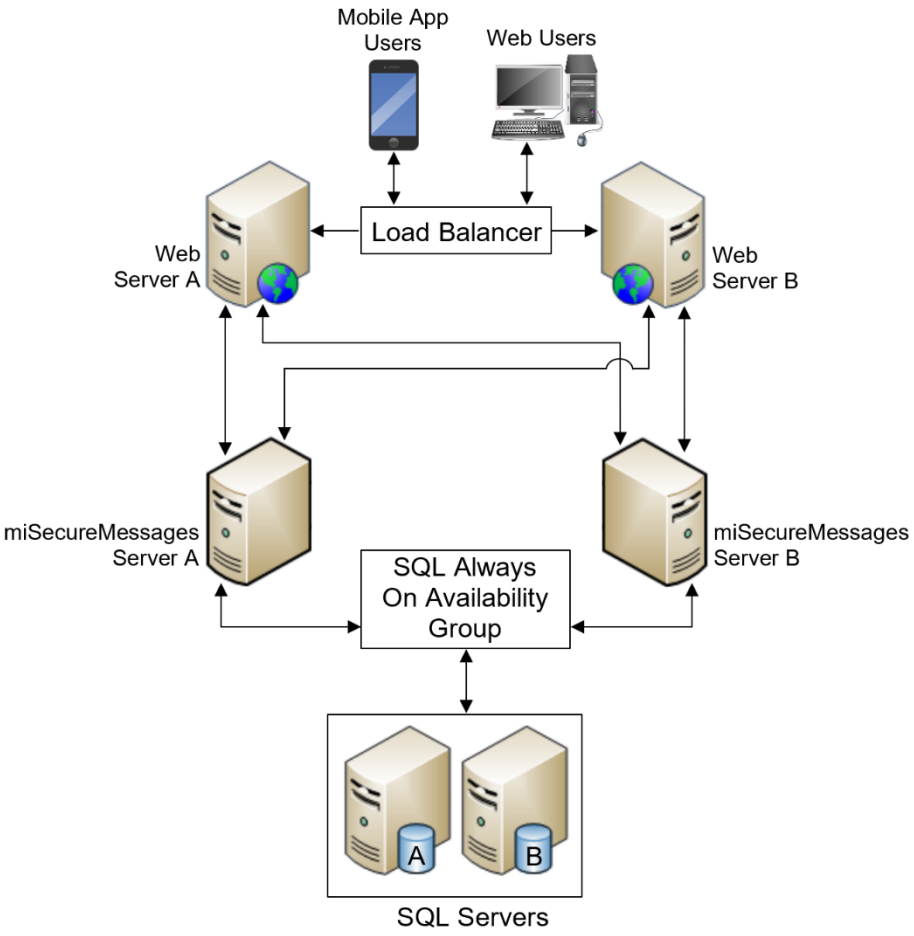
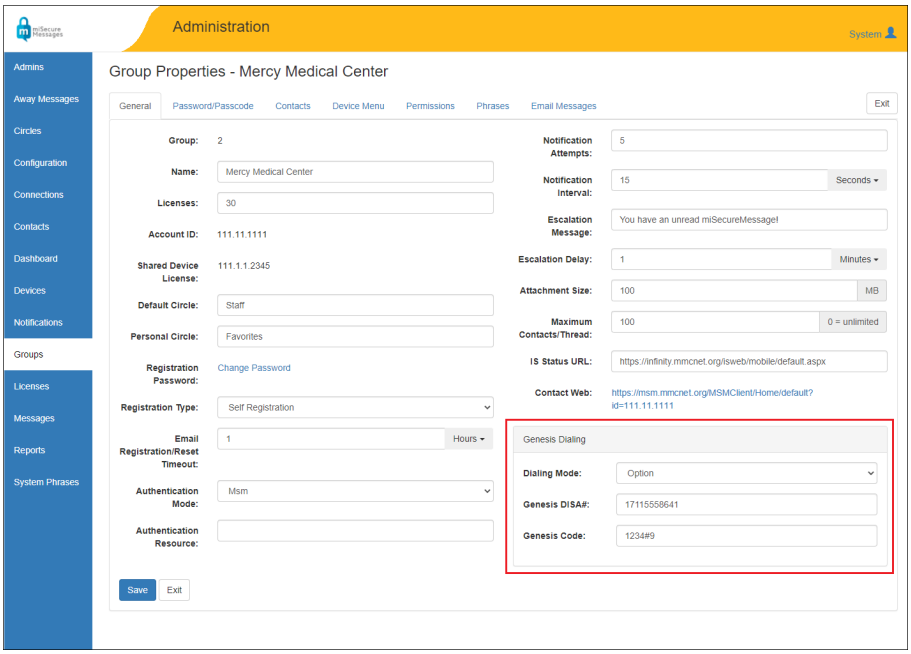
American Tel-A-Systems Inc.
4800 Curtin Drive, McFarland, Wisconsin USA 53558-9424
www.amtelco.com

