Amtelco Secure Messages

On-Site System Guide

amtelco

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

Confidentiality Agreement

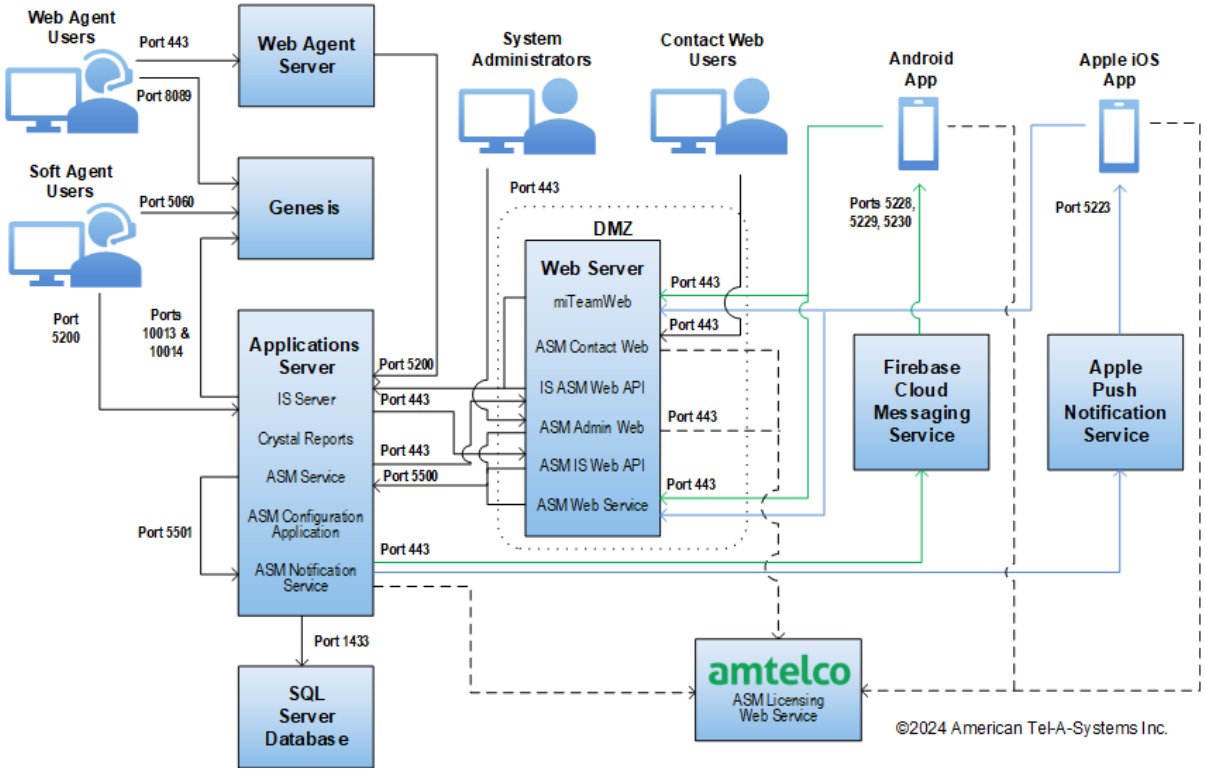
Trademarks and Copyrights

Additional Documentation

Amtelco offers a number of proprietary manuals describing the functions and features of its product lines. Further information and instructions concerning topics included in this publication can be found in several of Amtelco documents. If you do not have these documents on hand, contact Amtelco Telemarketing at 1-800-356-9148 between 8 a.m. and 5 p.m., Central Time.

Contents

Amtelco Secure Messages On-Site System Guide



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

Amtelco Secure Messages (ASM) on-site solution uses an encrypted web service to send secure messages to Android and Apple devices. Recipients are notified about incoming messages via customizable visual and audio alerts and view the messages through the Amtelco Secure Messages app. Recipients can select from a list of Quick Phrases or can enter a custom reply, which is sent securely as well. Secure messages can be initiated via a web or mobile interface.

Amtelco Secure Messages is integrated with both Amtelco's Intelligent Series (IS) software and Amtelco's Infinity automated call distribution and unified messaging system. Secure messages can be sent from one or both of these systems. Messages sent from mobile devices are processed by the ASM Web Service installed on your web server. Messages initiated from the IS Server are sent to the ASM Notification Service using two Web Application Program Interfaces (Web APIs), one connected to the ASM Service and one connected to the IS Server. Messages sent from Infinity are processed by the ASM Service installed on your applications server and passed to the ASM Notification Service.

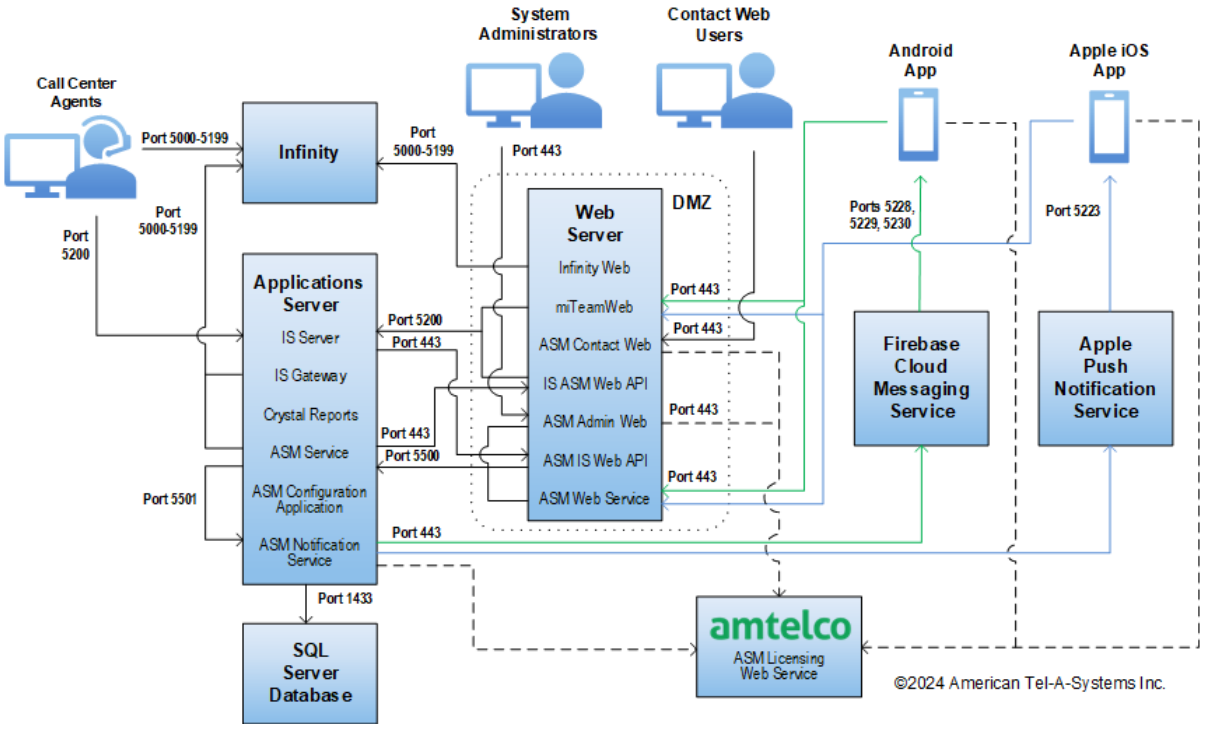
When a message is sent, the ASM Notification Service sends a notification through the Google Firebase Cloud Messaging Service or Apple Push Notification Service to the appropriate mobile device. When the message notification arrives on the mobile device, an

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 ASM recipient must acknowledge the notification and can then summon the message from the web server with the ASM 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 has the option to route phone calls placed from the Amtelco Secure Messages apps through Amtelco's Genesis soft switch to protect staff's phone numbers from being visible to patients.

Amtelco Secure Messages is available as an on-site solution and as a cloud-based solution. This document covers the setup, configuration, and operation of the on-site solution.



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

Components

SQL Server Database: The SQL Server Database is used to store information about secure messages.

ASM Service: The ASM Service receives notification of secure messages from the Infinity and IS Servers and notifies the ASM Notification Service. The ASM Service also 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 Infinity and IS Servers to the ASM Web Service for display on smartphone devices. When Amtelco Secure

Messages licenses are installed or updated, the ASM Service receives licensing information from the Amtelco Secure Messages Admin Web.

ASM Configuration Application: The Amtelco Secure Messages Server Configuration application is used to configure the ASM Service.

ASM Notification Service: The ASM Notification Service receives notification of messages from the ASM Service and notifies the Google Firebase Cloud Messaging Service for Android devices and the Apple Push Notification Service for Apple devices.

ASM Web Service: The ASM Web Service receives transmission receipts, read receipts, replies, and completion notifications from the Amtelco Secure Messages apps installed on smartphone 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 Amtelco Secure Messages app on the device that sent the read request.

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.

SSL/TLS Certificate: In the on-site solution, an SSL/TLS (Secure Socket Layer/Transport Layer Security) Certificate is required on your web server. This certificate allows the ASM Web Service to encrypt messages transmitted to mobile devices.

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 iPhone, iPad, and iPod Touch 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.

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.

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 (IS) (optional): Amtelco Secure Messages can be integrated into the Intelligent Series suite of applications. The Intelligent Series integration makes it possible to send secure messages using the Infinity Telephone Agent, Intelligent Soft Agent, miTeamWeb, and IS Web applications using the Secure Messaging Contact Method. Contact Methods are assigned to IS Directory listings in the IS Supervisor application using the IS Directory Contacts feature.

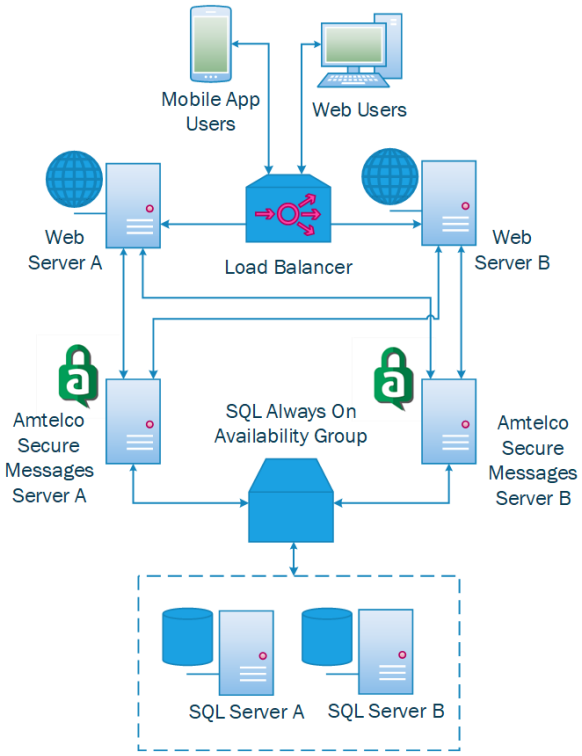
ASM IS Web API (optional): The ASM IS Web API is used to send secure messages from ASM version 7.0 and later to IS version 5.7 or later.

IS ASM Web API (optional): The IS ASM Web API is used to send secure messages from IS version 5.7 or later to ASM version 7.0 and later.

Infinity (optional): Amtelco Secure Messages can be integrated into the Infinity automated call distribution and unified messaging system using a dedicated Amtelco Secure Messages login, a route number, and two special dial-string codes. The Infinity integration makes it possible to send secure messages using the Infinity Telephone Agent and Infinity Web applications.

Additional High Availability Components

The optional High Availability (HA) 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. This feature provides continuous uptime during server upgrades and prevents downtime due to a single server failure.



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.

Dual Web Servers: Two web servers are required to provide high-availability access to Amtelco Secure Messages data from the Amtelco Secure Messages apps and web applications.

Network Load Balancer: A network load balancer with sticky sessions is required to manage access to the dual web servers.

Dual Amtelco Secure Messages Servers: Two application servers are required to provide high-availability access to the ASM Service, the ASM Configuration Application, and the ASM Notification Service.

File Share Archive Location or Amazon Storage: A file share location or Amazon for storage can be used to provide access to archived message threads.

Dual SQL Servers: Two SQL Server are required to provide high-availability access to the SQL Server database.

SQL Always On Availability Groups: SQL Always On Availability Groups are used to maintain duplicate data on the two SQL Servers.

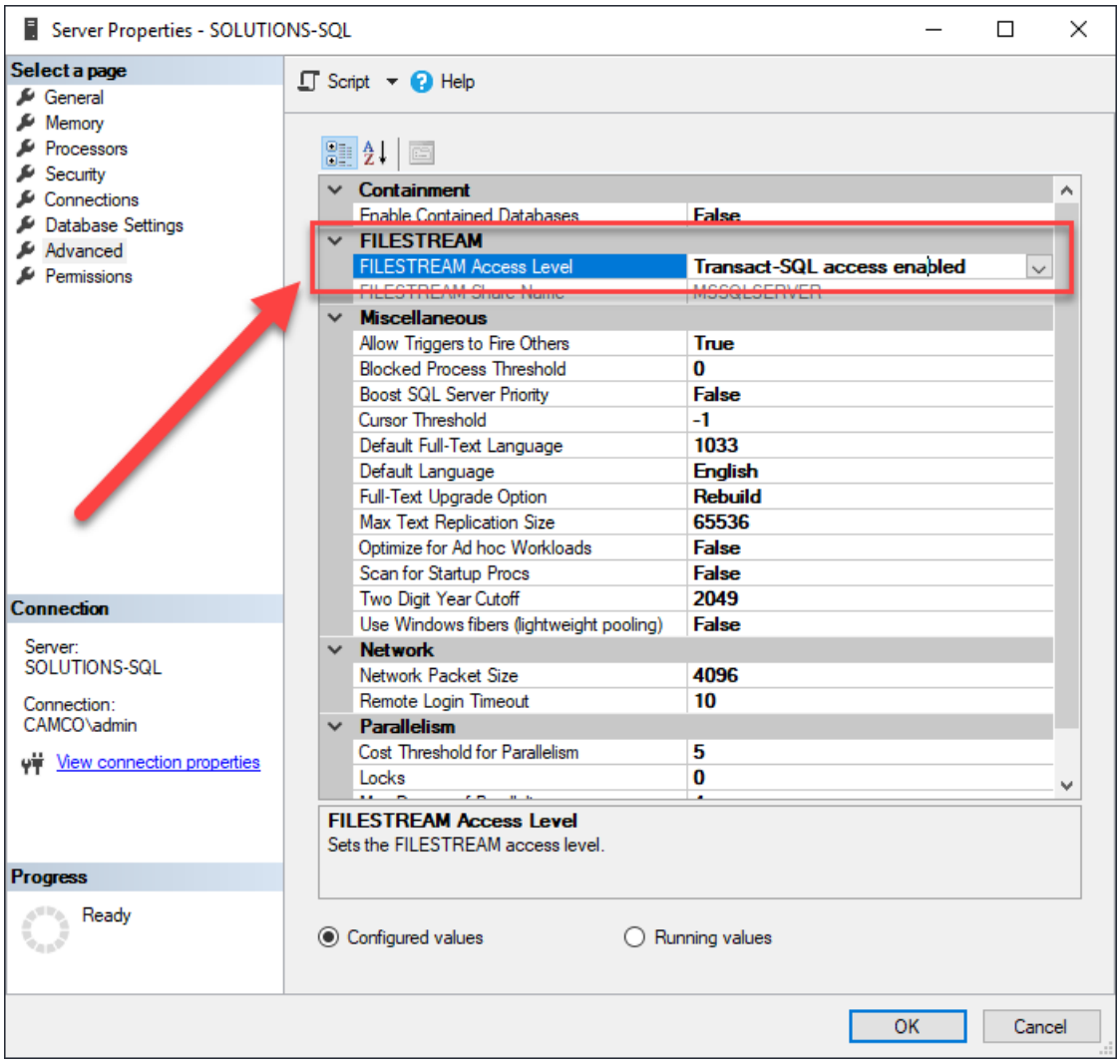
Creating and Configuring the ASM SQL Database

The SQL Server Database is used to store information about secure messages. An ASM database must be created on your SQL Server.

Note: If you are implementing the optional High Availability feature, you will need to configure SQL Always On Availability Groups to replicate the database on a second SQL Server.

To create an ASM SQL database, open the SQL Server Management Studio application on your SQL Server.

The Microsoft SQL Server Management Studio window is displayed.



In the Server Properties, set the FILESTREAM Access Level to "Transact-SQL access enabled" or higher.

Click the OK button to save your changes.

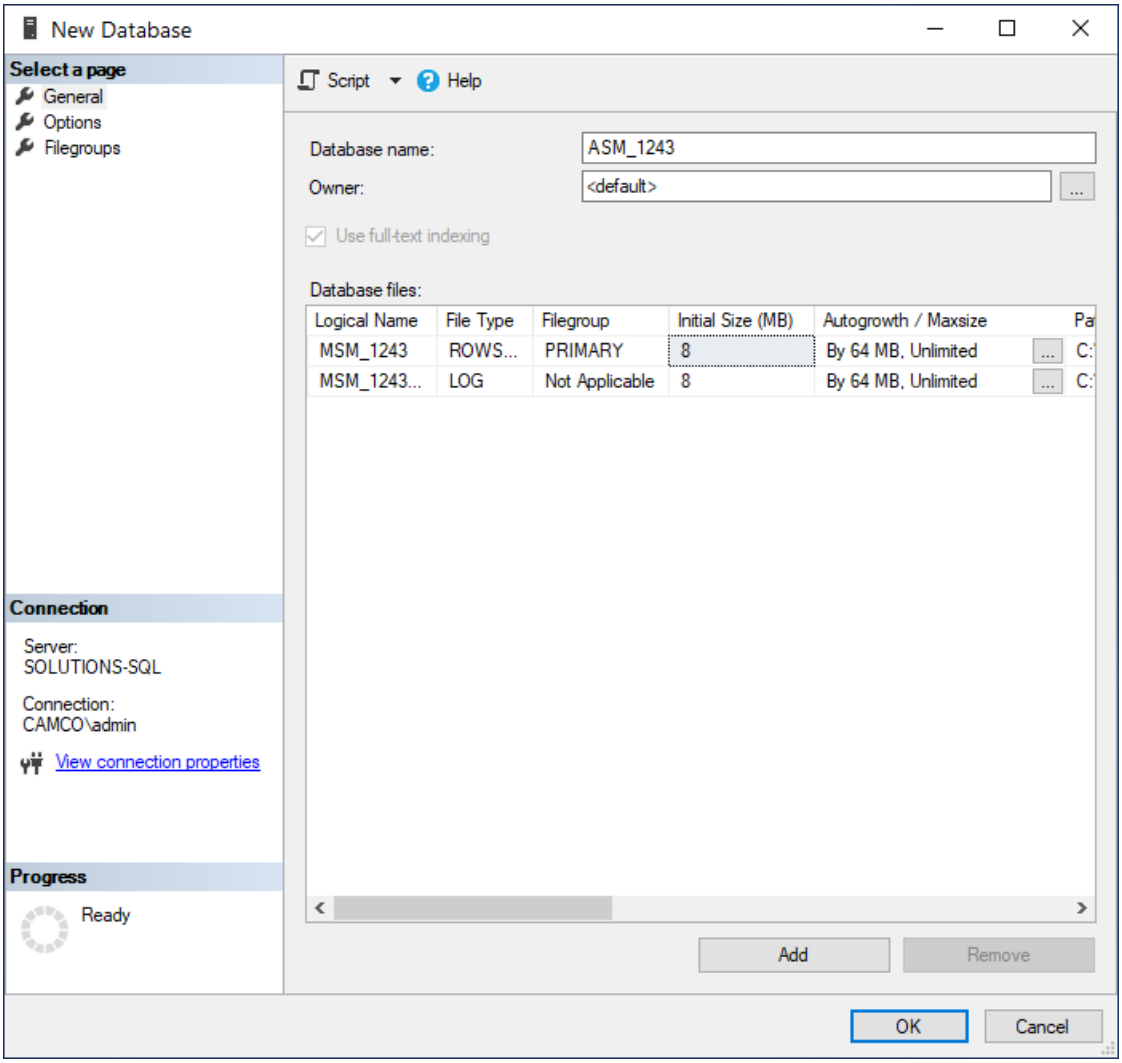
Note: Changing the FILESTEAM Access Level requires a SQL Service restart in order for the change to take effect.

