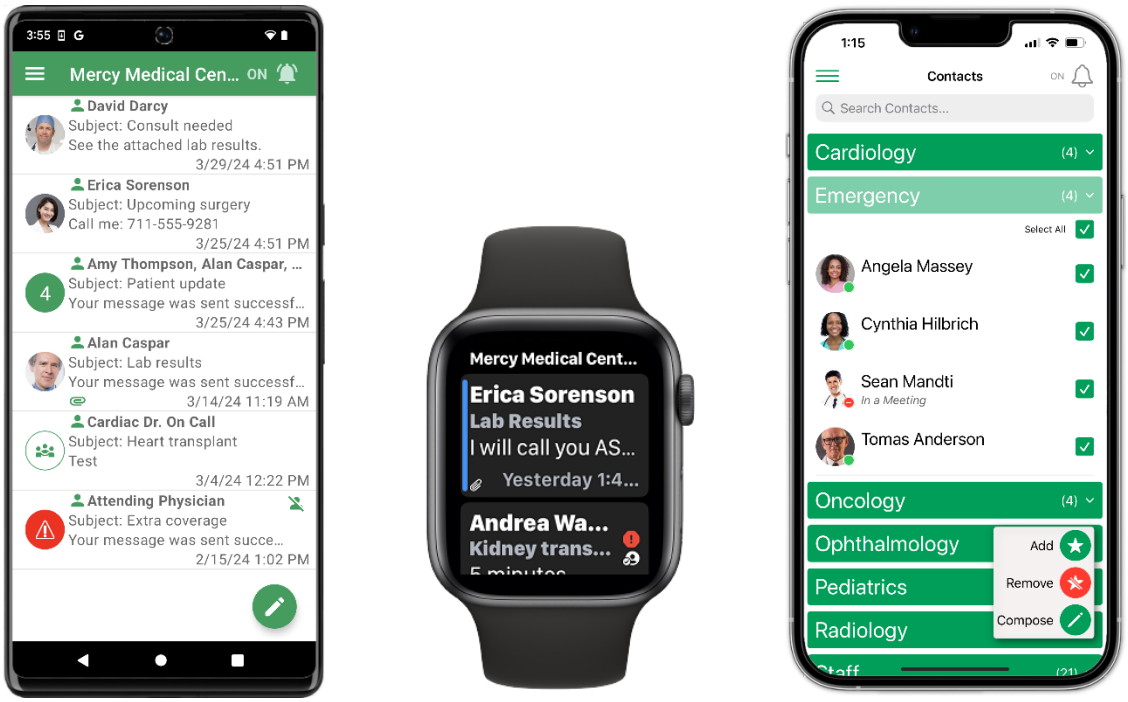
Secure Messages

amtelco

R&D Software Department
4800 Curtin Drive, McFarland, WI USA 53558
www.amtelco.com

Amtelco Secure Messages Technical Notes



Amtelco Secure Messages (ASM) brings secure messaging and paging services to mobile devices. Unlike SMS, Amtelco Secure Messages encrypts messages, keeping your protected health information (PHI) secure. Messages are not stored on your devices, passcodes or fingerprint scans can be required, and access can be remotely disabled, making Amtelco Secure Messages HIPAA and HITECH compliant.

The Amtelco Secure Messages solution uses an encrypted web service to send secure messages to Android and Apple iOS based devices. Amtelco Secure Messages can be tailored to meet each site's secure messaging and paging needs. Amtelco Secure Messages is available as an on-site solution and as a cloud-based solution.

Recipients are notified of incoming messages via customizable audio and visual alerts and view their messages using the Amtelco Secure Messages app on their devices. Recipients can select from a list of pre-defined reply messages or can enter a custom reply, which is sent as securely as was the original inbound message. Amtelco Secure Messages documents messaging activity with detailed delivery and read receipts for every message.

Amtelco Secure Messages can be initiated by enterprise staff via a web interface and a mobile device app, and optionally by call center operators using Amtelco's Intelligent Web Agent, Soft Agent, and Infinity Telephone Agent workstation applications. Amtelco Secure Messages does

not have the character limits of SMS text messaging, and is a secure method for transmitting images, audio files, and other materials as message attachments.

Amtelco Secure Messages can be integrated with Amtelco's Genesis and Intelligent Series call center solutions to provide scripted messaging, integrated directory and on-call scheduling, Intelligent Online Directories, and Intelligent Operator Services.

Amtelco Secure Messages Communication Process

A message is initiated by a mobile device user using the Amtelco Secure Messages mobile device app, an enterprise user using the Amtelco Secure Messages Contact Web user interface, or a console operator using the optional Intelligent Web Agent, Soft Agent, or Infinity Telephone Agent application. Messages sent from mobile devices are processed by the ASM Web Service running on a web server. Messages sent from the Intelligent Series and Infinity platforms are processed by the ASM Service running on that system's applications server and are passed to the ASM Notification Service.

When a message is sent, the ASM Notification Service sends a notification through the Google Firebase Cloud Messaging service or Apple Push Notification Service to the appropriate mobile device. When the message notification arrives on the mobile device, an informative alert is popped, an optional audio alert is generated, and a delivery receipt is sent back to the ASM Web Service.

When a notification is received, the recipient must acknowledge the notification and can then summon the message from the web server with the Amtelco Secure Messages mobile device app using Transport Layer Security (TLS) encryption. Opening and viewing the message results in a read receipt being returned from the user device to the ASM Web Service. After reading the message, the recipient can deliver a TLS-encrypted reply through the web service and can mark the message "Completed." Replies are processed by the ASM Web Service.

Amtelco Secure Messages Features and Functions

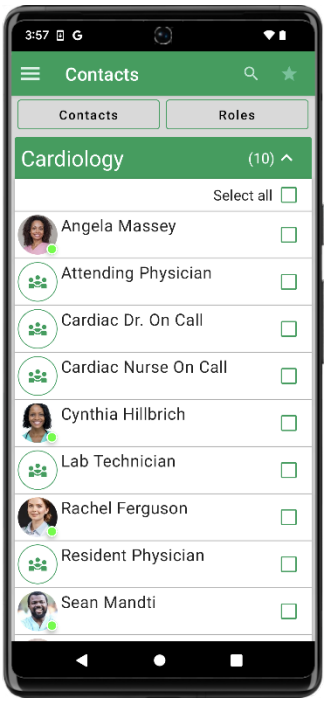
The Amtelco Secure Messages secure mobile device messaging solution is designed to:

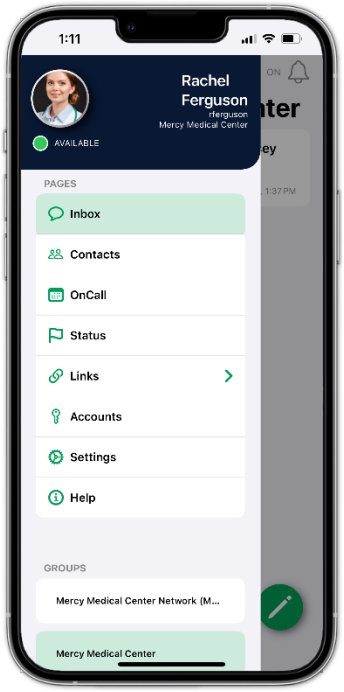
- Provide two-way encrypted text messaging in a next-generation smartphone-based paging solution.
- Enable a user to define custom audio and visual alerting options for all messages.
- Provide persistent alerting that continues until the recipient acknowledges a message.
- Provide a separate Inbox for secure messages, distinct from e-mail and SMS text messaging.
- Enable senders to specify the priority of their messages.
- Provide a secure and directed method for transmitting images, audio files, and other materials as message attachments.
- Provide encrypted message delivery receipts, documenting that a user's mobile device has received a message.
- Provide encrypted message read receipts, documenting that a user has read a message.
- Enable a user to reply to a received message with an encrypted, pre-defined or custom response message, with the reply being documented in the message history and viewable by the sender.

- Enable a user to mark a message as “Completed,” resulting in no further actions being required on the message.
- Integrate with Amtelco’s Genesis and Intelligent Series (IS) suite of call center solutions.
- Optionally route phone calls through Amtelco’s Genesis soft switch to protect staff’s phone numbers from being visible to patients.

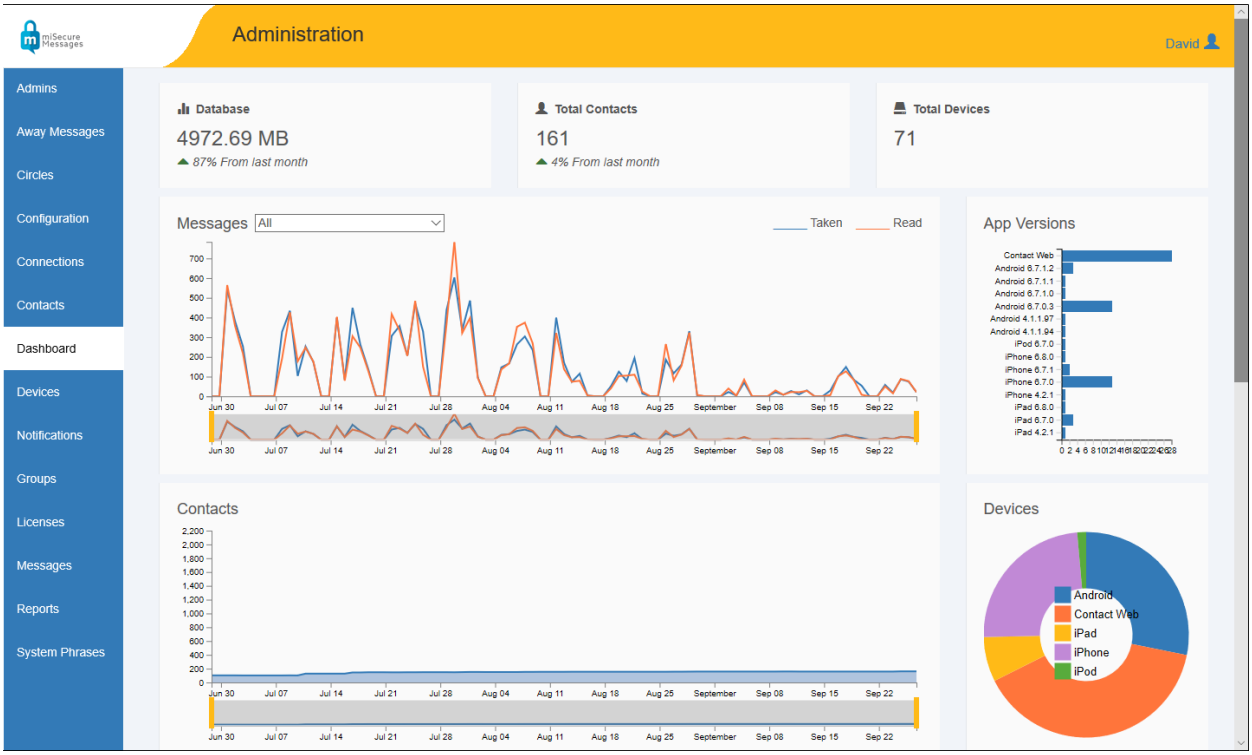
Amtelco Secure Messages Mobile Device Apps

The Amtelco Secure Messages apps for Android and Apple iOS based devices and for Apple Watches are the end-user interfaces for secure messaging and paging activities. Mobile device users can view and respond to messages and can initiate new messages to other users and groups of users.



