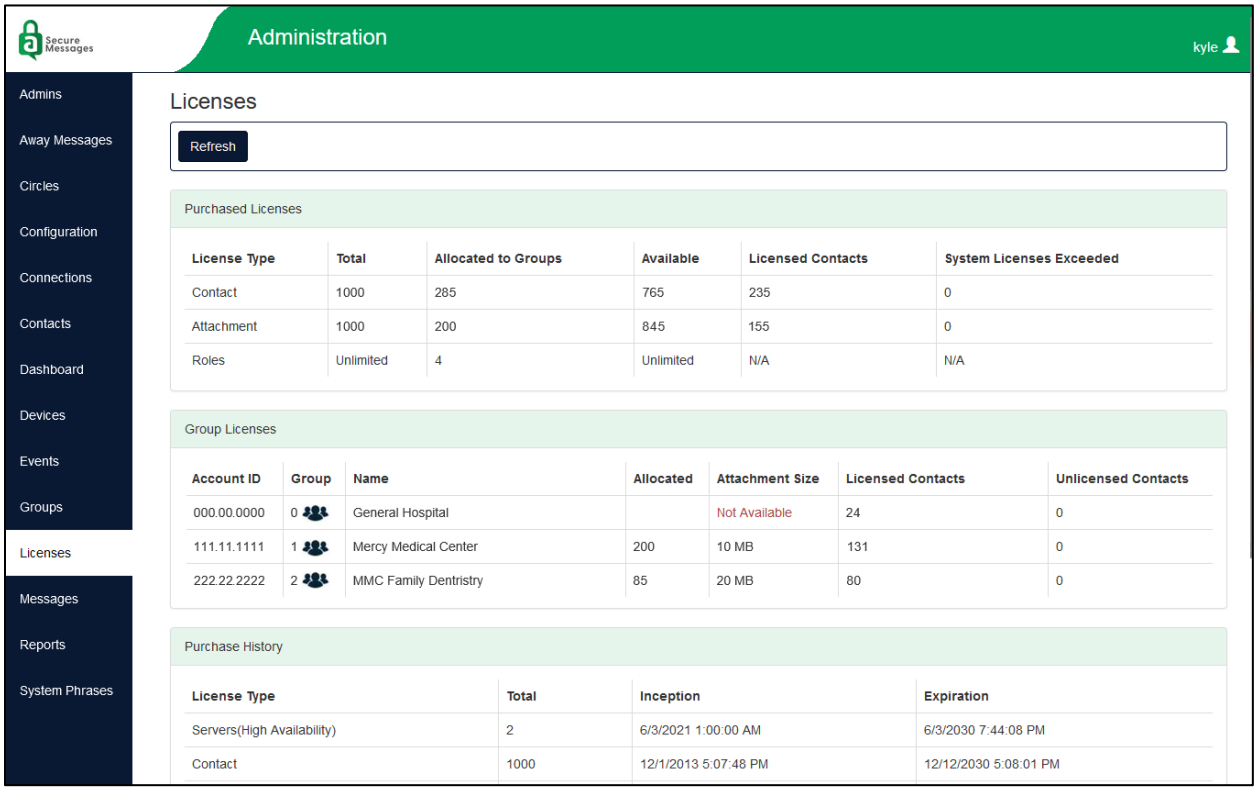
For more information regarding the different icons and commands available in the Messages menus and toolbars, refer to the Message Menus and Toolbars table in the appendixes of this document.

Return to Contacts
Return to General
Return to Groups
Return to Contact Group Settings
Return to Index

Licenses

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

Click the Licenses command on the navigation menu to access the Licenses page.



Purchased Licenses

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

Column	Description
License Type	There are three types of licenses. • Each Contact license enables one contact to use the Amtelco Secure Messages app or Contact Web on any number of devices. • Each Attachment license enables one user to use Amtelco Secure Messages attachments. • A Roles license enables the Role-Based Messaging feature.
Total	Total indicates the total number of licenses that have been purchased and are not expired.

Column	Description
Allocated to Groups	Allocated to Groups indicates the number of licenses that have been allocated to Amtelco Secure Messages 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 contacts until the number of Available licenses is zero.
Available	Available indicates the number of licenses that are available for new users.
Licensed Contacts	Licensed Contacts indicates the number of contacts that are registered for licenses.
System Licenses Exceeded	System Licenses Exceeded indicates the number of contacts that attempted to register for Amtelco Secure Messages but were unable to obtain a license because none were available.

Group Licenses

The Group Licenses table displays information about the Amtelco Secure Messages groups that have been created for your Amtelco Secure Messages 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 Amtelco Secure Messages Admin Web.

Groups are used to separate Amtelco Secure Messages users into different Contact Lists. Each group is assigned a separate Account ID. Users that register the Amtelco Secure Messages app using an Account ID will have a Contact List that only shows users that have been registered with that same Account ID. Users can register for more than account and can switch between them by selecting an Account Name in the Amtelco Secure Messages app.

Groups are configured on the Groups page of the Amtelco Secure Messages Admin Web.

Column	Description
Account ID	Account ID indicates the Account ID used to register a device for the group.
Group	Group indicates the unique Group number. If the optional Role-Based Messaging feature is enabled for the group, the roles icon is displayed next to the Group number.
Name	Name indicates the name of the group. The group name is displayed in the Amtelco Secure Messages apps as the Account Name in the Amtelco Secure Messages apps and the Amtelco Secure Messages Contact Web. Users select an Account Name to switch from one account to another.
Allocated	Allocated indicates the maximum number of contacts that are allowed to register for the group. This number limits the number of contacts that can register for the group.

Column	Description
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 Contacts	Licensed Contacts indicates the number of contacts that are registered for the group.
Unlicensed Contacts	Unlicensed Contacts indicates the number of contacts 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 Amtelco Secure Messages account.

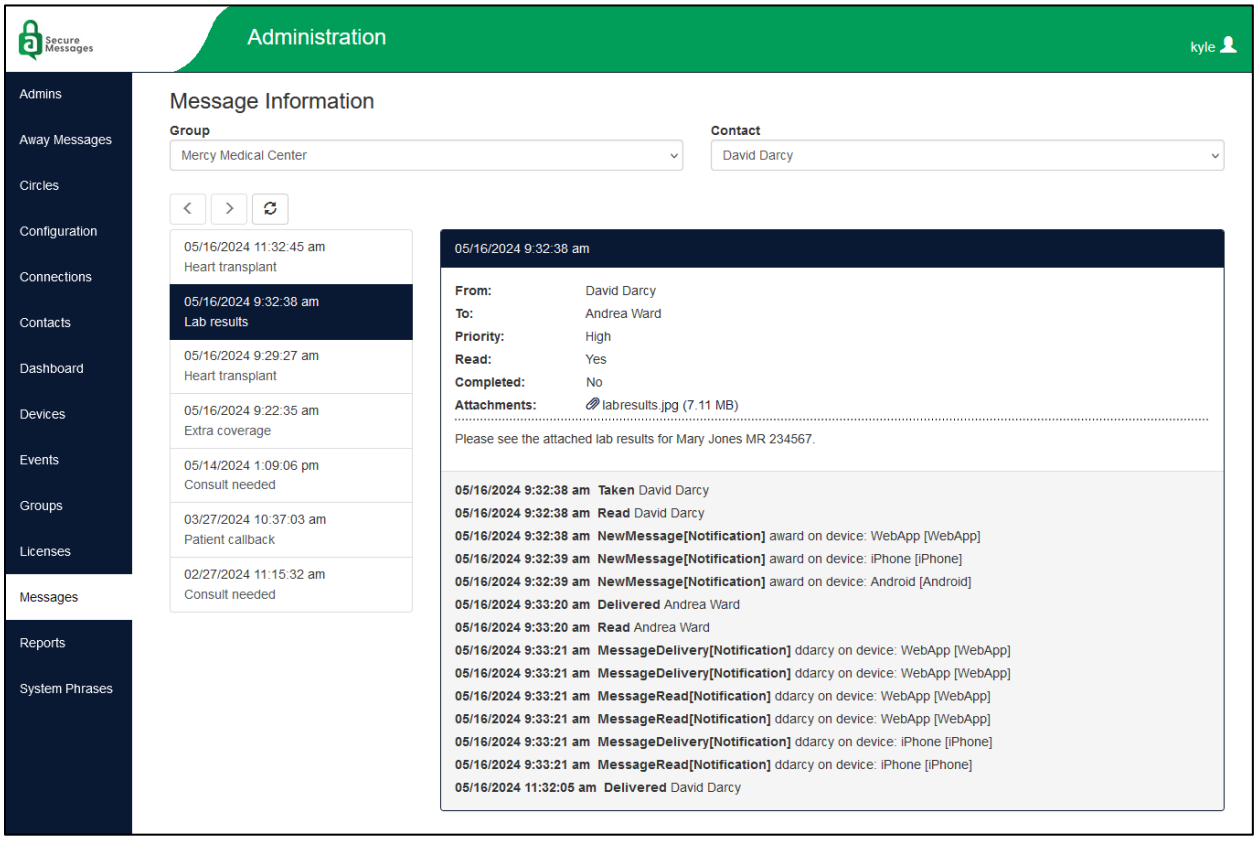
Column	Description
License Type	License Type indicates the type of licenses purchased.
Total	Total indicates the number of licenses purchased.
Inception	Inception indicates the date and time that the licenses were activated.
Expiration	Expiration indicates the date and time that the licenses will expire.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

Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

Message Information

The Message Information page is used to view secure messages that were transmitted. The messages can be viewed by contact and by group.

Click the Messages command on the navigation menu to access the Message Information page.



Group

The Group menu is used to search for messages transmitted using a specific Amtelco Secure Messages group.

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

Contact

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

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

The date, time, and subject of the secure messages for the selected group and contact 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 display an attachment, click the attachment file name and follow your browser's prompts to open or download the attachment.

To display the next page of messages, click the Next Message Threads icon. ›

To display the previous page of messages, click the Previous Message Threads icon. ‹

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

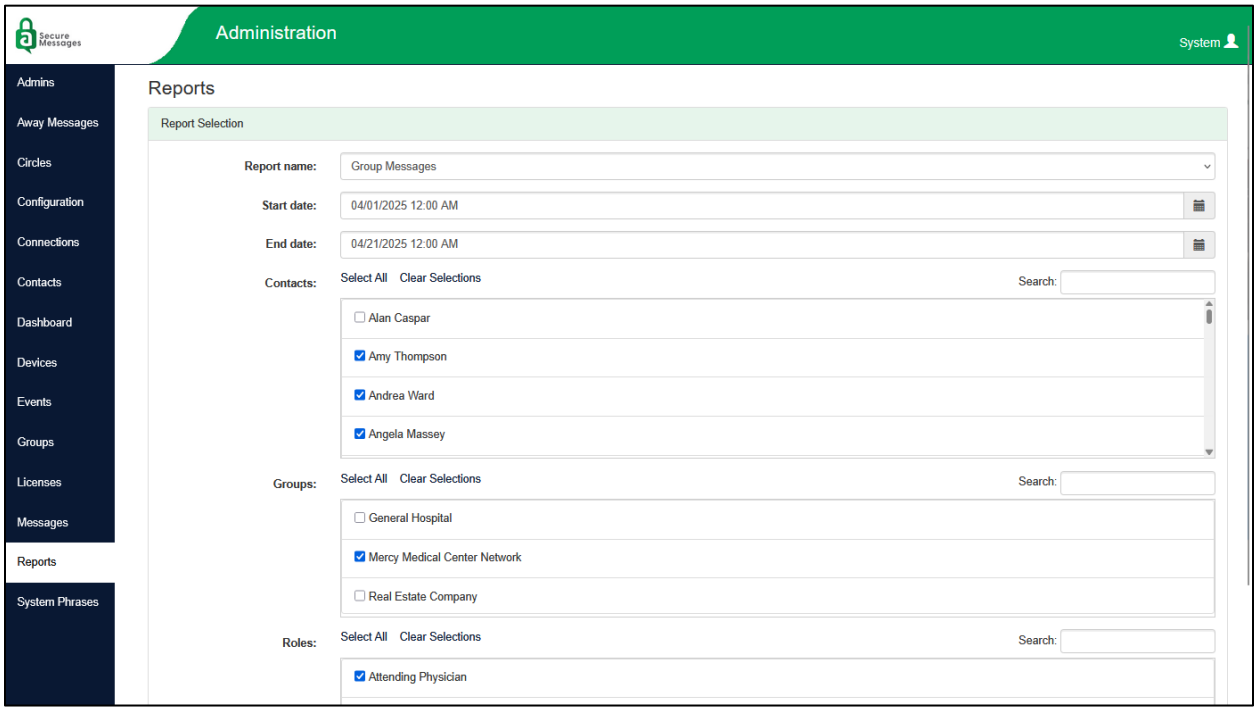
Return to Navigating in Amtelco Secure Messages Admin Web

Return to Index

Reports

The Reports page is used to run reports on the Amtelco Secure Messages data.

Click the Reports command on the navigation menu to access the Reports page.



Report Name

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 Amtelco Secure Messages group.
Audit Report	The Audit Report displays all the actions that have occurred in the Amtelco Secure Messages Admin Web Server during the specified date and time range.
Contact List	The Contact List Report displays a list of contacts and a summary of contact settings for each.
Contacts Without Devices	The Contacts Without Devices Report displays a list of contacts in the Amtelco Secure Messages system that do not have any devices registered to their username. These contacts are either using Shared Devices, or are taking up a license but are not using Amtelco Secure Messages.
Database Size Report	The Database Size Report displays the history of the Amtelco Secure Messages database size and unallocated disk space.

Report	Description
Device List	The Device List Report displays a list of devices registered for Amtelco Secure Messages. The devices are listed by contact name.
Device Versions	The Device Versions Report displays a list of device types and the number of devices registered for each version of the Amtelco Secure Messages app.
Event Log Report	The Event Log Report displays all the events that have occurred in the Amtelco Secure Messages Admin Web Server during the specified date and time range.
Group Audit Report	The Group Audit Report enables you to view an Audit Report for specific groups.
Group Contact List	The Group Contact List Report enables you to view a Contact List Report for specific contacts and groups.
Group Device List	The Group Device List Report enables you to view a Device List Report for specific groups.
Group Device Versions	The Group Device Versions Report enables you to view a Device Versions Report for specific groups.
Group Message Counts	The Group Message Counts Report enables you to view a Message Counts Report for specific groups.
Group Message Details	The Group Message Details Report enables you to view a comprehensive Messages Report for specific contacts, groups and roles. A row is displayed for each time a contact sent or received a message.
Group Messages - Formatted	The Group Messages - Formatted Report enables you to view a Messages Report for specific contacts, groups and roles in an easy-to-read format.
Group Messages	The Group Messages Report enables you to view a comprehensive Messages Report for specific contacts, groups and roles.
Message Counts	The Message Counts Report displays counts of all secure messages sent by each contact during the specified date and time range.
Message Details	The Message Details Report displays comprehensive information about secure messages sent during the specified date and time range. A row is displayed for each time a contact sent or received a message.
Messages - Formatted	The Messages - Formatted Report displays information about secure messages sent during the specified date and time range in an easy-to-read format.

Reports

Report	Description
Messages	The Messages Report displays comprehensive information about secure messages sent during the specified date and time range.
Notifications	The Notifications Report displays counts of notification successes and failures for device types in each group for a specified date and time range. The counts are listed by group ID.
Orphaned Contacts	The Orphaned Contacts Report displays a list of contacts in the Amtelco Secure Messages system that are not registered to any groups. These contacts are taking up a license but are unable to send or receive Amtelco Secure Messages messages.

Start Date

The Start Date parameter is displayed when the Audit Report, Database Size Report, Event Log Report, Group Audit Report, Group Message Counts Report, Group Messages - Formatted Report, Group Messages Report, Message Counts Report, Messages - Formatted Report, Messages Report, or Notifications Report is selected. The Start Date 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 at the bottom of the calendar.**

  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 Date

The End parameter is displayed when the Audit Report, Database Size Report, Event Log Report, Group Audit Report, Group Message Counts Report, Group Messages - Formatted Report, Group Messages Report, Message Counts Report, Messages - Formatted Report, Messages Report, or Notifications Report is selected. The End Date 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 Group Contact List Report, Group Messages - Formatted Report, or Group Messages 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 the Select All hyperlink.**
- **To clear all selections, click the Clear Selections hyperlink.**
- **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 Group Audit Report, Group Contact List Report, Group Device List Report, Group Device Versions Report, Group Message Counts Report, Group Messages - Formatted Report, or Group Messages 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 the Select All hyperlink.**
- **To clear all selections, click the Clear Selections hyperlink.**
- **To search for a group, click the Search field and type all or part of the group name.**

Roles

The Roles parameter is displayed when the Group Message Details, Group Messages, or Group Messages - Formatted report is selected. The Roles parameter is used to indicate which roles' data should be included in the report.

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

Report Type

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.

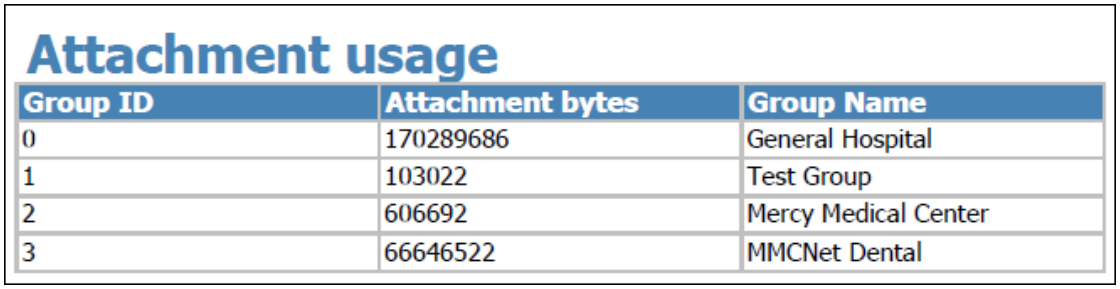
The report is displayed in a new browser window.