After the SQL Service has been restarted, navigate to the Object Explorer pane and connect to an instance of the SQL Server Database Engine.

Click the Expand icon ⊞ next to the Databases folder to expand it.

Right-click the Databases folder and select "New Database."

The New Database window is displayed.



Enter the Database Name using the following naming convention:

ASM_*CustomerID*

Replace *CustomerID* with your Amtelco Secure Messages customer ID provided by Amtelco.

Make any other properties changes if necessary.

Click the OK button to create the database.

The new database is displayed under the Databases folder.

Installing and Configuring the ASM Service

The Amtelco Secure Messages (ASM) Service receives notification of secure messages from the Infinity and IS Servers 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 Infinity and IS Servers to the ASM Web Service for display on smartphone devices.

When Amtelco Secure Messages licenses are installed or updated, the ASM Service receives licensing information from the Amtelco Secure Messages Admin Web.

Installing the ASM Service

The ASM Service must be installed on an applications server. If Infinity will be used to send secure messages, the Infinity Server must have network access to the applications server that hosts the ASM Service. If IS will be used to send secure messages, the IS Server must have network access to the applications server that hosts the ASM Service. The applications server can be the same server as the IS Server.

Note: If you are implementing the optional High Availability feature, you will need to install the ASM Service on two application servers.

To install the ASM Service, run the Setup.msi file on the applications server.

The Setup.msi file installs the ASM Service and the ASM Server Configuration application. The ASM Server Configuration application is used to configure the ASM Service.

Configuring the ASM Service

The ASM Server Configuration application is located within the Amtelco program folder in a subfolder labeled “miSecureMessages.”

To configure the ASM Service, navigate to the Amtelco program folder, open the miSecureMessages subfolder, and double click “Configuration.”

The MSM Admin window is displayed.

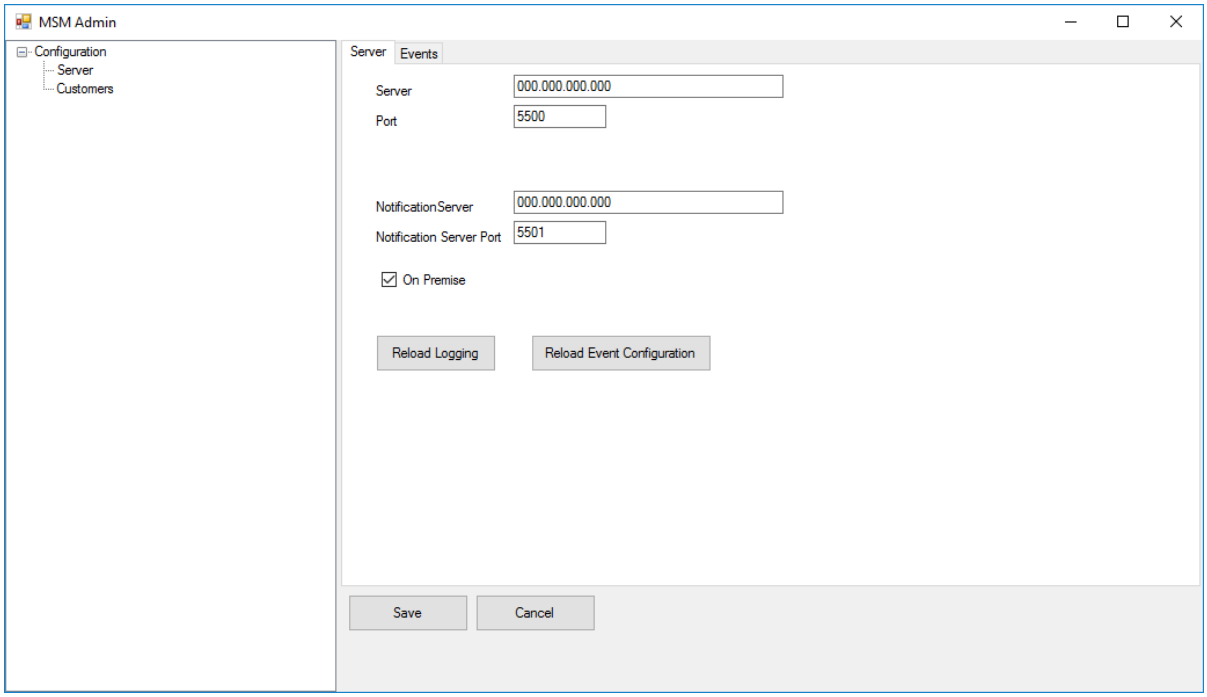
The MSM Admin window is divided into a navigation tree on the left and a properties pane on the right. The Configuration node is displayed in the navigation tree.

Click the Expand icon ⊞ next to the Configuration node to expand it.

The Server and Customers nodes are displayed.

Click the Server node to display the Server Properties.

Server



The Server Properties are used to configure the ASM Service to communicate with the ASM Web Service, the Amtelco Secure Messages Admin Web, and the ASM Notification Service. The Server page also includes buttons for reloading the logging configuration and for reloading the system-wide event configuration.

Server

The Server setting is used to specify the name or IP address of the server where the ASM Service is installed.

Type the server name or IP address of the applications server on which the ASM Service is installed.

Port

The Port is used to specify an unused port on the applications server that the ASM Web Service and the Amtelco Secure Messages Admin Web can use to talk to the ASM Service.

Type the port number of an unused port on the applications server.

The default value is 5500.

Notification Server

The Notification Server setting is used to specify the name or IP address of the web server where the ASM Notification Service is installed.

Type the server name or IP address of the web server on which the ASM Notification Service is installed.

Notification Server Port

The Port is used to specify an unused port on the applications server that the ASM Web Service and the Amtelco Secure Messages Admin Web can use to talk to the ASM Notification Service. This port must be a different port than the port used by the ASM Service.

Type the port number that the ASM Web Service and the ASM Administration application can use to talk to the ASM Notification Service.

The same port must be specified in the appSettings section of the Amtelco.SecureMessaging.NotificationServer.Service.exe.config file. The default value is 5501.

☑ On Premise

The On Premise check box is used to configure the system for an on-site installation versus a hosted solution.

Select the On Premise check box to configure this system as an on-site installation.

Reload Logging

The Reload Logging button is provided for troubleshooting purposes. The Reload Logging button is used to reload the logging configuration without restarting the ASM Service.

Reload Event Configuration

The Reload Event Configuration button is used to reload the Events Properties configured for hosted Amtelco Secure Messages systems. The Reload Event Configuration button is not needed for on-site installations.

Save

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

OR

Click the Cancel button to discard your changes.

Events

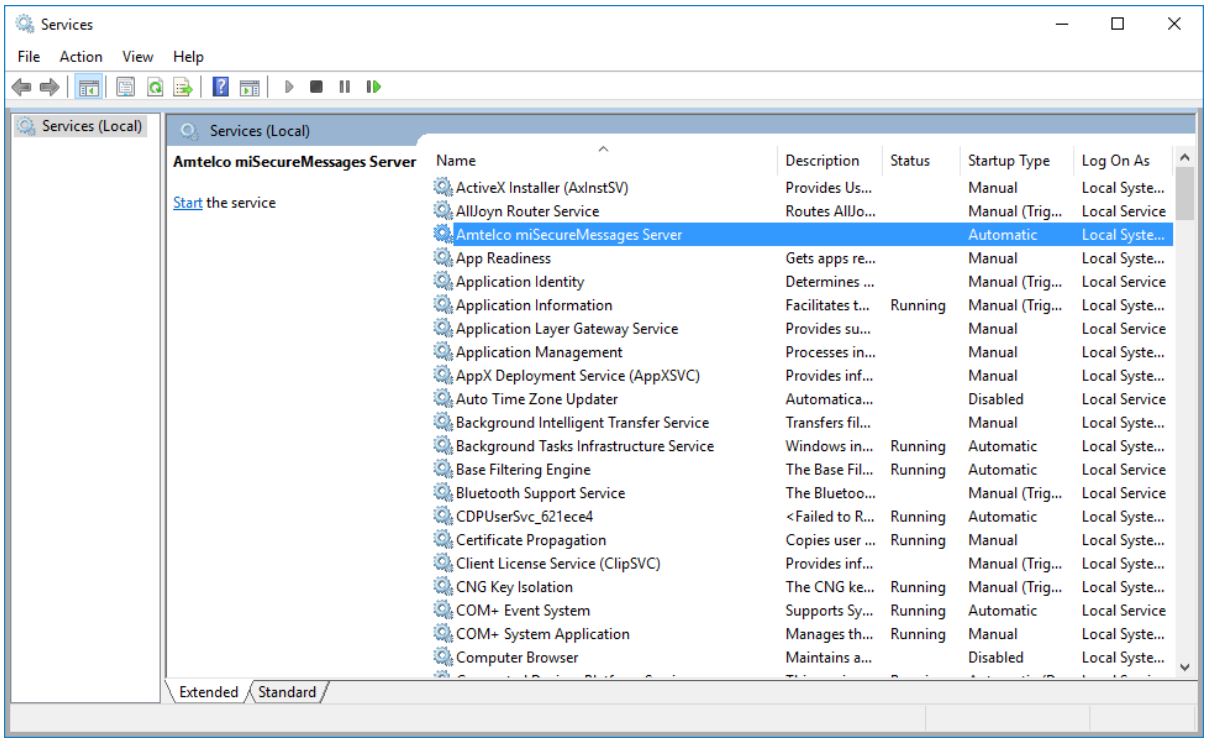
The Events tab is only used with hosted Amtelco Secure Messages systems. No changes need to be made for on-site installations.

Starting the ASM Service

After the ASM Service is configured, the ASM Service must be started in order to configure customer data.

To start the ASM Service, open the Windows Services application on the applications server.

The Services window is displayed.



Click "Services (Local)" if it is not already selected.

The names, descriptions, and statuses of the local services are displayed along with other information.

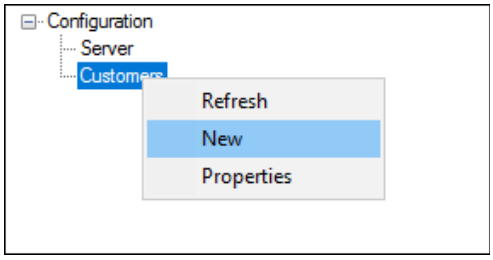
In the Name column, select "Amtelco miSecureMessages Server."

Click the Start hyperlink.

The status in the Status column changes to "Running."

Configuring Customer Data

Once the ASM Service has been started, customer data can be configured in the MSM Server Configuration application.

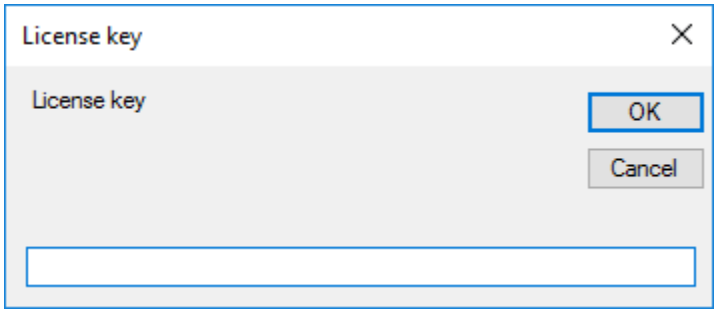


To add a customer ID, right-click the Customers node in the MSM Admin window.

A menu is displayed.

Select "New."

The License Key window is displayed.



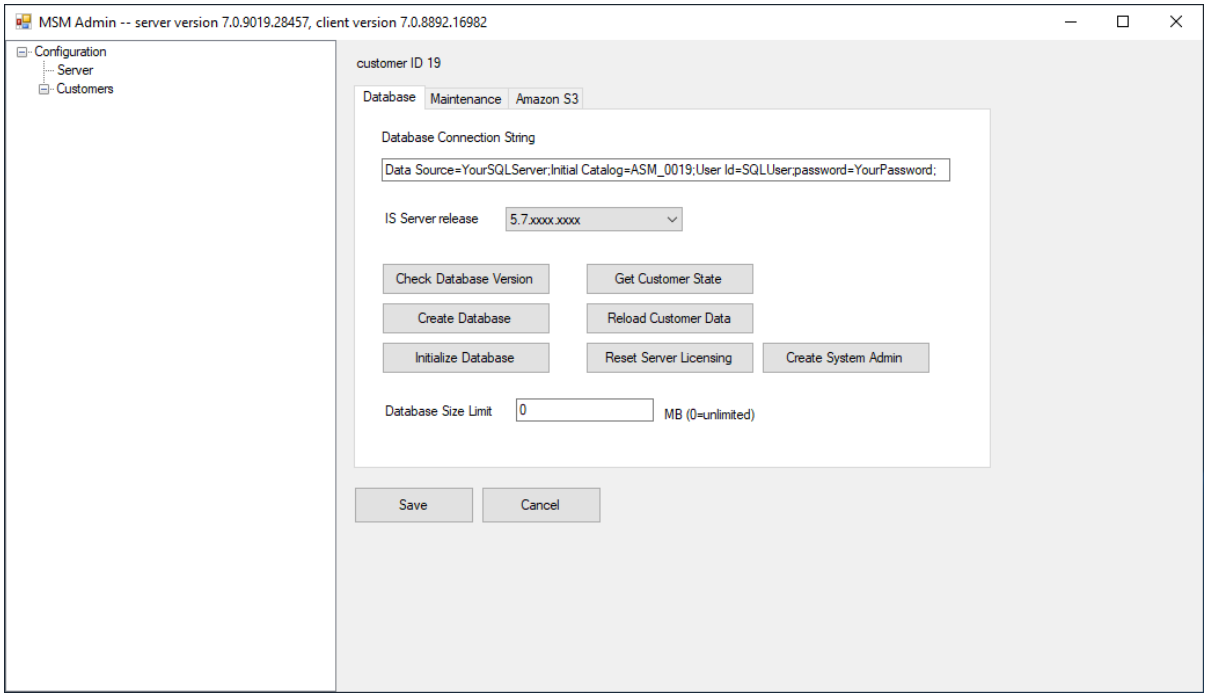
License Key

Enter your Amtelco Secure Messages license key provided by Amtelco.

Click the OK button.

The Database Properties for the new customer ID are displayed.

Database



The Database Properties are used to configure a customer ID to connect to the SQL database.

Database Connection String

The Database Connection String is used to communicate with the Secure Messaging SQL database.

Note: The Secure Messaging database must already exist on the SQL Server. Instructions for creating the Secure Messaging database are provided in this document under the topic "Creating a Secure Messaging SQL Database."

Enter the connection string required to communicate with the Secure Messaging SQL database.

The connection string syntax varies. Two simple examples are provided here. Contact your Information Technology department to determine the appropriate connection string for your system.

Example of a connection string using Windows Security to connect to the database:

Data Source=*server*;Initial Catalog= ASM_*CustomerID*;Integrated Security=SSPI;

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

Replace *CustomerID* with your Amtelco Secure Messages customer ID provided by Amtelco.

Example of a connection string using SQL Security to connect to the database:

Data Source=*server*;Initial Catalog= ASM_*CustomerID*;User Id=*user*;Password=*password*;

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

Replace *CustomerID* with your Amtelco Secure Messages customer ID provided by Amtelco.

Replace *user* with a user ID that has access to the SQL Server.

Replace *password* with the password that is associated with the user ID.

IS Server Release

The IS Server Release setting configures the ASM Service to use the correct the Application Programming Interface (API) required to communicate with your IS Server version.

To find your IS Server version:

1. Log into the IS Supervisor application.
2. Click the version number displayed on the menu bar. The IS Supervisor version and IS Server version are displayed in the Version Information dialog box.
3. Click the OK button to close the dialog box.

Select the version of IS Server software that is installed on your system.

OR

If you do not have an IS Server, select "No IS connection."

Database Size Limit

The Database Size Limit property determines the maximum size, in megabytes (MB), the Secure Messaging database is allowed to reach. This setting is generally used for hosted Amtelco Secure Messages systems.

To limit the database size, enter the maximum number of megabytes of space the database should be allowed to use.

OR

To allow an unlimited database size, enter zero (0).

Save

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

OR

Click the Cancel button to discard your changes.

Note: Your customer configuration settings will not take effect until after the customer is started. If the customer was already started, your customer configuration settings will not take effect until the customer data is reloaded. Instructions for performing these actions are provided in this document under the topics "Starting the Customer" and "Reloading Customer Data."

Check Database Version

The Check Database Version button is provided for troubleshooting purposes.

To check the database version, click the Check Database Version button.

The database version, the expected version, and information about the database server are displayed in a dialog box.

Click the OK button to return to the Database Properties.

Create Database

The Create Database button is provided as an alternate way to create and initialize a database. If you already have created a Secure Messaging database on your SQL Server, you do not need to use the Create Database button.

Initialize Database

After configuring and saving the Database Properties for the first time, the SecureMessaging database must be initialized.

If the Database Properties are being configured for the first time, click the Initialize Database button.

If the database was initialized successfully, the message "Database successfully initialized" is displayed.

Click the OK button to return to the Database Properties.

Get Customer State

The Get Customer State button is provided for troubleshooting purposes.

To retrieve and display the current customer state, click the Get Customer State button.

The customer state is displayed in a dialog box.

Click the OK button to return to the Database Properties.

Upgrade from 6.3

The "Upgrade from 6.3" button is used to upgrade registry settings from the format used in miSecureMessages version 6.3 to the format used in miSecureMessages version 6.4 and later.

If you are upgrading from miSecureMessages version 6.3 to miSecureMessages version 6.4 or later, click the "Upgrade from 6.3" button to upgrade your registry settings.

Reload Customer Data

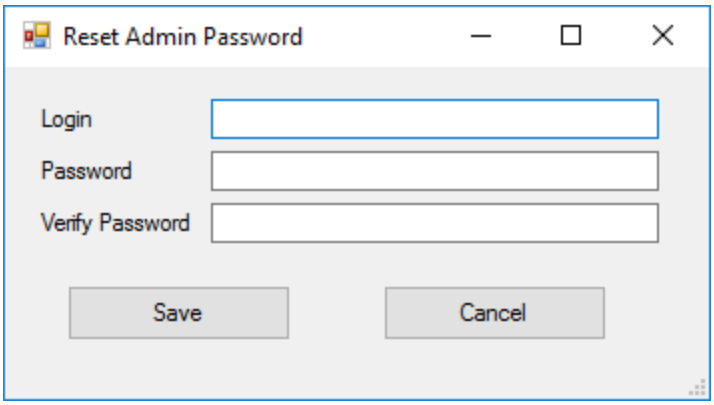
The Reload Customer Data button is used to reload the customer configuration. The customer data must be reloaded if any changes are made to the IS Server Release, the Database Size Limit, the Maintenance Properties, and the Amazon S3 Properties after the customer has been started.

Create System Admin

The Create System Admin button is provided as a method of creating a new ASM System Admin username and password in the event that all of the existing System Admin users are locked out.

To create a new ASM System Admin username and password, click the Create System Admin button.

The Reset Admin Password window is displayed.



Login
Type a new username in the Login field.