New Features in miSecureMessages 6.8

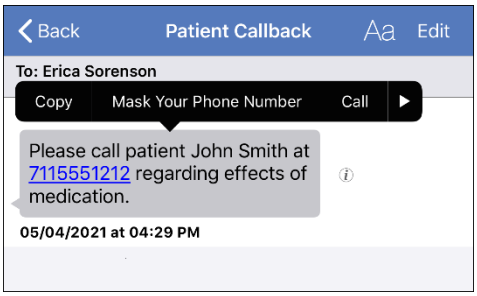
FEATURE	DESCRIPTION
High Availability configuration *Requires additional equipment*	The miSecureMessages (MSM) optional High Availability feature allows the MSM solution to be configured for multiple servers, with automated failover from one server to another when a server goes down. This feature can provide continuous uptime during some server upgrades and prevents downtime due to a single server failure.  • The thread archive path (if not archiving to Amazon) should be set up on a file share. Otherwise, archives could end up being split between the servers, making it harder to find archived messages.

FEATURE	DESCRIPTION
	• Configure the MSM Service on the additional server just like the initial server. It will need its own IP address, but should point to the same database. The additional server should have its own MSM Notification Service installed. • MSM Web Service and MSM Administration Web need to be configured to use the additional server. This is done by adding the new server (formatted as server:port) to the comma separated list of servers in the Servers key in the web.config file. • Configure the events for "Inactive server" to be notified if a server is down, and "Unlicensed server" to be notified if an unlicensed server is running. • Configure loading balancing and enable sticky sessions on the Web servers.
Genesis Protected Dialing *Requires IS Server 5.5 or later, Genesis 5.7 or later, the Protected Dialing feature, an implementation fee, and the Auto Attendant feature*	New Genesis Protected Dialing settings allow phone calls placed from the miSecureMessages 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. (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.) The Genesis Dialing settings are located under the General tab on the Group Properties screen in the MSM Administration Web. 

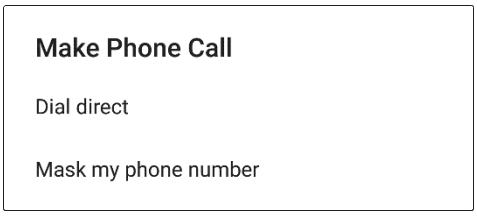
Dialing Mode

The Genesis Dialing settings in the MSM Group Properties provides three options for dialing phone numbers from within the miSecureMessages apps:

- Phone: Phone numbers are dialed directly from the user's device, displaying the device's phone number.
- DISA: Direct Inward System Access uses a Genesis Direct Inward Dialing (DID) Phone Number and a Protected Dialing Passcode to create an overdial, displaying the organization or call center's phone number rather than the device's phone number.
- Option: Each time the user places a call from the miSecureMessages App, the user is prompted to choose between dialing directly from the device or using DISA to dial through Genesis.