- Attachment Usage Report
- Audit Report
- Contact List Report
- Contacts Without Devices Report
- Database Size Report
- Device List Report
- Device Versions Report
- Event Log Report
- Group Audit Report
- Group Contact List Report
- Group Device List Report
- Group Device Versions Report
- Group Message Counts Report
- Group Messages - Formatted Report
- Group Messages Report
- Message Counts Report
- Messages - Formatted Report
- Messages Report
- Notifications Report
- Orphaned Contacts Report

Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

Attachment Usage Report

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



Attachment usage

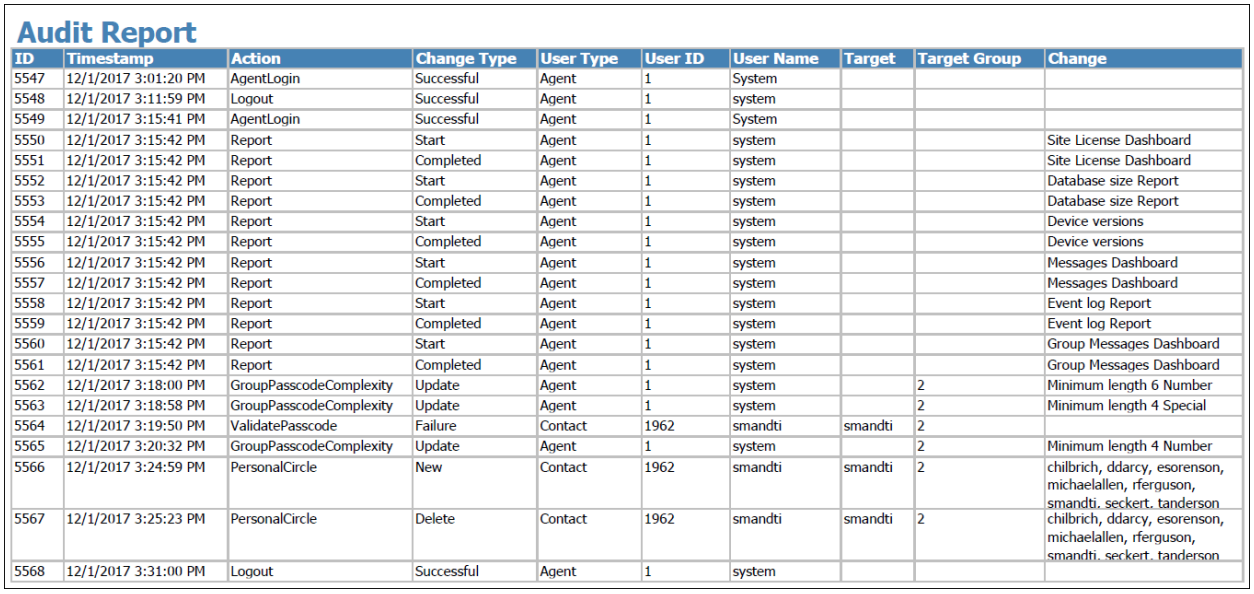
Group ID	Attachment bytes	Group Name
0	170289686	General Hospital
1	103022	Test Group
2	606692	Mercy Medical Center
3	66646522	MMCNet Dental

Column	Description
Group ID	Group ID indicates the unique ID associated with each group that has been allocated space for storing attachments.
Attachment Bytes	Attachment Bytes indicates the amount of disk space, in bytes, that is currently being used to store attachments for the group.
Group Name	Group Name indicates the name of the group.

Return to Reports
Return to Index

Audit Report

The Audit Report displays all the actions that have occurred in the Amtelco Secure Messages Admin Web Server during the specified date and time range. Actions include updates made to configuration, Circles, groups, admins, and contacts settings, Amtelco Secure Messages Admin Web administrator log ins and log outs, initiated reports, and more.



Audit Report

ID	Timestamp	Action	Change Type	User Type	User ID	User Name	Target	Target Group	Change
5547	12/1/2017 3:01:20 PM	AgentLogin	Successful	Agent	1	System			
5548	12/1/2017 3:11:59 PM	Logout	Successful	Agent	1	system			
5549	12/1/2017 3:15:41 PM	AgentLogin	Successful	Agent	1	System			
5550	12/1/2017 3:15:42 PM	Report	Start	Agent	1	system			Site License Dashboard
5551	12/1/2017 3:15:42 PM	Report	Completed	Agent	1	system			Site License Dashboard
5552	12/1/2017 3:15:42 PM	Report	Start	Agent	1	system			Database size Report
5553	12/1/2017 3:15:42 PM	Report	Completed	Agent	1	system			Database size Report
5554	12/1/2017 3:15:42 PM	Report	Start	Agent	1	system			Device versions
5555	12/1/2017 3:15:42 PM	Report	Completed	Agent	1	system			Device versions
5556	12/1/2017 3:15:42 PM	Report	Start	Agent	1	system			Messages Dashboard
5557	12/1/2017 3:15:42 PM	Report	Completed	Agent	1	system			Messages Dashboard
5558	12/1/2017 3:15:42 PM	Report	Start	Agent	1	system			Event log Report
5559	12/1/2017 3:15:42 PM	Report	Completed	Agent	1	system			Event log Report
5560	12/1/2017 3:15:42 PM	Report	Start	Agent	1	system			Group Messages Dashboard
5561	12/1/2017 3:15:42 PM	Report	Completed	Agent	1	system			Group Messages Dashboard
5562	12/1/2017 3:18:00 PM	GroupPasscodeComplexity	Update	Agent	1	system		2	Minimum length 6 Number
5563	12/1/2017 3:18:58 PM	GroupPasscodeComplexity	Update	Agent	1	system		2	Minimum length 4 Special
5564	12/1/2017 3:19:50 PM	ValidatePasscode	Failure	Contact	1962	smandti	smandti	2	
5565	12/1/2017 3:20:32 PM	GroupPasscodeComplexity	Update	Agent	1	system		2	Minimum length 4 Number
5566	12/1/2017 3:24:59 PM	PersonalCircle	New	Contact	1962	smandti	smandti	2	chilbrich, ddarcy, esorenson, michaelallen, rferguson, smandti, seckert, tanderson
5567	12/1/2017 3:25:23 PM	PersonalCircle	Delete	Contact	1962	smandti	smandti	2	chilbrich, ddarcy, esorenson, michaelallen, rferguson, smandti, seckert, tanderson
5568	12/1/2017 3:31:00 PM	Logout	Successful	Agent	1	system			

Column	Description
ID	ID indicates the unique ID assigned to each action.
Timestamp	Timestamp indicates the date and time the action occurred.
Action	Action indicates the type of action that was initiated. Each action type is described in the following section. For more information regarding the different action types that may appear in the Group Audit Report, refer to the Actions table in the appendixes of this document.
Change Type	Change Type indicates the type of change that resulted from the action.
User Type	User Type indicates the type of user that initiated the action. User Type could be “Agent,” indicating an Amtelco Secure Messages Admin Web administrator, or “Contact,” indicating a Amtelco Secure Messages contact.
User ID	User ID indicates the unique ID associated with the user who initiated the action.
User Name	User Name indicates the username of the user who initiated the action.
Target	Target indicates the name of the Amtelco Secure Messages user, group, or Circle to which the change was applied.
Target Group	Target Group indicates the unique ID associated with the group to which the change was applied.
Change	Change indicates details about the change that occurred.

Return to Reports
Return to Index

Contact List Report

The Contact List Report displays a list of contacts in the Amtelco Secure Messages system and a summary of Contact Settings for each.

Contact list

Name	User Name	Phone Number	Interval	Notifications	Away Start	Away End	Locked Out	Inception	Licensed	Devices
Alan Caspar	acaspar	7115552938	16	5	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/29/2017 2:55:27 PM	True	2
Andrea Ward	award	7115555213	16	5	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/29/2017 2:55:45 PM	True	2
Angela Massey	amassey	7115559715	16	5	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/29/2017 2:56:05 PM	True	2
Cynthia Hilbrich	chilbrich	7115556481	16	5	8/28/2019 9:07:32 AM	8/28/2019 12:00:00 PM	False	6/29/2017 2:56:29 PM	True	2
David Darcy	ddarcy	7115554862	22	10	10/2/2019 1:16:13 PM	10/2/2019 2:15:00 PM	False	5/8/2018 4:04:57 PM	True	3
Erica Sorenson	esorenson	7115550029	15	10	9/16/2019 12:24:28 PM	9/16/2019 1:24:28 PM	False	8/26/2019 9:58:01 AM	True	2
James Thompson	jthompson	7115554567	15	10	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/5/2018 8:48:00 AM	True	2
Infinity	Infinity		20	10	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	5/9/2017 9:49:53 AM	True	1
IS	IS		20	10	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	7/13/2018 8:36:46 AM	True	1
Michael Allen	mallen	7115554194	18	7	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/7/2019 3:49:06 PM	True	2
Rachel Ferguson	rferguson	7115550293	15	5	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	7/31/2019 12:52:32 PM	True	2
REDAlert	REDAlert	7115558946	20	10	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	2/18/2019 2:14:36 PM	True	1
Sean Mandti	smandti	7115554444	15	10	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/21/2019 8:47:38 AM	True	2
Shere Krauss	skrauss	7115552335	20	10	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	8/18/2017 10:47:09 AM	True	2
Spectrum	Spectrum		20	10	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	5/9/2017 9:46:52 AM	True	1
Steven Eckert	seckert	7115559988	20	10	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	8/18/2017 10:48:51 AM	True	2
Wilma Anderson	wanderson	7115553362	15	5	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	7/31/2019 12:52:07 PM	True	2

Note: Not all fields in the Contact List Report are shown in the screenshot.

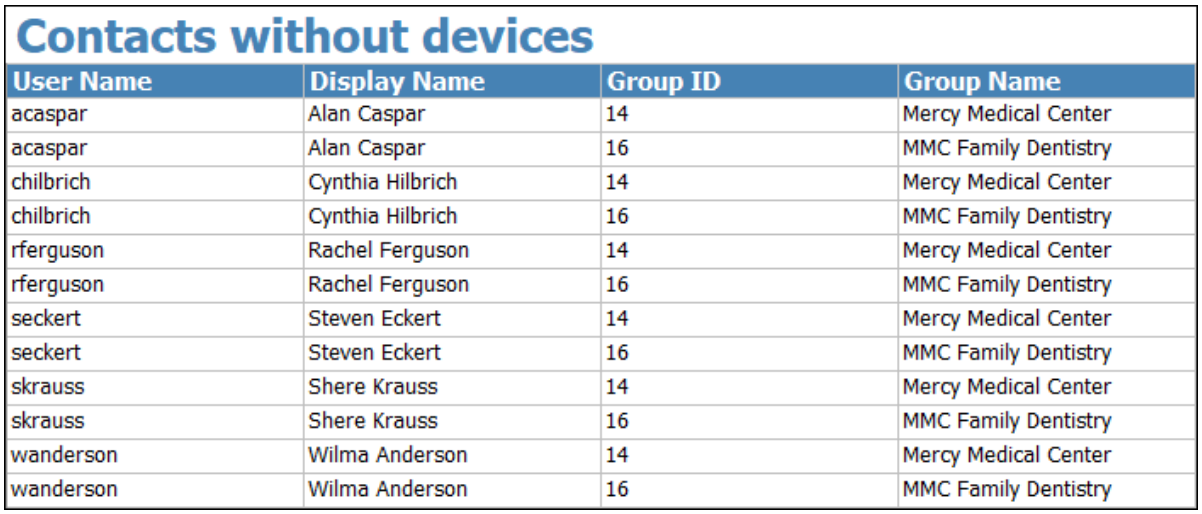
Column	Description
Name	Name indicates the display name of each contact as registered for Amtelco Secure Messages.
User Name	User Name indicates the username of the contact.
Phone Number	Phone Number indicates the phone number of the contact as programmed in the Amtelco Secure Messages Admin Web Contact Settings.
Interval	Interval indicates the number of seconds to wait between notifications when the contact has received a message and has not read the message
Notifications	Notifications indicates the maximum number of notifications to send for one secure message. Message notifications are sent until the message is read by the contact or the maximum number of notifications is reached.
Away Start	Away Start indicates the starting date and time of the most recently selected away message for the contact. If no away message has been selected, the minimum value of “12/31/1752 6:00:00 PM” is displayed.
Away End	Away End indicates the ending date and time of the most recently selected away message for the contact. If no away message has been selected, the minimum value of “12/31/1752 6:00:00 PM” is displayed.
Locked Out	Locked Out is a True or False value that indicates whether the contact is locked out of the Amtelco Secure Messages system. “True” indicates that the contact is locked out, and “False” indicates that the contact is not locked out.
Inception	Inception indicates the date and time that the contact was created.
Licensed	Licensed is a True or False value that indicates whether a valid license is assigned to the contact. “True” indicates that a valid license is assigned, and “False” indicates that the license has expired and needs to be renewed.
Devices	Devices indicates the number of devices that are registered for Amtelco Secure Messages in that user’s name.

Column	Description
Sound	Sound indicates the sound that is played when notifications are on and the user receives a normal priority secure message. “Silent” indicates that no sound is played.
High Priority Sound	High Priority Sound indicates the sound that is played when notifications are on and the user receives a high priority secure message. “Silent” indicates that no sound is played.

Return to Reports
Return to Index

Contacts Without Devices Report

The Contacts Without Devices Report displays a list of contacts in the Amtelco Secure Messages system that do not have any devices registered to their username. These contacts are either using Shared Devices, or are taking up a license but are not using Amtelco Secure Messages.



Contacts without devices

User Name	Display Name	Group ID	Group Name
acaspar	Alan Caspar	14	Mercy Medical Center
acaspar	Alan Caspar	16	MMC Family Dentistry
chilbrich	Cynthia Hilbrich	14	Mercy Medical Center
chilbrich	Cynthia Hilbrich	16	MMC Family Dentistry
rferguson	Rachel Ferguson	14	Mercy Medical Center
rferguson	Rachel Ferguson	16	MMC Family Dentistry
seckert	Steven Eckert	14	Mercy Medical Center
seckert	Steven Eckert	16	MMC Family Dentistry
skrauss	Shere Krauss	14	Mercy Medical Center
skrauss	Shere Krauss	16	MMC Family Dentistry
wanderson	Wilma Anderson	14	Mercy Medical Center
wanderson	Wilma Anderson	16	MMC Family Dentistry

Column	Description
User Name	User Name indicates the username of each contact that does not have any registered devices.
Display Name	Display Name indicates the display name of the contact as registered in the Amtelco Secure Messages app settings or programmed in the Amtelco Secure Messages Admin Web Contact Settings.
Group ID	Group ID indicates the unique ID of each group to which the contact is registered.
Group Name	Group Name indicates the name of the group as programmed in the Amtelco Secure Messages Admin Web Group Properties.

Return to Reports
Return to Index

Database Size Report

The Database Size Report displays the hourly history of the Amtelco Secure Messages database size and unallocated disk space for the specified date and time range.

Database size Report

Time Stamp	Size MB	Unallocated MB
12/8/2017 12:48:24 AM	681.81	0.35
12/8/2017 1:48:25 AM	681.81	0.35
12/8/2017 2:48:26 AM	681.81	0.29
12/8/2017 3:48:26 AM	681.81	0.29
12/8/2017 4:48:26 AM	681.81	0.23
12/8/2017 5:48:27 AM	681.81	0.23
12/8/2017 6:48:27 AM	681.81	0.23
12/8/2017 7:48:28 AM	681.81	0.23
12/8/2017 8:48:28 AM	681.81	0.23
12/8/2017 9:48:28 AM	681.81	0.23
12/8/2017 10:48:29 AM	681.81	0.16
12/8/2017 11:48:30 AM	681.81	0.1
12/8/2017 12:48:30 PM	681.81	0.16
12/8/2017 1:48:30 PM	681.81	0.16
12/8/2017 2:48:31 PM	681.81	0.1
12/8/2017 3:48:31 PM	681.81	0.1
12/8/2017 4:48:31 PM	681.81	0.1
12/8/2017 5:48:31 PM	681.81	0.1
12/8/2017 6:48:32 PM	681.81	0.1
12/8/2017 7:48:33 PM	681.81	0.1
12/8/2017 8:48:34 PM	682.81	1.1
12/8/2017 9:48:34 PM	682.81	1.1
12/8/2017 10:48:34 PM	682.81	1.04
12/8/2017 11:48:35 PM	682.81	1.04

Column	Description
Time Stamp	Time Stamp indicates the date and time of the database size data. Database size data points are displayed in one-hour intervals for the specified date and time range.
Size MB	Size MB indicates the total amount of disk space, in megabytes, that was occupied by the Amtelco Secure Messages database at each date and time.
Unallocated MB	Unallocated MB indicates the amount of disk space, in megabytes, within the Amtelco Secure Messages database that is no longer in use.