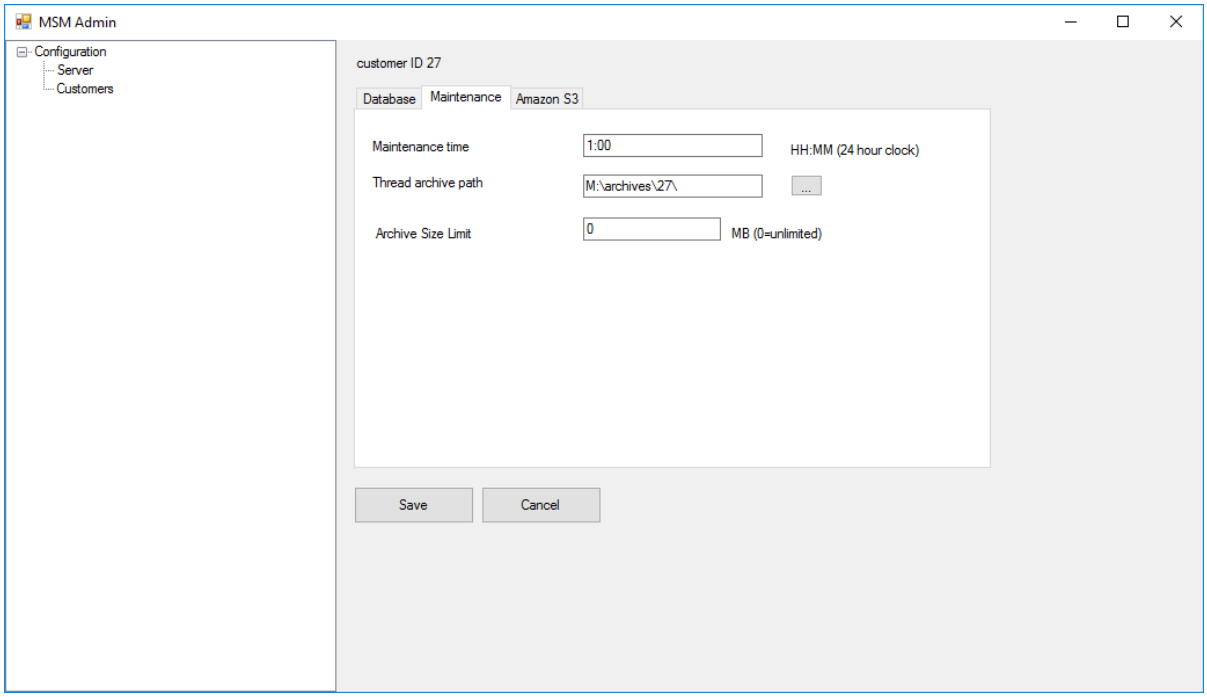
Password
Type a password in the Password field.

Verify Password
Re-type the password in the Verify Password field.

Save
Click the Save button.

A new login with the username and password specified is created and is granted System Admin access to the Amtelco Secure Messages Admin Web.

Maintenance



The Maintenance Properties are used to configure the archive settings for the ASM database.

This option requires the purchase of the Archive feature.

To configure the archive settings for the ASM database, click the Maintenance tab.

The Maintenance Properties are displayed.

Maintenance Time

The Maintenance Time setting determines the time that the archive task is performed each day.

Specify the time to begin archiving Amtelco Secure Messages data each day.

The time must be specified using 24-hour notation in the following format.

HH:*MM*

Replace *HH* with the two-digit number of hours past midnight, in the range of 00 to 23.

Replace *MM* with the two-digit number of minutes past the hour, in the range of 00 to 59.

Thread Archive Path

The Thread Archive Path determines where Amtelco Secure Messages archive files are stored when using the Local Storage Archive Mode.

To configure the archive path, click the Browse button. 

The Browse for Folder window is displayed.

Browse to the location where you want to store the archive files.

The account that runs the ASM Service must have permission to read and write to the selected archive location. If you are using the optional High Availability configuration, the thread archive path on both Amtelco Secure Messages servers should be set up to Amazon or to a file share. If this is not done, archives could end up being split between the servers, making it harder to find archived messages.

Note: Archive files should be stored in a secure location that is protected by appropriate access restrictions to prevent unauthorized access to message content and attachments.

Click the OK button.

The path to the selected location is displayed in the Thread Archive Path field.

Archive Size Limit

The Archive Size Limit is the maximum total allowed size for all Amtelco Secure Messages archive files, in megabytes (MB).

- **To limit the amount of disk space that can be consumed by Amtelco Secure Messages archive files, enter the maximum total number of megabytes of space that all archive files are allowed to use.**
- **To allow unlimited archive file storage, enter zero (0).**

Save

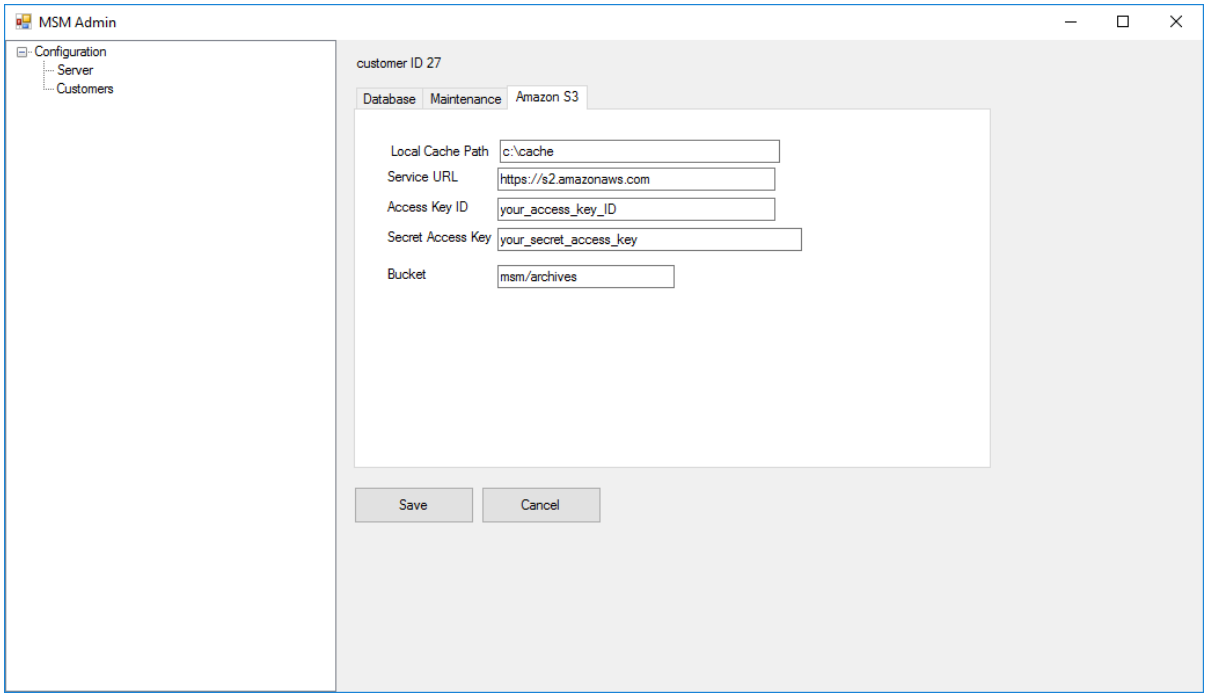
When you have finished making changes to the Maintenance Properties, click the Save button to save your changes.

OR

Click the Cancel button to discard your changes.

Note: Your customer configuration settings will not take effect until after the customer is started. If the customer was already started, your customer configuration settings will not take effect until the customer data is reloaded. Instructions for performing these actions are provided in this document under the topics “Starting the Customer” and “Reloading Customer Data.”

Amazon S3



The Amazon S3 Properties are used to configure the ASM Service to archive Amtelco Secure Messages data to the Amazon Simple Storage Service (S3).

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

To configure the ASM Service to use the Amazon Simple Storage Service, click the Amazon S3 tab.

The Amazon S3 Properties are displayed.

Local Cache Path

The Local Cache Path indicates a location to cache data on your applications server while it is being downloaded from Amazon S3.

Specify the path to the location where you want to cache data on your local server.

Service URL

The Service URL is the pre-signed URL provided by Amazon for uploading objects to Amazon S3.

Enter the Service URL provided by Amazon.

Access Key ID

Amazon S3 uses the access key ID to look up your secret access key.

Enter the Amazon S3 user access key ID provided by Amazon.

Secret Access Key

The secret access key specified in the Secret Access Key field must match the secret access key on file at Amazon S3.

Enter the Amazon S3 user secret access key provided by Amazon.

Bucket

The Bucket setting is used to specify which Amazon S3 bucket to use to store Amtelco Secure Messages archives.

Specify the Amazon S3 bucket that you want to use to store the Amtelco Secure Messages archives.

Save

When you have finished making changes to the Amazon S3 Properties, click the Save button to save your changes.

OR

Click the Cancel button to discard your changes.

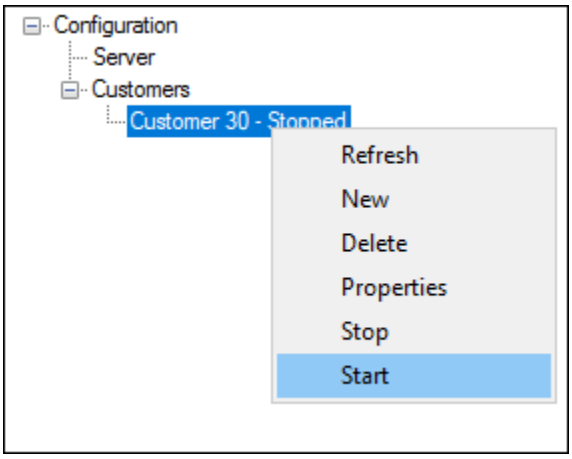
Note: Your customer configuration settings will not take effect until after the customer is started. If the customer was already started, your customer configuration settings will not take effect until the customer data is reloaded. Instructions for performing these actions are provided in this document under the topics “Starting the Customer” and “Reloading Customer Data.”

Starting the Customer

Once the customer database settings have been configured and saved, the customer must be started in order for the customer ID to be used.

To start the customer, right click the customer ID beneath the Customers node.

A menu is displayed.



Click Start.

The word “Started” is displayed to the right of the Customer ID.

Reloading Customer Data

If you make additional changes to the customer configuration after the customer has been started, you must reload the customer data in order for those changes to take effect.

The Reload Customer Data button on the Database page is used to reload the customer configuration.

If you make additional changes to the customer configuration after the customer has been started, click the Reload Customer Data button on the Database page to reload the customer configuration.

Installing and Configuring the ASM Notification Service

The Amtelco Secure Messages (ASM) Notification Service receives notification of messages from the ASM Service and notifies the Google Firebase Cloud Messaging Service for Android devices and the Apple Push Notification Service for Apple devices.

Installing the ASM Notification Service

The ASM Notification Service requires access to the Internet so that it has access to the Apple Push Notification Service and the Google Firebase Cloud Messaging Service.

Note: If you are implementing the optional High Availability feature, you will need to install the ASM Notification Service on two servers, preferably the two application servers.

To install the ASM Notification Service, run the NotificationServerSetup.msi file on a server that has access to the Internet.

The NotificationServerSetup.msi file installs the ASM Notification Service.

Configuring the ASM Notification Service

After the ASM Notification Service has been installed, the app settings must be configured in the Amtelco.SecureMessaging.NotificationServer.Service.exe.config file. The default location of the file is:

Program Files\miSecureMessages Notification Server\
Amtelco.SecureMessaging.NotificationServer.Service.exe.config

App Settings

The ASM Notification Service uses app settings to connect to the server where the ASM Service is installed.

```
<appSettings>
  <!-- Configuration Settings -->
  <add key="Server" value="123.456.7.890"/>
  <add key="Port" value="5501"/>
</appSettings>
```

Edit the following lines in the appSettings section of the Amtelco.SecureMessaging.NotificationServer.Service.exe.config file.

```
<add key="Server" value="Server"/>
```

```
<add key="Port" value="Port"/>
```

Replace *Server* with the server name or IP address of the applications server where the ASM Service is located.

Replace *Port* with the Notification Server Port specified in the ASM Service Configuration. The default value is 5501.

If you are connecting to more than one ASM Service, use the following format instead:

```
<add key="Server" value="ServerA:PortA, ServerB:PortB"/>
```

Replace *ServerA* with the server name or IP address of the applications server where the first ASM Service is located.

Replace *PortA* with the Notification Server Port specified in the first ASM Service Configuration. The default value is 5501.

Replace *ServerB* with the server name or IP address of the applications server where the second ASM Service is located.

Replace *PortB* with the Notification Server Port specified in the second ASM Service Configuration. The default value is 5501.

Starting the ASM Notification Service

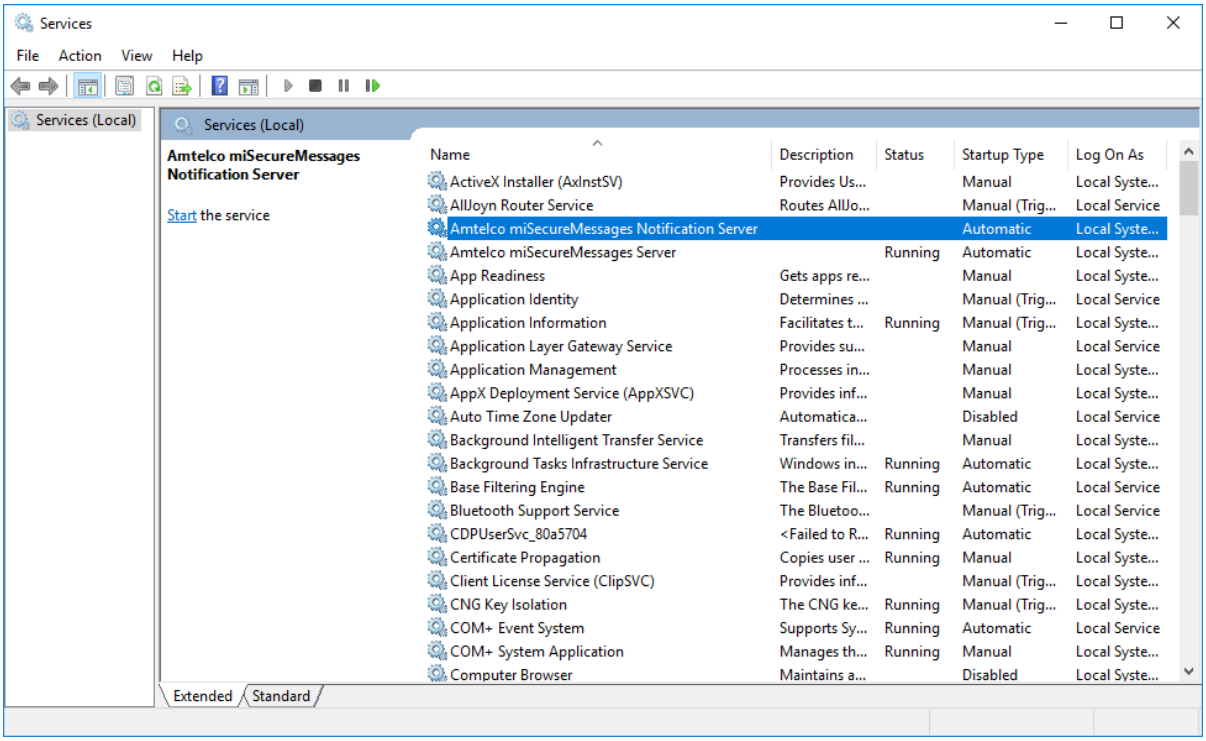
To start the ASM Notification Service, open the Windows Services application on the applications server.

The Services window is displayed.

Click "Services (Local)" if it is not already selected.

The names, descriptions, and statuses of the local services are displayed along with other information.

In the Name column, select "Amtelco miSecureMessages Notification Server."



Click the Start hyperlink.

The status in the Status column changes to "Running."

Installing and Configuring the ASM Web Service

The Amtelco Secure Messages (ASM) Web Service receives transmission receipts, read receipts, replies, and completion notifications from the Amtelco Secure Messages app installed on smartphone 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 Amtelco Secure Messages app on the device that sent the read request.

Installing the ASM Web Service

The ASM Web Service must be installed on a on a public web server so that it can be accessed from the Amtelco Secure Messages app on smartphone devices.

Note: If you are implementing the optional High Availability feature, you will need to install the ASM Web Service on two public web servers managed by a Network Load Balancer with sticky sessions enabled.

To install the ASM Web Service, run the MsmWebSetup.msi file on a public web server.

The MsmWebSetup.msi file installs the ASM Web Service.

The default location that the application installs to is inetpub\wwwroot\msmWebSetup, but the location of the folder can be changed during the installation.

Configuring the ASM Web Service

After the ASM Web Service has been installed, the app settings must be configured in the Web.config file. The default location of the file is:

inetpub\wwwroot\msmWebSetup\Web.config

App Settings

The ASM Web Service uses app settings to connect to the server where the ASM Service is installed.

```
<appSettings>
  <!-- Configuration Settings -->
  <add key="Server" value="123.456.7.890:5500"/>
</appSettings>
```

Edit the following line in the appSettings section of the Web.config file.

```
<add key="Server" value="Server:Port"/>
```

Replace *Server* with the server name or IP address of the applications server where the ASM Service is located.

Replace *port* with the port that was selected in the ASM Service Configuration. The default value is 5500.

If there is a Port key in the web.config file, it should be deleted.

Remove this line of code:

```
<add key="Port" value="Port"/>
```

If you are implementing the optional High Availability feature, you will need to add a second Amtelco Secure Messages Server to the configuration.

If you are using the optional High Availability feature, add a comma and the second server to the Server key as shown in the following example:

```
<add key="Server" value="ServerA:PortA,ServerB:PortB"/>
```

Replace *ServerA* with the server name or IP address of the first Amtelco Secure Messages server.

Replace *PortA* with the port specified in the first server's ASM Service configuration.

Replace *ServerB* with the server name or IP address of the second Amtelco Secure Messages server.

Replace *PortB* with the port specified in the second server's ASM Service configuration.

Installing and Configuring the 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 configure system settings, monitor licenses, configure connections, edit the list of Quick Phrases available to users, manage contacts, view device information, set up groups, set up Contact Circles, and run reports.

Installing the ASM Admin Web

The ASM Web must be installed on a web server. The web server must be configured to allow access to external Hypertext Transfer Protocol Secure (HTTPS) sites. When the service is first started and when new licenses are purchased, the Amtelco Secure Messages Admin Web connects to the Amtelco License Manager at Amtelco to verify the Amtelco Secure Messages licenses that have been purchased. Once the licenses have been verified, the service does not need to connect to the Amtelco License Manager until licenses are renewed or additional licenses are purchased.

To install the ASM Admin Web, run the AdminWebSetup.msi file on the web server.

The AdminWebSetup.msi file installs the Amtelco Secure Messages Admin Web.

The default location that the application installs to is inetpub\wwwroot\msmAdmin, but the location of the folder can be changed during the installation.

Configuring the ASM Admin Web

After the ASM Admin Web has been installed, the app settings must be configured in the Web.config file. The default location of the file is:

inetpub\wwwroot\msmAdmin\Web.config

App Settings

The ASM Admin Web uses app settings to connect to the server where the ASM Service is installed.

```
<appSettings>
  <!-- Configuration Settings -->
  <add key="server" value="123.456.7.890:5500"/>
  <add key="customer" value="CustomerID"/>
</appSettings>
```

Edit the following lines in the appSettings section of the Web.config file:

```
<add key="Server" value="Server:Port" />
<add key="customer" value="CustomerID">
```

Replace *Server* with the server name or IP address of the applications server where the ASM Service is located.

Replace *Port* with the port that was selected in the ASM Service Configuration. The default value is 5500.

Replace *CustomerID* with your unique customer ID provided by Amtelco.

If there is a channel key in the web.config file, it should be deleted.

Remove this line of code:

```
<add key="channel" value="Channel" />
```

If you are implementing the optional High Availability feature, you will need to add a second Amtelco Secure Messages Server to the configuration.

If you are using the optional High Availability feature, add a comma and the second server to the Server key as shown in the following example:

```
<add key="Server" value="ServerA:PortA, ServerB:PortB" />
```

Replace *ServerA* with the server name or IP address of the first Amtelco Secure Messages server.

Replace *PortA* with the port specified in the first server's ASM Service configuration.

Replace *ServerB* with the server name or IP address of the second Amtelco Secure Messages server.