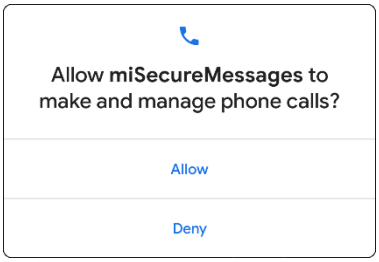


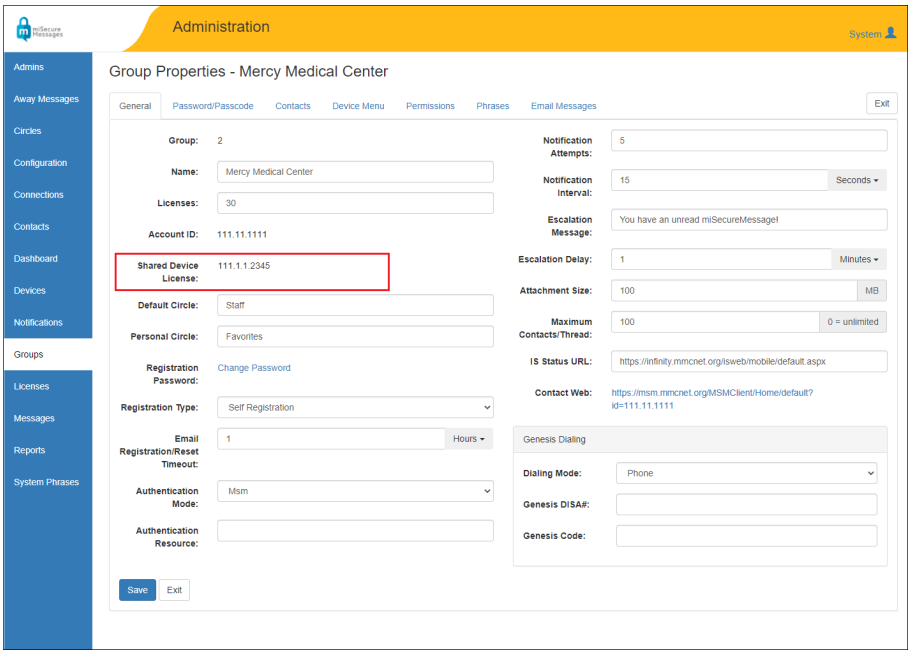
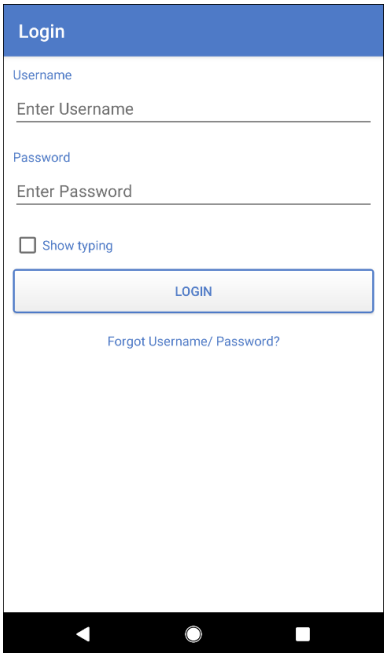
Placing a call from the Apple App