Return to Reports
Return to Index

Device List Report

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

Device list

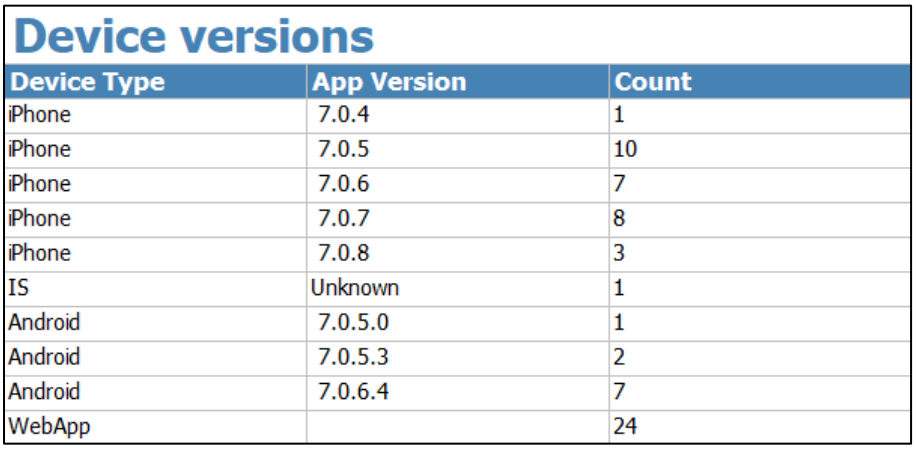
Name	User Name	Device Type	Device Model	App Version	Os Version	Last Login	Device Mode	Phone Number
Amy Thompson	athompson	WebApp				5/20/2024 12:03:27 PM	Normal	
Andrea Ward	award	iPhone	iPhone	7.0.5	17.2.1	11/25/2024 2:48:22 PM	Normal	
Andrea Ward	award	iPhone	iPhone	7.0.5	17.2.1	11/25/2024 2:51:18 PM	Normal	
Andrea Ward	award	iPhone	iPhone	7.0.5	17.2.1	12/2/2024 9:47:35 AM	Normal	
Andrea Ward	award	iPhone	iPhone	7.0.5	17.2.1	12/2/2024 12:11:48 PM	Normal	
Andrea Ward	award	iPhone	iPhone	7.0.6	17.5.1	12/11/2024 1:58:29 PM	Normal	
Andrea Ward	award	iPhone	iPhone	7.0.8	18.3.1	2/26/2025 9:05:33 PM	Shared	7115559565
Andrea Ward	award	WebApp				4/7/2025 3:51:09 PM	Normal	
Angela Massey	amassey	WebApp				4/25/2024 11:21:56 AM	Normal	
David Darcy	ddarcy	iPhone	iPhone	7.0.6	17.5.1	1/7/2025 2:42:40 PM	Normal	
David Darcy	ddarcy	iPhone	iPhone	7.0.7	17.5.1	1/8/2025 11:38:46 AM	Normal	
DeAnn Womson	dwomson	WebApp				5/20/2024 12:23:40 PM	Normal	
Demo	Demo	WebApp				3/6/2025 11:10:56 AM	Normal	
Erica Sorenson	esorenson	WebApp				4/15/2025 2:20:08 PM	Normal	
Erica Sorenson	esorenson	Android	Pixel 7(panther)	7.0.6.4	16	4/9/2025 4:02:43 PM	Normal	
Kori Anderson	kanderson	WebApp				5/20/2024 12:04:24 PM	Normal	
Maren Gonzalez	mgonzalez	WebApp				5/20/2024 12:04:39 PM	Normal	
Mary Edwards	medwards	WebApp				5/20/2024 12:04:48 PM	Normal	
Patty Anderson	panderson	iPhone	iPhone	7.0.6	18.3.1	3/7/2025 3:52:09 PM	Normal	
Robert Smith	rsmith	WebApp				5/20/2024 12:05:02 PM	Normal	
Ryan Sauter	rsauter	iPhone	iPhone	7.0.6	17.6.1	12/19/2024 9:09:37 AM	Normal	
Ryan Sauter	rsauter	WebApp				11/12/2024 12:30:42 PM	Normal	
Sarah Zimoneck	szimoneck	iPhone	iPhone	7.0.5	18.1	11/20/2024 12:23:58 PM	Normal	
Sarah Zimoneck	szimoneck	iPhone	iPhone	7.0.6	18.2	12/16/2024 7:26:53 AM	Normal	
Sarah Zimoneck	szimoneck	iPhone	iPhone	7.0.7	18.3.1	4/1/2025 9:11:51 AM	Normal	
Sarah Zimoneck	szimoneck	WebApp				10/16/2024 12:28:47 PM	Normal	
Sarah Zimoneck	szimoneck	iPhone	iPhone	7.0.5	18.1	10/21/2024 9:33:59 AM	Normal	

Column	Description
Name	Name indicates the display name of each contact as registered for Amtelco Secure Messages on a device app or the Amtelco Secure Messages Contact Web.
User Name	User Name indicates the username of the contact.
Device Type	Device Type indicates the type of each device registered to the contact. Possible device types are Android, Infinity, iPhone, iPad, iPod, IS, and WebApp (for Contact Web access).
Device Model	Device Model indicates the model of the device, if available.
App Version	App Version indicates the version number of the Amtelco Secure Messages app that is installed on the device, if available.
OS Version	OS Version indicates the operating system running on the device, if available, or the API Level for Android devices.
Last Login	Last Login indicates the most recent date and time that the user logged into Amtelco Secure Messages on the device.
Device Mode	Device Mode indicates whether or not the device is registered as a Shared Device. “Normal” indicates that the device is registered as a single-user device. “Shared” indicates that the device is registered as a Shared Device.
Phone Number	Phone Number indicates the Device Phone Number associated with the device, if one has been configured.

Return to Reports
Return to Index

Device Versions Report

The Device Version Report displays a list of device types and the number of devices registered for each version of the Amtelco Secure Messages app.



Device versions

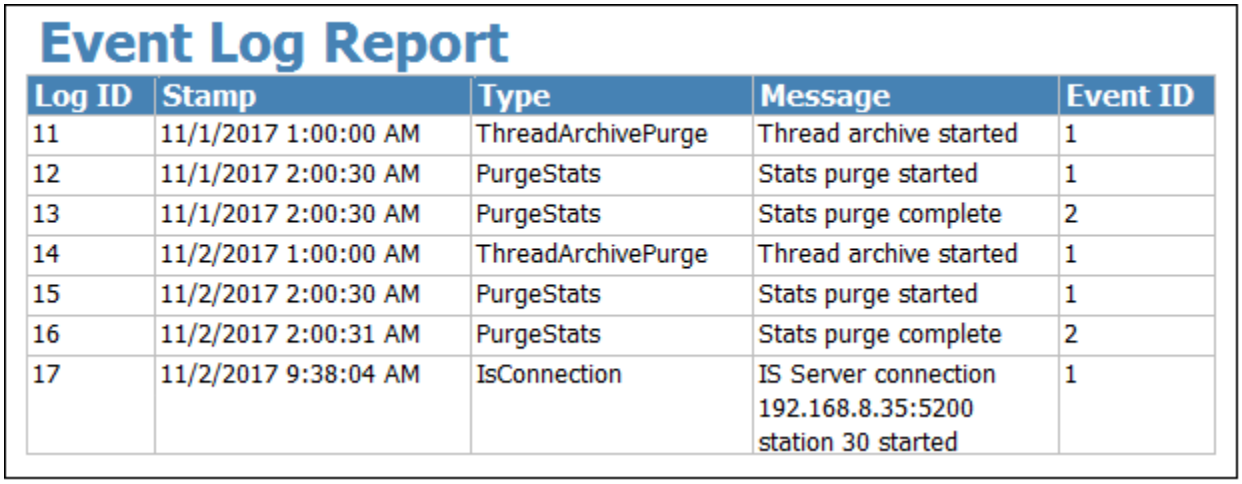
Device Type	App Version	Count
iPhone	7.0.4	1
iPhone	7.0.5	10
iPhone	7.0.6	7
iPhone	7.0.7	8
iPhone	7.0.8	3
IS	Unknown	1
Android	7.0.5.0	1
Android	7.0.5.3	2
Android	7.0.6.4	7
WebApp		24

Column	Description
Device Type	Device Type indicates the type of each device registered for Amtelco Secure Messages. Possible device types are Android, iPhone, iPad, iPod, and Contact Web. The connections configured on the Connections page are also listed.
App Version	App Version indicates the version number of the Amtelco Secure Messages app that is installed on the device. No version is listed for connections.
Count	Count indicates the number of devices that are running the app version listed or the number of connections configured for each connection type.

Return to Reports
Return to Index

Event Log Report

The Event Log Report displays all the events that have occurred in the Amtelco Secure Messages Admin Web Server during the specified date and time range.



Event Log Report

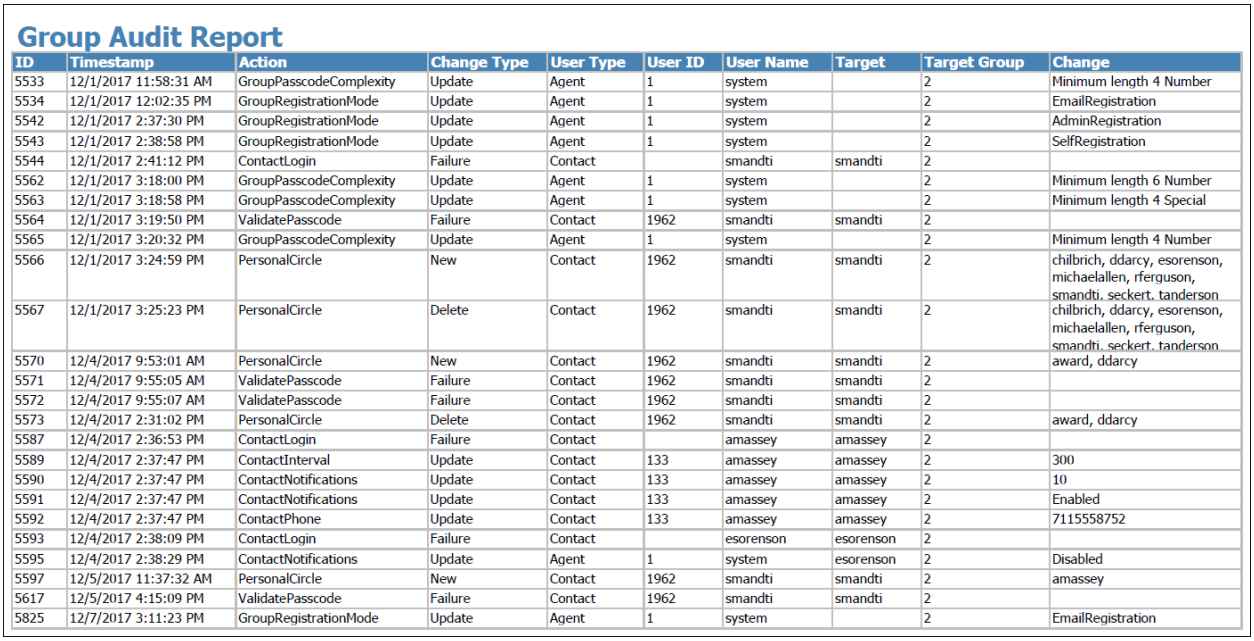
Log ID	Stamp	Type	Message	Event ID
11	11/1/2017 1:00:00 AM	ThreadArchivePurge	Thread archive started	1
12	11/1/2017 2:00:30 AM	PurgeStats	Stats purge started	1
13	11/1/2017 2:00:30 AM	PurgeStats	Stats purge complete	2
14	11/2/2017 1:00:00 AM	ThreadArchivePurge	Thread archive started	1
15	11/2/2017 2:00:30 AM	PurgeStats	Stats purge started	1
16	11/2/2017 2:00:31 AM	PurgeStats	Stats purge complete	2
17	11/2/2017 9:38:04 AM	IsConnection	IS Server connection 192.168.8.35:5200 station 30 started	1

Column	Description
Log ID	Log ID indicates the unique ID associated with each log entry.
Stamp	Stamp indicates the date and time the event occurred.
Type	Type indicates the type of event that occurred.
Message	Message indicates details about the event.
Event ID	Event ID is a number representing the following kinds of events: 0: None 1: Start 2: Complete 3: Error 4: Connected 5: Offline 6: Stopped

Return to Reports
Return to Index

Group Audit Report

The Group Audit Report enables you to view an Audit Report for specific groups. The Group Audit Report displays all the actions that have occurred in the Amtelco Secure Messages Admin Web Server for the specified groups during the specified date and time range. Actions include updates made to configuration, Circles, groups, admins, and contacts settings, Amtelco Secure Messages Admin Web administrator log ins and log outs, initiated reports, and more.



Group Audit Report

ID	Timestamp	Action	Change Type	User Type	User ID	User Name	Target	Target Group	Change
5533	12/1/2017 11:58:31 AM	GroupPasscodeComplexity	Update	Agent	1	system		2	Minimum length 4 Number
5534	12/1/2017 12:02:35 PM	GroupRegistrationMode	Update	Agent	1	system		2	EmailRegistration
5542	12/1/2017 2:37:30 PM	GroupRegistrationMode	Update	Agent	1	system		2	AdminRegistration
5543	12/1/2017 2:38:58 PM	GroupRegistrationMode	Update	Agent	1	system		2	SelfRegistration
5544	12/1/2017 2:41:12 PM	ContactLogin	Failure	Contact		smandti	smandti	2	
5562	12/1/2017 3:18:00 PM	GroupPasscodeComplexity	Update	Agent	1	system		2	Minimum length 6 Number
5563	12/1/2017 3:18:58 PM	GroupPasscodeComplexity	Update	Agent	1	system		2	Minimum length 4 Special
5564	12/1/2017 3:19:50 PM	ValidatePasscode	Failure	Contact	1962	smandti	smandti	2	
5565	12/1/2017 3:20:32 PM	GroupPasscodeComplexity	Update	Agent	1	system		2	Minimum length 4 Number
5566	12/1/2017 3:24:59 PM	PersonalCircle	New	Contact	1962	smandti	smandti	2	chilbrich, ddarcy, esorenson, michaelallen, rferguson, smandti, seckert, tanderson
5567	12/1/2017 3:25:23 PM	PersonalCircle	Delete	Contact	1962	smandti	smandti	2	chilbrich, ddarcy, esorenson, michaelallen, rferguson, smandti, seckert, tanderson
5570	12/4/2017 9:53:01 AM	PersonalCircle	New	Contact	1962	smandti	smandti	2	award, ddarcy
5571	12/4/2017 9:55:05 AM	ValidatePasscode	Failure	Contact	1962	smandti	smandti	2	
5572	12/4/2017 9:55:07 AM	ValidatePasscode	Failure	Contact	1962	smandti	smandti	2	
5573	12/4/2017 2:31:02 PM	PersonalCircle	Delete	Contact	1962	smandti	smandti	2	award, ddarcy
5587	12/4/2017 2:36:53 PM	ContactLogin	Failure	Contact		amassey	amassey	2	
5589	12/4/2017 2:37:47 PM	ContactInterval	Update	Contact	133	amassey	amassey	2	300
5590	12/4/2017 2:37:47 PM	ContactNotifications	Update	Contact	133	amassey	amassey	2	10
5591	12/4/2017 2:37:47 PM	ContactNotifications	Update	Contact	133	amassey	amassey	2	Enabled
5592	12/4/2017 2:37:47 PM	ContactPhone	Update	Contact	133	amassey	amassey	2	7115558752
5593	12/4/2017 2:38:09 PM	ContactLogin	Failure	Contact		esorenson	esorenson	2	
5595	12/4/2017 2:38:29 PM	ContactNotifications	Update	Agent	1	system	esorenson	2	Disabled
5597	12/5/2017 11:37:32 AM	PersonalCircle	New	Contact	1962	smandti	smandti	2	amassey
5617	12/5/2017 4:15:09 PM	ValidatePasscode	Failure	Contact	1962	smandti	smandti	2	
5825	12/7/2017 3:11:23 PM	GroupRegistrationMode	Update	Agent	1	system		2	EmailRegistration

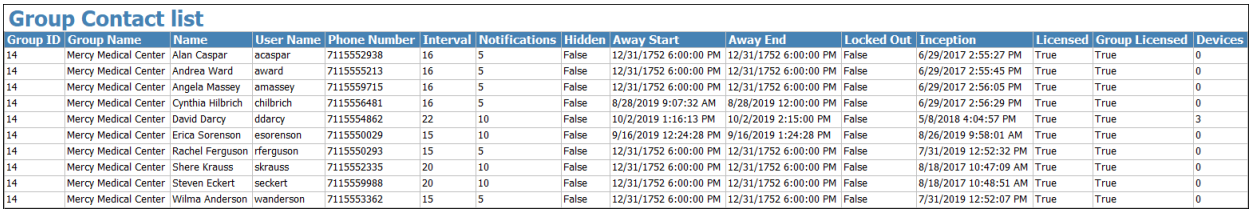
Column	Description
ID	ID indicates the unique ID associated with each action.
Timestamp	Timestamp indicates the date and time the action occurred.
Action	Action indicates the type of action that was initiated. For more information regarding the different action types that may appear in the Group Audit Report, refer to the Actions table in the appendixes of this document.
Change Type	Change Type indicates the type of change that resulted from the action.
User Type	User Type indicates the type of user that initiated the action. User Type could be “Agent,” indicating an Amtelco Secure Messages Admin Web administrator, or “Contact,” indicating a Amtelco Secure Messages contact.
User ID	User ID indicates the unique ID associated with the user who initiated the action.
User Name	User Name indicates the username of the user that initiated the action.
Target	Target indicates the name of the Amtelco Secure Messages user, group, or Circle to which the changes were applied.
Target Group	Target Group indicates the unique ID associated with the group to which the change was applied.

Column	Description
Change	Change indicates details about the change that occurred.

Return to Reports
Return to Index

Group Contact List Report

The Group Contact List Report enables you to view a Contact List Report for specific contacts and groups. The Contact List Report displays a list of contacts that are registered to the specified groups and a summary of Contact Settings for each.



Group Contact list

Group ID	Group Name	Name	User Name	Phone Number	Interval	Notifications	Hidden	Away Start	Away End	Locked Out	Inception	Licensed	Group Licensed	Devices
14	Mercy Medical Center	Alan Caspar	acaspar	7115552938	16	5	False	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/29/2017 2:55:27 PM	True	True	0
14	Mercy Medical Center	Andrea Ward	award	7115555213	16	5	False	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/29/2017 2:55:45 PM	True	True	0
14	Mercy Medical Center	Angela Massey	amassey	7115559715	16	5	False	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	6/29/2017 2:56:05 PM	True	True	0
14	Mercy Medical Center	Cynthia Hilbrich	chilbrich	7115556481	16	5	False	8/28/2019 9:07:32 AM	8/28/2019 12:00:00 PM	False	6/29/2017 2:56:29 PM	True	True	0
14	Mercy Medical Center	David Darcy	ddarcy	7115554862	22	10	False	10/2/2019 1:16:13 PM	10/2/2019 2:15:00 PM	False	5/8/2018 4:04:57 PM	True	True	3
14	Mercy Medical Center	Erica Sorenson	esorenson	7115550029	15	10	False	9/16/2019 12:24:28 PM	9/16/2019 1:24:28 PM	False	8/26/2019 9:58:01 AM	True	True	0
14	Mercy Medical Center	Rachel Ferguson	rferguson	7115550293	15	5	False	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	7/31/2019 12:52:32 PM	True	True	0
14	Mercy Medical Center	Shere Krauss	skrauss	7115552335	20	10	False	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	8/18/2017 10:47:09 AM	True	True	0
14	Mercy Medical Center	Steven Eckert	seckert	7115559988	20	10	False	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	8/18/2017 10:48:51 AM	True	True	0
14	Mercy Medical Center	Wilma Anderson	wanderson	7115553362	15	5	False	12/31/1752 6:00:00 PM	12/31/1752 6:00:00 PM	False	7/31/2019 12:52:07 PM	True	True	0

Note: Not all fields in the Contact List Report are shown in the screenshot.