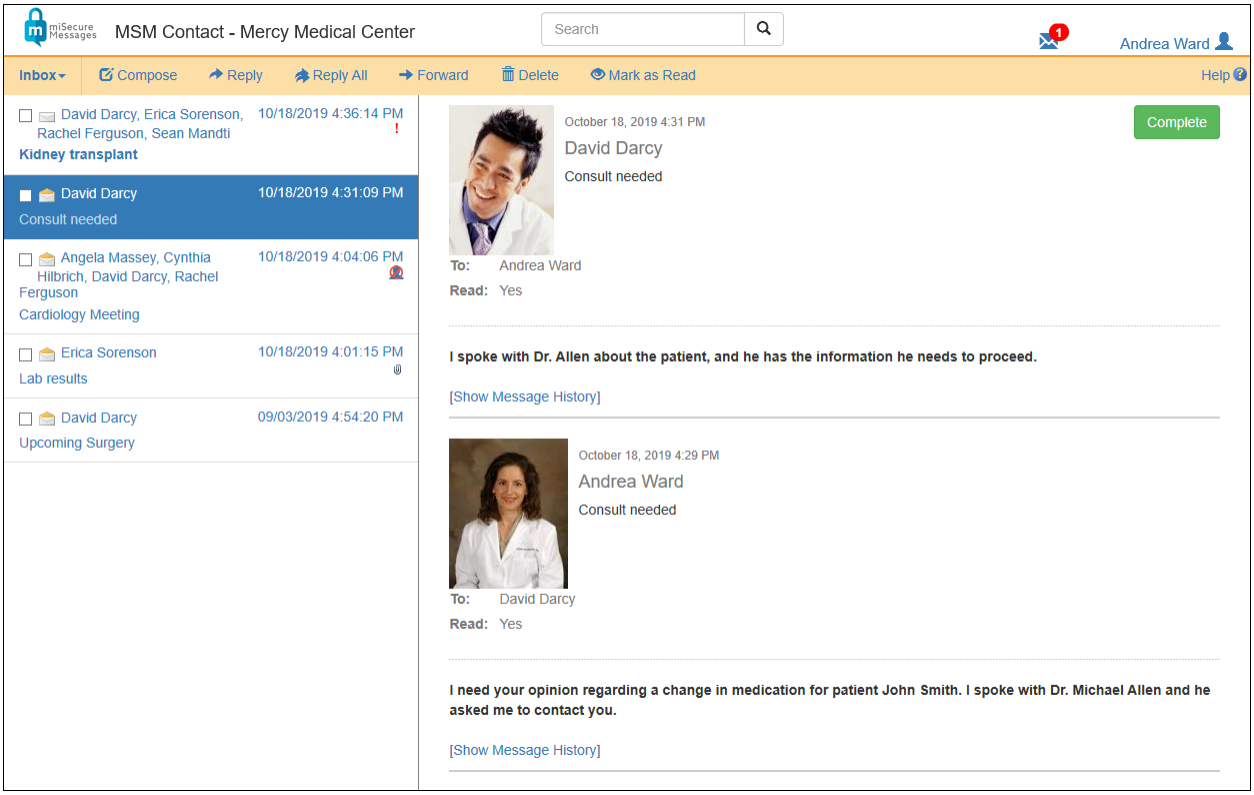


Amtelco Secure Messages Admin Web



The Amtelco Secure Messages (ASM) Admin Web is used to administer the Amtelco Secure Messages secure mobile device messaging solution. Administrators can use the ASM 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.

Amtelco Secure Messages Contact Web



The Amtelco Secure Messages Contact Web provides access to secure messaging and paging services from the convenience of a web browser. The Contact Web lets users view secure messages using Transport Layer Security (TLS) encryption with username, password, and Account ID authentication. Users can respond to secure messages and can initiate new messages to other Amtelco Secure Messages users within their company or organization.

Amtelco Secure Messages Technology

The Amtelco Secure Messages mobile device messaging and paging solution can be deployed as an on-site implementation or a cloud-based solution. For on-site implementations, the system is deployed as a software-only solution that can run on dedicated, shared, or virtual servers. Cloud-based solutions are offered by Amtelco as a Software as a Service (SaaS) subscription service that is operated from geographically diverse hardened data centers.

The Amtelco Secure Messages solution encompasses:

ASM Service: The ASM Service receives notification of secure messages from the input methods and notifies the ASM Notification Service. The ASM Service receives read requests, replies, and completion notifications from the ASM Web Service. When the ASM Service receives a read request, it pushes message data from the input methods to the ASM Web Service for display on mobile devices.

ASM Notification Service: The ASM Notification Service receives notification of messages from the ASM Service and notifies the Google Firebase Cloud Messaging service and Apple Push Notification Service which send notifications of new message traffic to Amtelco Secure Messages users.

ASM Web Service: The ASM Web Service receives transmission receipts, read receipts, replies, and completion notifications from the apps running on the users' mobile devices. When a read request is received, the ASM Web Service requests the message information from the ASM Service and displays the message information to the app on the device that sent the read request.

ASM Configuration Application: The ASM Configuration Application is used to configure the ASM Service.

Amtelco Secure Messages Admin Web: The Amtelco Secure Messages (ASM) Admin Web is used to administer Amtelco Secure Messages. Administrators can use the ASM Admin Web to create and edit the list of Quick Phrases available to users, to set up Amtelco Secure Messages groups, and to remove contact names and devices.

Amtelco Secure Messages Contact Web (optional): The Amtelco Secure Messages Contact Web provides access to secure messaging and paging services from the convenience of a web browser. The ASM Contact Web lets users view secure messages using Transport Layer Security (TLS) encryption with username, password, and license key authentication. Users can respond to secure messages and can initiate new messages to other Amtelco Secure Messages users.

Amtelco Secure Messages Android App: The Amtelco Secure Messages Android app provides secure messaging and paging services for Android devices using Amtelco's ASM Service. The Amtelco Secure Messages Android app receives message notifications from the ASM Notification Service via the Google Firebase Cloud Messaging Service. Users can view and respond to messages and can initiate messages to other Amtelco Secure Messages users.

Amtelco Secure Messages Apple App: The Amtelco Secure Messages Apple app provides secure messaging and paging services for Apple iOS devices using Amtelco's ASM Service. The Amtelco Secure Messages Apple app receives message notifications from the ASM Notification Service via the Apple Push Notification Service. Users can view and respond to messages and can initiate messages to other Amtelco Secure Messages users.

Genesis (optional): The Protected Dialing feature can route phone calls placed from the Amtelco Secure Messages apps through the Genesis soft switching platform to display your organization's information in the Caller ID and keep the user's personal phone number private.

Intelligent Series (optional): The Intelligent Series (IS) is Amtelco's suite of call center applications. Secure Messaging Contact Methods can be configured for individual IS Directory listings to enable Amtelco Secure Messages messaging. The Contact Methods are used to push messages from the IS Server to the ASM Web Service for processing. Delivery options are set in the properties of the Intelligent Messaging script response elements or in the message settings.

Infinity (optional): The Infinity appliance is Amtelco's operator services call center system. Dial strings are used to push messages from Infinity to the ASM Web Service for processing. An account option can be set to distribute the message to a console operator when a reply is received. Another account setting indicates when a message should be marked as "Delivered."

Amtelco Secure Messages Communication Protocols

The Amtelco Secure Messages application uses a proprietary protocol implemented over encrypted socket connections in addition to secure TCP/IP networking protocols.

The Transport Layer Security (TLS) protocol is used for outbound traffic from the Amtelco Secure Messages notification service to the Android and Apple push services. The TLS protocol is an internationally accepted method for client-server applications to communicate in a way designed to prevent eavesdropping and tampering.

The Hypertext Transfer Protocol Secure (HTTPS) protocol is used for traffic between the Amtelco Secure Messages web service and the individual device apps and web-based users. HTTPS connections are used worldwide for Internet-based payment transactions and for sensitive transactions in corporate information systems.

The Amtelco Secure Messages solution makes a limited number of ports available to external traffic to minimize exposure beyond the enterprise. All of these ports are secured by HTTPS security. Communication with the Google Firebase Cloud Messaging service uses port 443. Communication with the Apple Push Notification Service uses port 443. Communication with the web-based Amtelco Secure Messages users moves through port 443.

The following table details the communications protocol used by the Amtelco Secure Messages system components.