Replace *PortB* with the port specified in the second server's ASM Service configuration.

System Username and Password

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

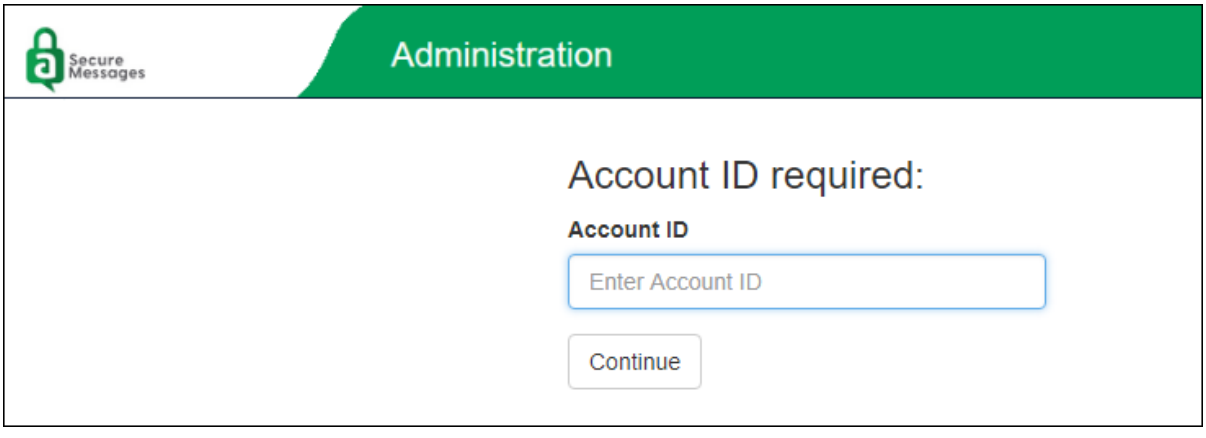
The ASM Admin Web can be accessed through a web browser.

Enter the following path into the address field of your web browser:

WebServerAddress/msmadmin/Main.aspx

Replace *WebServerAddress* with the web address of your web server where the msmadmin folder was installed.

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



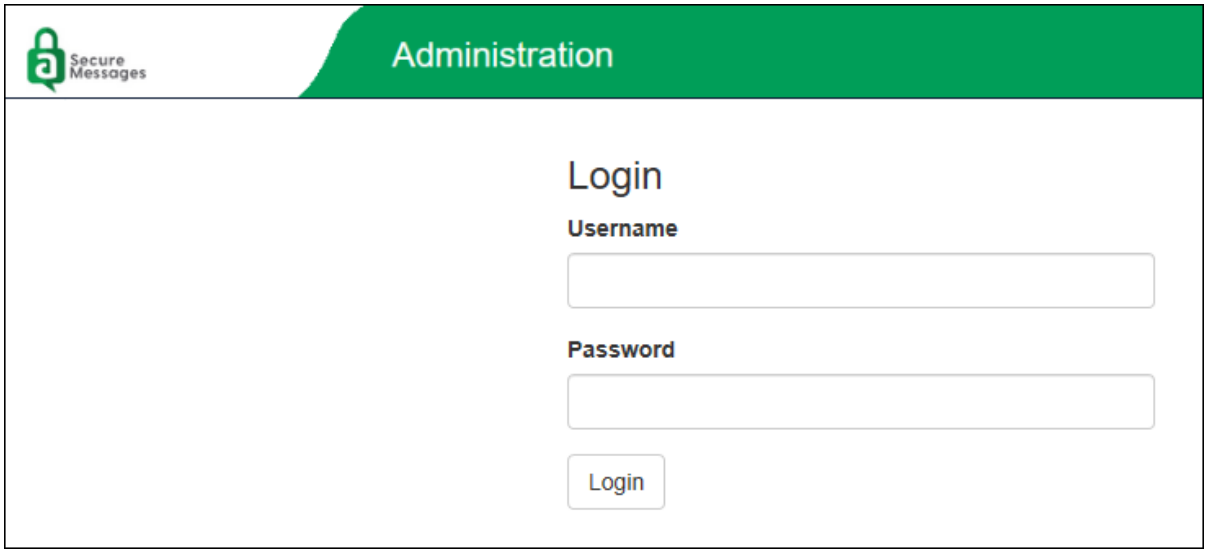
Account ID

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 ASM Admin Web Login screen is displayed.



Username

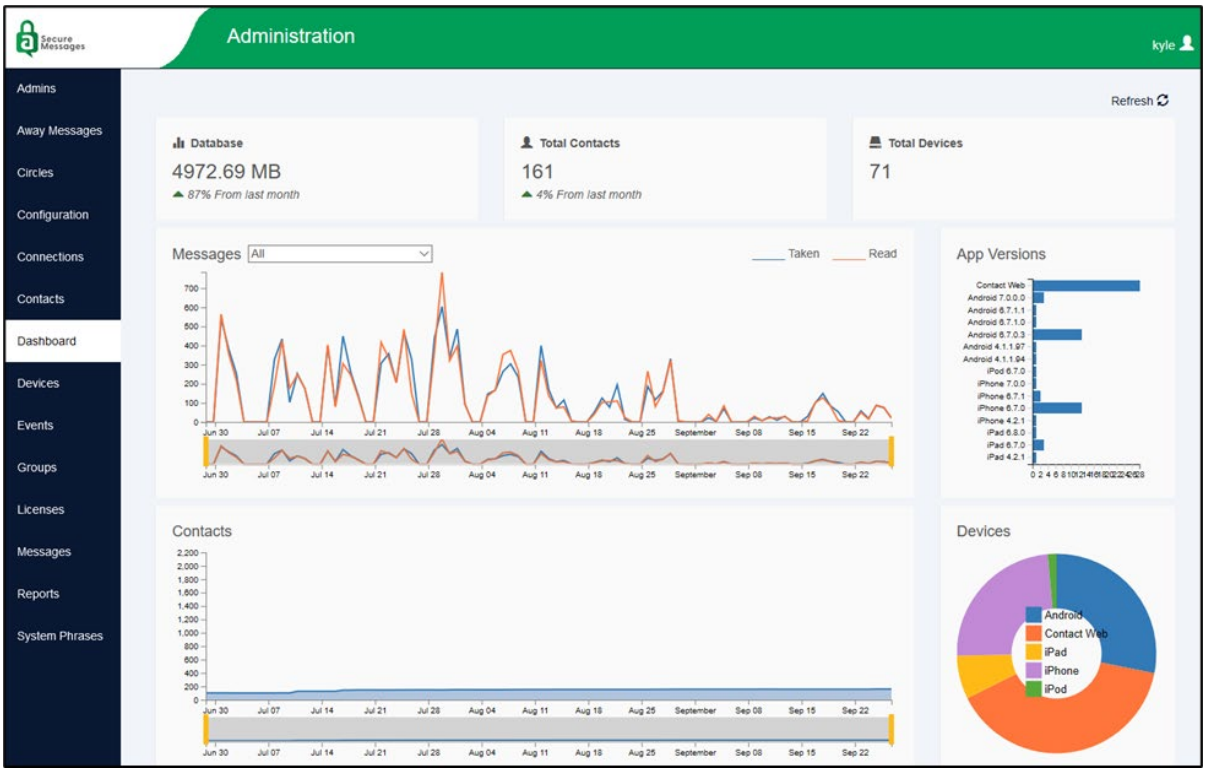
Enter “system.”

Password

Enter “password.”

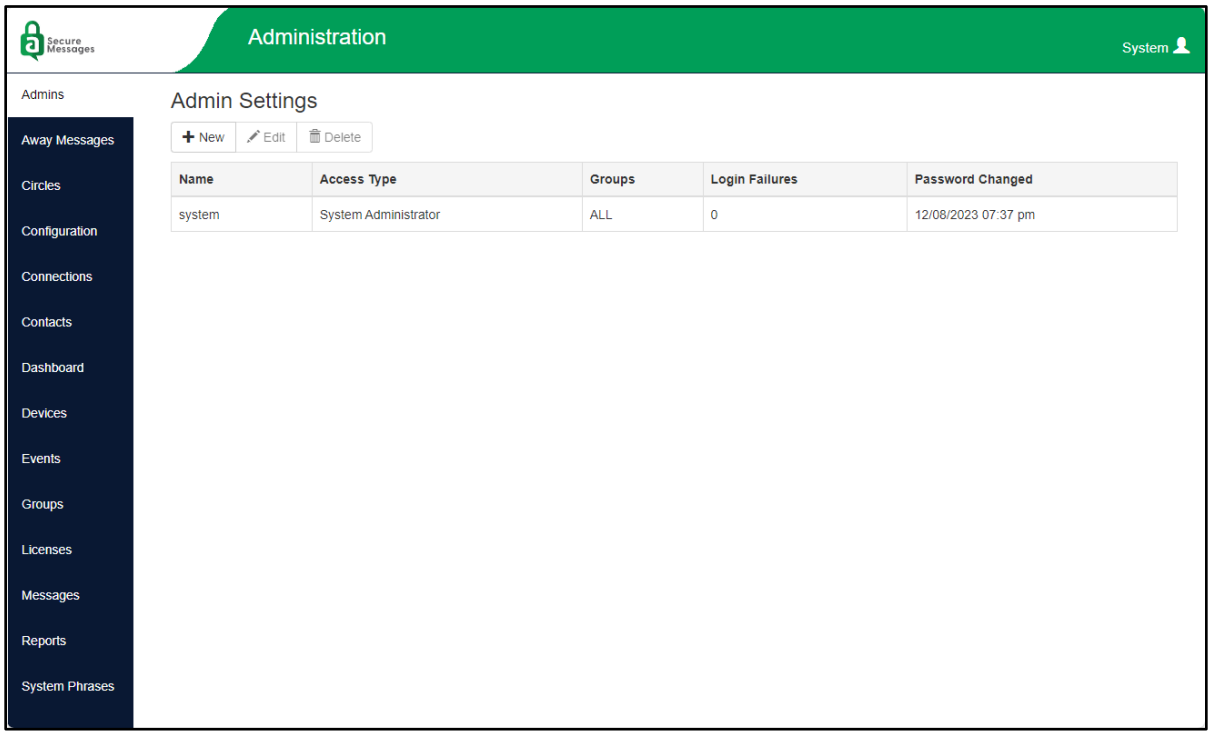
Click the Login button.

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



Click the Admins command in the navigation menu.

The Admin Settings page is displayed. The Admin Settings page is used to add, edit, and delete ASM Admin Web agents. ASM Admin Web agents are agents 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 agent's access type.



The Admin Settings page displays a table of all existing ASM Admin Web agents in alphabetical order by username. The default agent username is *system*.

To change your *system* password, select the *system* agent in the table and then click the Edit icon.

The Admin Settings window displays the settings for the *system* agent.

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 *system* username.

Re-Type Password

Type the same password.

Note: It is important to keep your *system* password a secret to prevent unauthorized access to your ASM Admin Web settings.

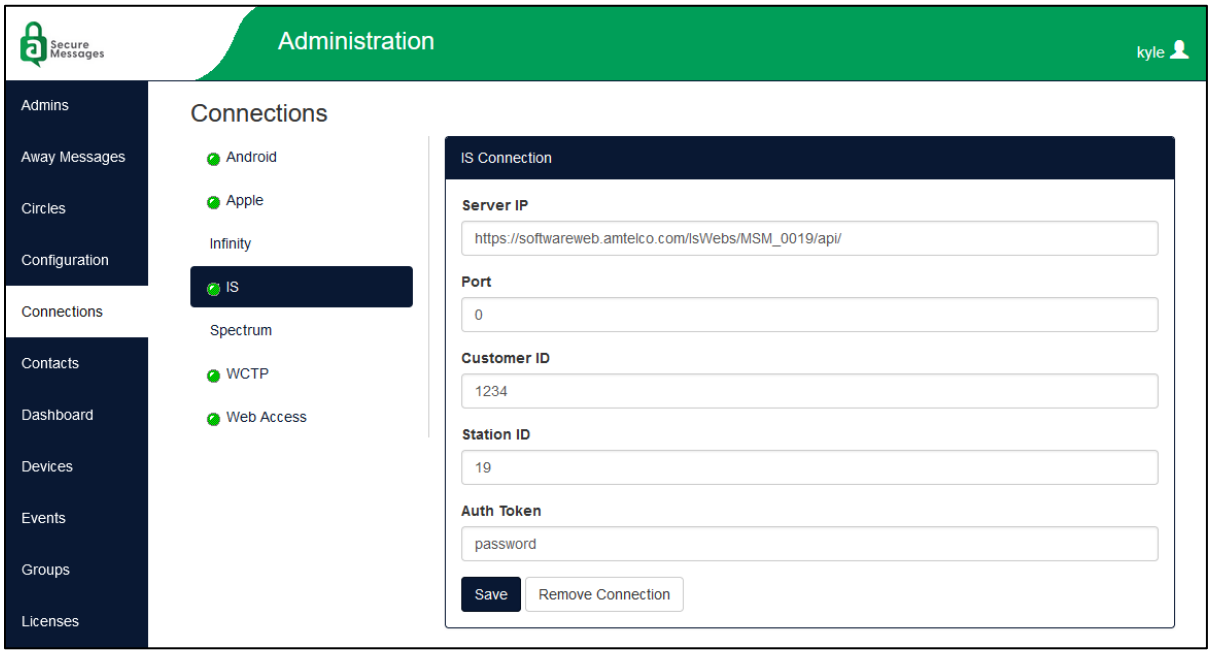
Click the Save button to save the new *system* password.

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.

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.

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

When connecting to older versions of Intelligent Series, 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.

Signing Out

To log out of the ASM Admin Web, click the username in the upper right corner of the screen.

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

Click the Sign Out hyperlink.

More information about configuring the ASM Admin Web is provided in the *Amtelco Secure Messages Admin Web Guide*.

Configuring the Amtelco Secure Messages Android App

The Amtelco Secure Messages Android app provides secure messaging and paging services for Android devices using Amtelco's Amtelco Secure Messages service. The Amtelco Secure Messages Android app receives notification of secure messages sent from the Amtelco Secure Messages Web 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 within their company or organization.

The user or an administrator can install the Amtelco Secure Messages Android app on an Android device by downloading it from Google Play. Once the app is downloaded, the app must be registered.

Each Amtelco Secure Messages account can be configured for Self Registration, E-mail Registration, or Admin Registration. More information about registration types is provided in the *Amtelco Secure Messages Admin Web Guide*.

To register for an Amtelco Secure Messages account using Self Registration, the user will need either login information or registration information.

Login Information

If a contact has been created for the user in the ASM Admin Web, the user will need the following information:

Account ID

An Amtelco Secure Messages Account ID is required for Self Registration. Provide the Account ID number that is listed under the General settings for the group in the ASM Admin Web.

Username

Provide the username that is configured in the user's Contact Settings in the ASM Admin Web.

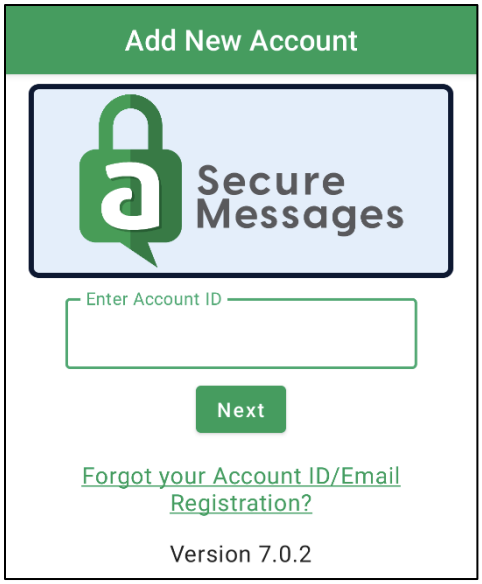
Password

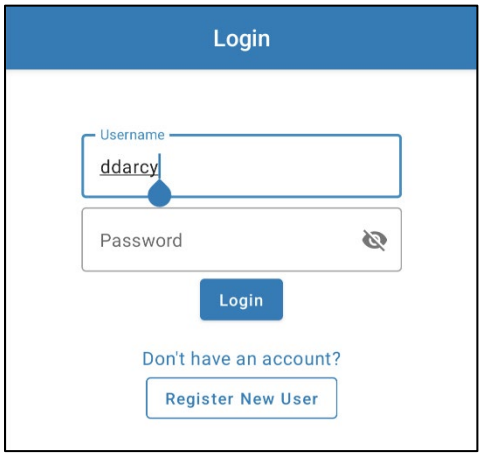
Provide the password that is configured in the user's Contact Settings in the ASM Admin Web. Instruct the user to keep his or her password a secret so that no one else can connect to the ASM Web Service in that user's name.

In addition, the user will need to provide the following information:

Passcode

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.





Passcode requirements are specified under the General settings for the group in the ASM Admin Web. If passcode requirements are specified, instruct the user to choose a passcode that he or she will remember. The user will be required to enter the passcode each time the user opens the Amtelco Secure Messages app unless Fingerprint Authentication is enabled.

Registration Information

If a contact has not been created for the user in the ASM Admin Web, the user will need the following information:

Account ID

An Amtelco Secure Messages Account ID is required for Self Registration. Provide the Account ID number that is listed under the General settings for the group in the ASM Admin Web.

In addition, the user will need to provide the following information:

Display Name

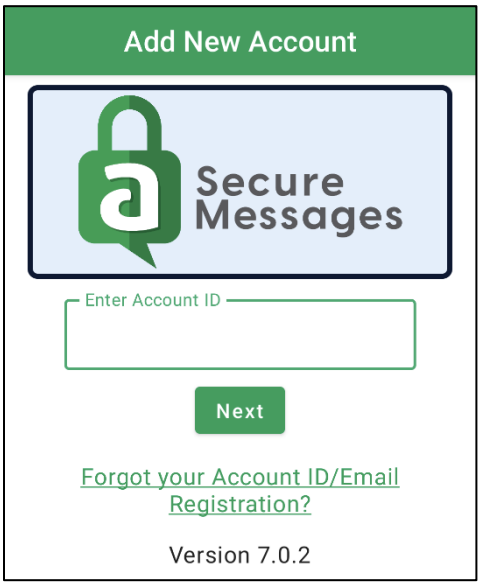
The Display Name the user chooses will be displayed in the Amtelco Secure Messages Contacts directory and on all messages that the user sends. First name and last name are recommended (for example, “John Smith”).

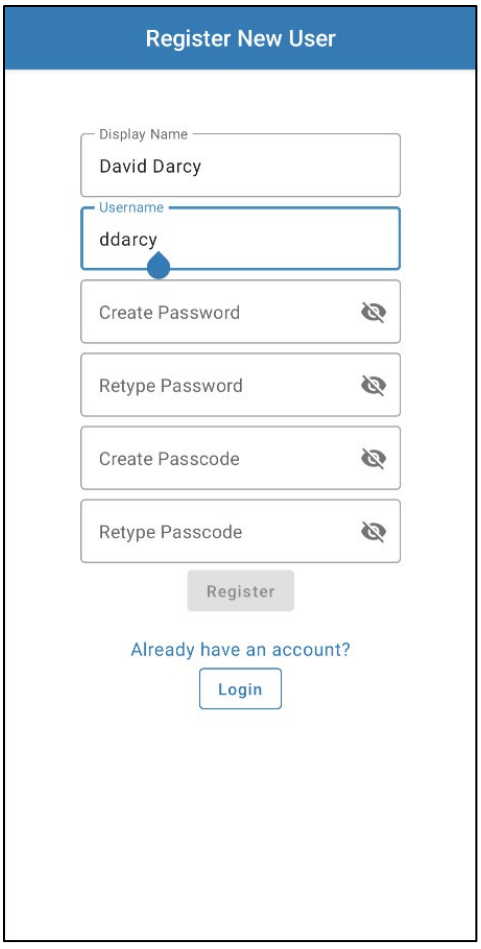
Username

The user must choose a username to identify the user when connecting to the ASM Web Service (for example, “jsmith”). The user will need to remember this username in order to register additional devices and to log into the Contact Web application. Usernames can be up to 50 characters long and must be unique. The use of spaces in a username is not recommended.