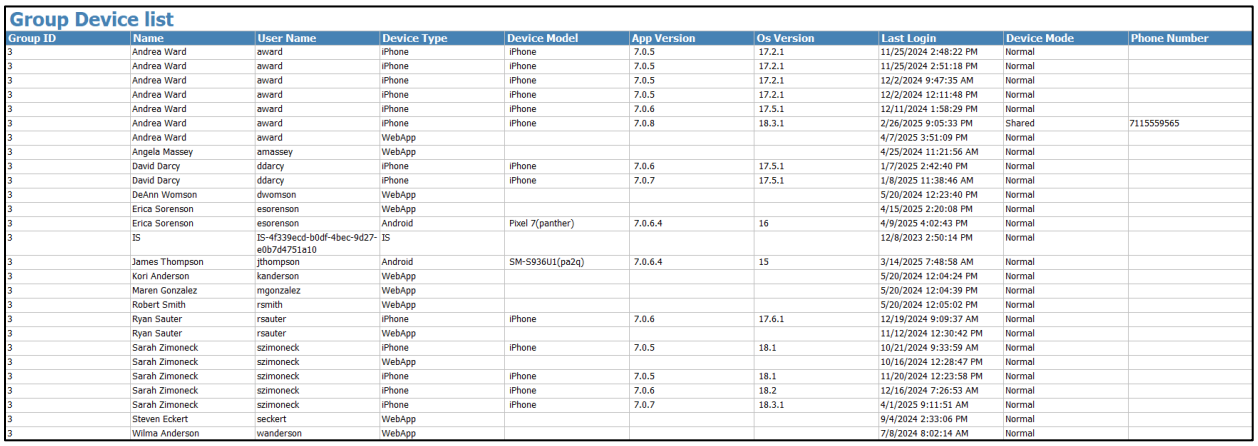
Column	Description
Group ID	Group ID indicates the unique ID associated with each group included within the report parameters.
Group Name	Group Name indicates the name of the group as programmed in the Amtelco Secure Messages Admin Web Group Properties.
Name	Name indicates the display name of each contact registered for the group.
User Name	User Name indicates the username of the contact.
Phone Number	Phone Number indicates the phone number of the contact as programmed in the Amtelco Secure Messages Admin Web Contact Settings.
Interval	Interval indicates the number of seconds to wait between notifications when the contact has received a message and has not read the message
Notifications	Notifications indicates the maximum number of notifications to send for one secure message. Message notifications are sent until the message is read by the contact or the maximum number of notifications is reached.
Hidden	Hidden is a True or False that indicates whether the contact is hidden from the Contact List for the group. “True” indicates the contact is hidden, and “False” indicates the contact is not hidden.
Away Start	Away Start indicates the starting date and time of the most recently selected away message for the contact. If no away message has been selected, the minimum value of “12/31/1752 6:00:00 PM” is displayed.
Away End	Away End indicates the ending date and time of the most recently selected away message for the contact. If no away message has been selected, the minimum value of “12/31/1752 6:00:00 PM” is displayed.
Locked Out	Locked Out is a True or False value that indicates whether the contact is locked out of the Amtelco Secure Messages system. “True” indicates that the contact is locked out, and “False” indicates that the contact is not locked out.
Inception	Inception indicates the date and time that the contact was created.

Column	Description
Licensed	Licensed is a True or False value that indicates whether a valid license is assigned to the contact. “True” indicates that a valid license is assigned, and “False” indicates that the license has expired and needs to be renewed.
Group Licensed	Group Licensed is a True or False value that indicates whether a group license is assigned to the contact. A group license is assigned when a contact registers for a group other than Group 0. “True” indicates that a group license is assigned. “False” indicates the group license has expired, or that the Group ID listed in the Group ID column is zero (0).
Devices	Devices indicates the number of devices that are registered for Amtelco Secure Messages in the user’s name.
Active	Active is a True or False value that indicates whether or not the contact is marked as active. “True” indicates that the contact is marked as active and is allowed to log into the group. “False” indicates that the contact is not marked as active and is prevented from logging into the group.
Sound	Sound indicates the sound that is played when notifications are on and the user receives a normal priority secure message. “Silent” indicates that no sound is played.
High Priority Sound	High Priority Sound indicates the sound that is played when notifications are on and the user receives a high priority secure message. “Silent” indicates that no sound is played.

Return to Reports
Return to Index

Group Device List Report

The Group Device List Report enables you to view a Device List Report for specific groups. The Device List Report displays a list of devices registered for Amtelco Secure Messages within the specified groups. The devices are listed by Group ID.



Group Device list

Group ID	Name	User Name	Device Type	Device Model	App Version	Os Version	Last Login	Device Mode	Phone Number
3	Andrea Ward	award	iPhone	iPhone	7.0.5	17.2.1	11/25/2024 2:48:22 PM	Normal	
3	Andrea Ward	award	iPhone	iPhone	7.0.5	17.2.1	11/25/2024 2:51:18 PM	Normal	
3	Andrea Ward	award	iPhone	iPhone	7.0.5	17.2.1	12/2/2024 9:47:35 AM	Normal	
3	Andrea Ward	award	iPhone	iPhone	7.0.5	17.2.1	12/2/2024 12:11:48 PM	Normal	
3	Andrea Ward	award	iPhone	iPhone	7.0.6	17.5.1	12/11/2024 1:58:29 PM	Normal	
3	Andrea Ward	award	iPhone	iPhone	7.0.8	18.3.1	2/26/2025 9:05:33 PM	Shared	7115559565
3	Andrea Ward	award	WebApp				4/7/2025 3:51:09 PM	Normal	
3	Angela Massey	amassey	WebApp				4/25/2024 11:21:56 AM	Normal	
3	David Darcy	ddarcy	iPhone	iPhone	7.0.6	17.5.1	1/7/2025 2:42:40 PM	Normal	
3	David Darcy	ddarcy	iPhone	iPhone	7.0.7	17.5.1	1/8/2025 11:38:46 AM	Normal	
3	DeAnn Womson	dwomson	WebApp				5/20/2024 12:23:40 PM	Normal	
3	Erica Sorenson	esorenson	WebApp				4/15/2025 2:20:08 PM	Normal	
3	Erica Sorenson	esorenson	Android	Pixel 7(panther)	7.0.6.4	16	4/9/2025 4:02:43 PM	Normal	
3	IS	IS-4f339ecd-b0df-4bec-9d27-e0b7d4751a10	IS				12/8/2023 2:50:14 PM	Normal	
3	James Thompson	jthompson	Android	SM-S936U1(pa2q)	7.0.6.4	15	3/14/2025 7:48:58 AM	Normal	
3	Kori Anderson	kanderson	WebApp				5/20/2024 12:04:24 PM	Normal	
3	Maren Gonzalez	mgonzalez	WebApp				5/20/2024 12:04:39 PM	Normal	
3	Robert Smith	rsmith	WebApp				5/20/2024 12:05:02 PM	Normal	
3	Ryan Sauter	rsauter	iPhone	iPhone	7.0.6	17.6.1	12/19/2024 9:09:37 AM	Normal	
3	Ryan Sauter	rsauter	WebApp				11/12/2024 12:30:42 PM	Normal	
3	Sarah Zimoneck	szimoneck	iPhone	iPhone	7.0.5	18.1	10/21/2024 9:33:59 AM	Normal	
3	Sarah Zimoneck	szimoneck	WebApp				10/16/2024 12:28:47 PM	Normal	
3	Sarah Zimoneck	szimoneck	iPhone	iPhone	7.0.5	18.1	11/20/2024 12:23:58 PM	Normal	
3	Sarah Zimoneck	szimoneck	iPhone	iPhone	7.0.6	18.2	12/16/2024 7:26:53 AM	Normal	
3	Sarah Zimoneck	szimoneck	iPhone	iPhone	7.0.7	18.3.1	4/1/2025 9:11:51 AM	Normal	
3	Steven Eckert	seckert	WebApp				9/4/2024 2:33:06 PM	Normal	
3	Wilma Anderson	wanderson	WebApp				7/8/2024 8:02:14 AM	Normal	

Column	Description
Group ID	Group ID indicates the unique ID associated with each group included within the report parameters.
Name	Name indicates the display name of the contact as registered in the Amtelco Secure Messages app settings or programmed in the Amtelco Secure Messages Admin Web Contact Settings.
User Name	User Name indicates the username of the contact.
Device Type	Device Type indicates the type of device. Possible device types are Android, Infinity, iPhone, iPad, iPod, IS, and WebApp (for Contact Web access).
Device Model	Device Model indicates the model of the device, if available.
App Version	App Version indicates the version number of the Amtelco Secure Messages app that is installed on the device, if available.
OS Version	OS Version indicates the operating system running on the device, if available, or the API Level for Android devices.
Last Login	Last Login indicates the most recent date and time that the user logged into Amtelco Secure Messages on the device.
Device Mode	Device Mode indicates whether or not the device is registered as a Shared Device. “Normal” indicates that the device is registered as a single-user device. “Shared” indicates that the device is registered as a Shared Device.
Phone Number	Phone Number indicates the Device Phone Number associated with the device, if one has been configured.

Return to Reports
Return to Index

Group Device Versions Report

The Group Device Versions Report enables you to view a Device Versions Report for specific groups. The Group Device Versions Report displays counts of all device types in the specified groups. The counts are listed by group name.

Group Device versions

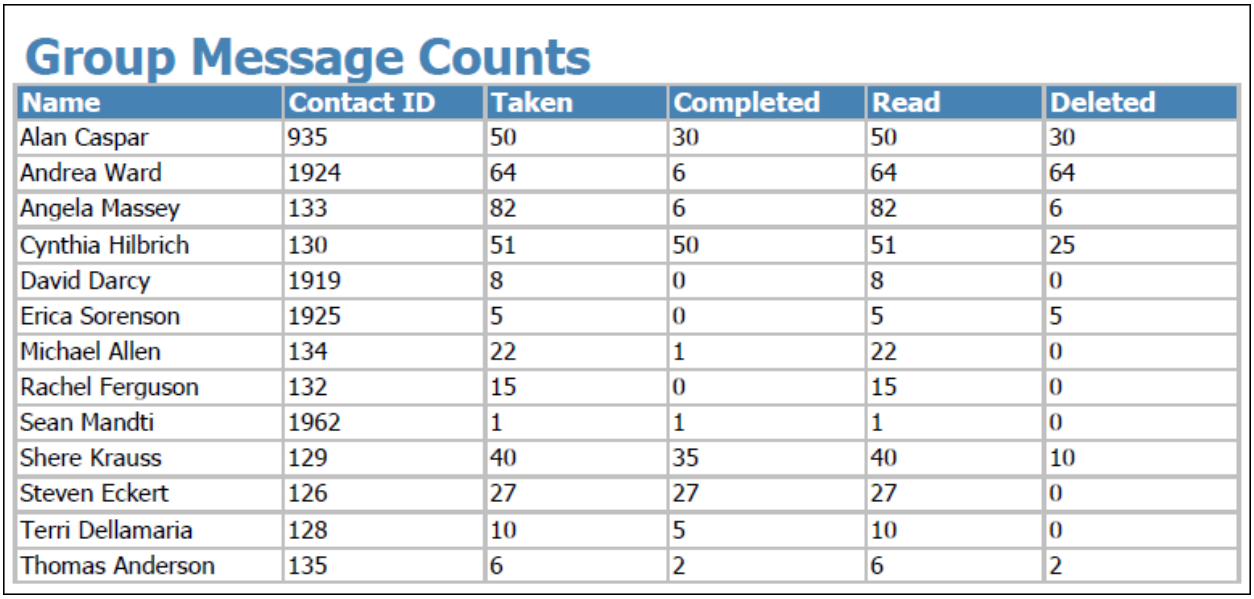
Name	Group ID	Device Type	App Version	Count
General Hospital	0	iPhone	7.0.7	6
General Hospital	0	IS	Unknown	1
General Hospital	0	Android	7.0.5.0	1
General Hospital	0	Android	7.0.5.3	2
General Hospital	0	Android	7.0.6.4	5
General Hospital	0	WebApp		11
Mercy Medical Center Network	3	iPhone	7.0.7	2
Mercy Medical Center Network	3	iPhone	7.0.8	1
Mercy Medical Center Network	3	IS	Unknown	1
Mercy Medical Center Network	3	Android	7.0.6.4	3
Mercy Medical Center Network	3	WebApp		12
Real Estate Company	29	iPhone	7.0.7	1
Real Estate Company	29	iPhone	7.0.8	1
Real Estate Company	29	Android	7.0.6.4	3
Real Estate Company	29	WebApp		12

Column	Description
Name	Name indicates the name of the group included within the report parameters.
Group ID	Group ID indicates the unique ID number associated with the group.
Device Type	Device Type indicates the type of device. Possible device types are Android, iPhone, iPad, iPod, and Contact Web. The connections configured on the Connections page are also listed.
App Version	App Version indicates the version number of the Amtelco Secure Messages app that is installed on the device. No version is listed for connections.
Count	Count indicates the number of devices in the specified group that are running the app version listed or the number of connections configured for each connection type.

Return to Reports
Return to Index

Group Message Counts Report

The Group Message Counts Report enables you to view a Message Counts Report for specific groups. The Message Counts Report displays counts of all secure messages sent by each contact in the specified groups during the specified date and time range. The counts are listed by contact name according to the contact that sent the message.



Group Message Counts

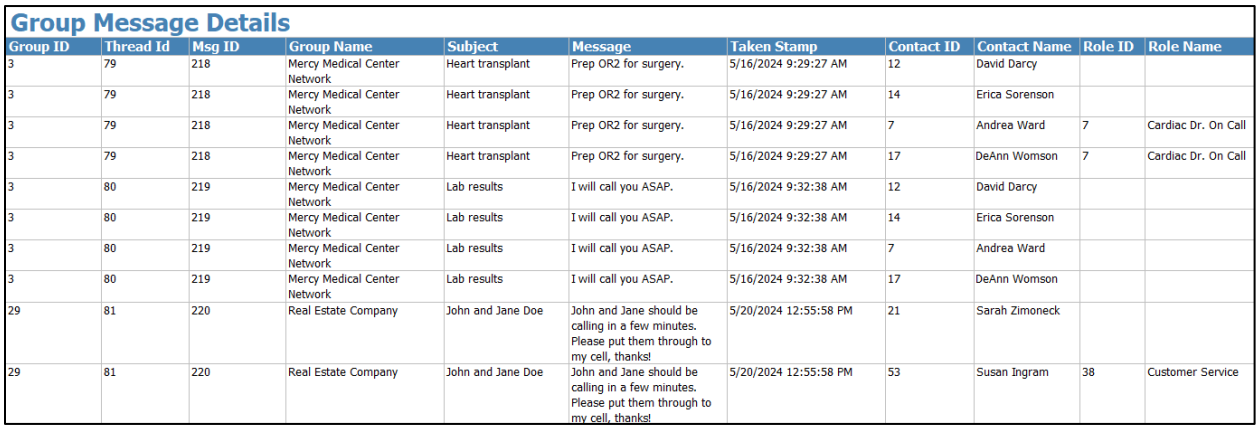
Name	Contact ID	Taken	Completed	Read	Deleted
Alan Caspar	935	50	30	50	30
Andrea Ward	1924	64	6	64	64
Angela Massey	133	82	6	82	6
Cynthia Hilbrich	130	51	50	51	25
David Darcy	1919	8	0	8	0
Erica Sorenson	1925	5	0	5	5
Michael Allen	134	22	1	22	0
Rachel Ferguson	132	15	0	15	0
Sean Mandti	1962	1	1	1	0
Shere Krauss	129	40	35	40	10
Steven Eckert	126	27	27	27	0
Terri Dellamaria	128	10	5	10	0
Thomas Anderson	135	6	2	6	2

Column	Description
Name	Name indicates the name of each contact registered for a group that is included in the report parameters.
Contact ID	Contact ID indicates the unique ID associated with the contact.
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.

[Return to Reports]
[Return to Index]

Group Message Details Report

The Group Message Details Report allows you to view a comprehensive messages report for specific contacts and groups. The Group Message Details Report displays information about secure messages sent during the specified date and time range for the specified groups. A table displays the following columns of information about all messages sent or received by the specified contacts, with a row displayed for each time a contact sent or received a message.



Group Message Details

Group ID	Thread Id	Msg ID	Group Name	Subject	Message	Taken Stamp	Contact ID	Contact Name	Role ID	Role Name
3	79	218	Mercy Medical Center Network	Heart transplant	Prep OR2 for surgery.	5/16/2024 9:29:27 AM	12	David Darcy		
3	79	218	Mercy Medical Center Network	Heart transplant	Prep OR2 for surgery.	5/16/2024 9:29:27 AM	14	Erica Sorenson		
3	79	218	Mercy Medical Center Network	Heart transplant	Prep OR2 for surgery.	5/16/2024 9:29:27 AM	7	Andrea Ward	7	Cardiac Dr. On Call
3	79	218	Mercy Medical Center Network	Heart transplant	Prep OR2 for surgery.	5/16/2024 9:29:27 AM	17	DeAnn Womson	7	Cardiac Dr. On Call
3	80	219	Mercy Medical Center Network	Lab results	I will call you ASAP.	5/16/2024 9:32:38 AM	12	David Darcy		
3	80	219	Mercy Medical Center Network	Lab results	I will call you ASAP.	5/16/2024 9:32:38 AM	14	Erica Sorenson		
3	80	219	Mercy Medical Center Network	Lab results	I will call you ASAP.	5/16/2024 9:32:38 AM	7	Andrea Ward		
3	80	219	Mercy Medical Center Network	Lab results	I will call you ASAP.	5/16/2024 9:32:38 AM	17	DeAnn Womson		
29	81	220	Real Estate Company	John and Jane Doe	John and Jane should be calling in a few minutes. Please put them through to my cell, thanks!	5/20/2024 12:55:58 PM	21	Sarah Zimoneck		
29	81	220	Real Estate Company	John and Jane Doe	John and Jane should be calling in a few minutes. Please put them through to my cell, thanks!	5/20/2024 12:55:58 PM	53	Susan Ingram	38	Customer Service

Note: Not all fields in the Group Message Details Report are shown in the screenshot.