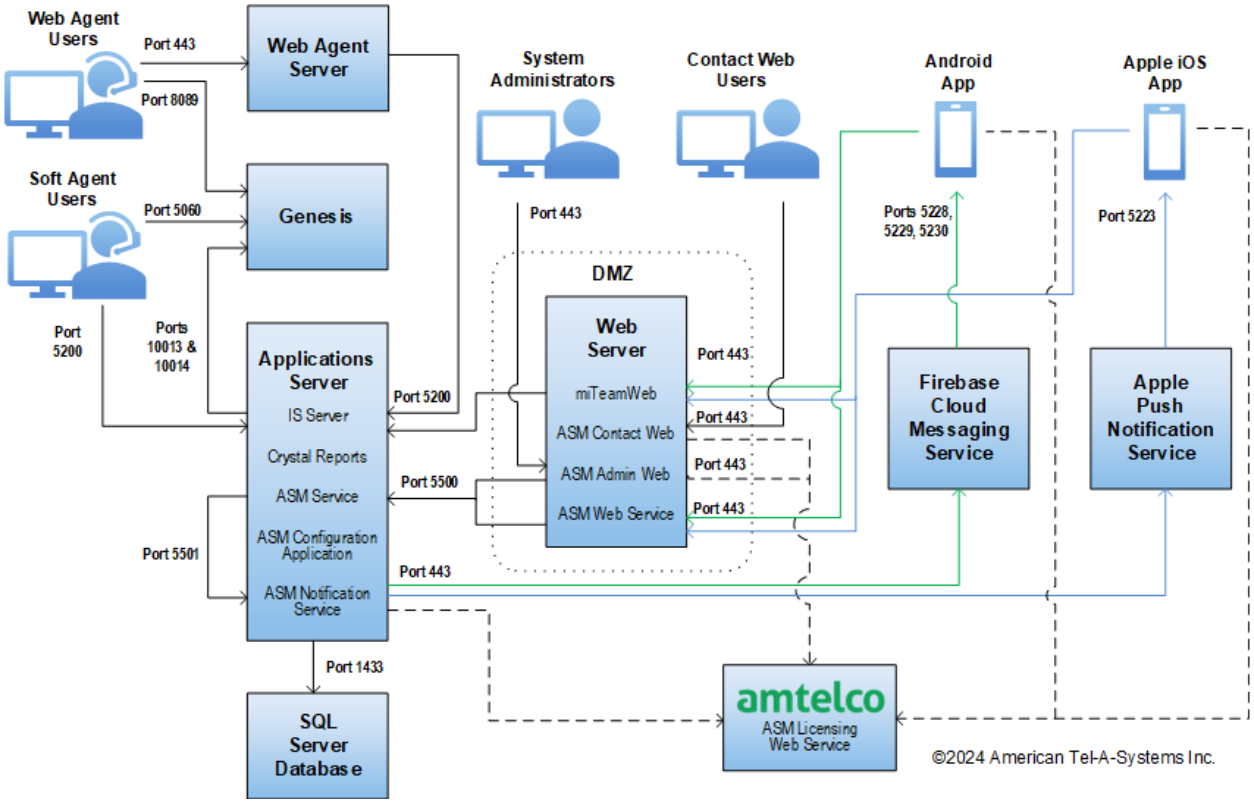
Component	Communicates with	Using
Amtelco Secure Messages App (operating system-specific)	ASM Web Service	HTTPS
Amtelco Secure Messages App (operating system-specific)	Licensing Web Service (located at Amtelco)	HTTPS
ASM Notification Service	Push Service (Android, Apple iOS)	HTTPS for Android HTTP/2 for Apple iOS
ASM Notification Service	Licensing Web Service (located at Amtelco)	HTTPS
ASM Web Service	ASM Service	256-bit AES socket encryption
ASM Service	ASM Notification Service	256-bit AES socket encryption
ASM Admin Web (administrator's web browser)	ASM Service	HTTPS and 256-bit AES socket encryption
ASM User Web Client (user's web browser)	ASM Web Service	HTTPS

Amtelco Secure Messages System Options

The Amtelco Secure Messages solution is available as an on-site solution and as a cloud-based solution. The Amtelco Secure Messages solution can be tailored to meet each site's secure messaging and paging needs.

Amtelco Secure Messages On-Site Solution

Amtelco Secure Messages requires communication between the ASM servers, the users' mobile devices and the Intelligent Series and Genesis or Infinity servers in the system configuration at the customer location.



Amtelco Secure Messages in a complete on-site environment with IS and Genesis

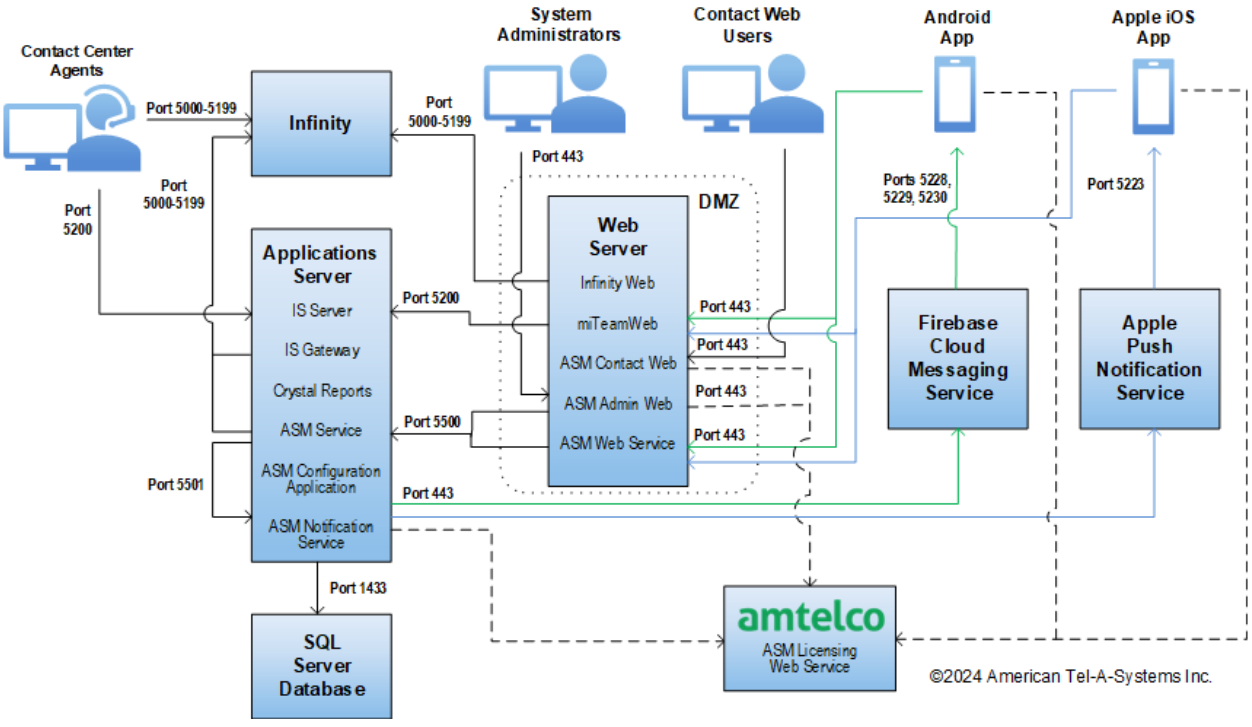
- An application server is required. The Amtelco Secure Messages Service can be loaded on the IS Server or on an equivalent server. The ASM Configuration Application and the ASM Notification Service also are loaded on the application server.
- A Microsoft SQL Server database is required. Client setup information, messages and configuration options are stored in this system database. Database sizes vary based on the number of users and the volume of messages being stored, but a database size of less than 20 GB can be expected.
- A web server is required. Port 443 is used for external two-way Internet traffic. A Secure Sockets Layer/Transport Layer Security (SSL/TLS) certificate is required for encrypted traffic and must be loaded prior to the Amtelco Secure Messages installation.