Password

The user must choose a password. Password requirements are specified under the General settings for the group in the ASM Admin Web. Instruct the user to keep his or her password a secret so that no one else can connect to the ASM Web Service in that user’s name.





Passcode

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.

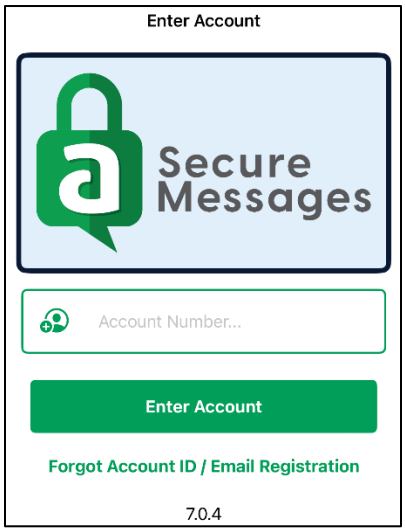
Passcode requirements are specified under the General settings for the group in the ASM Admin Web. If passcode requirements are specified, instruct the user to choose a passcode that he or she will remember. The user will be required to enter the passcode each time the user opens the Amtelco Secure Messages app unless Fingerprint Authentication is enabled.

Instructions for using the Amtelco Secure Messages Android app are provided in the *Amtelco Secure Messages Android App User Guide*.

Configuring the Amtelco Secure Messages Apple App

The Amtelco Secure Messages Apple app provides secure messaging and paging services for iPhone, iPad, and iPod Touch devices using Amtelco's Amtelco Secure Messages service. The Amtelco Secure Messages Apple app receives notification of secure messages sent from the Amtelco Secure Messages Web Service via the Apple Push Notification Service. Users can view and respond to messages and can initiate messages to other Amtelco Secure Messages users within their company or organization.

The user or an administrator can install the Amtelco Secure Messages Apple app on an Apple device by downloading it from the Apple iTunes store. Once the app is downloaded, the app must be registered.



Each Amtelco Secure Messages account can be configured for Self Registration, E-mail Registration, or Admin Registration. More information about registration types is provided in the *Amtelco Secure Messages Admin Web Guide*.

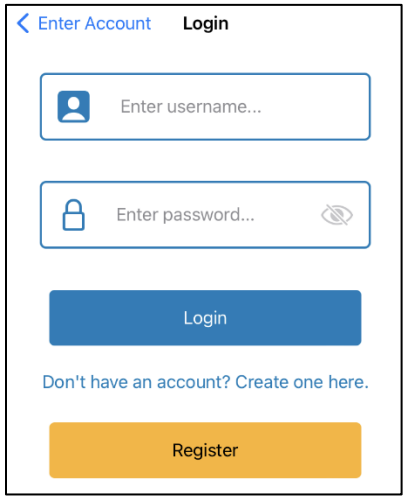
To register for an Amtelco Secure Messages account using Self Registration, the user will need either login information or registration information.

Login Information

If a contact has been created for the user in the ASM Admin Web, the user will need the following information:

Account ID

An Amtelco Secure Messages Account ID is required for Self Registration. Provide the Account ID number that is listed under the General settings for the group in the ASM Admin Web.



Username

Provide the Username that is configured in the user's Contact Settings in the ASM Admin Web.

Password

Provide the password that is configured in the user's Contact Settings in the ASM Admin Web. Instruct the user to keep his or her password a secret so that no one else can connect to the ASM Web Service in that user's name.

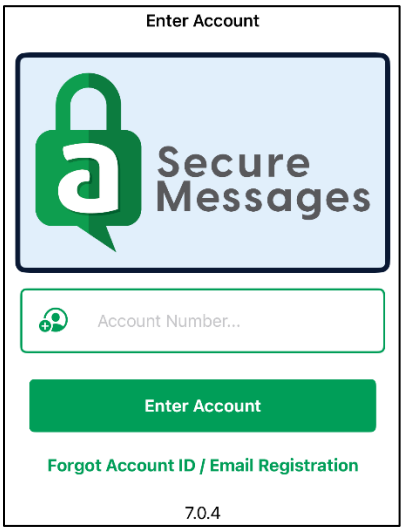
In addition, the user will need to provide the following information:

Passcode

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.

Passcode requirements are specified under the General settings for the group in the ASM Admin Web. If passcode requirements are specified, instruct the user to choose a passcode that he or she will remember. The user will be required to enter the passcode each time the user opens the Amtelco Secure Messages app unless Touch/Face ID is enabled.

Registration Information



If a contact has not been created for the user in the ASM Admin Web, the user will need the following information:

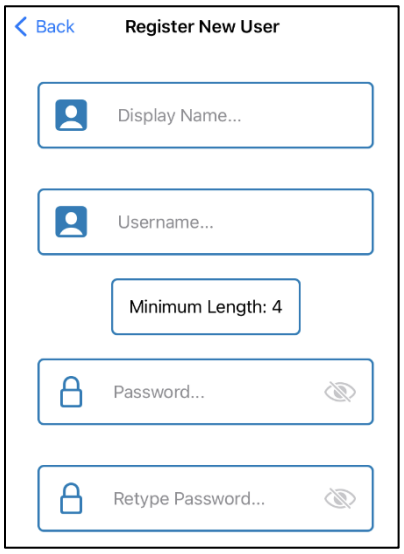
Account ID

An Amtelco Secure Messages Account ID is required for Self Registration. Provide the Account ID number that is listed under the General settings for the group in the ASM Admin Web.

In addition, the user will need to provide the following information:

Display Name

The Display Name the user chooses will be 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”).



Username

The user must choose a username to identify the user when connecting to the ASM Web Service (for example, “jsmith”). The user will need to remember this username in order to register additional devices and to log into the Contact Web application. Usernames can be up to 50 characters long and must be unique. The use of spaces in a username is not recommended.

Password

The user must choose a password. Password requirements are specified under the General settings for the group in the ASM Admin Web. Instruct the user to keep his or her password a secret so that no one else can connect to the ASM Web Service in that user’s name.

Passcode

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.

Passcode requirements are specified under the General settings for the group in the ASM Admin Web. If passcode requirements are specified, instruct the user to choose a passcode that he or she will remember. The user will be required to enter the passcode each time the user opens the Amtelco Secure Messages app unless Touch/Face ID is enabled.

Instructions for using the Amtelco Secure Messages Apple app are provided in the *Amtelco Secure Messages Apple App User Guide*.

Configuring the Amtelco Secure Messages Apple Watch App

The Amtelco Secure Messages Apple Watch app enables users to receive and respond to Amtelco Secure Messages notifications on their Apple Watch. The Apple Watch app displays the last three threads in the user's inbox as well as the last three messages for each of those threads. The Message Threads screen has an indicator for new messages, high priority, and attachments. Attachments can't be viewed on the watch, but a message is displayed informing the user that the attachments are available on the phone.

A reply can be sent to the threads using either Quick Phrases, dictation, or the Scribble feature. If a passcode is required, the user is only asked to enter it once while the watch is on their wrist. If the user takes off the watch, the passcode must be entered again to access the app.

Installing the Amtelco Secure Messages Watch App

The Amtelco Secure Messages Apple Watch app must be installed onto the watch through the Watch app on an iPhone that is paired with the watch.

Note: Before the Amtelco Secure Messages Apple Watch app can be installed on an Apple watch, the Amtelco Secure Messages app must be installed and registered on an iPhone that is paired with the watch.

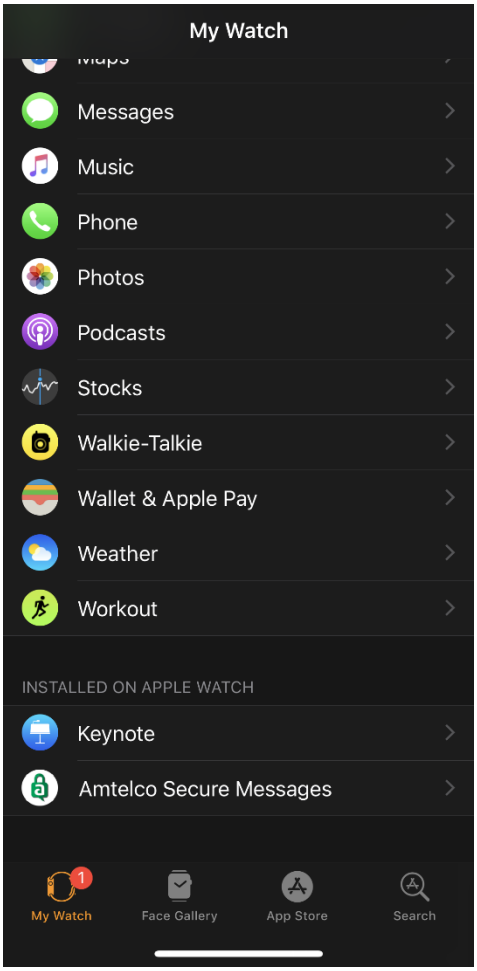
To install Amtelco Secure Messages on an Apple Watch, open the **Watch** app on the paired iPhone.

Tap **My Watch** in the Tab Bar at the bottom of the screen if it is not already selected.

At the My Watch screen, scroll down to the **Available Apps** section and find **Amtelco Secure Messages**.

Tap the **Install** button in the same row as "miSecureMessages."

When the installation is finished, "Amtelco Secure Messages" is listed in the "Installed on Apple Watch" section of the My Watch screen.



Launching the Amtelco Secure Messages Watch App

To open the Amtelco Secure Messages Watch app from the Apple Watch Home screen, tap the Amtelco Secure Messages icon.

Note: Before launching the Amtelco Secure Messages Watch app on the watch for the first time, launch the Amtelco Secure Messages app on the iPhone that is paired with the watch. If the error "Invalid Account Info" is displayed, force close the Amtelco Secure Messages app on the paired phone and relaunch it. If the error "No account" is displayed on the Apple Watch, make sure an account is registered on the paired phone.

Instructions for using the Amtelco Secure Messages Apple Watch app are provided in the *Amtelco Secure Messages Apple App User Guide*.

Logging into the 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.

The Contact Web is enabled by starting the Web Access connection in the ASM Admin Web.

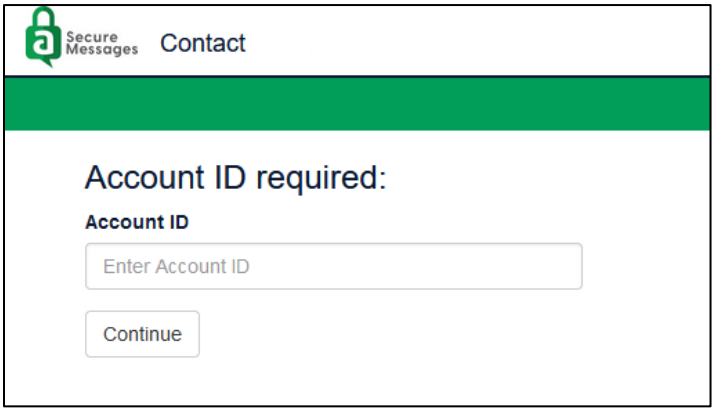
The Amtelco Secure Messages Contact Web application is tested with the latest release of the following browsers:

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

Login Information

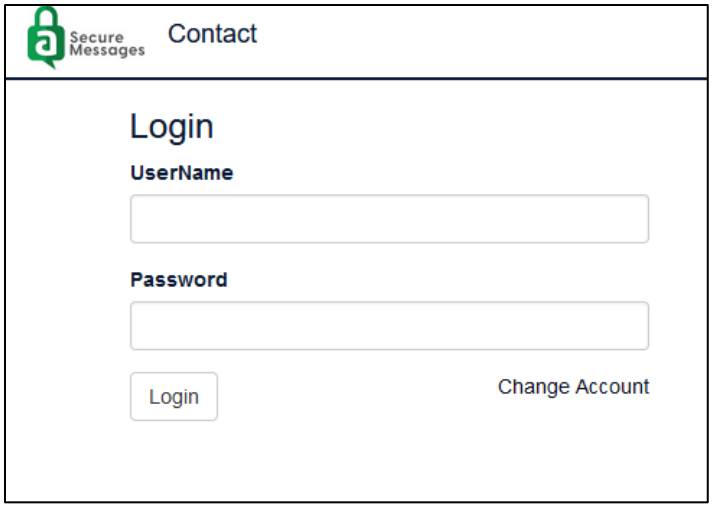
The user will need the Contact Web URL (Uniform Resource Locator) indicated under the General settings for the group in the ASM Admin Web. Each Group has a different Contact Web URL.

The user will also need the following login information.



Account ID

The user must enter the Amtelco Secure Messages Account ID each time the user wants to log into the ASM Contact Web. Provide the Account ID number that is listed under the General settings for the group in the ASM Admin Web.



UserName

Provide the username that is configured in the user's Contact Settings in the ASM Admin Web.

Password

Provide the password that is configured in the user's Contact Settings in the ASM Admin Web. Instruct the user to keep his or her password a secret so that no one else can connect to the ASM Web Service in that user's name.

Instructions for using the Amtelco Secure Messages Contact Web are provided in the *Amtelco Secure Messages Contact Web User Guide*.

Adding Amtelco Secure Messages to IS

Amtelco Secure Messages can be integrated into the Intelligent Series (IS) suite of applications using Network Encryption, Unsolicited Client settings, Event Notifications, and the Secure Messaging Contact Method. Contact Methods are assigned to IS Directory listings in the IS Supervisor application with the IS Directory Contacts feature. If you have an IS system and want to use it to send secure messages, follow the instructions in this section.

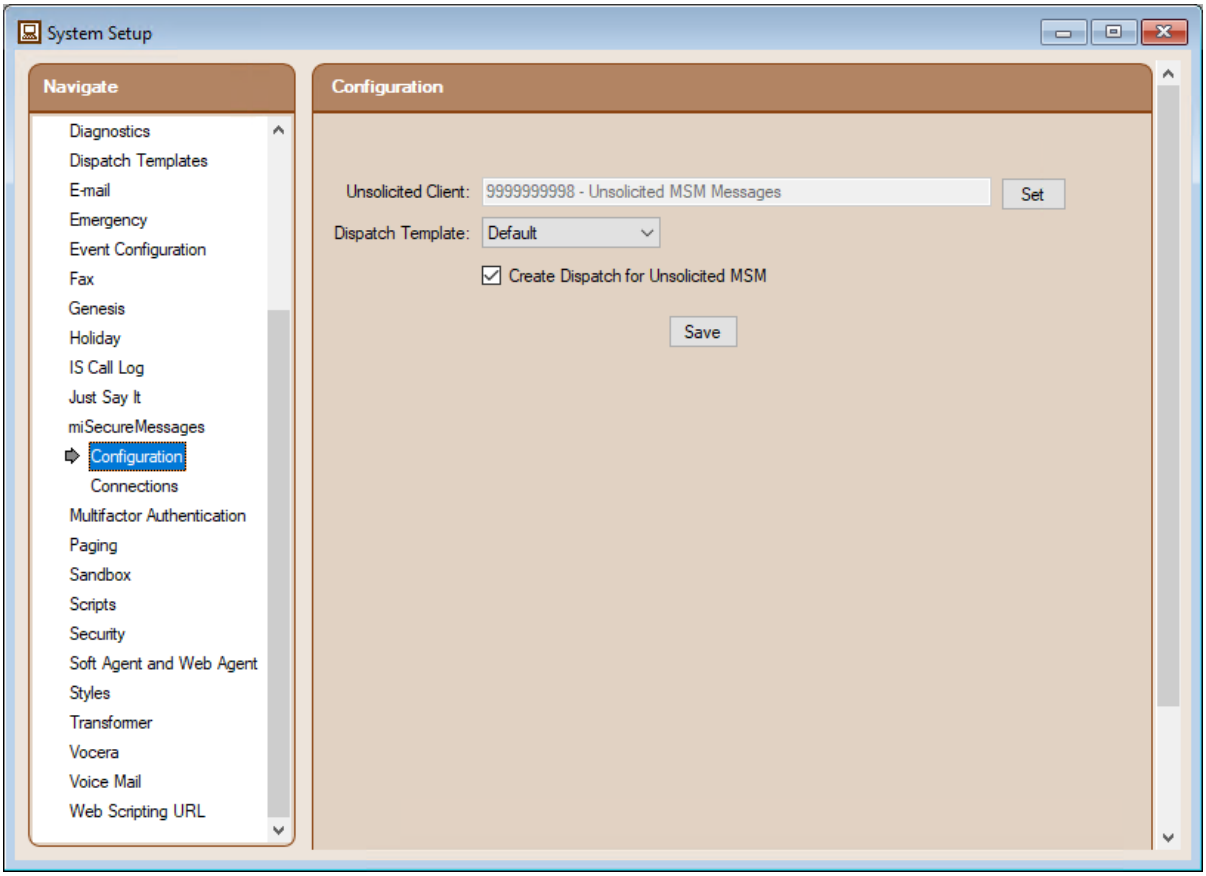
Enabling Network Encryption

Starting with IS Supervisor version 5.6.8259.01, the 256-bit Advanced Encryption Standard (AES) is used to encrypt all network packets transmitted between the IS Server and IS client applications. This encryption is built into the IS application and does not require any additional technology such as third-party certificates.

If you are using an older version of IS Supervisor, follow the instructions for setting your Network Encryption Mode to AES 256 encryption in the “System Setup” section of the *Intelligent Series Supervisor Reference Guide*.

Configuring Unsolicited Client Settings

The Configuration page is used to configure the handling of inbound unsolicited messages sent from the Amtelco Secure Messages (ASM) app or the Amtelco Secure Messages Contact Web.



To open the Configuration page, follow these steps:

On the System Setup Navigation Menu, click the miSecureMessages hyperlink.

Hyperlinks for the Configuration and Connections pages are displayed.

If the Configuration page is not displayed, click the Configuration hyperlink.

The Configuration page is displayed.

Unsolicited Client

When an unsolicited secure message comes in to IS, IS compares the Amtelco Secure Messages username that sent the message with a database that keeps track of the last username that was sent an ASM message from each Client. IS routes the message to the first matching Client it finds. If no match is found, the message is sent to the Unsolicited Client specified here.

To select a Client for unsolicited secure messages, click the Set button.

The Select Client window is displayed. The Select Client window is used to select a Client. It shows a list of all Clients, sorted by Client Number.

Search
The search field located at the top of the Select Client window is used to search for a specific Client Number or Client Name.

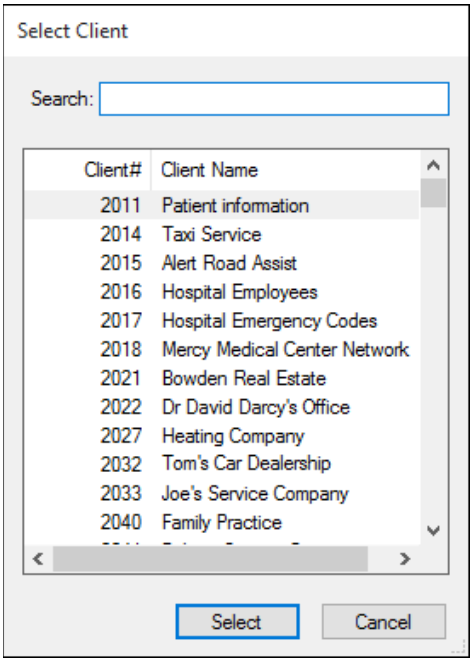
To search for a specific Client, type all or part of the Client Number or Client Name.
OR
Use the scroll bar to scroll through the client list.

Client# | Client Name
All of the Client Numbers and Client Names are listed numerically in the Select Client window.

Select the Client that should receive unsolicited ASM messages.

Click the Select button to save your Unsolicited Client setting and return to the Configuration page.
OR
Click the Cancel button to return to the Configuration page without saving your Unsolicited Client settings.

If you clicked the Select button, the Client Number and Client Name that you selected are displayed in the Unsolicited Client field.