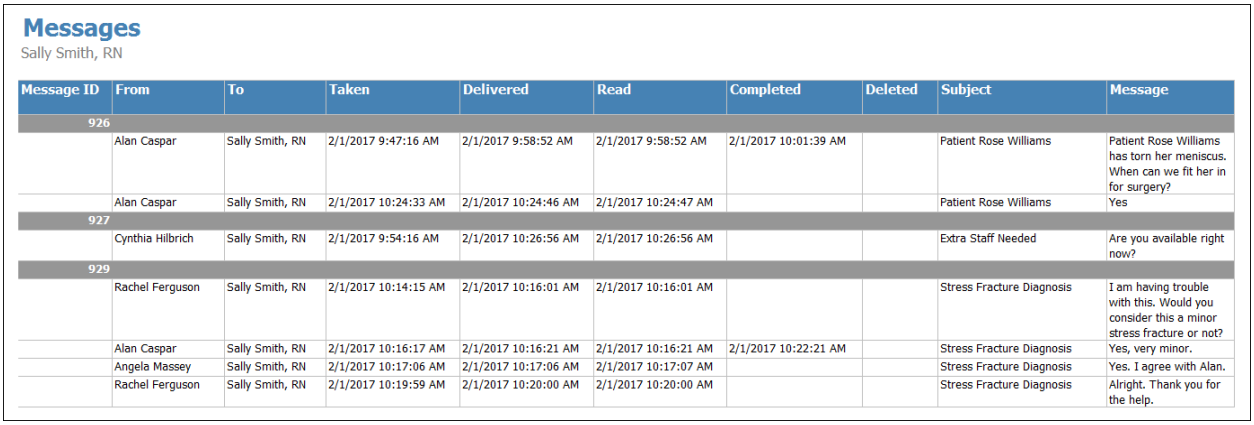
Column	Description
Group ID	Group ID indicates the unique ID of the group that was used to send the secure message.
Thread ID	Thread ID indicates the unique ID associated with the message thread. Each message thread contains one new secure message and all of the replies to that secure message.
Msg ID	Msg ID indicates the unique ID associated with the message.
Group Name	Group Name indicates the name of the group that was used to send the secure message.
Subject	Subject indicates the subject of the message.
Message	Message indicates the content of the message.
Taken Stamp	Message indicates the date and time the message was sent.
Contact ID	Contact ID indicates the unique ID associated with the contact that sent or received the message.
Contact Name	Contact Name indicates the contact name of the person that sent or received the message.
Role ID	Role ID indicates the unique ID of the role that sent or received the message.
Role Name	Role Name indicates the name of the role that sent or received the message.

Column	Description
Delivered Stamp	Delivered Stamp indicates the date and time that the message was downloaded to the recipient's device.
Read Stamp	Read Stamp indicates the date and time that the message was displayed on the recipient's device.
Completed Stamp	Completed Stamp indicates the date and time that the recipient marked the message Completed.
Deleted Stamp	Deleted Stamp indicates the date and time that the recipient deleted the message.

Return to Reports
Return to Index

Group Messages - Formatted Report

The formatted version of the Group Messages Report enables you to view a Messages Report for specific contacts, groups, and roles in an easy-to-read format. The Group Messages Report displays information about secure messages sent during the specified date and time range to and from the specified contacts and roles for the specified groups. The report is divided into separate pages by contact name. The contact name is displayed at the top of the page. A table displays the following columns of information about all messages received by that contact or role.



Messages

Sally Smith, RN

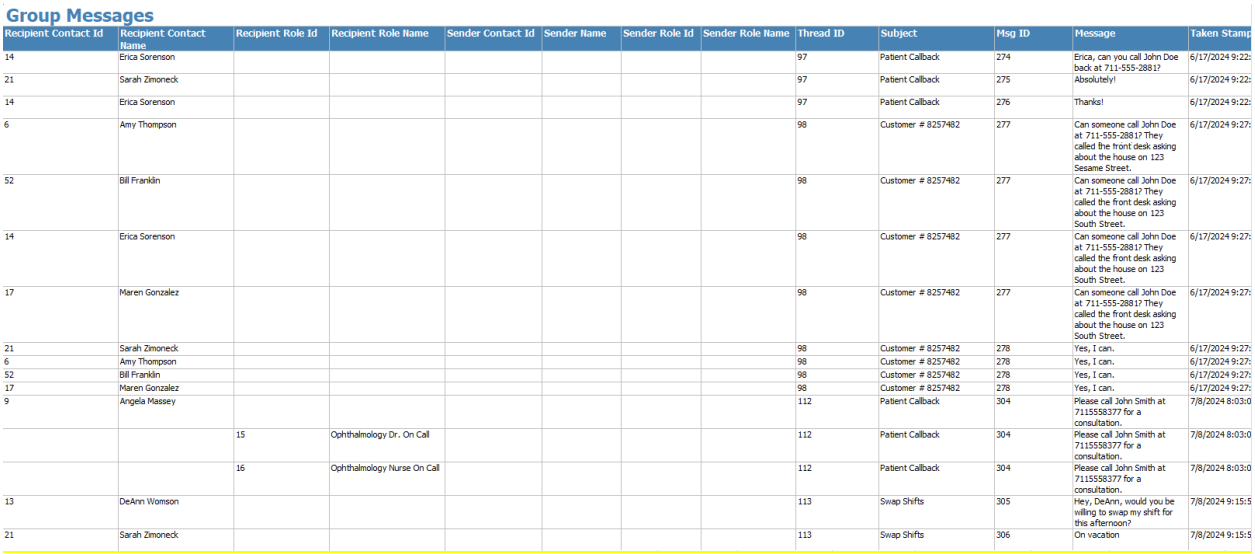
Message ID	From	To	Taken	Delivered	Read	Completed	Deleted	Subject	Message
926									
	Alan Caspar	Sally Smith, RN	2/1/2017 9:47:16 AM	2/1/2017 9:58:52 AM	2/1/2017 9:58:52 AM	2/1/2017 10:01:39 AM		Patient Rose Williams	Patient Rose Williams has torn her meniscus. When can we fit her in for surgery?
	Alan Caspar	Sally Smith, RN	2/1/2017 10:24:33 AM	2/1/2017 10:24:46 AM	2/1/2017 10:24:47 AM			Patient Rose Williams	Yes
927									
	Cynthia Hilbrich	Sally Smith, RN	2/1/2017 9:54:16 AM	2/1/2017 10:26:56 AM	2/1/2017 10:26:56 AM			Extra Staff Needed	Are you available right now?
929									
	Rachel Ferguson	Sally Smith, RN	2/1/2017 10:14:15 AM	2/1/2017 10:16:01 AM	2/1/2017 10:16:01 AM			Stress Fracture Diagnosis	I am having trouble with this. Would you consider this a minor stress fracture or not?
	Alan Caspar	Sally Smith, RN	2/1/2017 10:16:17 AM	2/1/2017 10:16:21 AM	2/1/2017 10:16:21 AM	2/1/2017 10:22:21 AM		Stress Fracture Diagnosis	Yes, very minor.
	Angela Massey	Sally Smith, RN	2/1/2017 10:17:06 AM	2/1/2017 10:17:06 AM	2/1/2017 10:17:07 AM			Stress Fracture Diagnosis	Yes. I agree with Alan.
	Rachel Ferguson	Sally Smith, RN	2/1/2017 10:19:59 AM	2/1/2017 10:20:00 AM	2/1/2017 10:20:00 AM			Stress Fracture Diagnosis	Alright. Thank you for the help.

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.
Delivered	Delivered indicates the date and time that the message was downloaded to the recipient's device.
Read	Read indicates the date and time that the message was displayed on the recipient's device.
Completed	Completed indicates the date and time that the recipient marked the message Completed.
Deleted	Deleted indicates the date and time that the recipient deleted the message.
Subject	Subject indicates the subject of the message.
Message	Message indicates the content of the message.

Return to Reports
Return to Index

Group Messages Report

The Group Messages Report allows you to view a comprehensive Messages Report for specific contacts, groups, and roles. The Group Messages Report displays information about secure messages sent during the specified date and time range for the specified groups. A table displays the following columns of information about all messages sent or received by the specified contacts and roles.



Group Messages

Recipient Contact Id	Recipient Contact Name	Recipient Role Id	Recipient Role Name	Sender Contact Id	Sender Name	Sender Role Id	Sender Role Name	Thread ID	Subject	Msg ID	Message	Taken Stamp
14	Erica Sorenson							97	Patient Callback	274	Erica, can you call John Doe back at 711-555-2881?	6/17/2024 9:22:
21	Sarah Zimoneck							97	Patient Callback	275	Absolutely!	6/17/2024 9:22:
14	Erica Sorenson							97	Patient Callback	276	Thanks!	6/17/2024 9:22:
6	Amy Thompson							98	Customer # 8257482	277	Can someone call John Doe at 711-555-2881? They called the front desk asking about the house on 123 Sesame Street.	6/17/2024 9:27:
52	Bill Franklin							98	Customer # 8257482	277	Can someone call John Doe at 711-555-2881? They called the front desk asking about the house on 123 South Street.	6/17/2024 9:27:
14	Erica Sorenson							98	Customer # 8257482	277	Can someone call John Doe at 711-555-2881? They called the front desk asking about the house on 123 South Street.	6/17/2024 9:27:
17	Maren Gonzalez							98	Customer # 8257482	277	Can someone call John Doe at 711-555-2881? They called the front desk asking about the house on 123 South Street.	6/17/2024 9:27:
21	Sarah Zimoneck							98	Customer # 8257482	278	Yes, I can.	6/17/2024 9:27:
6	Amy Thompson							98	Customer # 8257482	278	Yes, I can.	6/17/2024 9:27:
52	Bill Franklin							98	Customer # 8257482	278	Yes, I can.	6/17/2024 9:27:
17	Maren Gonzalez							98	Customer # 8257482	278	Yes, I can.	6/17/2024 9:27:
9	Angela Massey							112	Patient Callback	304	Please call John Smith at 7115558377 for a consultation.	7/8/2024 8:03:0
		15	Ophthalmology Dr. On Call					112	Patient Callback	304	Please call John Smith at 7115558377 for a consultation.	7/8/2024 8:03:0
		16	Ophthalmology Nurse On Call					112	Patient Callback	304	Please call John Smith at 7115558377 for a consultation.	7/8/2024 8:03:0
13	DeAnn Womson							113	Swap Shifts	305	Hey, DeAnn, would you be willing to swap my shift for this afternoon?	7/8/2024 9:15:5
21	Sarah Zimoneck							113	Swap Shifts	306	On vacation	7/8/2024 9:15:5

Note: Not all fields in the Group Messages Report are shown in the screenshot.

Column	Description
Recipient Contact ID	Recipient Contact ID indicates the unique ID associated with the contact to whom the message was addressed.
Recipient Contact Name	Recipient Contact Name indicates the contact name of the person to whom the message was addressed.
Recipient Role ID	Recipient Role ID indicates the unique ID associated with the role to which the message was addressed.
Recipient Role Name	Recipient Role Name indicates the name of the role to which the message was addressed.
Sender Contact ID	Sender Contact ID indicates the unique ID of the contact that sent the message.
Sender Name	Sender Name indicates the contact name of the person who sent the message.
Sender Role ID	Sender Role ID indicates the unique ID of the role that sent the message.
Sender Role Name	Sender Role Name indicates the name of the role that sent the message.

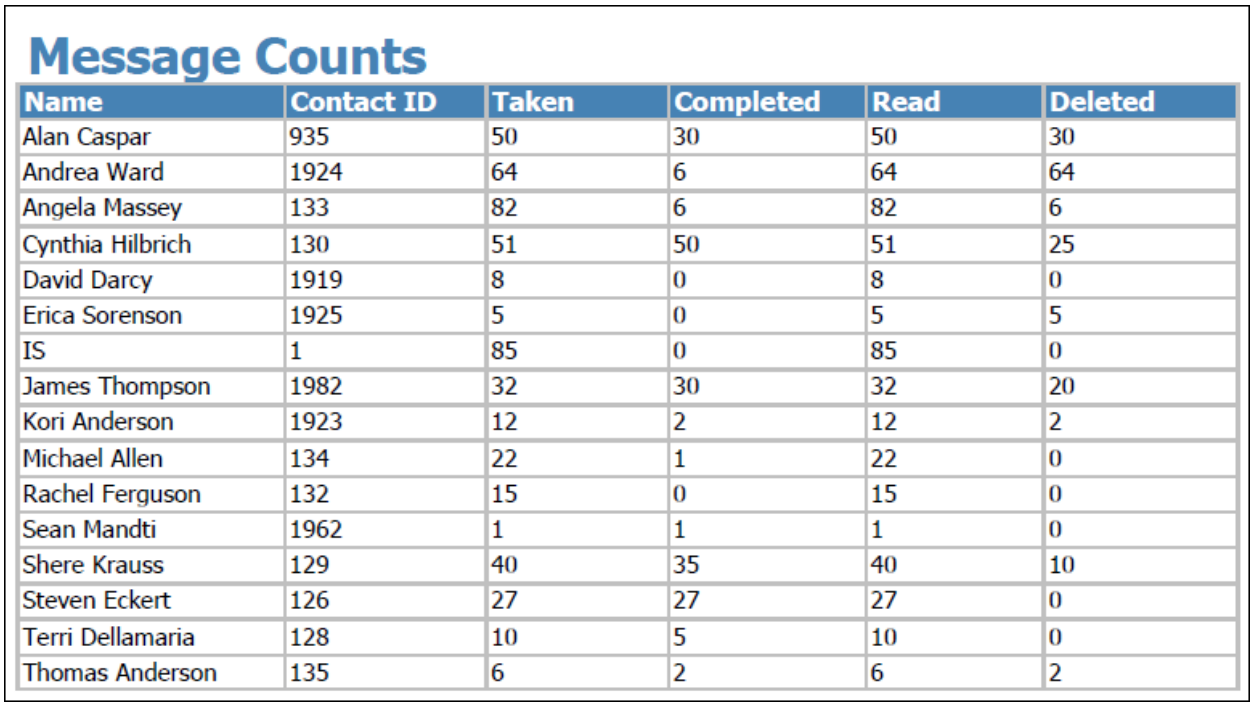
Column	Description
Thread ID	Thread ID indicates the unique ID associated with the message thread. Each message thread contains one new secure message and all of the replies to that secure message.
Subject	Subject indicates the subject of the message.
Msg ID	Msg ID indicates the unique ID associated with the message.
Message	Message indicates the content of the message.
Taken Stamp	Taken Stamp indicates the date and time that the message was sent.
Completed	Completed is a True or False value that indicates whether the recipient has marked the messages Completed.
Completed Stamp	Completed indicates the date and time that the recipient marked the message Completed.
Completed Contact ID	Completed Contact ID indicates the unique ID of the contact that marked the message Completed.
Completed Contact Name	Completed Contact Name indicates the contact name of the person who marked the message Completed.
Read	Read is a True or False value that indicates whether the message has been displayed on the recipient's device.
Read Stamp	Read Stamp indicates the date and time that the message was displayed on the recipient's device.
Read Contact ID	Read Contact ID indicates the unique ID of the recipient on whose device the message was displayed.
Read Contact Name	Read Contact Name indicates the contact name of the recipient on whose device the message was displayed.
Deleted	Deleted is a True or False value that indicates whether the recipient has deleted the message.
Deleted Stamp	Deleted Stamp indicates the date and time that the recipient deleted the message.
Deleted Contact ID	Deleted Contact ID indicates the unique ID of the recipient that deleted the message.
Deleted Contact Name	Deleted Contact Name indicates the contact name of the recipient that deleted the message.
Delivered	Delivered is a True or False value that indicates whether the message has been downloaded to the recipient's device.

Column	Description
Delivered Stamp	Delivered Stamp indicates the date and time that the message was downloaded to the recipient's device.
Delivered Contact ID	Delivered Contact ID indicates the unique ID of the recipient on whose device the message was downloaded.
Delivered Contact Name	Delivered Contact Name indicates the contact name of the recipient on whose device the message was downloaded.
Group ID	Group ID indicates the unique ID of the group that was used to send the secure message.
Contact Group	Contact Group indicates the name of the group that was used to send the secure message.
Priority	Priority indicates whether the message was marked as normal priority or high priority. "1" indicates a normal priority message. "2" indicates a high priority message.

Return to Reports
Return to Index

Message Counts Report

The Message Counts 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 that sent the message.



Message Counts

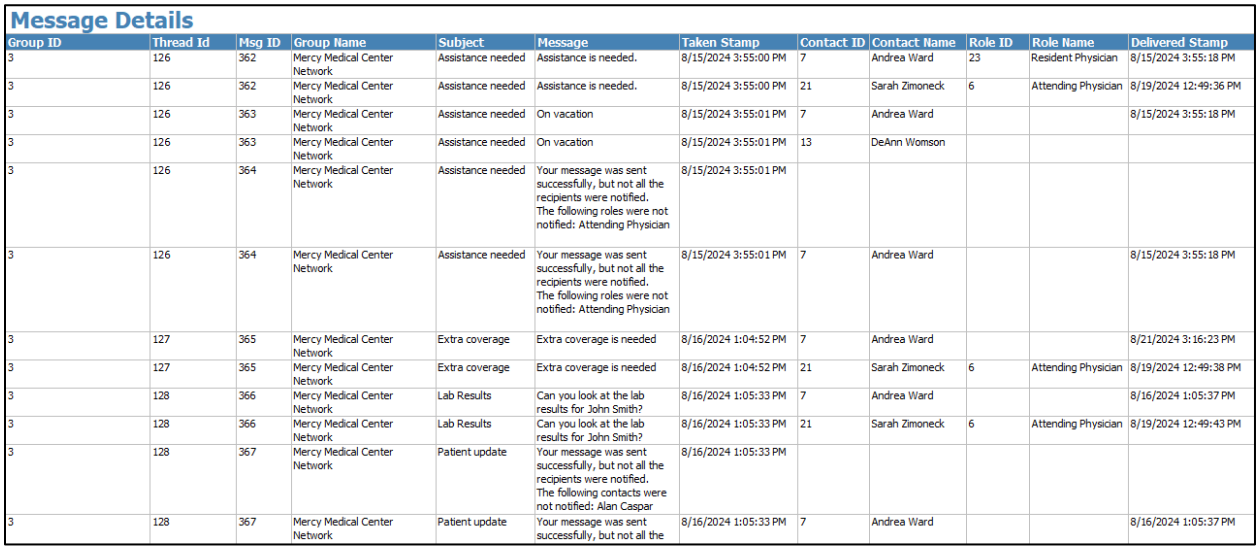
Name	Contact ID	Taken	Completed	Read	Deleted
Alan Caspar	935	50	30	50	30
Andrea Ward	1924	64	6	64	64
Angela Massey	133	82	6	82	6
Cynthia Hilbrich	130	51	50	51	25
David Darcy	1919	8	0	8	0
Erica Sorenson	1925	5	0	5	5
IS	1	85	0	85	0
James Thompson	1982	32	30	32	20
Kori Anderson	1923	12	2	12	2
Michael Allen	134	22	1	22	0
Rachel Ferguson	132	15	0	15	0
Sean Mandti	1962	1	1	1	0
Shere Krauss	129	40	35	40	10
Steven Eckert	126	27	27	27	0
Terri Dellamaria	128	10	5	10	0
Thomas Anderson	135	6	2	6	2

Column	Description
Name	Name indicates the name of each contact.
Contact ID	Contact ID indicates the unique ID associated with the contact.
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.

Return to Reports
Return to Index

Message Details Report

The Message Details Report displays comprehensive information about secure messages sent during the specified date and time range. A table displays the following columns of information about all messages sent or received by the specified contacts, with a row displayed for each time a contact sent or received a message.