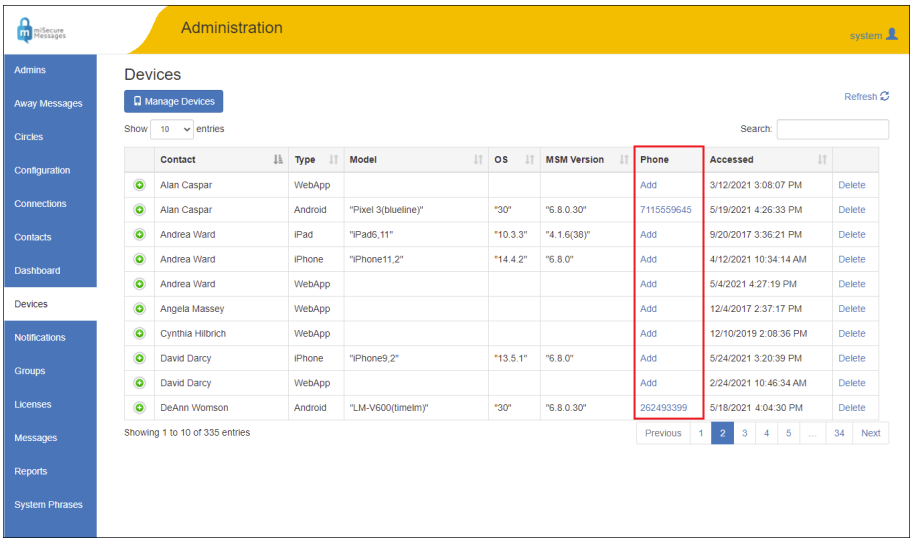


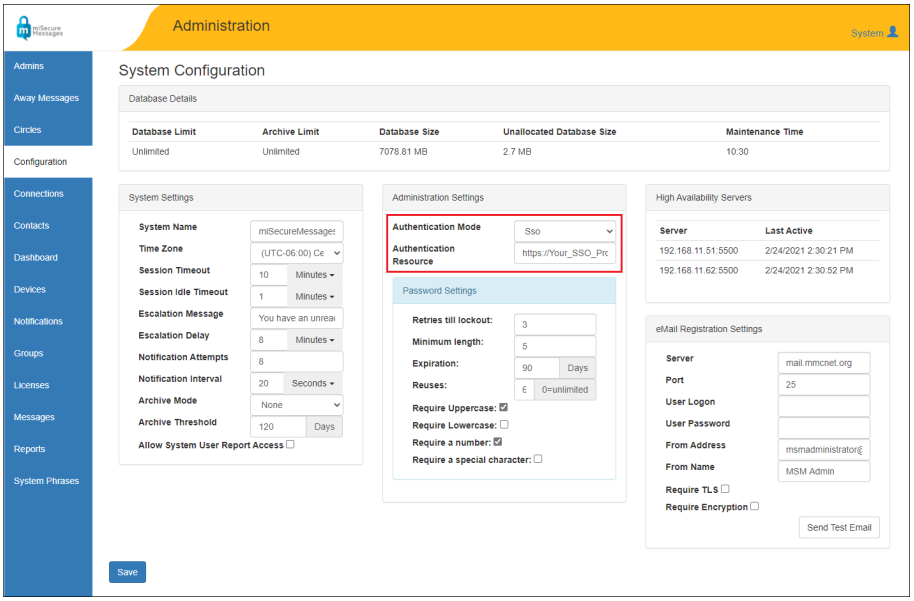
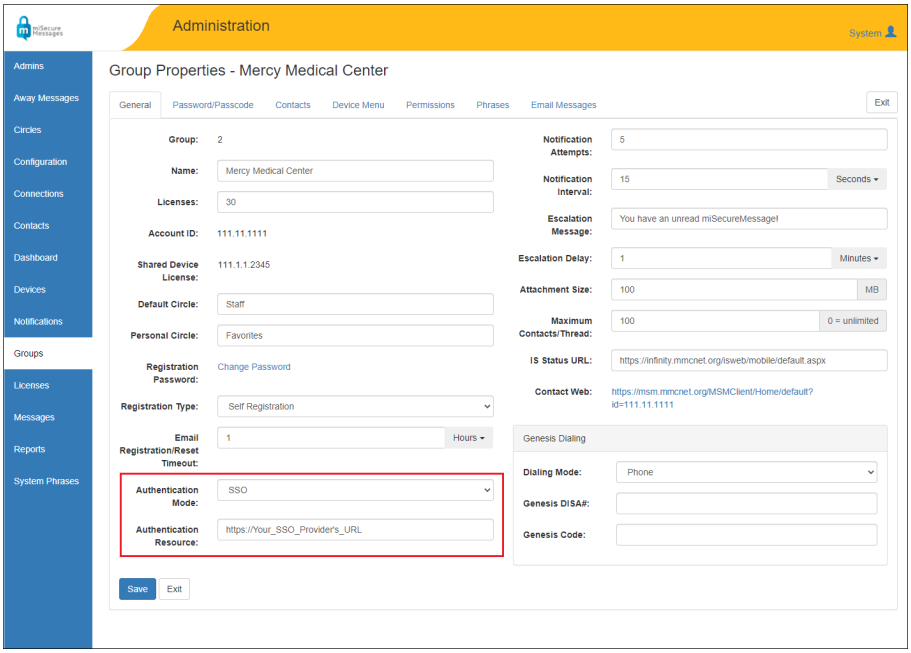
Placing a call from the Android App