Dispatch Template

The Dispatch Template setting indicates the dispatch settings to use to create a dispatch job when an unsolicited inbound ASM message is received or when an outbound ASM message fails and no dispatch job exists. Dispatch templates are configured on the Dispatch Templates page of IS Supervisor System Setup.

Select the dispatch template to use for unsolicited inbound ASM messages and failed outbound ASM messages when no dispatch job exists.

☑ Create Dispatch for Unsolicited MSM

If you are using Intelligent Dispatching, a dispatch job can be sent to the Dispatch List whenever an ASM message is routed to the Unsolicited Client.

- **Select this check box to create a dispatch job whenever an unsolicited secure message is received.**
- **Clear this check box if no dispatch job is desired for unsolicited secure messages.**

Saving Your Entries

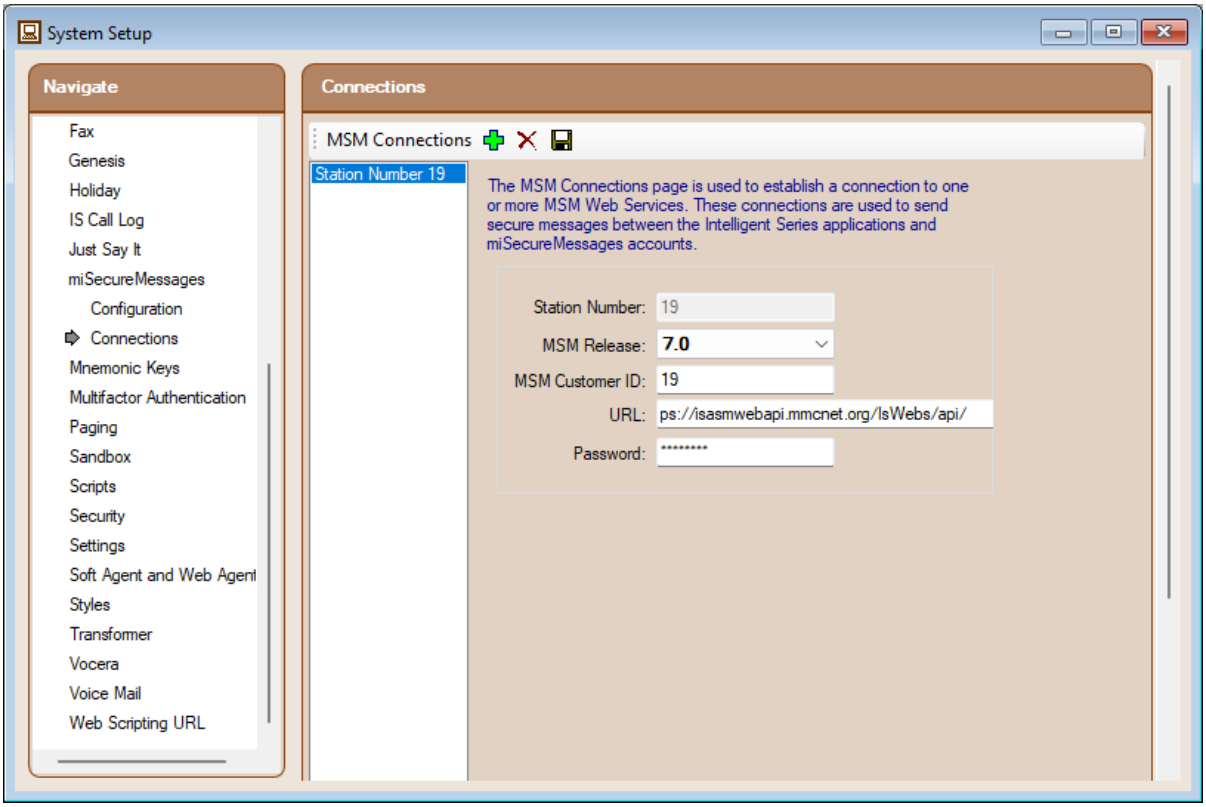
When you have finished entering ASM settings, click the Save button to save your changes.

Configuring Connections to ASM Web Services

The Connections page is used to establish a connection to one or more Amtelco Secure Messages (ASM) Web Services. These connections are used to send secure messages between the Intelligent Series version 5.7 and later applications and ASM version 7.0 and later accounts.

Click the Connections hyperlink on the System Setup Navigation Menu.

The Connections page is displayed.



Adding and Editing Connections

- **To add a new connection, click the Add MSM Connection icon.**

  A new MSM connection is created with blank properties.

- **To edit an existing connection, select the name of the connection in the Connections list.**

  The Connection screen is updated to display the settings for the selected connection.

Station Number

The Station Number field is used to assign a station number to an ASM Web Service. The Station Number is used when programming IS Directory Contact Methods to indicate which ASM Web Service to use to send secure messages from Intelligent Series applications.

If you are connecting to Amtelco Secure Messages version 7.0 or later, a unique station number should be used.

If you are connecting to an older version of Amtelco Secure Messages, the Station Number must match the Station ID programmed in the Intelligent Series Server settings on the Connections page of the Amtelco Secure Messages Admin Web. More information about Station IDs is provided in the *Amtelco Secure Messages Admin Web User Guide*.

If you are connecting to Amtelco Secure Messages version 7.0 or later, enter a unique station number to assign to the ASM Web Service.

If you are connecting to an older version of Amtelco Secure Messages, enter the Station ID programmed under the IS Connection settings in the Amtelco Secure Messages Admin Web.

The Station Number is displayed in the MSM Connections list when changes made to the connection are saved.

MSM Release

The MSM Release field is used to specify the version of Amtelco Secure Messages server used by the ASM Web Service.

Select the Amtelco Secure Messages version used by the ASM Web Service.

MSM Customer ID

The MSM Customer ID field is used to specify your unique Amtelco Secure Messages customer identification number provided by Amtelco.

Enter your ASM customer identification number.

URL

The URL field is used to specify the Uniform Resource Locator (URL) of the ASM Web Service.

Enter the URL of the ASM Web Service.

Password

The Password field is used to specify the password used to login to the ASM Web Service. It must match the Auth Token programmed in the IS Connection settings on the Connections page of the Amtelco Secure Messages Admin Web.

Enter the password used to login to the ASM IS Web API.

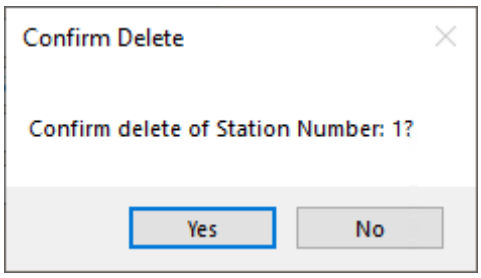
Click the Save icon to save your changes.

The connection is added to the MSM Connections list.

Deleting a Connection

To delete a connection, select the name of the connection in the MSM Connections list and then click the Delete icon. ✕

The Delete Connection dialog box is displayed.



To delete the connection, click the Yes button.

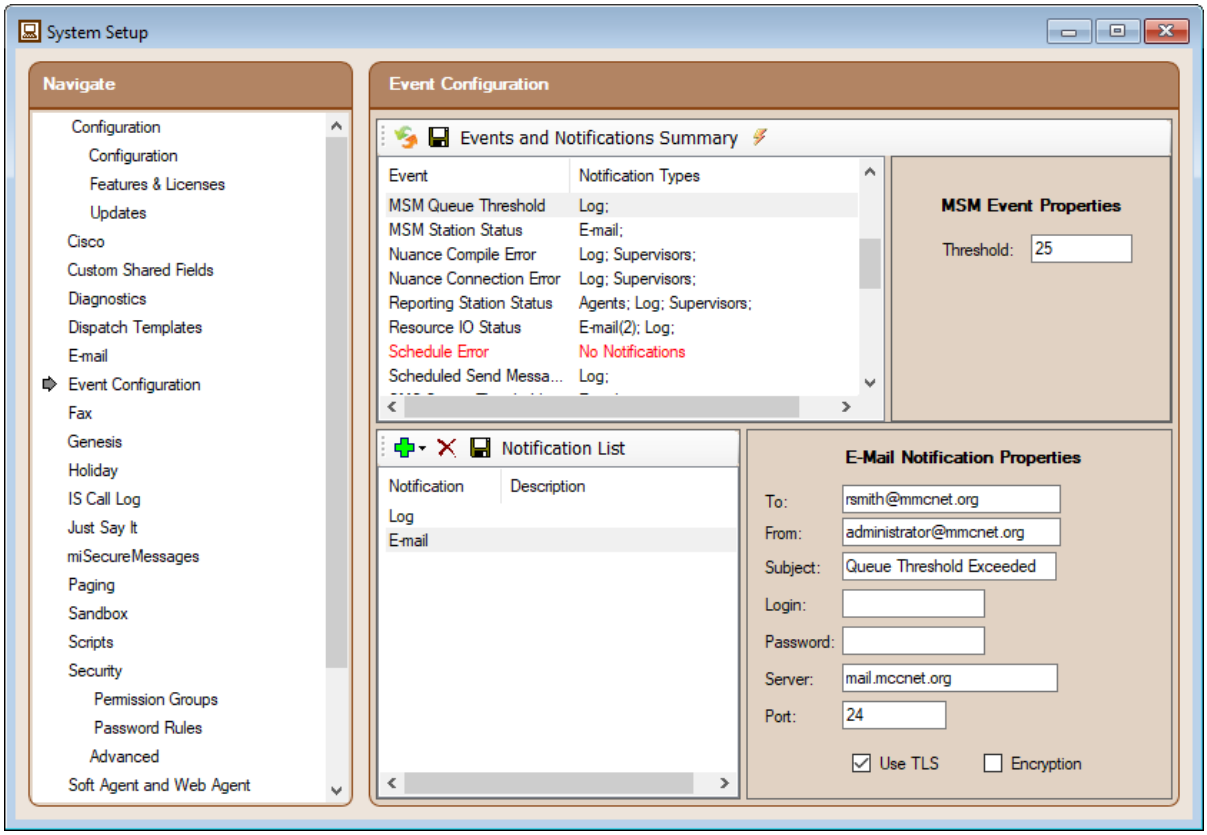
OR

To return to the Connections page without deleting the connection, click the No button.

Configuring Event Notifications

The Event Configuration page is used to configure event notifications to be sent to e-mail addresses, Short Message Service (SMS) devices, Amtelco Secure Messages devices, the IS Server log, and agent and supervisor stations.

Click the Event Configuration hyperlink on the System Setup Navigation Menu to display the Event Configuration page.



Events and Notifications Summary

The Events and Notifications Summary pane contains a toolbar and a table.

Events and Notifications Summary Toolbar

The toolbar is used to refresh the table and to save changes to the notification settings for events.

Icon	Description
	The **Refresh** icon updates the list of events and notification types displayed in the Events and Notifications Summary table.
	The **Save** icon saves all changes made to the events and notification types.
	The **Test** icon sends a test notification for the selected event.

The Event column displays a list of IS Server events that can generate notifications.

The Notification Types column displays a summary of the types of notifications that are sent each time the event occurs. If no notifications have been configured for an event, the words "No Notifications" are displayed in red text.

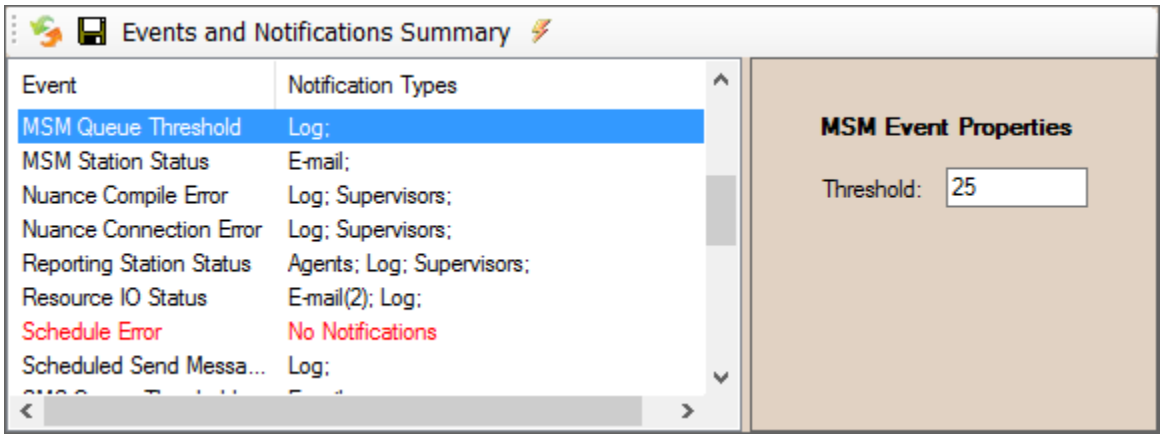
There are two IS events that relate to Amtelco Secure Messages.

Event	Description
MSM Queue Threshold	The MSM Queue Threshold event occurs when the number of jobs in the Amtelco Secure Messages (ASM) queue exceeds the threshold set in the MSM Event Properties.
MSM Station Status	The MSM Station Status event occurs when the ASM Station loses its connection to IS.

To view or edit the notification settings for an event, click the name of the event in the Events and Notifications Summary table.

The notifications for the event are displayed in the Notification List pane.

Event Properties



If the event selected in the Events and Notifications Summary table has configurable properties, the properties are displayed to the right of the table.

Threshold

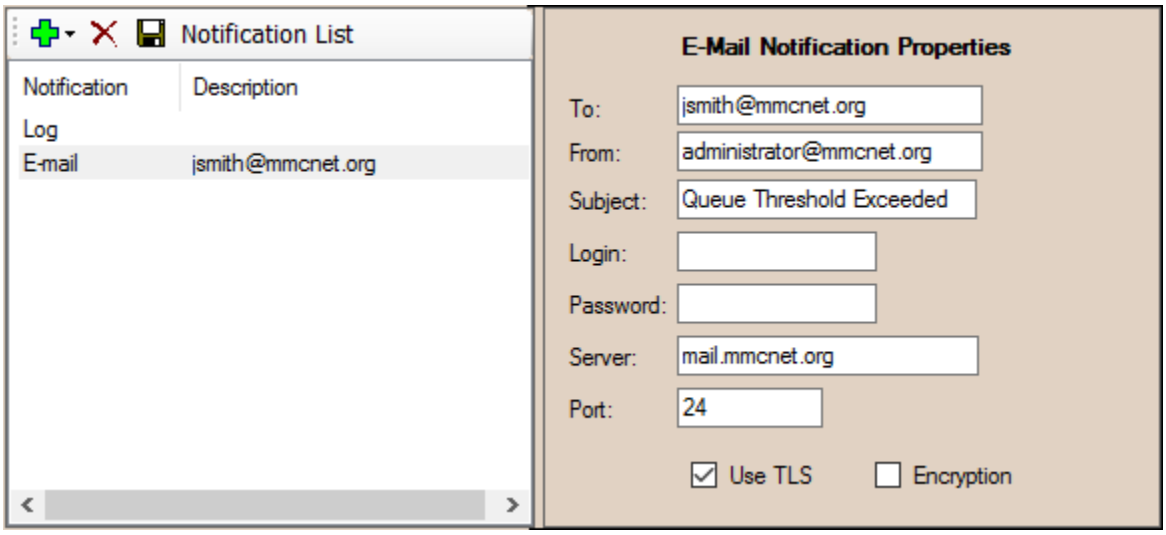
The MSM Queue Threshold event has a Threshold property. The Threshold property determines the number of messages waiting to be sent from IS to the ASM Service that will trigger the event. This property should be set to a value slightly higher than the number of messages that are expected be sent from IS to ASM Service at one time, so that the event only is triggered when there is an issue that prevents messages from being sent.

Enter a number slightly higher than the number of secure messages expected to be sent from IS at one time.

Click the Save icon on the Events and Notifications Summary Toolbar to save the property settings.

Notification List

The Notification List pane displays the notification settings for the event selected in the Events and Notifications Summary table.



Notification List Toolbar

The Notification List Toolbar is used to add and remove notification settings for the event that is selected in the Events and Notifications Summary table.

Icon	Description
	The **Add** icon displays a menu of notification types that can be added. Select a notification type to add it to the Notification List.
	The **Delete** icon removes the notification type that is selected in the Notification List.
	The **Save** icon saves all changes made to the settings for the selected notification type. **Note:** The Save icon on the Notification List Toolbar only saves changes to the settings for the selected notification type. You must also click the Save icon on the Events and Notifications Summary Toolbar to save additions and deletions to the Notification List.

Adding and Editing Event Notifications

To add or edit an event notification, select an event in the Events and Notifications Summary pane.

The notifications that have been configured for that event are displayed in the Notification List.

- **To edit a notification, select the notification type in the Notification List.**
  OR
- **To add a notification, click the Add icon on the Notification List Toolbar.**

  A menu of notification types is displayed.

Select the type of notification to add.

The notification type is added to the Notification List.

Notification Type	Description
E-mail	The E-mail notification type is used to send e-mail event notifications to an e-mail address.
Log	The Log notification type is used to save event notifications in the IS Event Log. The Event Log can be viewed through the Monitors & Logs pages of IS Supervisor.
MSM	The MSM notification type is used to send secure event notifications to a device using the optional Amtelco Secure Messages app.
SMS	The SMS notification type is used to send event notification text messages to a Short Message Service (SMS) device.
Stations	The Stations notification type is used to send event notifications to agents and operators logged into IS applications.

The properties for the selected notification type are displayed to the right of the Notification List. The properties vary for each notification type.

E-mail Notification Properties

The E-mail Notification Properties are displayed when an E-mail notification is selected in the Notifications List.

To

Type the e-mail address that should receive an event notification whenever the event occurs.

From

Type the return address to use for the event notification e-mail messages.

Note: The From address should be for an account that can authenticate on the server domain. Otherwise, it could cause relay errors or be classified as spam.

Subject

Type the text to display in the subject line of the event notification e-mail messages.

Login

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

Password

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

Server

Type the name of your mail server.

Port

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

☑ Use TLS

The "Use TLS" option determines whether Transport Layer Security (TLS) is used to send event notification e-mail messages.

- **Select this check box to use Transport Layer Security to send the event notification e-mail messages.**
- **Clear this check box to disable Transport Layer Security when sending the event notification e-mail messages.**

☑ Encryption

The "Encryption" option determines whether e-mail encryption is used to send event notification e-mail messages.

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

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

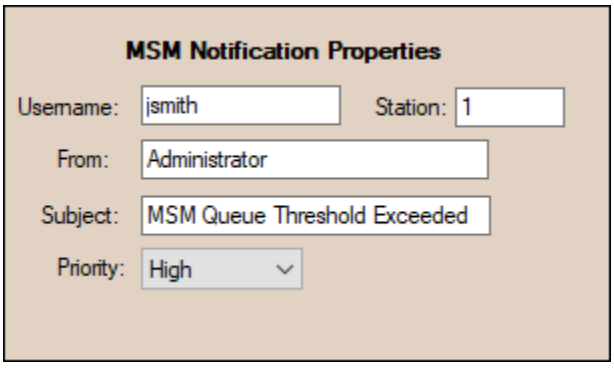
When e-mail encryption is enabled, the IS E-mail Service communicates with the enterprise e-mail server. When an e-mail message is generated by IS, the IS E-mail Service uses your Public Key Certificate to encrypt the message. The IS E-mail Service then sends the encrypted message to the enterprise e-mail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

Click the Save icon on the Notification List Toolbar to save your changes to the E-Mail Notification Properties.

When you have finished adding notifications to an event, click the Save icon on the Events and Notifications Summary Toolbar to save your notification changes.

Click the Refresh icon on the Events and Notifications Summary Toolbar to display your changes.

MSM Notification Properties



The MSM Notification Properties are displayed when an MSM notification is selected in the Notifications List.

Username

An Amtelco Secure Messages Username can be used to send a secure message to an Amtelco Secure Messages Contact Web user and all of a contact's devices that are registered with the Amtelco Secure Messages App.