Message Details

Group ID	Thread Id	Msg ID	Group Name	Subject	Message	Taken Stamp	Contact ID	Contact Name	Role ID	Role Name	Delivered Stamp
3	126	362	Mercy Medical Center Network	Assistance needed	Assistance is needed.	8/15/2024 3:55:00 PM	7	Andrea Ward	23	Resident Physician	8/15/2024 3:55:18 PM
3	126	362	Mercy Medical Center Network	Assistance needed	Assistance is needed.	8/15/2024 3:55:00 PM	21	Sarah Zimoneck	6	Attending Physician	8/19/2024 12:49:36 PM
3	126	363	Mercy Medical Center Network	Assistance needed	On vacation	8/15/2024 3:55:01 PM	7	Andrea Ward			8/15/2024 3:55:18 PM
3	126	363	Mercy Medical Center Network	Assistance needed	On vacation	8/15/2024 3:55:01 PM	13	DeAnn Womson			
3	126	364	Mercy Medical Center Network	Assistance needed	Your message was sent successfully, but not all the recipients were notified. The following roles were not notified: Attending Physician	8/15/2024 3:55:01 PM					
3	126	364	Mercy Medical Center Network	Assistance needed	Your message was sent successfully, but not all the recipients were notified. The following roles were not notified: Attending Physician	8/15/2024 3:55:01 PM	7	Andrea Ward			8/15/2024 3:55:18 PM
3	127	365	Mercy Medical Center Network	Extra coverage	Extra coverage is needed	8/16/2024 1:04:52 PM	7	Andrea Ward			8/21/2024 3:16:23 PM
3	127	365	Mercy Medical Center Network	Extra coverage	Extra coverage is needed	8/16/2024 1:04:52 PM	21	Sarah Zimoneck	6	Attending Physician	8/19/2024 12:49:38 PM
3	128	366	Mercy Medical Center Network	Lab Results	Can you look at the lab results for John Smith?	8/16/2024 1:05:33 PM	7	Andrea Ward			8/16/2024 1:05:37 PM
3	128	366	Mercy Medical Center Network	Lab Results	Can you look at the lab results for John Smith?	8/16/2024 1:05:33 PM	21	Sarah Zimoneck	6	Attending Physician	8/19/2024 12:49:43 PM
3	128	367	Mercy Medical Center Network	Patient update	Your message was sent successfully, but not all the recipients were notified. The following contacts were not notified: Alan Caspar	8/16/2024 1:05:33 PM					
3	128	367	Mercy Medical Center Network	Patient update	Your message was sent successfully, but not all the	8/16/2024 1:05:33 PM	7	Andrea Ward			8/16/2024 1:05:37 PM

Note: Not all fields in the Message Details Report are shown in the screenshot.

Group ID — Group ID indicates the unique ID of the group that was used to send the secure message.

Thread ID — Thread ID indicates the unique ID associated with the message thread. Each message thread contains one new secure message and all of the replies to that secure message.

Msg ID — Msg ID indicates the unique ID associated with the message.

Group Name — Group Name indicates the name of the group that was used to send the secure message.

Subject — Subject indicates the subject of the message.

Message — Message indicates the content of the message.

Taken Stamp — Message indicates the date and time the message was sent.

Contact ID — Contact ID indicates the unique ID associated with the contact that sent or received the message.

Contact Name — Contact Name indicates the contact name of the person that sent or received the message.

Role ID — Role ID indicates the unique ID associated with the role that sent or received the message.

Role Name — Role Name indicates the name of the role that sent or received the message.

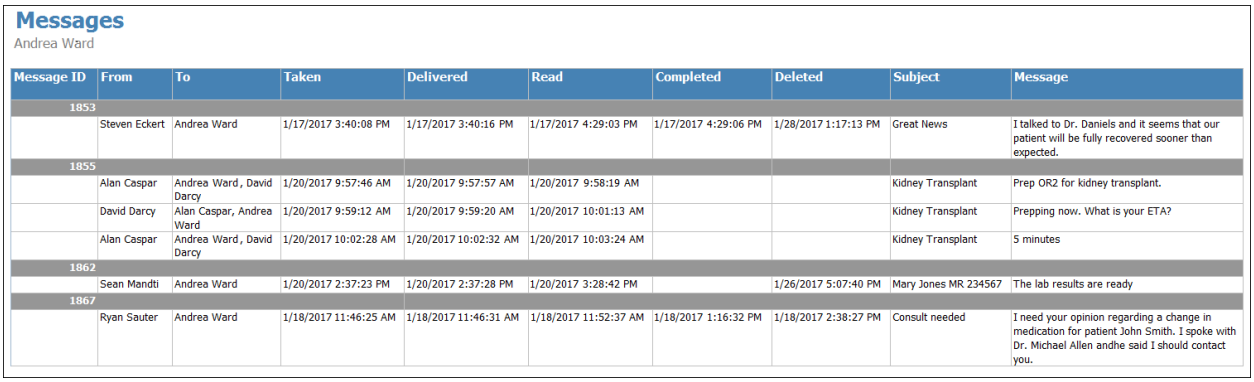
Delivered Stamp	Delivered Stamp indicates the date and time that the message was downloaded to the device of the recipient.
Read Stamp	Read Stamp indicates the date and time that the message was displayed on the device of the recipient.
Completed Stamp	Completed Stamp indicates the date and time that the recipient marked the message Completed.
Deleted Stamp	Deleted Stamp indicates the date and time that the recipient deleted the message.

Return to Reports
Return to Index

Messages - Formatted Report

The formatted version of the Messages Report displays information about secure messages sent during the specified date and time range in an easy-to-read format. The report is divided into separate pages by contact name. The contact name is displayed at the top of the page. A table displays the following columns of information about all messages received by that contact.

Note: If you want to view a message sent by the contact, you must look at the page for the contact to which the message was sent.



Messages

Andrea Ward

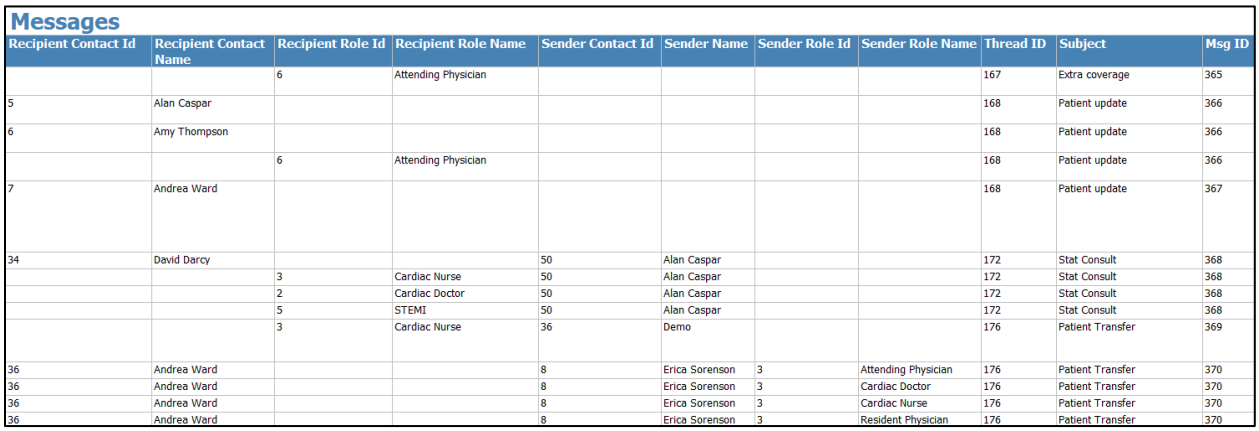
Message ID	From	To	Taken	Delivered	Read	Completed	Deleted	Subject	Message
1853									
	Steven Eckert	Andrea Ward	1/17/2017 3:40:08 PM	1/17/2017 3:40:16 PM	1/17/2017 4:29:03 PM	1/17/2017 4:29:06 PM	1/28/2017 1:17:13 PM	Great News	I talked to Dr. Daniels and it seems that our patient will be fully recovered sooner than expected.
1855									
	Alan Caspar	Andrea Ward, David Darcy	1/20/2017 9:57:46 AM	1/20/2017 9:57:57 AM	1/20/2017 9:58:19 AM			Kidney Transplant	Prep OR2 for kidney transplant.
	David Darcy	Alan Caspar, Andrea Ward	1/20/2017 9:59:12 AM	1/20/2017 9:59:20 AM	1/20/2017 10:01:13 AM			Kidney Transplant	Prepping now. What is your ETA?
	Alan Caspar	Andrea Ward, David Darcy	1/20/2017 10:02:28 AM	1/20/2017 10:02:32 AM	1/20/2017 10:03:24 AM			Kidney Transplant	5 minutes
1862									
	Sean Mandti	Andrea Ward	1/20/2017 2:37:23 PM	1/20/2017 2:37:28 PM	1/20/2017 3:28:42 PM		1/26/2017 5:07:40 PM	Mary Jones MR 234567	The lab results are ready
1867									
	Ryan Sauter	Andrea Ward	1/18/2017 11:46:25 AM	1/18/2017 11:46:31 AM	1/18/2017 11:52:37 AM	1/18/2017 1:16:32 PM	1/18/2017 2:38:27 PM	Consult needed	I need your opinion regarding a change in medication for patient John Smith. I spoke with Dr. Michael Allen andhe said I should contact you.

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.
Delivered	Delivered indicates the date and time that the message was downloaded to the recipient's device.
Read	Read indicates the date and time that the message was displayed on the recipient's device.
Completed	Completed indicates the date and time that the recipient marked the message "Completed."
Deleted	Deleted indicates the date and time that the recipient deleted the message.
Subject	Subject indicates the subject of the message.
Message	Message indicates the content of the message.

Return to Reports
Return to Index

Messages Report

The Messages Report displays comprehensive information about secure messages sent during the specified date and time range. A table displays the following columns of information about all messages.



Messages

Recipient Contact Id	Recipient Contact Name	Recipient Role Id	Recipient Role Name	Sender Contact Id	Sender Name	Sender Role Id	Sender Role Name	Thread ID	Subject	Msg ID
		6	Attending Physician					167	Extra coverage	365
5	Alan Caspar							168	Patient update	366
6	Amy Thompson							168	Patient update	366
		6	Attending Physician					168	Patient update	366
7	Andrea Ward							168	Patient update	367
34	David Darcy			50	Alan Caspar			172	Stat Consult	368
		3	Cardiac Nurse	50	Alan Caspar			172	Stat Consult	368
		2	Cardiac Doctor	50	Alan Caspar			172	Stat Consult	368
		5	STEMI	50	Alan Caspar			172	Stat Consult	368
		3	Cardiac Nurse	36	Demo			176	Patient Transfer	369
36	Andrea Ward			8	Erica Sorenson	3	Attending Physician	176	Patient Transfer	370
36	Andrea Ward			8	Erica Sorenson	3	Cardiac Doctor	176	Patient Transfer	370
36	Andrea Ward			8	Erica Sorenson	3	Cardiac Nurse	176	Patient Transfer	370
36	Andrea Ward			8	Erica Sorenson	3	Resident Physician	176	Patient Transfer	370

Note: Not all fields in the Messages Report are shown in the screenshot.

Column	Description
Recipient Contact ID	Recipient Contact ID indicates the unique ID associated with the contact to whom the message was addressed.
Recipient Contact Name	Recipient Contact Name indicates the contact name of the person to whom the message was addressed.
Recipient Role ID	Recipient Role ID indicates the unique ID associated with the role to which the message was addressed.
Recipient Role Name	Recipient Role Name indicates the name of the role to which the message was addressed.
Sender Contact ID	Sender ID indicates the unique ID associated with the person who sent the message.
Sender Name	Sender Name indicates the contact name of the person who sent the message.
Sender Role ID	Sender Role ID indicates the unique ID of the role that sent the message.
Sender Role Name	Sender Role Name indicates the name of the role that sent the message.
Thread ID	Thread ID indicates the unique ID associated with the message thread. Each message thread contains one new secure message and all of the replies to that secure message.
Subject	Subject indicates the subject of the message.

Column	Description
Msg ID	Message ID indicates the unique ID associated with the message.
Message	Message indicates the content of the message.
Taken Stamp	Taken Stamp indicates the date and time that the message was sent.
Completed	Completed is a True or False value that indicates whether the recipient has marked the message "Completed."
Completed Stamp	Completed indicates the date and time that the recipient marked the message "Completed."
Completed Contact ID	Completed Contact ID indicates the unique ID of the contact that marked the message Completed.
Completed Contact Name	Completed Contact Name indicates the contact name of the person who marked the message Completed.
Read	Read is a True or False value that indicates whether the message has been displayed on the recipient's device.
Read Stamp	Read Stamp indicates the date and time that the message was displayed on the recipient's device.
Read Contact ID	Read Contact ID indicates the unique ID of the recipient on whose device the message was displayed.
Read Contact Name	Read Contact Name indicates the unique ID of the recipient on whose device the message was displayed.
Deleted	Deleted is a True or False value that indicates whether the recipient has deleted the message.
Deleted Stamp	Deleted Stamp indicates the date and time that the recipient deleted the message.
Deleted Contact ID	Deleted Contact ID indicates the unique ID of the recipient that deleted the message.
Deleted Contact Name	Deleted Contact Name indicates the name of the recipient that deleted the message.
Delivered	Delivered is a True or False value that indicates whether the message has been downloaded to the recipient's device.
Delivered Stamp	Delivered Stamp indicates the date and time that the message was downloaded to the recipient's device.
Delivered Contact ID	Delivered Contact ID indicates the unique ID of the recipient on whose device the message was downloaded.
Delivered Contact Name	Delivered Contact Name indicates the name of the recipient on whose device the message was downloaded.

Column	Description
Group ID	Group ID indicates the unique ID of the group that was used to send the secure message.
Contact Group	Contact Group indicates the name of the group that was used to send the secure message.
Priority	Priority indicates whether the message was marked as normal priority or high priority. “1” indicates a normal priority message. “2” indicates a high priority message.

Return to Reports
Return to Index

Notifications Report

The Notifications Report displays counts of notification successes and failures for device types in each group for a specified date and time range. The counts are listed by group ID.

Notifications

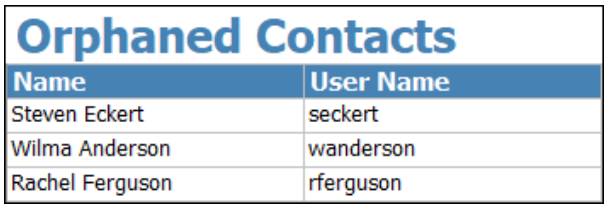
Group ID	Name	Android Successes	Android Failures	Apple Successes	Apple Failures	Wctp Successes	Wctp Failures
0	General Hosptial	102	67	216	3	0	0
1	Mercy Medical Center	143	1	227	1	0	0
2	MMC Family Dentistry	276	248	24	0	0	0

Column	Description
Group ID	Group ID indicates the unique ID number associated with each group.
Name	Name indicates the name of the group.
Android Successes	Android Successes indicates the number of Amtelco Secure Messages notifications that were successfully sent to the Google Cloud Messaging Service.
Android Failures	Android Failures indicates the number of Amtelco Secure Messages notifications that were returned as failures from the Google Cloud Messaging Service.
Apple Successes	Apple Successes indicates the number of Amtelco Secure Messages notifications that were successfully sent to the Apple Push Notification Service.
Apple Failures	Apple Failures indicates the number of Amtelco Secure Messages notifications that were returned as failures from the Apple Push Notification Service.
WCTP Successes	WCTP Successes indicates the number of escalation messages that were successfully sent to the WCTP text messaging provider.
WCTP Failures	WCTP Failures indicates the number of escalation messages that were returned as failures from the WCTP text messaging provider.

Return to Reports
Return to Index

Orphaned Contacts Report

The Orphaned Contacts Report displays a list of contacts in the Amtelco Secure Messages system that are not registered to any groups. These contacts are taking up a license but are unable to send or receive secure messages.



Orphaned Contacts

Name	User Name
Steven Eckert	seckert
Wilma Anderson	wanderson
Rachel Ferguson	rferguson

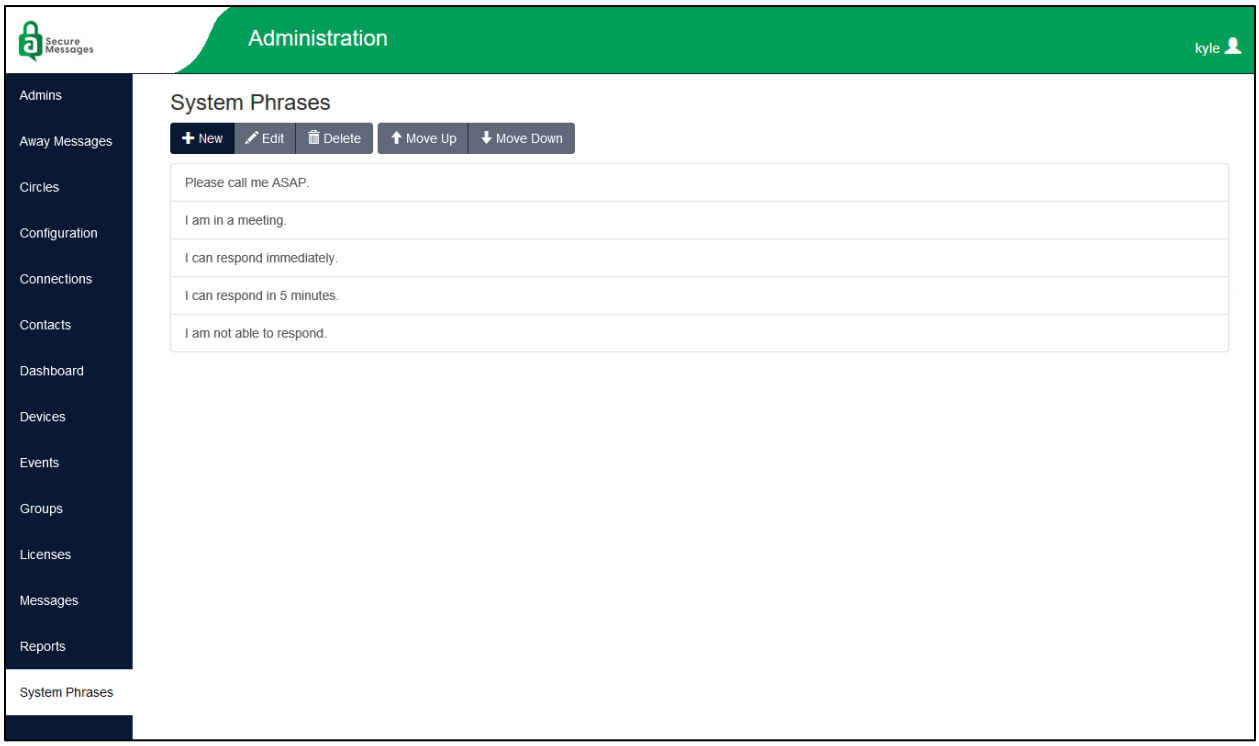
Column	Description
Display Name	Display Name indicates the display name of each contact that is not registered to any groups.
User Name	User Name indicates the username of the contact.