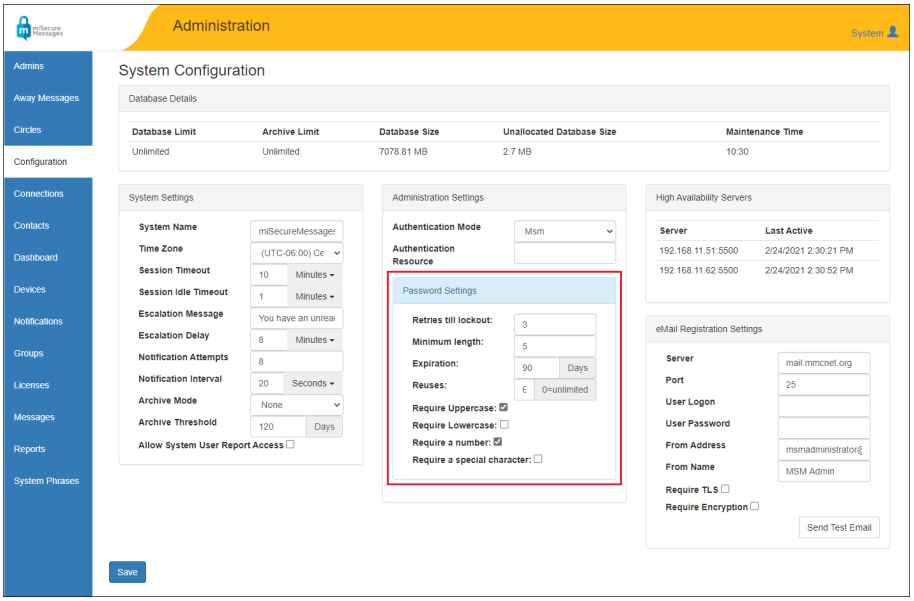
The first time that a miSecureMessages App user attempts to place a phone call using DISA, a prompt is displayed asking the user to allow miSecureMessages to make and manage phone calls. The user must tap or touch Allow in order to route phone calls through Genesis.



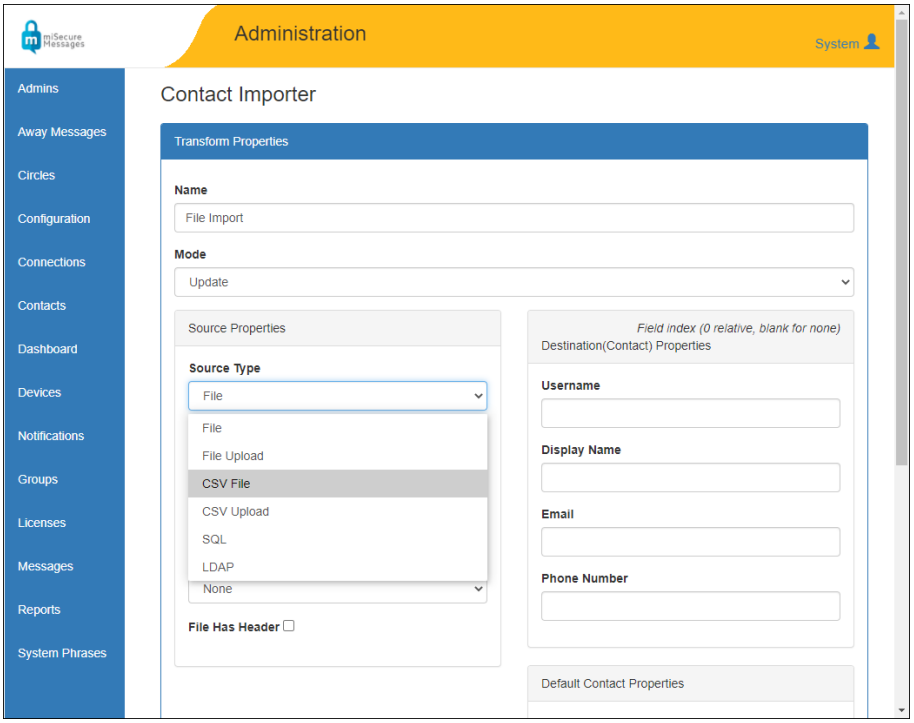
FEATURE	DESCRIPTION
Shared Device Licenses	Shared Device Licenses allow devices to be registered for use by multiple MSM users. Users are able to log into a device at the start of their shift and log out of it at the end of their shift, allowing another person to use the device. This feature enables healthcare organizations to provide their employees with a pool of devices to use at work and keep personal devices off of the network. A Shared Device License is automatically generated for each MSM Group, and is displayed under the General tab of Group Properties.  An administration username and password is required to add a Shared Device License to a device. Once the device has been registered as a Shared Device, users are prompted with a Login screen that asks for their miSecureMessages username and password. 