- An SSL/TLS certificate for encrypted traffic must be installed on the web server prior to the Amtelco Secure Messages installation. The certificate should be signed using an SHA256 or greater signature hash algorithm, with either a 2048-bit or greater RSA key or a 256-bit or greater ECC key. It is the customer's responsibility to renew the certificate every year.

Note: The servers that comprise the Amtelco Secure Messages system can be individual dedicated servers, a single server housing some or all of the system components, or multiple server instances in a virtual server environment. A single server running the Microsoft Windows Server operating system can house the IS Server, the ASM application server and the ASM web server; however, Amtelco recommends that the web server be separate from the system's other server components. The web server often is located in the Demilitarized Zone (DMZ) of the customer's Information Technology (IT) infrastructure for reasons of system security. The ASM applications server and the IS Server need not be subjected to such security.

Port Requirements

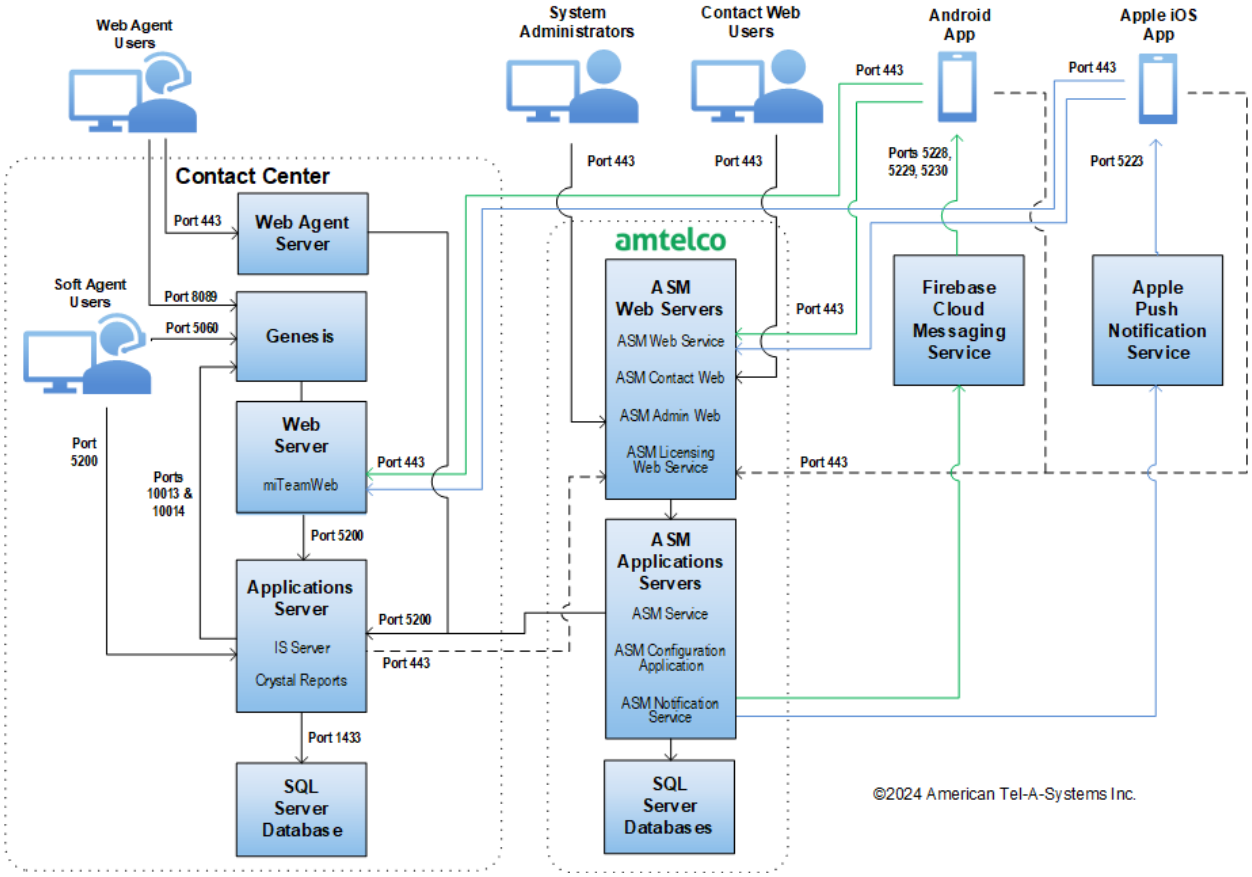
- Inbound ports 5228, 5229 and 5230 must be open in the site's WiFi network to enable Android device users to receive message notifications from the Firebase Cloud Messaging service.
- Inbound port 5223 must be open in the site's WiFi network to enable Apple iOS device users to receive message notifications from the Apple Push Notification Service.
- Outbound port 443 must be open in the site's WiFi network to allow Android device users to send message notifications to the Firebase Cloud Messaging service and to allow Apple iOS device users to send message notifications to the Apple Push Notification Service.



Amtelco Secure Messages in a complete on-site environment with IS and Infinity

Amtelco Secure Messages Cloud-Based Solution

The Amtelco Secure Messages cloud-based solution requires communication between Amtelco's hosting servers, the users' mobile devices and the Intelligent Series and Genesis or Infinity servers located at the customer's location.