Return to Reports
Return to Index

System Phrases

The System Phrases page is used to customize the system Quick Phrases that are available to any group that is enabled for system phrases. When an Amtelco Secure Messages user composes or replies to a secure message, the user can select one of these Quick Phrases, select one of the group Quick Phrases, or type a custom message.

Click the System Phrases command on the navigation menu to access the System Phrases page.



System Phrases Toolbar

The System Phrases Toolbar is displayed near the top of the System Phrases page. The System Phrases Toolbar is used to make changes to the Quick Phrases that are available to Amtelco Secure Messages users when composing or replying to a secure message.

Icon	Description
	Click the **New** icon to add a new system phrase.
	Click the **Edit** icon to edit the selected system phrase.
	Click the **Delete** icon to delete the selected system phrase.
	Click the **Move Up** icon to move the selected system phrase closer to the top of the list.
	Click the **Move Down** icon to move the selected system phrase closer to the bottom of the list.

Adding and Editing System Phrases

- **To add a system phrase, click the New icon.**

  The System Phrase window is displayed with a blank text field.

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

  The cSystem Phrase window displays the selected system phrase in a text field.

System Phrase

Type the system phrase that you want to add, or edit the existing system phrase.

Click the Save Changes button.

The new or edited phrase is displayed in the list.

Repositioning a System Phrase

To reposition a system 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.

Deleting a System Phrase

To remove a system 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.

If you clicked the Delete button, the phrase is removed from the list.

Return to Navigating in Amtelco Secure Messages Admin Web
Return to Index

Appendixes

The appendixes in this section contain detailed information about functions that can be accessed from multiple locations within the Amtelco Secure Messages Admin Web application.

The following topics are covered.

A. Actions

B. Message Menus and Toolbars

Return to Index

Actions

Each type of action that may be displayed in the Action column of the Audit Report and in the Action column of the Group Audit Report is described in the following table.

Action	Description
Agent Force Password Change	Agent Force Password Change indicates the "Force Password Change" check box was selected or cleared in an administrator's Admin Settings properties. • The Change Type column displays "Update." • The Change column displays "True" if the check box was selected or "False" if the check box was cleared. • The Target column displays the username of the administrator to which the action was applied.
Agent Groups	Agent Groups indicates the groups to which an administrator has been granted access in Admin Settings has changed. • The Change Type column displays "Update." • The Change column displays numbers representing the group IDs that were assigned to the administrator. • The Target column displays the username of the administrator to which the action was applied.
Agent Login	Agent Login indicates that an Amtelco Secure Messages Admin Web administrator attempted to log in to the Amtelco Secure Messages Admin Web. An Agent Login entry is also displayed in the audit report each time a new session key is generated for a logged-in administrator. • The Change Type column displays "Successful" if the login attempt succeeded or "Failure" if the login attempt failed due to an incorrect password or other reason.
Agents	Agents indicates that an Amtelco Secure Messages Admin Web administrator was created, edited, or removed, or an administrator's password was reset. • The Change Type column displays "New" if an administrator was created, "Update" if an administrator's settings were edited, "Delete" if an administrator was removed, or "ResetPassword" if an administrator's password was reset. • The Change column displays the settings that were activated or updated for the administrator. • The Target column displays the username of the administrator to which the action was applied.

Action	Description
Agent Type	Agent Type indicates and administrator's Access Type was changed in the Admin Settings properties. • The Change Type column displays "Update." • The Change column displays the Access Type that was applied. • The Target column displays the username of the administrator to which the action was applied.
Circle	Circle indicates that an Amtelco Secure Messages Contact Circle was created, edited, or removed. • The Change Type column displays "New" if a Circle was created, "Update" if a Circle's settings were edited, or "Delete" if a Circle was removed. • The Change column indicates the name of the Circle to which the action was applied.
Circle Contact	Circle Contact indicates that a contact was added to or removed from a Contact Circle. • The Change Type column indicates "New" if a contact was added to the Circle or "Delete" if a contact was removed from the Circle. • The Change column displays the username of the contact that was added or removed. • The Target column displays the name of the Circle to which the action was applied.
Connection	Connection indicates that a Connection was added, updated, or removed. • The Change Type column displays "New" if a connection was added, "Update" if a connection was updated, or "Delete" if a connection was removed. • The Target column displays the name of the Connection to which the action was applied.

Action	Description
Contact Api Client	Contact Api Client indicates that Application Programming Interface (API) access was added or removed for a contact. • The Change Type column displays “New” if an API App ID was added, or “Delete” if an API App ID was deleted. • The Change column displays the App ID. • The Target column displays the username of the contact to which the action was applied.
Contact Email	Contact Email indicates that the Email setting was changed for a contact. • The Change Type column displays “Update.” • The Change column displays the new e-mail address. • The Target column displays the username of the contact to which the action was applied.
Contact Force Password Change	Contact Force Password Change indicates the “Force Password Change” check box was selected or cleared in the Contact Settings properties. • The Change Type column displays “Update.” • The Change column displays “True” if the check box was selected or “False” if the check box was cleared. • The Target column displays the username of the contact to which the action was applied.
Contact Hidden	Contact Hidden indicates the “Visible” check box was selected or cleared in the Contact Settings properties. • The Change Type column displays “Update.” • The Change column displays “True” if the check box was selected or “False” if the check box was cleared. • The Target column displays the username of the contact to which the action was applied.

Action	Description
Contact Import	Contact Import indicates that a Contact Importer transform was run. • The Change Type column displays “Started” if an import was started, “ImportAppend” if a new contact record was appended to the database, “ImportUpdate” if an existing contact record was updated in the database, “Failure” if an append or update failed, or “Completed” if an import was completed. • The Change column displays the name of the transform if a transform was started or completed. • The Target column displays the username of the contact if a contact was appended or updated.
Contact Inactive	Contact Inactive indicates the “Active” check box was selected or cleared in the Contact Group Settings properties. • The Change Type column displays “Update.” • The Change column displays “True” if the check box was selected or “False” if the check box was cleared. • The Target column displays the username of the contact to which the action was applied.
Contact Interval	Contact Interval indicates that the Notification Interval setting was changed for a contact. • The Change Type column displays “Update.” • The Change column displays the new interval. • The Target column displays the username of the contact to which the action was applied.
Contact Login	Contact Login indicates that a contact unsuccessfully attempted to log in to the Amtelco Secure Messages app on a registered device or the Contact Web. • The Change Type column displays “LockedOut” if the login attempt resulted in the contact being locked out or “Failure” if the login attempt failed. • The Target column displays the username with which the contact tried to log in.

Action	Description
Contact Name	Contact Name indicates that the Display Name setting was changed for a contact. • The Change Type column displays “Update.” • The Change column displays the new name. • The Target column displays the username of the contact to which the action was applied.
Contact Notifications	Contact Notifications indicates that the Notification Alert (On/Off) setting was changed for a contact. • The Change Type column displays “Update.” • The Change column displays “Enabled” if the setting was enabled or “Disabled” and the start and end time in parenthesis if the setting was disabled. • The Target column displays the username of the contact to which the action was applied.
Contact Phone	Contact Phone indicates that the Phone Number setting was changed for a contact. • The Change Type column displays “Update.” • The Change column displays the new phone number. • The Target column displays the username of the contact to which the action was applied.
Contact Picture	Contact Picture indicates that the Contact Photo was added, changed, or removed for a contact. • The Change Type column displays “Update” if a new photo was added or “Delete” if the photo was deleted. • The Target column displays the username of the contact to which the action was applied.
Contacts	Contacts indicates that a contact was created, removed, locked out, or the contact’s password or passcode was reset. • The Change Type column displays “New” if a Contact was created, “Delete” if a contact was removed, “LockedOut” if a contact was locked out, “ResetPassword” if the contact’s password was reset, or “ResetPasscode” if the contact’s passcode was reset. • The Target column displays the username of the contact to which the action was applied.

Action	Description
Device Phone Number	Device Phone Number indicates that a phone number was added to a device, was changed for a device, or was removed from a device. • The Change Type column displays "Update." • The Change column displays the phone number if a phone number was added or changed. • The Target column displays a number representing the Device ID.
Email	Email indicates the failure of any outbound e-mail sent by the Amtelco Secure Messages Service. • The Change Type column displays "Failure."
Group	Group indicates that an Amtelco Secure Messages group was created or removed. • The Change Type column displays "New" if a group was created or "Delete" if a group was removed. • The Change column displays the name of the group to which the action was applied.
Group Admin Permissions	Group Admin Permissions indicates that the Group Administrator Permissions settings were changed for a group. • The Change Type column displays "Update." • The Change column displays a list of all of the Group Administrator Permission settings and their values.
Group Allow Contact Access Gallery	Group Allow Contact Access Gallery indicates that the Contact Permissions Access Media Gallery setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Group Allow Contact Away Message Edit	Group Allow Contact Away Message Edit indicates that the Contact Permissions Modify Away Message setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.

Action	Description
Group Allow Contact Quick Phrase Edit	Group Allow Contact Quick Phrase Edit indicates that the Contact Permissions Modify Personal Quick Phrases setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Group Allow User Disable Notifications	Group Allow User Disable Notifications indicates that the Contact Permissions Toggle Notifications (On/Off) setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Group Allow User Edit Display Name	Group Allow User Edit Display Name indicates that the Contact Permissions Modify Display Name setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Group Allow User Edit Email	Group Allow User Edit Email indicates that the Contact Permissions Modify Email setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Group Allow User Edit Interval	Group Allow User Edit Interval indicates that the Contact Permissions Modify Notification Interval setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Group Allow User Edit Personal Circle	Group Allow User Edit Personal Circle indicates that the Contact Permissions Modify Personal Circle setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.

Action	Description
Group Allow User Edit Phone Number	Group Allow User Edit Phone Number indicates that the Contact Permissions Edit Phone Number setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays “True” if the setting was enabled or “False” if the setting was disabled.
Group Allow User Edit Picture	Group Allow User Edit Picture indicates that the Contact Permissions Modify Picture setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays “True” if the setting was enabled or “False” if the setting was disabled.
Group Attachment Size	Group Attachment Size indicates that the Attachment Size setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays the new value.
Group Authentication Mode	Group Authentication Mode indicates that the Authentication Mode setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays the new value.
Group Authentication Resource	Group Authentication Resource indicates that the Authentication Resource setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays the new value.
Group Away Message	Group Away Message indicates that a group away message was created, edited, reordered, or removed. • The Change Type column displays “New” if an away message was created, “Update” if an away message was edited, “Reordered” if an away message was reordered, or “Delete” if an away message was removed.

Action	Description
Group Contact	Group Contact indicates that a contact was added to or removed from a group. • The Change Type column displays "New" if a contact was added to a group, or "Delete" if a contact was removed from a group. • The Change column displays the username of the contact that was added or removed. • The Target column displays the name of the group to which the action was applied.
Group Default Circle Name	Group Default Circle Name indicates that the Default Circle setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new default Circle name.
Group Device To Device	Group Device To Device indicates that the Contact Permissions Allow Device to Device Messaging setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Group Dialing Mode	Group Dialing Mode indicates that the Dialing Mode setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new value.
Group Escalation Delay	Group Escalation Delay indicates that the Escalation Delay setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new value.
Group Escalation Text	Group Escalation Text indicates that the Escalation Message setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new escalation message.
Group Genesis Code	Group Genesis Code indicates that the Access Code setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new value.

Action	Description
Group Genesis Disa Num	Group Genesis Disa Num indicates that the DISA setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays the new value.
Group Hide Contact Phone	Group Hide Contact Phone indicates that the Contact Permissions Hide Phone Number setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays “True” if the setting was enabled or “False” if the setting was disabled.
Group Licenses	Group Licenses indicates that the Allocated Licenses setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays the new value.
Group Max Contacts Per Thread	Group Max Contacts Per Thread indicates that the Maximum Contacts per Thread setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays the new value.
Group Menu Url	Group Menu Url indicates that a device menu hyperlink was created, edited, reordered, or removed. • The Change Type column displays “New” if a hyperlink was created, “Update” if a hyperlink was edited, “Reordered” if a hyperlink was reordered, or “Delete” if hyperlink was removed. • The Change column displays a number representing the group ID and position of the hyperlink, the name of the hyperlink, and in parenthesis, the URL.
Group Name	Group Name indicates that the Name setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays the new name.
Group Notification Interval	Group Notification Interval indicates that the Notification Interval setting was changed for a group. • The Change Type column displays “Update.” • The Change column displays the new interval.

Action	Description
Group Notifications	Group Notifications indicates that the Notification Attempts setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new value.
Group Passcode Complexity	Group Passcode Complexity indicates that Passcode Settings were changed for a group. • The Change Type column displays "Update." • The Change column displays a list of the Passcode Complexity settings that were changed.
Group Password Complexity	Group Password Complexity indicates that Password Settings were changed for a group. • The Change Type column displays "Update." • The Change column displays a list of the Password Complexity settings that were changed.
Group Password Reset Mail Body	Group Password Reset Mail Body indicates the Reset Password Email Message was changed for a group. • The Change Type column displays "Update." • The Change column displays the new message.
Group Password Reset Mail Subject	Group Password Reset Mail Subject indicates the Reset Password Email Subject was changed for a group. • The Change Type column displays "Update." • The Change column displays the new subject.
Group Registration 2 Mail Body	Group Registration 2 Mail Body indicates the Multiple Device Registration Email Message was changed for a group. • The Change Type column displays "Update." • The Change column displays the new message.
Group Registration 2 Mail Subject	Group Registration 2 Mail Subject indicates the Multiple Device Registration Email Subject was changed for a group. • The Change Type column displays "Update." • The Change column displays the new subject.
Group Registration Mail Body	Group Registration Mail Body indicates the Initial Registration Email Message was changed for a group. • The Change Type column displays "Update." • The Change column displays the new message.

Action	Description
Group Registration Mail Subject	Group Registration Mail Subject indicates the Initial Registration Email Subject was changed for a group. • The Change Type column displays "Update." • The Change column displays the new subject.
Group Registration Mail Timeout	Group Registration Mail Timeout indicates that the Email Registration/Reset Timeout setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new value.
Group Registration Mode	Group Registration Mode indicates that the Registration Type setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new value.
Group Response	Group Response indicates that a group Quick Phrase was created, edited, reordered, or removed for a group. • The Change Type column displays "New" if a phrase was created, "Update" if a phrase was edited, "Reordered" if a phrase was reordered, or "Delete" if a phrase was removed. • The Change column displays the phrase to which the action was applied.
Group Status Url	Group Status URL indicates that the IS Web URL setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new URL.
Group Temp Password Reset Mail Body	Group Temp Password Reset Mail Body indicates the Reset Temporary Password Email Message was changed for a group. • The Change Type column displays "Update." • The Change column displays the new message.
Group Temp Password Reset Mail Subject	Group Temp Password Reset Mail Subject indicates the Reset Temporary Password Email Subject was changed for a group. • The Change Type column displays "Update." • The Change column displays the new subject.

Action	Description
Group User Circle Name	Group User Circle Name indicates that the Personal Circle setting was changed for a group. • The Change Type column displays "Update." • The Change column displays the new personal circle name.
Group User Permissions	Group User Permissions indicates that the Group User Permissions settings were changed for a group. • The Change Type column displays "Update." • The Change column displays a list of the settings that were changed.
Group Use System Away Messages	Group Use System Away Messages indicates that the Contact Permissions Use System Away Messages setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Group Use System Response	Group Use System Response indicates that the Use System Phrases setting was changed for a group. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
Is Password	Is Password indicates that the IS Agent Login Password was changed for a contact. • The Change Type column displays "Update." • The Target column displays the username of the contact to which the action was applied.
Is Username	Is Username indicates that the IS Agent Login Username was changed for a contact. • The Change Type column displays "Update." • The Change column displays the new username. The Target column displays the username of the contact to which the action was applied.
Logout	Logout indicates that an administrator logged out of the Amtelco Secure Messages Admin Web. • The Change Type column displays "Successful" if the administrator logged out successfully.

Action	Description
Personal Circle	Personal Circle indicates that a contact or role was added or removed from a user's Personal Circle. • The Change Type column indicates "New" if a contact or role was added to the Circle or "Delete" if a contact or role was removed from the Circle. • The Change column displays the username of the contact or role that was added or removed. • The Target column displays the username of the user whose Personal Circle was changed.
Report	Report indicates that a report was run on the Amtelco Secure Messages data. • The Change Type column displays "Start" if the report was started or "Completed" if the report was completed. • The Change column displays the name of the report that was run.
Role	Role indicates that a role was added, updated, or removed from a group. • The Change Type column displays "New" if a role was added, "Update" if a role was updated, or "Delete" if a role was removed. • The Change column displays the name of the role to which the action was applied. • The Target column displays the role ID to which the action was applied.
Role Assignment	Role Assignment indicates that role was assigned to a contact or unassigned from a contact. • The Change Type column displays "Assigned" if a role was assigned to a contact, or "Unassigned" if a role was unassigned from a contact. • The Change column displays the name of the contact that the role was assigned to or unassigned from. • The Target column displays the username of the contact that the role was assigned to or unassigned from.
Role Assignment Resync	Role Assignment Resync indicates that the list of roles and contacts under the Roles tab on the Groups page was refreshed. • The Change Type column displays "New."

Action	Description
Role Assignment Resync Requested	Role Assignment Resync Requested indicates that a request was sent to refresh the list of roles and contacts under the Roles tab on the Groups page. • The Change Type column displays "New."
System Agent Password Complexity	System Agent Password Complexity indicates that Password Settings were changed for administrators. • The Change Type column displays "Update." • The Change column displays a list of the Password Complexity settings that were changed.
System Archive Mode	System Archive Mode indicates that the Archive Mode setting on the System Configuration page was changed. • The Change Type column displays "Update." • The Change column displays the new archive mode.
System Archive Threshold	System Archive Threshold indicates that the Archive Threshold setting on the System Configuration page was changed. • The Change Type column displays "Update." • The Change column displays the new value.
System Authentication Mode	System Authentication Mode indicates that the Authentication Mode setting in the System Configuration Administration Settings was changed. • The Change Type column displays "Update." • The Change column displays the new value.
System Authentication Resource	System Authentication Resource indicates that the Authentication Resource setting in the System Configuration Administration Settings was changed. • The Change Type column displays "Update." • The Change column displays the new value.
System Away Message	System Away Messages indicates that a system away message was created, edited, or removed. • The Change Type column displays "New" if an away message was created, "Update" if an away message was edited, or "Delete" if an away message was removed. • The Change column displays the system away message to which the action was applied.