FEATURE	DESCRIPTION
Device Phone Numbers	Device phone numbers can be added to devices from the Devices page of the MSM Administration Web or from the Devices table in Contact Properties on the MSM Administration Web. Device phone numbers are tied to a device rather than to a contact person.  Device phone numbers can be used with the Shared Device feature to allow miSecureMessages users to call a contact person who doesn't use the same device every day. When a contact person is logged into a shared device, the phone number of whichever device the user is logged into is displayed in the miSecureMessages apps on the Contact Info page for the contact.
Single Sign-On (SSO) *Requires a certificate from an ID provider and purchase of the MSM Single Sign-On feature*	The optional MSM Single Sign-On (SSO) feature provides authentication with a Single Sign-On Identity Provider. This option requires a certificate from a SSO Identity Provider and the installation and configuration of the MSM Assertion Consumer Web. This feature has been tested with the following SSO Identity Providers: • Active Directory Federation Services (ADFS) • Azure Active Directory (AD) The SSO settings for agent logins area located on the System Configuration screen of the MSM Administration Web.

FEATURE	DESCRIPTION
	 MSM Administration Web agent logins can be configured for one of two authentication modes: • MSM: The MSM server keeps track of passwords and performs authentication. • SSO: Single Sign-On Identity Provider keeps track of passwords and performs authentication. The SSO settings for Groups are located under the General tab on the Group Properties screen in the MSM Administration Web. 