Enter the Username of the contact as configured in the user's Amtelco Secure Messages App and in the user's Contact Settings in the Amtelco Secure Messages Admin Web.

Station

The Station field is used to indicate which ASM Web Service to use on systems that have more than one ASM Web Service. It must match a Station Number configured for one of the MSM Connections in the System Setup pages of IS Supervisor.

Enter the Station Number of the ASM Web Service that you want to use to send the notification.

From

Type the name to display as the sender of the event notification messages.

Subject

Type the text to display as the subject of the event notification messages.

Priority

Select the priority to use for the event notification messages.

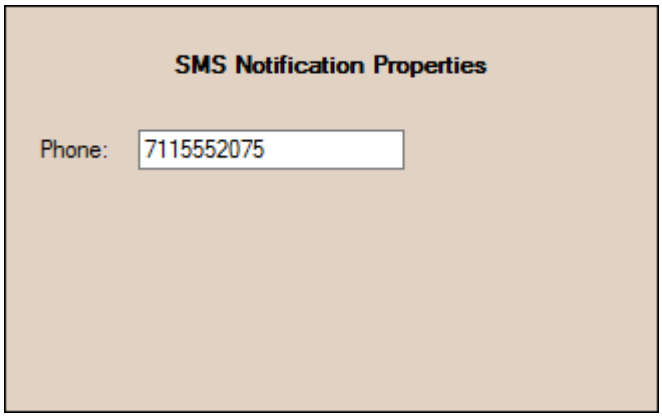
Click the Save icon on the Notification List Toolbar to save your changes to the MSM Notification Properties.

When you have finished adding notifications to an event, click the Save icon on the Events and Notifications Summary Toolbar to save your notification changes.

Click the Refresh icon on the Events and Notifications Summary Toolbar to display your changes.

SMS Notification Properties

The SMS Notification Properties are displayed when an SMS notification is selected in the Notifications List.



Phone

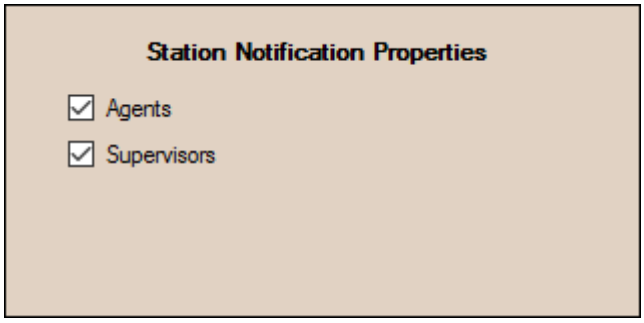
Type the phone number of the SMS device to receive event notification text messages.

Click the Save icon on the Notification List Toolbar to save your changes to the SMS Notification Properties.

When you have finished adding notifications to an event, click the Save icon on the Events and Notifications Summary Toolbar to save your notification changes.

Click the Refresh icon on the Events and Notifications Summary Toolbar to display your changes.

Station Notification Properties



The Station Notification Properties are displayed when a Station notification is selected in the Notifications List.

☑ Agents

Select the Agents check box to send event notifications to all users logged into the Infinity Telephone Agent application and to all users logged into the Soft Agent application.

The event notifications will appear for twelve seconds in the Infinity Telephone Agent Answer Window and twenty seconds in the Soft Agent Status Bar.

☑ Supervisors

Select the Supervisors check box to send event notifications to all users logged into the IS Supervisor application.

The background of the Event hyperlink in the upper right corner of the IS Supervisor menu bar will turn yellow to indicate an event notification. Supervisors can click the Event hyperlink to view the event notification.

Click the Save icon on the Notification List Toolbar to save your changes to the Station Notification Properties.

When you have finished adding notifications to an event, click the Save icon on the Events and Notifications Summary Toolbar to save your notification changes.

Click the Refresh icon on the Events and Notifications Summary Toolbar to display your changes.

Testing Event Notifications

The Test icon is used to send a test notification for a selected event.

To send a test notification for an event, select the event in the Events and Notifications Summary table and then click the Test icon on the Events and Notifications Summary Toolbar.

A test notification is sent to all of the notification types configured in the Notification List for the selected event.

Adding Secure Messaging to the IS Directory

The next step is to add the Secure Messaging Contact Method to your IS Directory listings.

To open the IS Directory, click the Directory & Scheduling icon 

on the IS Supervisor Toolbar.

The Directory and Scheduling window is displayed.

Enabling Contacts for a Directory Subjects

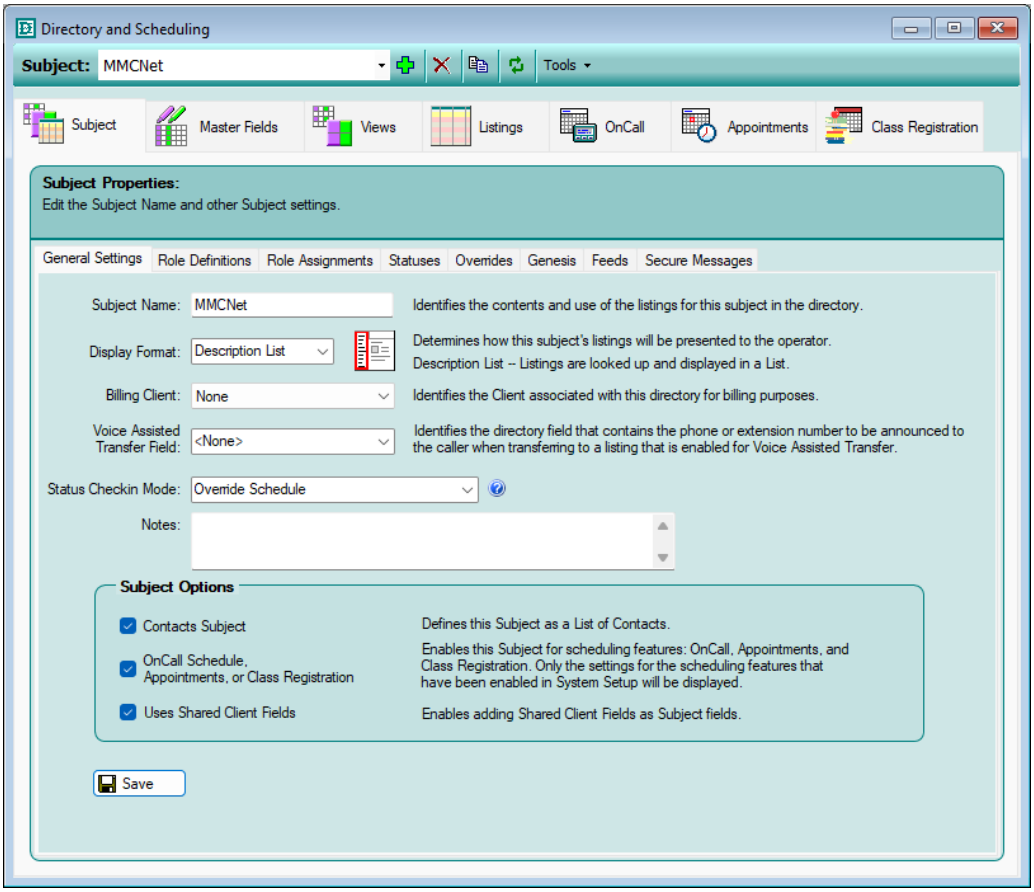
Contacts can be added to any IS Directory Subject by enabling the Contacts Subject option on the General Settings tab.

Subject Toolbar

The Subject Toolbar is displayed at the top of the Directory and Scheduling window. The Subject Toolbar contains a Subject menu, icons for creating Subjects, deleting Subjects, and copying Subject settings, and a Tools menu for exporting directory listings.

To select a Subject, open the Subject menu and select the desired directory Subject.

The General Settings for the selected subject are displayed unless you were already working under another tab in this Subject.



If you do not see the General Settings, click the Subject tab and then click the General Settings tab.

Subject Options

The Subject Options indicate how this directory Subject will be used.

☑ Contacts Subject

Enabling the Contacts Subject option allows you to set up Contact Methods for each of the listings in this directory Subject and Status Schedules that determine which Contact Methods are available for dispatching at specific times and dates.

This option is only available if the optional Directory Contacts feature is enabled on your system.

Select this check box to enable contact-based dispatching for the selected directory Subject.

☑ OnCall Schedule, Appointments, or Class Registration

The "OnCall Schedule, Appointments, or Class Registration" check box is used to enable IS Directory OnCall Scheduling, IS Appointments, and IS Class Registration for the selected directory Subject. All three features are enabled with the same check box.

IS Directory OnCall Scheduling is a requirement for the optional Role-Based Messaging feature.

Select this check box to create IS Directory OnCall schedules, IS Appointment schedules, or IS Class Registration courses based on this directory Subject's listings.

More information about IS Directory OnCall is provided in the "Directory OnCall Scheduling" section of the *Intelligent Series Supervisor Reference Guide*.

☑ Uses Shared Client Fields

Enabling the Uses Shared Client Fields option allows Shared Client Fields to be inserted into the directory. Shared Client Fields are fields that are common to every IS Client. These fields can be used to store information about each client in the IS Directory without having to create a separate field for each client.

Enabling this option also allows listings to be assigned to an IS Client for receiving messages and for viewing messages from miTeamWeb, the IS Web, and the IS Directory.

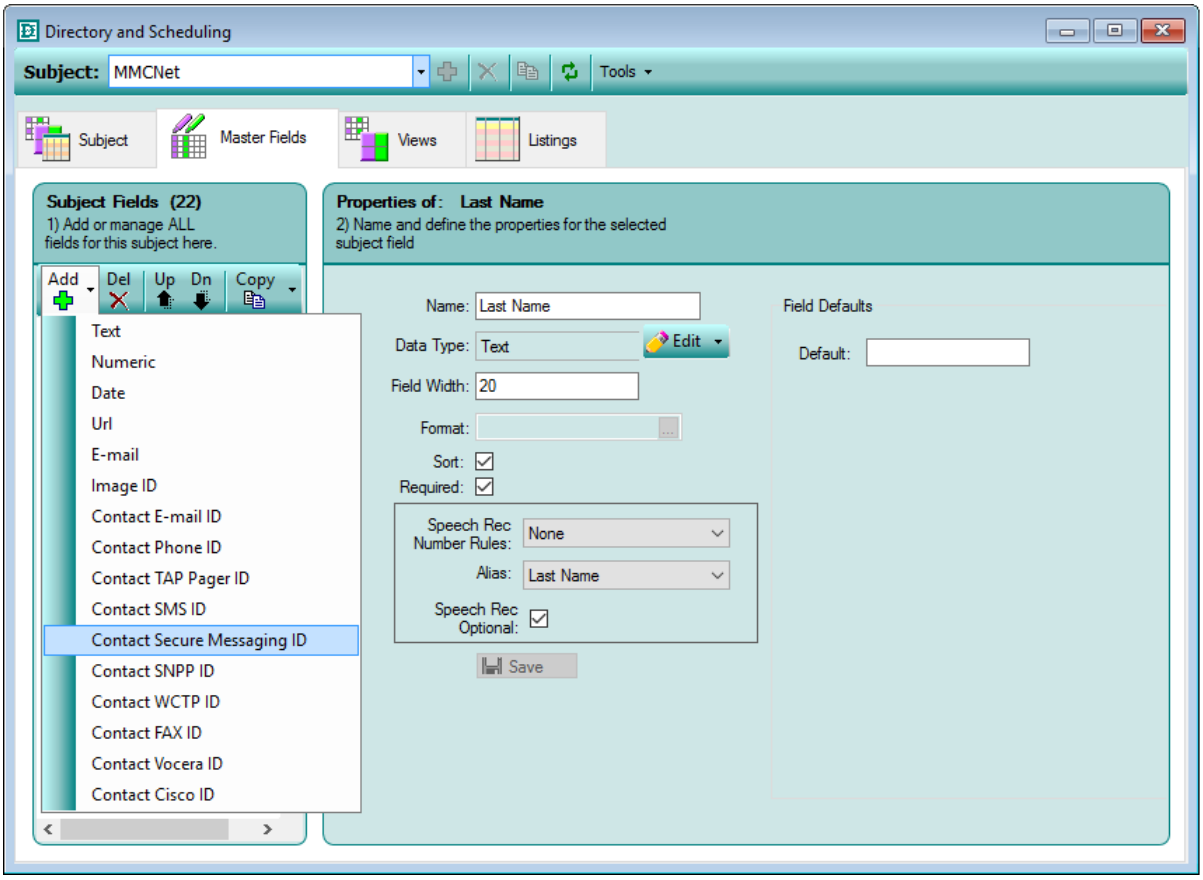
Select this check box to allow Client Fields to be incorporated into the selected directory Subject.

More information about Shared Client Fields is provided in the "System Setup" section of the *Intelligent Series Supervisor Reference Guide*.

Saving Your Entries

When you have finished making changes to the General Settings, click the Save button  **to save the settings.**

Creating a New Secure Messaging Master Field



Secure Messaging usernames can be displayed in the Fields of an IS Directory Subject by adding Contact Secure Messaging ID Fields to the Master Fields tab of the directory. Adding Contact Secure Messaging ID fields to the Master Fields of the directory is optional.

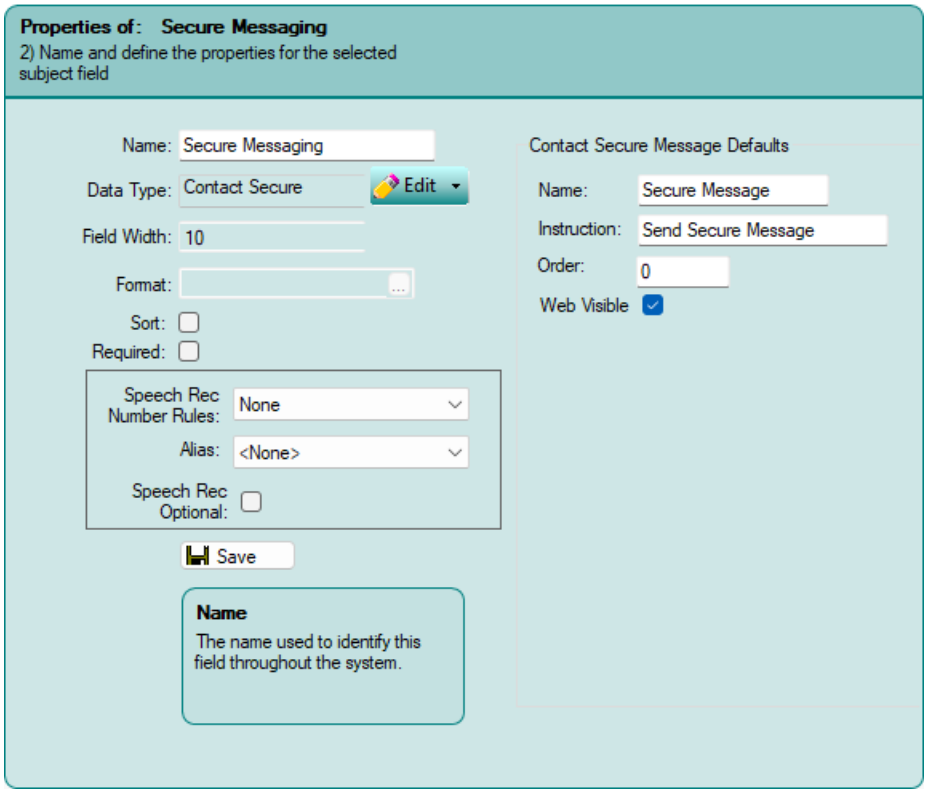
To create a new Secure Messaging Master Field, click the Add icon on the Subject Fields toolbar.

A menu of the available Data Types is displayed.

Select "Contact Secure Messaging ID."

A Master Field named "New Field" is added to the Subject Fields list.

Edit the properties displayed in the Properties pane.



Properties

The Properties pane controls the properties for the field selected in the Subject Fields menu. Any changes made on the Properties pane affect the type of values that are accepted for entries in the selected field.

Name

The Name property defines the visible name of the Subject Field when entries are inputted. This field can be overridden in each directory View if desired. The Name property accepts alphanumeric characters.

Type a name that describes the type of information you want to store in the field.

☑ Sort

The Sort property determines how directory listings are sorted. When this check box is selected, listings are sorted alphabetically, numerically, or chronologically according to the values contained in this Master Field. If more than one Master Field is enabled for sorting, the listings are sorted by the sort-enabled field that is closest to the top of the Subject Fields menu.

Select the Sort check box if you want to sort listings by the contents of this field.

OR

Clear the Sort check box if you do not want to sort listings by the contents of this field.

☑ Required

The Required property controls whether the field must have a value whenever a listing is saved.

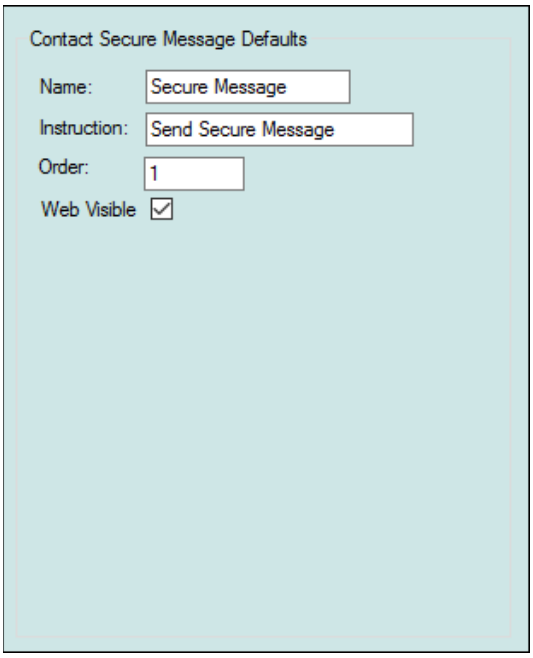
Select the Required check box to make this field required.

OR

Clear the Required check box to make this field optional.

More information about Master Field Properties is provided in the "Directory Setup" section of the *Intelligent Series Supervisor Reference Guide*.

Defaults



The Defaults pane is used to set default values for the field selected in the Subject Fields menu. Any values entered here will be filled in automatically when a new listing is created but can be changed in the listing properties.

Name

The Name field identifies the Contact Method in the IS Directory and in the Dispatching window.

If you would like new Contact Methods entered into this Contact field to have a default Contact Name, type a short, descriptive name for the Contact Method, like "Secure Message."

Instruction

The contents of the Instruction field are displayed to agents in the Contact Methods section of the IS Directory and in the Dispatching window.

If you would like new Contact Methods entered into this Contact field to have default instructions for the use of this Contact Method, type the instructions.

Order

The Order field determines which Contact Method is displayed first in the IS Directory when more than one of the same type of Contact Method (Phone, TAP Pager, E-mail, SMS, Secure Messaging, SNPP, or WCTP) is displayed. The Order field is also used with the IS Transformer feature to uniquely identify each Contact Method during an import.

If you would like new Contact Methods entered into this Contact field to have a default Order, type a number to indicate the order that this Contact Method should be displayed in the IS Directory.

☑ Web Visible

The Web Visible check box determines if this Contact Method can be accessed from the miTeamWeb and IS Web applications other than through User Settings or My Settings.

- **Select this check box if you would like new Contact Methods entered into this Contact field to be accessible from miTeamWeb and the IS Web by default."**
- **Clear this check box If you would like new Contact Methods entered into this Contact field to not be accessible from miTeamWeb and the IS Web by default.**

Note: If a listing is associated with an Agent ID, people logging into miTeamWeb or the IS Web with that Agent ID are able to access the listing's Contact Methods through the User Settings or My Settings page, even if the Web Visible check box is cleared.

Saving Your Entries

To save your property entries, click the Save button.

To continue setting up this directory Subject, click the Views tab.