Action	Description
System Device To Device	System Device To Device indicates that the Allow Device to Device Messaging setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays “True” if the setting was enabled or “False’ if the setting was disabled.
System Escalation Delay	System Escalation Delay indicates that the Escalation Delay setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new value.
System Escalation Text	System Escalation Text indicates that the Escalation Message setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new escalation message.
System Name	System Name indicates that the System Name setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new name.
System Notification Interval	System Notification Interval indicates that the Notification Interval setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new interval.
System Notifications	System Notifications indicates that the Notification Attempts setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new value.
System Registration Mail Address	System Registration Mail Address indicates that the eMail Registration Settings From Address on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new e-mail address.

Action	Description
System Registration Mail Display Name	System Registration Mail Display Name indicates that the eMail Registration Settings From Name on the System Configuration page was changed. • The Change Type column displays "Update." • The Change column displays the new name.
System Registration Mail Encrypted	System Registration Mail Encrypted indicates that the eMail Registration Settings Require Encryption setting on the System Configuration page was changed. • The Change Type column displays "Update." • The Change column displays "True" if the setting was enabled or "False" if the setting was disabled.
System Registration Mail Password	System Registration Mail Password indicates that the eMail Registration Settings User Password on the System Configuration page was changed. • The Change Type column displays "Update." • The Change column displays the new password.
System Registration Mail Port	System Registration Mail Port indicates that the eMail Registration Settings Port on the System Configuration page was changed. • The Change Type column displays "Update." • The Change column displays the new value.
System Registration Mail Server	System Registration Mail Server indicates that the eMail Registration Settings Server setting on the System Configuration page was changed. • The Change Type column displays "Update." • The Change column displays the new value.
System Registration Mail User Name	System Registration Mail User Name indicates that the eMail Registration Settings User Logon on the System Configuration page was changed. • The Change Type column displays "Update." • The Change column displays the new value.

Action	Description
System Registration Mail Use Tls	System Registration Mail Use Tls indicates that the eMail Registration Settings Require TLS setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays “True” if the setting was enabled or “False” if the setting was disabled.
System Response	System Response indicates that a system Quick Phrase was created, edited, reordered, or removed. • The Change Type column displays “New” if a phrase was created, “Update” if a phrase was edited, “Reordered” if a phrase was reordered, or “Delete” if a phrase was removed. • The Change column displays the system Quick Phrase to which the action was applied.
System Session Idle Timeout	System Session Idle Timeout indicates that the Session Idle Timeout setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new value.
System Session Timeout	System Session Timeout indicates that the Session Timeout setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new value.
System Time Zone	System Time Zone indicates that the Time Zone setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays the new time zone.
System User Permissions	System User Permissions indicates that the Allow System User Report Access setting on the System Configuration page was changed. • The Change Type column displays “Update.” • The Change column displays “True” if the setting was enabled or “False” if the setting was disabled.
Update Licenses	Update Licenses indicates that the Licenses page of the Amtelco Secure Messages Admin Web was updated using the Refresh Licenses button. • The Change Type column displays “Update.”

Action	Description
Validate Passcode	Validate Passcode indicates that an Amtelco Secure Messages user unsuccessfully attempted to log into a Amtelco Secure Messages app using their passcode. • The Change Type column displays “Failure” if the passcode validation attempt was unsuccessful or “LockedOut” if the unsuccessful passcode validation attempt resulted in the user being locked out. • The Target column displays the username of the Amtelco Secure Messages user who attempted the passcode validation.

Return to Appendixes
Return to Group Audit Report
Return to Audit Report
Return to Index

Message Menus and Toolbars

The following table describes the menu commands and toolbar icons that are available for use in customizing e-mail messages.

Location	Icon	Command	Description
File		**New document**	New Document clears the e-mail form.
		Print	Print opens the workstation's Print dialog box, which can be used to print the form.
Edit		**Undo**	Undo cancels the effect of the previous action. *The Undo command also can be performed using the Undo icon on the message toolbar.*
		Redo	Redo repeats the previous action. *The Redo command also can be performed using the Redo icon on the message toolbar.*
		Cut	Cut removes the selected text from the form and adds it to the clipboard.
		Copy	Copy copies the selected text to the clipboard.
		Paste	Paste pastes text from the clipboard.
		Paste as text	Paste as text converts clipboard contents into text before pasting it into the form.
		Select all	Select all selects all the content in the form.
		Find and replace	Find and replace displays the Find and Replace window. The Find and Replace window contains controls for finding text and replacing it.
Insert		**Media**	Media displays the Insert/Edit Media window. The Insert/Edit Media window contains controls for embedding visual media into the form. **Note:** Media only can be used with on-site systems that provide the e-mail recipient with access to the source file.
		Image	Image opens the Insert/Edit Image window. The Insert/Edit Image window contains controls for inserting an image into the e-mail form. **Note:** Images only can be used with on-site systems that provide the e-mail recipient with access to the source file. *The Image command also can be performed using the Image icon on the message toolbar.*

Location	Icon	Command	Description
		Link	Link opens the Insert Link window. The Insert Link window is used to link an icon, graphic, or text in a document to another file or object. *The Link command also can be performed using the Link icon on the message toolbar.*
	Ω	**Special character**	Special Character opens the Symbols window for selecting special typographical symbols to insert into the form
		Anchor	Anchor is used to insert an anchor point in the form.
		Date/time	The Date/Time menu displays options for insert the date or time. **Note:** The date and time are calculated when inserted, not when the e-mail message is sent.
View		**Show blocks**	Show Blocks is used to show or hide the block elements within the form.
		Visual aids	This command is not currently implemented.
		Preview	Preview opens a Preview window that shows what the e-mail will look like when sent.
		Fullscreen	Fullscreen used the full width of the browser window to display the e-mail form. To return to regular view from Fullscreen view, press the CTRL+SHIFT+F keys.
Format	B	**Bold**	Bold changes text to a bold typeface. *The Bold command also can be performed using the Bold icon on the message toolbar.*
	I	**Italic**	Italic changes text to an italic typeface. *The Italic command also can be performed using the Italic icon on the message toolbar.*
	U	**Underline**	Underline underlines text.
	S	**Strikethrough**	Strikethrough puts a line through text.
	x^2	**Superscript**	Superscript raises text above the standard base line and decreases the font size.
	x_2	**Subscript**	Subscript lowers text below the standard base line and decreases the font size.

Location	Icon	Command	Description
		Formats	The Formats menu contains heading, inline formatting, blocking, and alignment options. *The Formats menu also can be accessed from the message toolbar.*
		Clear formatting	Clear Formatting turns off Bold typeface, Italic typeface, and underlining.
Table		**Table**	Table is used to create a table by selecting the number of horizontal and vertical cells.
		Table properties	Table properties are used to edit the width, height, spacing, border, caption, and alignment of the table.
		Delete table	Delete table is used to delete a table created through the Table menu.
		Cell	Cell is used to edit cell properties, merge cells, and split cells.
		Row	Row is used to insert or delete a row in the table and to edit row properties.
		Column	Column is used to insert or delete a column in the table.
Tools		**Source code**	Source Code displays the HyperText Markup Language (HTML) of the message.
Toolbar		**Undo**	Undo cancels the effect of the previous action.
		Redo	Redo repeats the previous action.
		Formats	The Formats menu contains heading, inline formatting, blocking, and alignment options.
		Bold	Bold changes text to a bold typeface
		Italic	Italic changes text to an italic typeface
		Align left	Align Left aligns the selected paragraphs with the left margin of the form.
		Align center	Align Center centers the selected paragraphs between the left and right margins of the form.
		Align right	Align Right aligns the selected paragraphs with the right margin of the form.
		Justify	Justify aligns the selected paragraphs with both the left and right margins of the form.
		Bullet list	Bullet List formats text as a bulleted list.

Location	Icon	Command	Description
		Numbered list	Numbered List formats text as a numbered list.
		Decrease indent	Decrease Indent decreases the size of the indent of paragraphs.
		Increase indent	Increase Indent increases the size of the indent of paragraphs.
		Link	Link opens the Insert Link window. The Insert Link window is used to link an icon, graphic, or text in a document to another file or object.
		Image	Image opens the Insert/Edit Image window. The Insert/Edit Image window contains controls for inserting an image into the form. **Note:** Images only can be used with on-site systems that provide the e-mail recipient with access to the source file.
		ASM Items	ASM Items inserts a placeholder that will be filled the recipient's display name (Display Name), the registration URL or reset password URL (Registration URL), the recipient's username (Username), or the recipient's password (Temporary password).

Return to Appendixes
Return to Email Messages
Return to Index

Documentation Change Log

Software Version	Document Section	Changes	Published Date
N/A	Groups	Removed references of Escalation Message and Escalation Delay in System Configuration	9/15/2025
N/A	System Configuration	Changed the description of Escalation Message and Escalation Delay to clarify that the settings only effects new groups.	9/15/2025
N/A	Connections	Added descriptions to fields.	9/15/2025
N/A	Group Device Versions Report	Updated screenshot.	9/15/2025
N/A	Device Versions Report	Updated screenshot.	9/15/2025
7.0.9144.3	Licenses	Added role icon to Group column in Group Licenses table.	9/15/2025
7.0.9144.1	Reports	Added Roles parameter to reports.	9/15/2025
ASM Server 7.0.9281.19200	Reports	Added Group Message Details Report and Message Details Report.	9/15/2025
ASM Server 7.0.9281.19200	Contact List Report	Added Sound and High Priority Sound columns and a note that not all fields are shown in the screenshot.	9/15/2025
ASM Server 7.0.9281.19200	Device List Report	Updated screenshot. Added Device Mode and Phone Number columns.	9/15/2025
ASM Server 7.0.9281.19200	Group Contact List Report	Added Active, Sound, and High Priority Sound columns and a note that not all fields are shown in the screenshot.	9/15/2025
ASM Server 7.0.9281.19200	Group Device List Report	Updated screenshot. Added Device Mode and Phone Number columns.	9/15/2025
ASM Server 7.0.9281.19200	Group Message Details Report	Added section.	9/15/2025
ASM Server 7.0.9281.19200	Group Messages – Formatted Report	Updated description to include roles.	9/15/2025
ASM Server 7.0.9281.19200	Group Messages Report	Updated description to include roles. Updated screenshot. Changed Contact Name to “Recipient Contact Name,” changed Sender ID to “Sender Contact ID,” and changed Contact ID to “Recipient Contact ID.” Added Recipient Role ID, Recipient Role	9/15/2025

		Name, Sender Role ID, Sender Role Name, Completed Contact ID, Completed Contact Name, Read Contact ID, Read Contact Name, Deleted Contact ID, Deleted Contact Name, Delivered Contact ID, Delivered Contact Name, Group ID, and Priority columns.	
ASM Server 7.0.9281.19200	Message Details Report	Added section.	9/15/2025
ASM Server 7.0.9281.19200	Messages Report	Updated screenshot. Changed Contact Name to "Recipient Contact Name," changed Sender ID to "Sender Contact ID," and changed Contact ID to "Recipient Contact ID." Added Recipient Role ID, Recipient Role Name, Sender Role ID, Sender Role Name, Subject, Completed Contact ID, Completed Contact Name, Read Contact ID, Read Contact Name, Deleted Contact ID, Deleted Contact Name, Delivered Contact ID, Delivered Contact Name, Group ID, and Priority columns.	9/15/2025
7.0.8892.6	Groups	Added Role-Based Messaging icons to Groups table.	9/15/2025
7.0.8892.5 IS 5.7	Connections	Updated screenshot. Under IS Connection: • Renamed the Server IP field "URL" and updated the description. • Updated descriptions of Port, Customer, and Station ID. • Added Auth Token.	9/15/2025
IS 5.6	Protected Dialing	Updated the DISA description to include a pound sign (#). Updated the example to include a pound sign in after the DISA number.	9/15/2025
7.0.8892.5	Groups	Added Resync button under Roles tab. Added field for entering role name in Delete Role prompt under Roles tab.	9/15/2025

7.0.8892.4	System Configuration	Added Change Password and Change Secret buttons to eMail Registration Settings pane.	9/15/2025
7.0.8892.4	System Dashboard	Renamed “Event Audit” table to “Event Log.”	9/15/2025
7.0.8892.3	Admins	Added “Select All/Select None” hyperlinks when selecting Groups	9/15/2025
7.0.8892.3	System Dashboard	Added a manual refresh button	9/15/2025
7.0.8892.3	System Configuration	Changed the Authentication Mode dropdown to display “ASM” instead of “MSM” Changed email registration account type from “G-Suite” to “Google Workspace”	9/15/2025
7.0.8892.3	Contacts	Renamed column in Devices table from “MSM Version” to “Secure Messages Version” Changed the New Contact popup to display “Amtelco Secure Messages” instead of “MSM”	9/15/2025
7.0.8892.3	Devices	Renamed column in Devices table from “MSM Version” to “Secure Messages Version”	9/15/2025
7.0.8892.3	System Events	Changed email registration account type from “G-Suite” to “Google Workspace”	9/15/2025
7.0.8892.3	Groups	Renamed "Licenses" to "Allocated Licenses" Updated the E-mail templates with new verbiage and removed MSM references	9/15/2025
7.0.8892.1	Licenses	Renamed Purchase History "License" to "License Type"	9/15/2025
7.0.8892.1	Groups	Removed "Enable Copying Spectrum Links" Renamed Permission "Access Message" to "Access Messages in Admin Web" Renamed Permission "Change Default Circle Name" to "Rename Default Circle"	9/15/2025

		Renamed Permission "Change Personal Circle Name" to "Rename Personal Circle" Renamed Permission "Change Away Message" to "Modify Away Message" Renamed Permission "Change Display Name" to "Modify Display Name" Renamed Permission "Change Email" to "Modify Email" Renamed Permission "Change Interval" to "Modify Notification Interval" Renamed Permission "Change Notifications (On/Off)" to "Toggle Notifications (On/Off)" Renamed Permission "Change Phone Number" to "Edit Phone Number" Renamed Permission "Change Personal Circle" to "Modify Personal Circle" Renamed Permission "Change Personal Quick Phrases" to "Modify Personal Quick Phrases" Renamed Permission "Change Picture" to "Modify Picture" Renamed Permission "Enable Access Gallery" to "Access Media Gallery" Renamed Phrase "Phrase Editor" to "Quick Phrase" Renamed Phrase "Response Phrase" to "Phrase" Renamed Roles "Role Properties" to "Role" Renamed Roles "Name" to "Role Name" Renamed Roles "Contacts" to "Assigned Contacts"	
7.0.8892.1	System Phrases	Renamed "Phrase Editor" to "System Phrase" Renamed "Response Phrase" to "Phrase"	9/15/2025
7.0.8892.0	All	Updated screenshots, logos, and references throughout document for	9/15/2025

		rebranding from miSecureMessages to Amtelco Secure Messages	
7.0.8892.0	Admin Settings	Renamed "Agent Login" to "Admin Name"	9/15/2025
7.0.8892.0	Away Messages	Renamed "Away Messages" to "System Away Messages"	9/15/2025
7.0.8892.0	Circles	Renamed "Registered Contacts" to "Assign and Unassign"	9/15/2025
7.0.8892.0	System Configuration	Renamed "Password Settings" to "Admin Password Settings"	9/15/2025
7.0.8892.0	Contacts	Renamed "Name" to "Display Name" Renamed "Require password change..." to "Force Password Change" Renamed "IS Settings" to "IS Agent Login" Renamed "Change Password" to "Password and Confirm Password" Delete contact message displays "This action cannot be undone"	9/15/2025
7.0.8892.0	Groups	Renamed "Max Licenses" to "Allocated Licenses" Renamed "Maximum Contact/Thread" to "Maximum Contacts per Thread" Renamed "IS Status URL" to "IS Web URL" Renamed "Genesis Dialing" to "Protected Dialing" Renamed "Genesis DISA#" to "DISA" Renamed "Genesis DISA#" to "DISA" Renamed "Genesis Code" to "Access Code" Renamed "Registered Contacts" to "Licensed Contacts" Renamed "Register/UnRegister" buttons to "Add/Remove" Renamed "Registered To Group" to "Assigned to Group"	9/15/2025

		Renamed "Name" to "Display Name" Renamed "Name" to "Display Name" Renamed "Authenticate" to "Include IS Credentials" Renamed "Phrases" to "Phrases Access" Renamed "Roles" to "Roles Access"	
7.0.8892.0	System Events	Renamed "Notifications" to "Events" in the navigation menu Renamed "Event" page to "System Events" page	9/15/2025
7.0.8641.3	Groups	Changed Notification Interval Limit to include a selection for hours, minutes, seconds	9/15/2025
7.0.8641.2	All	Added the ability to add roles to Personal Circles	9/15/2025
7.0.8641.2	Groups	Added Devices column to Available Contacts menu, and Visible and Active columns to Registered to Group menu	9/15/2025
7.0.8641.1	Circles	Added Roles menu to Circle Details	9/15/2025
7.0.8641.1	Groups	Moved “Allow Device to Device Messaging,” “Use System Away Messages,” and “Use System Phrases” from the Permissions tab to Options	9/15/2025
7.0.8641.1	Appendixes	Added actions used for Role-Based Messaging	9/15/2025
7.0.8641.0	Notifications	Updated for new e-mail account types	9/15/2025
7.0.8641.0	System Configuration	Updated eMail Registration Settings for new e-mail account types	9/15/2025
7.0.8641.0	Groups	Added Roles tab to screenshots	9/15/2025
7.0.8641.0	Groups	Added “Allow Dial Function,” “Allow Roles,” “Allow Copying Web Links,” “Allow Copying Phone Links,” “Allow Copying Email Links,” and “Allow Copying Spectrum Links” to Options in the General settings	9/15/2025
7.0.8641.0	Groups	Added “Notification Interval Limit” setting to the General settings	9/15/2025

7.0.8641.0	Groups	Added Roles setting to the Permissions settings	9/15/2025
7.0	Connections	Under IS Connection, updated the instructions for the IP Address and Port fields.	9/15/2025

R&D Software Department
4800 Curtin Drive, McFarland, WI USA 53558
www.amtelco.com