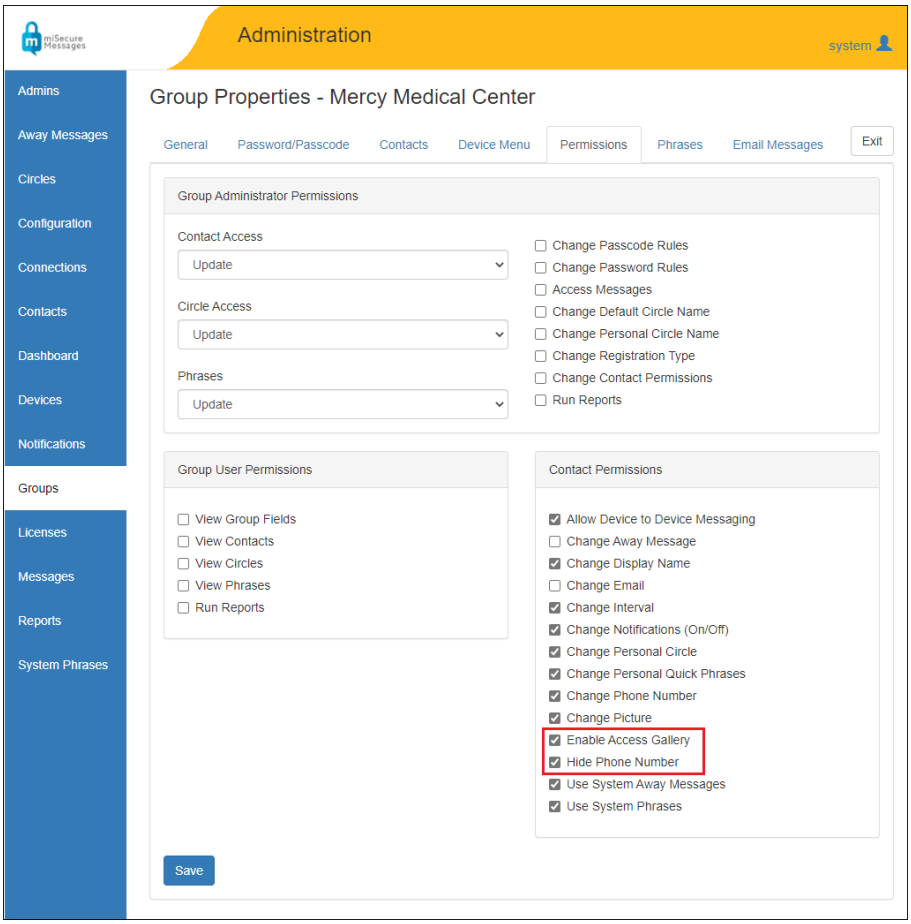
FEATURE	DESCRIPTION
	MSM Groups can be configured for one of two authentication modes: • MSM: The MSM server keeps track of passwords and performs authentication. • SSO: A Single Sign-On Identity Provider keeps track of passwords and performs authentication.
Password Settings for Agents	Password Settings have been added to the System Configuration screen of the MSM Web Administration Web to allow administrators to set complexity requirements for agent passwords used to log into the MSM Administration Web. These are similar to the Group password settings that set the parameters for the passwords used to register miSecureMessages on a device.  **Retries till lockout** This setting controls how many times someone can attempt to log into the MSM Administration Web with a valid agent name and an incorrect password before that agent name is locked. When an agent name is locked, it cannot be used to access miSecureMessages until the password is reset in the Admin Settings for that agent. If Retries till Lockout is set to zero (0), usernames are never locked due to failed login attempts. **Minimum Length** This setting enforces a minimum length for passwords. If Minimum Length is set to zero (0), no minimum is enforced.

FEATURE	DESCRIPTION
	Expiration Expiration indicates the number of days until an agent's current password will expire. Expired passwords need to be changed in order to continue using miSecureMessages. Reuses The Reuses setting determines the number of unique passwords that must be set for an agent before the agent can reuse an old password. ☑ Require Uppercase The "Require Uppercase" option requires passwords to contain at least one upper case letter. ☑ Require Lowercase The "Require Lowercase" option requires passwords to contain at least one lower case letter. ☑ Require a number The "Require a number" option requires 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: ` ~ ! @ # $ % ^ & * ( ) - _ + = { [}] | \ : ; " ' < , > . ? /
Automatic registration when adding existing users to a Group	If a user is already registered on a device, adding the user to another Group in the MSM Administration Web will grant the user access to that Group on that device without the user having to register on that again. This simplifies the device registration process by only requiring a user to register once on the device, rather than having to register for each group.

FEATURE	DESCRIPTION
Contact Importer supports CSV files	The Contact Importer in the MSM Administration Web now supports Comma-Separated Values (CSV) files. There are two options for importing from CSV files, based on whether you have an on-site installation or hosted miSecureMessages. Both options are found in the Source Type menu in the Transform Properties when adding or editing a Contact Importer transform.  • The CSV File option is used with on-site miSecureMessages installations. It is used to import contacts from a Comma-Separated Values file on your on-site network. • The CSV Upload option is used with hosted miSecureMessages. It prompts the user to select a Comma-Separated Values file to upload to the hosted MSM Server for importing contacts.

New Contact Permissions

Two new permissions settings have been added to Contact Permissions section of the Group Properties.



Hide Phone Number

The "Hide Phone Number" setting determines whether contacts in this group can view other contact phone numbers in the miSecureMessages apps and in the MSM Contact Web.