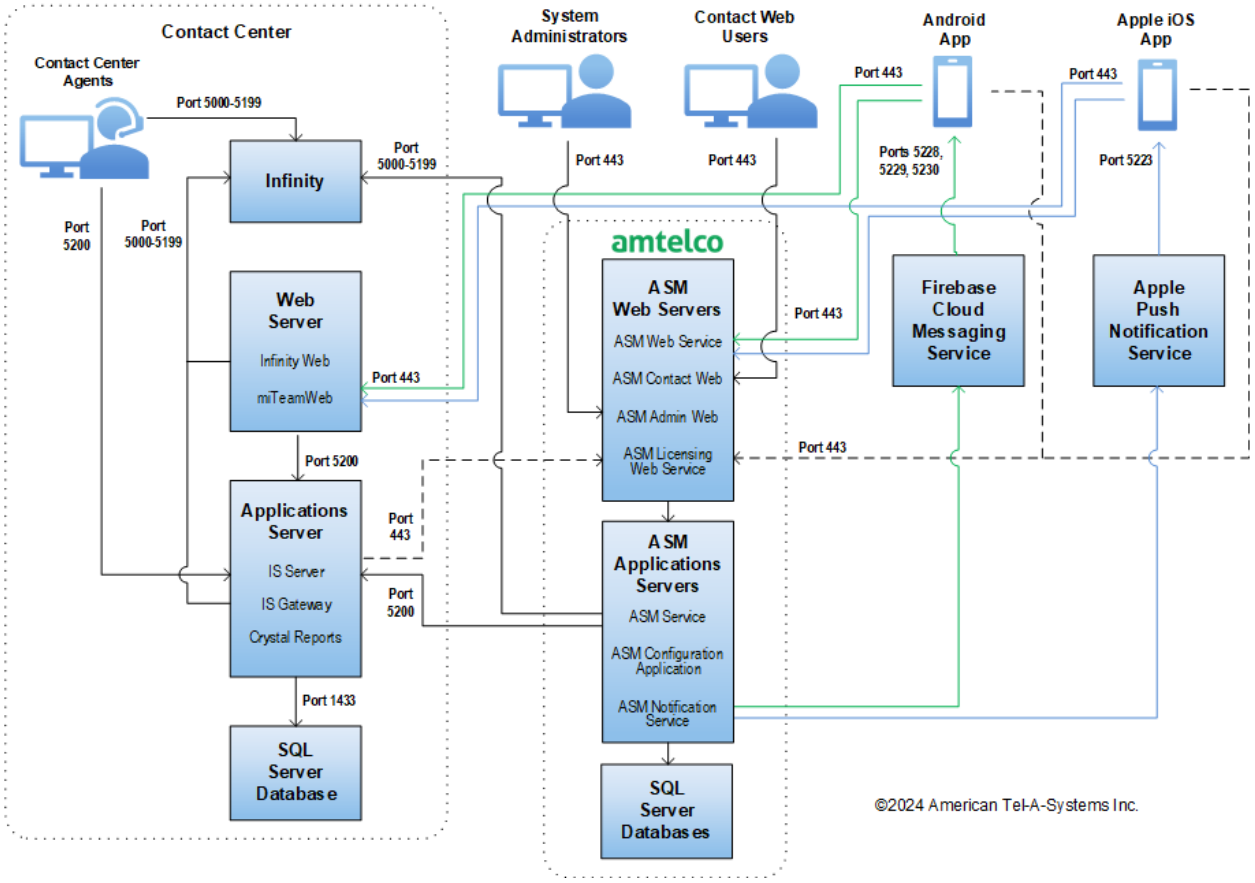


Amtelco Secure Messages cloud-based solution with IS and Genesis

- A public IP address with forwarding enabled for the IS Server port (typically 5200) must be provided. Only one open port is required.
- A public IP address with forwarding enabled for the ASM station number (5xxx) in the Infinity system configuration must be provided. Only one open port is required.

Port Requirements

- Inbound ports 5228, 5229 and 5230 must be open in the site's WiFi network to enable Android device users to receive message notifications from the Firebase Cloud Messaging service.
- Inbound port 5223 must be open in the site's WiFi network to enable Apple iOS device users to receive message notifications from the Apple Push Notification Service.
- Outbound port 443 must be open in the site's WiFi network to allow Android device users to send message notifications to the Firebase Cloud Messaging service and to allow Apple iOS device users to send message notifications to the Apple Push Notification Service.



Amtelco Secure Messages cloud-based solution with IS and Infinity

Amtelco Secure Messages System Requirements

The Amtelco Secure Messages smartphone messaging and pager replacement product is provided as a software-only solution comprised of required components and several optional components. The various components can be housed on individual servers or can be operated in a virtual environment, sharing underlying physical machine resources with other virtual machines, each running its own operating system.

If Amtelco Secure Messages is operated in a virtual environment, a unique Internet Protocol (IP) address is required for each virtual machine in the system configuration, but only one network connection is needed. If Amtelco Secure Messages is operated in a multi-server environment, one IP address and one network connection are required for each server in the system configuration.

Any firewalls in the system configuration need to be configured to provide access to the Amtelco Secure Messages services in order to process message replies.

Required Components for On-Site Solution:

- Applications server running 64-bit Microsoft Windows Server 2019 or later with Microsoft .NET Framework 4.7.2
  - ASM Service
  - ASM Configuration Application
  - ASM Notification Service
- Web server running 64-bit Microsoft Windows Server 2019 or later with Microsoft .NET Framework 4.7.2
  - Internet Information Services (IIS) 7.5 Compatibility or later
  - Secure Socket Layer/Transport Layer Security (SSL/TLS) security certificate
  - ASM Web Service
  - ASM Administration Application
- Database server running Microsoft SQL Server 2019 or later
  - Configured for memory optimized tables

User Device Requirements:

- Android OS 12 or later with a cellular data plan and a Google account
- Amtelco Secure Messages Android App 7.0 or later
- Apple iOS 15 or later with a Business Use data plan
- Amtelco Secure Messages Apple App 7.0 or later
- Apple watchOS 8.0 or later
- Apple Watch Series 3 or later

Note: The Amtelco Secure Messages Apple App is not tested on macOS or Apple Vision.

Browser Compatibility:

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

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

Optional Message Origination Components:

- Intelligent Series Server 5.3 or later
- IS Directory Contacts feature
- miTeamWeb 5.3 or later
- Intelligent Soft Agent 5.3 or later
- Web Agent 5.4 or later
- Infinity Telephone Agent 5.61 or later
- Infinity Appliance
- Infinity Web 5.61 or later

Optional Genesis Protected Dialing Components:

- Intelligent Series Server 5.5 or later
- Genesis 5.7.5 or later

Single Sign-On (SSO)

The Amtelco Secure Messages user logins and admin logins and can be configured to use a Single Sign-On Identity Provider to keep track of passwords and to perform authentication. SSO authentication requires an on-site implementation of Amtelco Secure Messages and a third-party SSO Identity Provider. Amtelco has tested Amtelco Secure Messages with the following SSO Identity Providers:

- Active Directory Federation Services (ADFS)
- Azure Active Directory (AD)

Optional Single Sign-On Components:

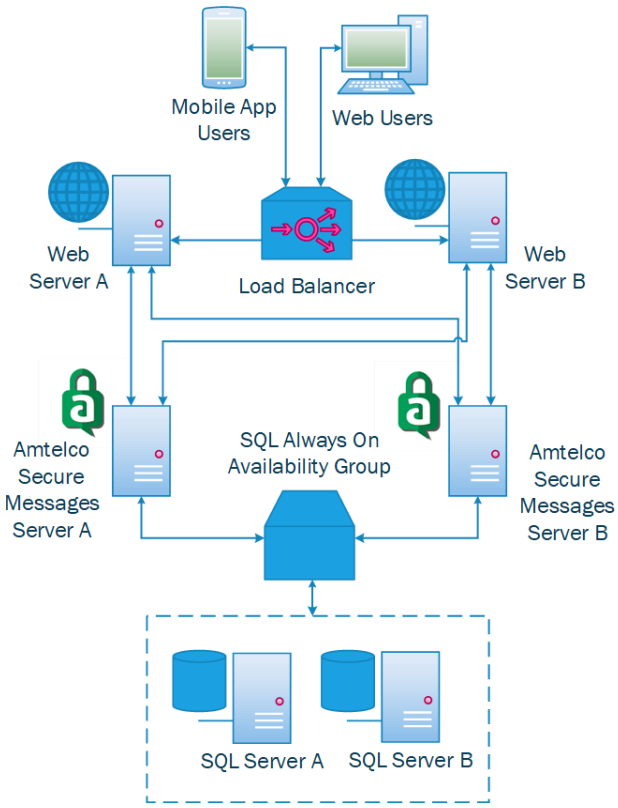
In order to use SSO authentication, the following components are required in addition to the standard components for an Amtelco Secure Messages on-site solution.

- An SSO Identity Provider who can supply the following:
    - Identity Provider certificate
    - Entity ID
    - SSO Service URL
- ASM Assertion Consumer Web
- Signed certificates*

*If your organization does not require signed certificates, Amtelco can generate self-signed certificates. It is up to your organization to maintain and renew your security certificates.

High Availability (HA)

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 a server goes down. This feature can provide continuous uptime during some server upgrades and prevents downtime due to a single server failure.



Optional High Availability (HA) Components:

In order to implement Amtelco Secure Messages with a High Availability configuration, the following components are required in addition to the standard Amtelco Secure Messages components.

- Second application server running 64-bit Microsoft Windows Server 2019 or later with Microsoft .NET Framework 4.7.2
  - ASM Service
  - ASM Configuration Application
  - ASM Notification Service
- File share location for thread archive if not using Amazon for storage
- Customer-provided High Availability solution for the Web server
  - Network Load Balancer
  - Sticky sessions enabled
- Customer-provided High Availability solution for the SQL database server
  - SQL Always On Availability Groups

Note: It is the customer's responsibility to implement a High Availability solution for the web server and SQL server, if one does not already exist.

Virtual Server Environment

The Amtelco Secure Messages solution is capable of being operated in a virtual environment, sharing underlying physical machine resources with other virtual machines, each running its own operating system. This virtualization capability encompasses the ASM Server, the SQL Database Server, and the ASM Web Server. Note that the database server and the web server can run on existing enterprise-level servers or on servers dedicated solely to the Amtelco Secure Messages platform.

Virtual Server Hardware Recommendations

Amtelco recommends that a virtual server housing the Amtelco Secure Messages solution be equipped with two 64-bit quad-core processors, 96 GB of RAM and a minimum of four 2 TB SATA or SAS hard disk drives, drives, and a minimum of one 1 GB network connection.

Integral Server Component Footprints

The following table lists the essential components of the Amtelco Secure Messages solution software along with the common installation location, the random access memory (RAM) allocation and the hard disk drive footprint of each that must be considered when configuring a virtual environment.

Note: These specifications are for a system with up to 1,000 users, separated into multiple Groups. For a system with more than 1,000 users, or all users in one Group, resource requirements will need to be discussed during your technical call.

Component	Location	Memory	Disk
ASM Administration Application	Computer in web DMZ	[1]	2.5 MB
ASM Configuration Application	Applications Server	15 MB	[2]
ASM Notification Service	Computer in web DMZ	15 MB	1 MB
ASM Web Service	Computer in web DMZ	[1]	500 KB
ASM Windows Service	Applications Server	20 MB	2 MB
SQL Server 2019 or later	Database Server	16 GB	1 TB
SQL Server Database	Database Server	[3]	10 GB

[1] Runs within the Internet Information Services (IIS) component of the Windows Server operating system and does not consume additional memory.

[2] Runs within the ASM Windows Service and does not consume additional disk space.

[3] The Microsoft SQL Server database is accessed only through the SQL engine and does not consume additional memory.

Physical Server Environment

The Amtelco Secure Messages solution also can be operated as separate physical servers, with the recommended configuration consisting of an ASM Server, a SQL Database Server, and an ASM Web Server. The physical server environment can be deployed with fault tolerance on fully redundant hardware platforms to provide service continuity and disaster recovery capabilities. A fully redundant system includes duplicate physical servers with operating system and Amtelco Secure Messages software installed on each.

Physical Server Hardware Recommendations

Amtelco recommends that dedicated physical servers housing the Amtelco Secure Messages software and the Microsoft SQL Server system database each be equipped with a minimum of one 64-bit quad-core processor, 16 GB of RAM, a 1 TB SATA or SAS hard disk drive, and a 1 GB network connection.

Note: Your site is responsible for monitoring your Central Processing Unit (CPU) usage and upgrading your memory and processor if needed. These specifications are for a system with up to 1,000 users, separated into multiple Groups. For a system with more than 1,000 users, or all users in one Group, resource requirements will need to be discussed during your technical call.

Service and Support

Amtelco provides customers operating an on-site Amtelco Secure Messages system and cloud-based solution customers with a 24-hour toll free telephone number to contact the Field Engineering Department to report and resolve any issues that may arise with the Amtelco Secure Messages solution.

Amtelco's customer support services are available around the clock to the customer. The Amtelco Secure Messages solution is backed by Amtelco's technical support staff of trained and experienced technicians providing Tier 1 and Tier 2 support and by a team of software and hardware development engineers providing Tier 2 support for service calls. Technical support is available 24 hours a day, 7 days a week, 365 days a year.

Amtelco's help desk is manned on-site from 7 a.m. to 7 p.m. (CST) with a demonstrated standard for answering calls of three telephones rings (18 seconds). Beyond standard support hours, service calls are answered by a full-service call center and dispatched immediately to an on-call Amtelco support technician equipped with a smart phone and a laptop computer who can diagnose a problem and initiate a solution from any Internet connection. Amtelco has a demonstrated track record of responding to all after-hours calls in 30 minutes or less.