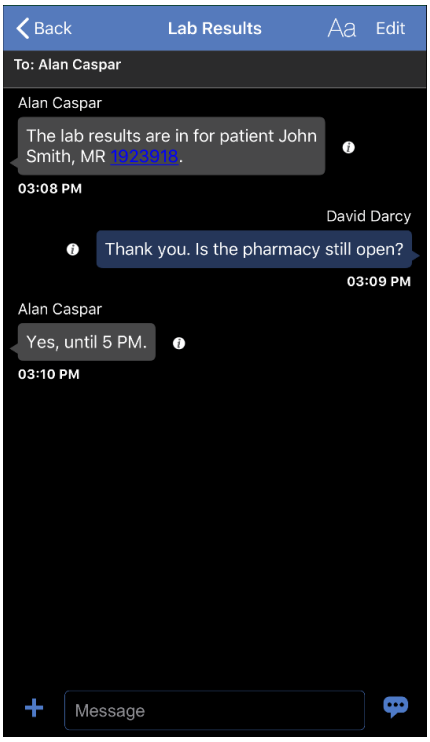
Note: This setting is used to hide contact phone numbers, but does not hide device phone numbers.

- Select the "Hide Phone Number" check box to hide contact phone numbers when displaying the Contact Info in the MSM apps or the MSM Contact Web.
- Clear the "Hide Phone Number" check box to show contact phone numbers when displaying the Contact Info in the MSM apps or the MSM Contact Web.

Enable Access Gallery

The "Enable Access Gallery" setting determines whether MSM users can access their device's Photo Gallery from the MSM app to attach

FEATURE	DESCRIPTION
	photos to an MSM message. Disabling this feature forces users to take a photo from the MSM app in order to attach it, and prevents the photo from being stored in the device's Photo Gallery. Users can still use their device's camera to take a photo outside of the app and store in in their gallery, but those photos cannot be attached to an MSM message. • Select the "Enable Access Gallery" to allow MSM app users to attach a photo from their device's Photo Gallery to MSM messages. • Clear the "Enable Access Gallery" check box to only allow photos taken from the MSM app to be attached to messages and to prevent those photos from being stored in the device's Photo Gallery.
Adjustable Font Size for Apple App	The miSecureMessages Apple App features an icon that allows the user to adjust the font size used for messages.  Tap the Aa icon on the Messages screen to display the Font Size controls. Use the slider or the Zoom Out and Zoom In icons to select a font size. Tap outside of the Font Size display to return to the Messages screen.

FEATURE	DESCRIPTION
Dark Mode for iOS	The miSecureMessages Apple App will switch to dark mode when used on a device that is set to the "Dark" appearance in the iOS settings. In dark mode, most screens are displayed as white text on a dark background, instead of black text on a light background.  Previously, dark mode only was available on Android devices.
Themes persisted on the server	Themes selected in the MSM apps are persisted on the server instead of the device, allowing the theme to apply to all of the user's devices.
New Notification Events	New notification event settings for server and device conflicts have been added to the Notifications page of the MSM Administration Web.

Requirements:

- MSM Server 6.8.7941.23671 or later
- MSM Administration Web 6.8.7657.11 or later
- MSM Contact Web 6.8.7657.10 or later
- MSM Apple App 6.8.0.24 or later
- Apple iOS 13.0 or later with Business Use data plan
- MSM Android App 6.8.0.16 or later
- Android OS 7.0 or later with cellular data plan and a Google account
- 64-bit Windows Server 2016 or later with .NET Framework 4.7.2
- IIS 7.5 Compatibility or later
- SSL security certificate
- SQL Server 2016 or later

Optional:

- Apple Watch Series 3 or later
- Apple watchOS 7.0 or later

High Availability Requirements:

- Additional web, application, and SQL Servers
- File share location for archives
- Load Balancer

Single Sign-On Requirements:

- MSM Single Sign-On Feature
- MSM Assertion Consumer Web
- ID provider certificate
- Service provider certificate

Genesis Protected Dialing Requirements:

- Intelligent Series Server 5.5 or later
- Genesis 5.7 or later
- Protected Dialing feature
- Implementation fee
- Auto Attendant feature

Browser Compatibility:

Amtelco Web applications are tested with the latest release of the following browsers.

- Apple Safari
- Google Chrome
- Microsoft Edge
- Mozilla Firefox