Service and support are available for individual end-users of on-site and cloud-based systems. Support options and contact information are available on the Amtelco website at: https://www.amtelco.com/products/secure-messaging-app.

Documentation Change Log

Software Version	Document Section	Changes	Published Date
Apple App 7.0.3	Introduction	Updated iPhone image.	12/11/2024
Apple App 7.0.3	Amtelco Secure Messages Mobile Device Apps	Updated iPhone image.	12/11/2024
Android App 7.0.2	Introduction	Updated Android image.	12/11/2024
Android App 7.0.2	Amtelco Secure Messages Mobile Device Apps	Updated Android image.	12/11/2024
7.0.0	All	Changed “miSecureMessages” to “Amtelco Secure Messages” and changed “MSM” to “ASM.”	12/11/2024
7.0.0	All	Replaced logo and icon.	12/11/2024
7.0.0	Amtelco Secure Messages System Options	Updated system diagrams and added captions.	12/11/2024
7.0.0	User Device Requirements	Changed Android OS from 7.0 to 12. Changed Android App version from 6.8 to 7.0. Changed Apple App version from 6.8 to 7.0. Changed Apple WatchOS from 5.0 to 8.0.	12/11/2024
7.0.0	High Availability (HA)	Updated diagram.	12/11/2024
N/A	All	Changed “Administration Web” to “Admin Web.”	12/11/2024
N/A	All	Changed “AMTELCO” to “Amtelco.”	12/11/2024
N/A	All	Changed references to “partnership,” “answering service partnership,” and “partnership with a telephone answering service” to “cloud-based” or “cloud-based solution.”	12/11/2024
N/A	Introduction and back cover	Updated Amtelco logo and contact information.	12/11/2024

Software Version	Document Section	Changes	Published Date
N/A	Introduction	Added, “Unlike SMS, miSecureMessages encrypts messages, keeping your protected health information (PHI) secure. Messages are not stored on your devices, passcodes or fingerprint scans can be required, and access can be remotely disabled, making miSecureMessages HIPAA and HITECH compliant.”	12/11/2024
N/A	Amtelco Secure Messages Admin Web	Removed “This document covers all of the functions of the MSM Administration Web.”	12/11/2024
N/A	Amtelco Secure Messages Technology	Expanded description of Amtelco Secure Messages Admin Web, Amtelco Secure Messages Contact Web, Amtelco Secure Messages Android App, and Amtelco Secure Messages Apple App. Added “(optional)” to Amtelco Secure Messages Contact Web.	12/11/2024
N/A	Amtelco Secure Messages System Options	Mentioned that the ASM Configuration Application is loaded on the application server. Changed “SSL/TSL” to “SSL/TLS.” Defined DMZ and IT.	12/11/2024
N/A	Required Components for On-Site Solution	Changed “Windows Server 2016” to “Windows Server 2019” on both servers. Changed “Secure Socket Layer (SSL) security certificate” to “Secure Socket Layer/Transport Layer Security (SSL/TLS) security certificate.” Changed “SQL Server 2016” to “SQL Server 2019.”	12/11/2024
N/A	User Device Requirements	Added note “The Amtelco Secure Messages Apple App is not tested on macOS or Apple Vision.”	12/11/2024

Software Version	Document Section	Changes	Published Date
N/A	Optional Message Origination Components	Added version numbers.	12/11/2024
N/A	Optional Genesis Protected Dialing Components	Specified Genesis version 5.7.5 and later for Genesis Protected Dialing.	12/11/2024
N/A	Single Sign-On (SSO)	Changed “user logins MSM Administration Web admin logins” to “user logins and admin logins.” Added “It is up to your organization to maintain and renew your security certificates.”	12/11/2024
N/A	High Availability (HA)	Changed “Windows Server 2016” to “Windows Server 2019.”	12/11/2024
N/A	Virtual Environment	Removed numbers in parenthesis. Added note: “These specifications are for a system with up to 1,000 users, separated into multiple Groups. For a system with more than 1,000 users, or all users in one Group, resource requirements will need to be discussed during your technical call.” Changed “SQL Server 2016” to “SQL Server 2019.” Corrected numbering of footnote references in table.	12/11/2024
N/A	Physical Server Environment	Changed “one (1) 64-bit quad-core processors, 16 GB of RAM, a minimum of one (1) 1 TB SATA or SAS hard disk drives, and a minimum of one (1) 1 GB network connection” to “a minimum of one 64-bit quad core processor, 16 GB of RAM, a 1 TB SATA or SAS hard disk drive, and a 1 GB network connection.” Added “Your site is responsible for monitoring your Central Processing Unit (CPU) usage and upgrading your memory and processor if needed. These specifications are for a system with up	12/11/2024

Software Version	Document Section	Changes	Published Date
		to 1,000 users, separated into multiple Groups. For a system with more than 1,000 users, or all users in one Group, resource requirements will need to be discussed during your technical call."	
N/A	Service and Support	Replaced reference to the miSecureMessages website with reference to the Amtelco Secure Messages landing page on the Amtelco website.	12/11/2024
N/A	All	Edited references to Infinity and added references to Genesis.	8/29/2023
N/A	MSM Communication Process	Changed "Secure Socket Layer (SSL)" to "Transport Layer Security (TLS)" and changed "SSL" to "TLS."	8/29/2023
6.8	MSM Features and Functions	Added "Optionally route phone calls through AMTELCO's Genesis soft switch to protect staff's phone numbers from being visible to patients."	8/29/2023
N/A	MSM Contact Web	Changed "Secure Socket Layer (SSL)" to "Transport Layer Security (TLS)."	8/29/2023
N/A	MSM Communication Protocols	For the MSM Notification Service, changed "TLS" to "HTTPS for Android" and "HTTP/2 for Apple iOS."	8/29/2023
N/A	MSM On-Site Solution	Changed "SSL certificate" to "Secure Socket Layer/Transport Layer Security (SSL/TLS) certificate" and changed "SSL" to "SSL/TSL." Changed "must be signed" to "should be signed."	8/29/2023
N/A	MSM On-Site Solution	Added a Genesis version of the system diagram for the on-site solution.	8/29/2023
N/A	MSM Partnership Solution	Added a Genesis version of the system diagram for a TAS partnership.	8/29/2023
N/A	MSM Communication Process	Removed "on the web server" because the MSM Notification Service can be installed on the application server.	8/29/2023

Software Version	Document Section	Changes	Published Date
N/A	MSM System Requirements	Updated to indicate that an on-site installation of miSecureMessages is required for Single Sign-On (SSO)	8/25/2023

N/A = Not applicable. This change is not related to a specific version of the software.

amtelco

R&D Software Department
4800 Curtin Drive, McFarland, WI USA 53558
www.amtelco.com