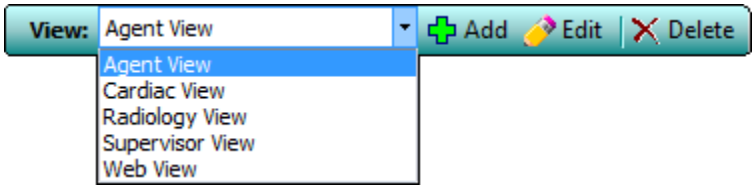
For more information about the Master Fields tab, refer to the "Directory Setup" section of the *Intelligent Series Supervisor Reference Guide*.

Adding Fields to a View

Views determine which fields appear in the directory when the directory is accessed by various groups of users in the Web Agent, Soft Agent, Infinity Telephone Agent, miTeamWeb, and IS Web applications. The Views feature allows certain pieces of information to be restricted from some Views while being displayed in other Views. In addition, the Views feature supports storing information in fields that are never shown in any View but exist for use in applications.

After adding Master Fields to a directory Subject, you must add those fields to each View in which you want those fields to appear.

To select a View, click the View menu and select the desired View.

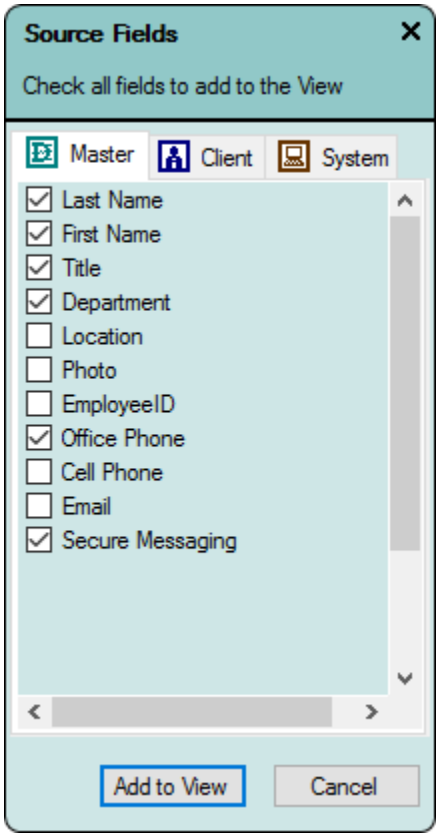


Information about the selected View is displayed.

To add fields to a View, click the Add icon on the View Fields toolbar.

The Source Fields window is displayed.

The IS Supervisor application provides three different types of fields for use in constructing a View: Master, Client, and System. Each of these types of fields is represented by a tab on the Source Fields window.



Master

Master Fields are the fields created for this directory Subject on the Master Fields page.

Select the check box next to each Master Field that you want to add to the View.

Click the "Add to View" button.

View Field Properties

View Field Properties determine how the fields are displayed in a View.

To edit the View Field Properties, select a field in the View Fields menu.

The properties for that field are displayed in the View Field Properties pane.

After making changes to the View Field Properties, click the Save button.

Adding Secure Messaging Contact Methods to a Listing

The Listings page allows you to see a directory Subject as it appears to agents in the Web Agent, Soft Agent, Infinity Telephone Agent, miTeamWeb, and IS Web applications.

When the Contacts Subject option is enabled for a directory Subject, Contact Methods can be created for each directory listing.

Listings Tab

The Listings tab on the Listings page allows you to see a directory Subject as it appears to agents in the Web Agent, Soft Agent, Infinity Telephone Agent, miTeamWeb, and IS Web applications. From the Listings tab, you can enter information into the directory, assign roles to contacts, set up Contact Methods, and create Status Schedules.

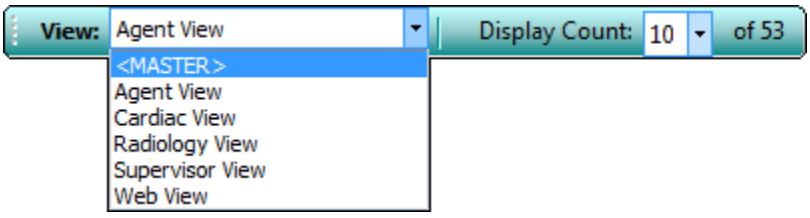
A listing can be added from any View provided the Permission Group that you belong to has Add rights for that View.

To add a listing to the directory, click the Add icon.

All Master Fields for the selected Subject are displayed in the Listing Properties pane.

Editing a listing is best done from Master View if you have rights to edit in Master View because Master View contains all of the Master Fields. If you edit a listing in a View other than Master View, you will only be allowed to edit the fields whose Edit property is enabled in View Field Properties.

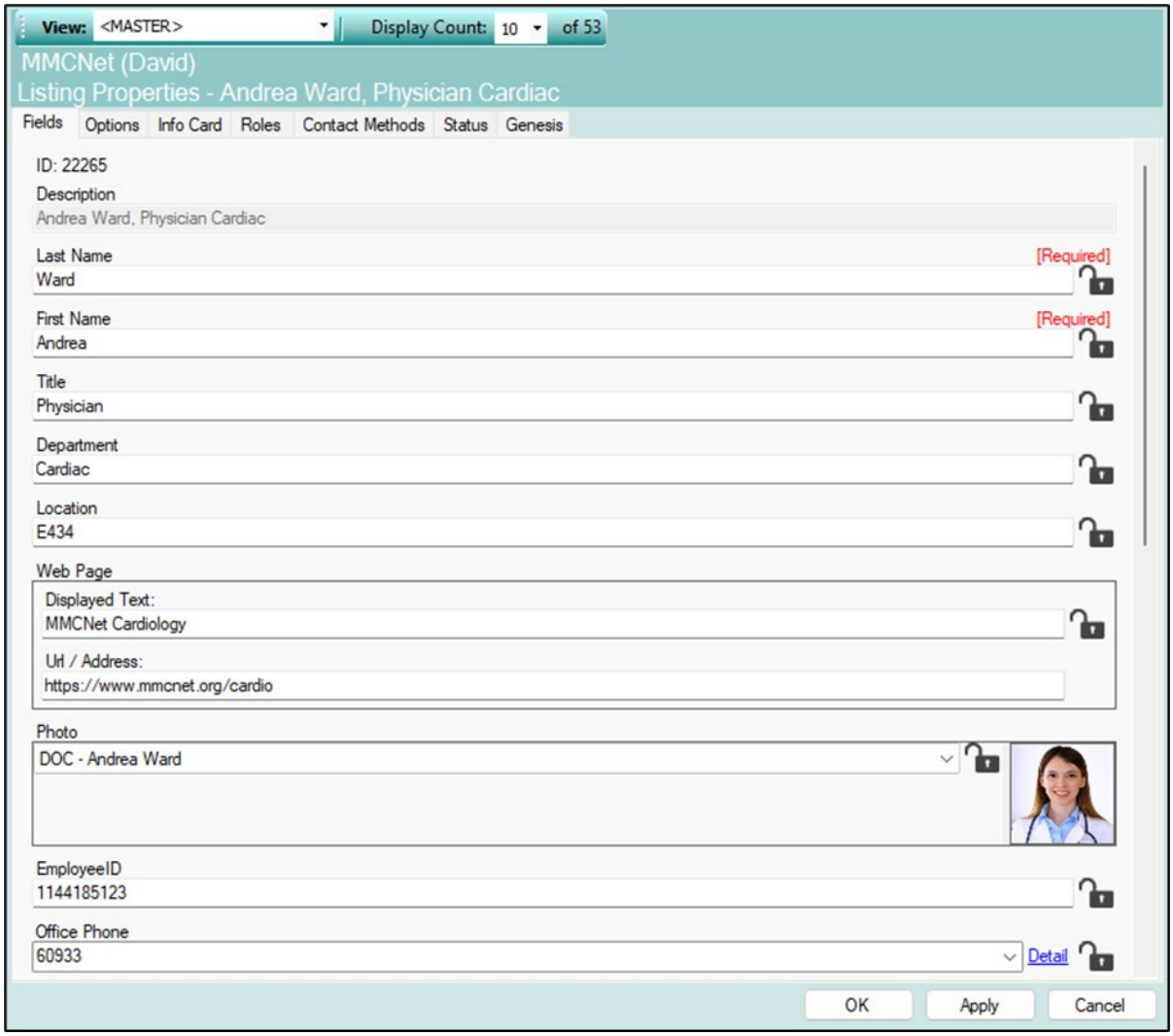
To edit a listing in the directory, select the Master View or another View for which Edit rights have been assigned to the fields that you need to edit.



Select the listing in the menu of listing Descriptions or the table of listing fields and then click the Edit icon.

All viewable fields for the selected View are displayed in the Listing Properties pane.

Listing Properties



The Listing Properties pane is used to add and edit information about a directory listing.

The properties are divided into tabs based on the options that are enabled.

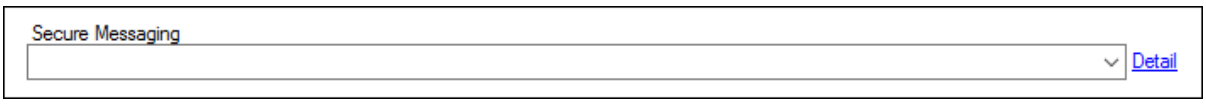
Fields

The Fields tab is used to add or edit information about a directory listing.

Click the Fields tab to display the directory fields.

When a listing is being added, all Master Fields for the selected Subject are displayed under the Fields tab. When a listing is being edited, only the fields that are marked Viewable in the View Field Properties for the selected View are displayed.

Contact Secure Messaging ID Fields



If a field has a Data Type of Contact Secure Messaging ID, a menu is displayed along with a Detail hyperlink.

To use a Secure Messaging Contact Method that has already been created for this listing, open the menu and select the name of the Contact Method.

OR

To create a new Contact Method, click the Detail hyperlink.

Clicking the Detail hyperlink displays the Contact fields for the Contact Secure Messaging ID field.

Contact Name

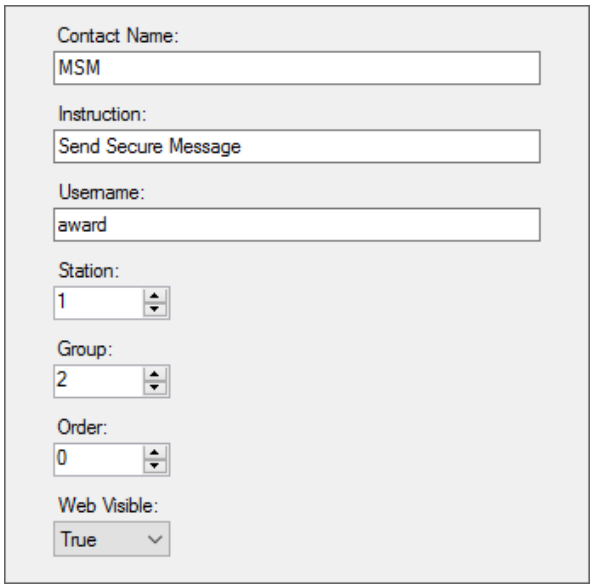
The Contact Name field identifies the Contact Method in the IS Directory and in the Dispatching window.

Type a short, descriptive name for the Contact Method, like "Secure Message."

Instruction

The contents of the Instruction field are displayed to agents in the Contact Methods section of the IS Directory and in the Dispatching window.

Type any special instructions for the use of this Contact Method.



Username

An Amtelco Secure Messages Username can be used to send a secure message to an Amtelco Secure Messages Contact Web user and all of a contact's devices that are registered with the Amtelco Secure Messages App.

Enter the Username of the contact as configured in the user's Amtelco Secure Messages App and in the user's Contact Settings in the Amtelco Secure Messages Admin Web.

Station

The Station field is used to indicate which ASM Web Service to use on systems that have more than one ASM Web Service. It must match a Station Number configured for one of the MSM Connections in the System Setup pages of IS Supervisor.

Enter the Station Number of the ASM Web Service used by this contact.

◉ Legacy Mode

The Legacy Mode option is displayed when a Contact Secure Messaging ID field for a Contact Method created on an older version of IS Supervisor is selected. For newer Contact Methods, this option is not displayed.

In Legacy Mode, when a message is sent to an Amtelco Secure Messages user who has more than one Amtelco Secure Messages account, the message can be sent to the account with the lowest Group ID number or to an account with a specific Group ID.

To send messages to the user's account that has the lowest Group ID, select the Legacy Mode option.

More information about Group IDs is provided in the *Amtelco Secure Messages Admin Web Guide*.

◉ Specific Group

The Specific Group option is displayed when a Contact Secure Messaging ID field for a Contact Method created on an older version of IS Supervisor is selected. For newer Contact Methods, this option is not displayed but is selected by default.

In Specific Group mode, when a message is sent to an Amtelco Secure Messages user who has more than one Amtelco Secure Messages account, the message can be sent to the account with the lowest Group ID number or to an account with a specific Group ID.

To send messages to an Amtelco Secure Messages account that has a specific Group ID, select the Specific Group option.

Group

The Group field is displayed when a Contact Secure Messaging ID field set to Specific Group mode is selected. The Group indicates the Group ID of the Amtelco Secure Messages account to message using this Contact ID field.

Type or use the up arrow ▲ or down arrow ▼ buttons to select the Group ID of the Amtelco Secure Messages account.

More information about Group IDs is provided in the *Amtelco Secure Messages Admin Web Guide*.

Order

The Order field determines which Contact Method is displayed first in the IS Directory when more than one of the same type of Contact Method is displayed. The Order field is also used with the IS Transformer feature to uniquely identify each Contact Method during an import.

Type a number or select a number with the up arrow ▲ or down arrow ▼ buttons to indicate the order that this Contact Method should be displayed in the IS Directory.

Web Visible

The Web Visible field determines if this Contact Method can be accessed from the miTeamWeb and IS Web applications other than through User Settings or My Settings.

If you would like new Contact Methods entered into this Contact field to be accessible from miTeamWeb and the IS Web by default, select "True."

OR

If you would like new Contact Methods entered into this Contact field to not be accessible from miTeamWeb and the IS Web by default, select "False."

Note: If a listing is associated with an Agent ID, people logging into miTeamWeb or the IS Web with that Agent ID are able to access the listing's Contact Methods through the User Settings or My Settings page, even if Web Visible is set to "False."

Saving Your Entries

After you have finished entering or editing field information, click the Apply button to save your entries.

OR

Click the OK button to save your entries and close the Listing Properties pane.

OR

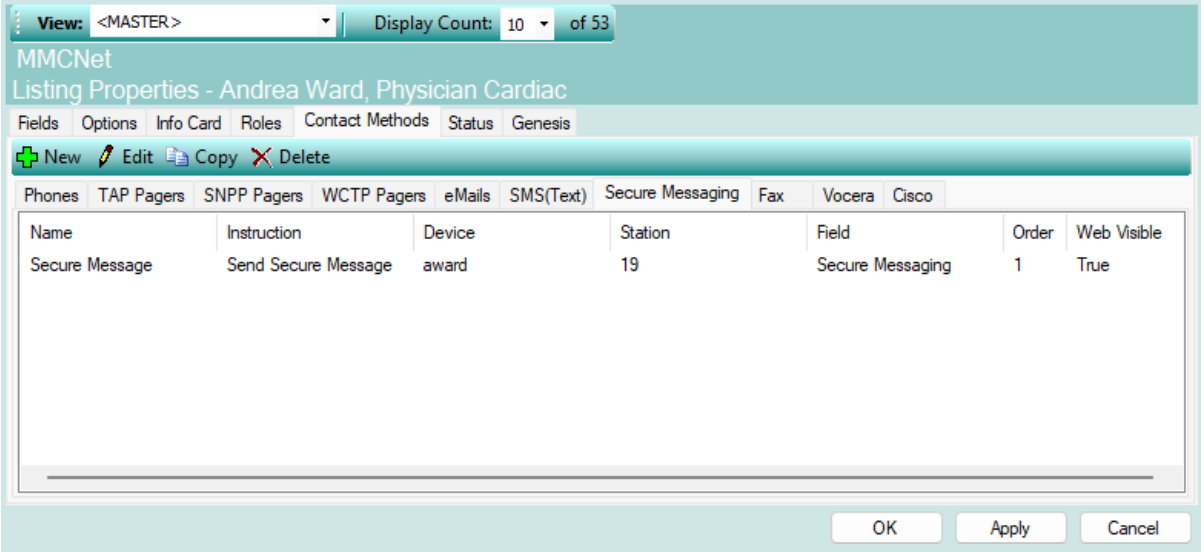
Click the Cancel button to discard your changes and close the Listing Properties pane.

For more information about the Fields tab, refer to the "Directory Setup" section of the *Intelligent Series Supervisor Reference Guide*.

Contact Methods

The Contact Methods tab is used to create additional Contact Methods for the selected listing. These Contact Methods do not have to be associated with a directory field, but are available for dispatching from the IS Directory and Intelligent Message scripts. All Contact Methods that are created under the Fields tab are displayed under the Contact Methods tab, and all Contact Methods created under the Contact Methods tab can be assigned to fields of a matching Data Type.

Click the Contact Methods tab to display the Contact Methods.



The Contact Methods settings are divided into tabs for each type of Contact Method.

To create, edit, or view Secure Messaging Contact Methods, click the tab labeled "Secure Messaging."

All of the listing's Secure Messaging Contact Methods are displayed in a table.

Contact Methods Toolbar

The Contact Methods Toolbar is used to add, edit, copy, and delete Contact Methods.

Icon	Description
	The **New** icon is used to add a new Contact Method.
	The **Edit** icon is used to edit the properties for the selected Contact Method.
	The **Copy** icon makes a copy of the selected Contact Method.
	The **Delete** icon removes the selected Contact Method.

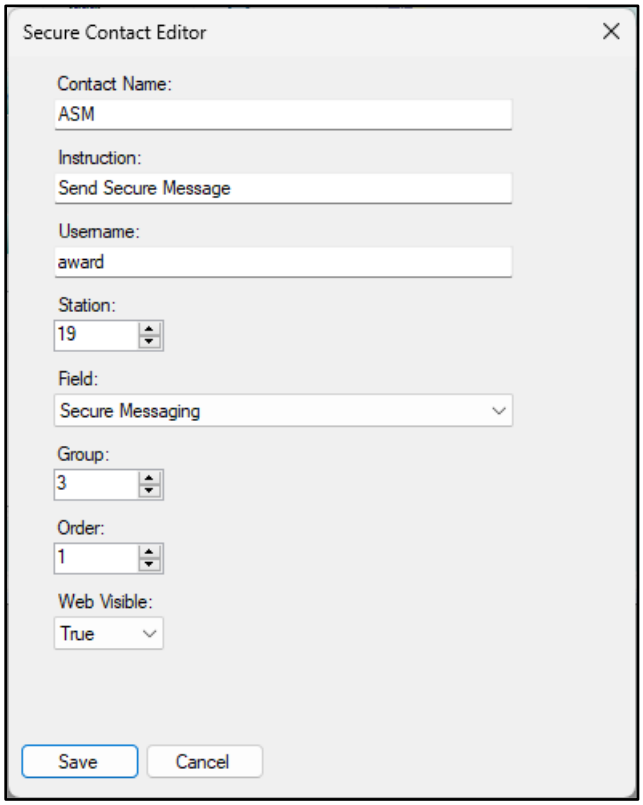
Adding or Editing a Contact Method

- **To add a Contact Method, click the New icon on the Contact Methods Toolbar.**
- **To edit the properties for a Contact Method, select the Contact Method and then click the Edit icon on the Contact Methods Toolbar.**

The editor window for the selected Contact Method tab is displayed.

Secure Message Contact Editor

The Secure Message Contact Editor window is displayed when adding or editing a Secure Messaging Contact Method.



Contact Name

The Contact Name field identifies the Contact Method in the IS Directory and in the Dispatching window.

Type a short, descriptive name for the Contact Method, like “Secure Message.”

Instruction

The contents of the Instruction field are displayed to agents in the Contact Methods section of the IS Directory and in the Dispatching window.

Type any special instructions for the use of this Contact Method.

Username

An Amtelco Secure Messages Username can be used to send a secure message to an Amtelco Secure Messages Contact Web user and all of a contact’s devices that are registered with the Amtelco Secure Messages App.

Enter the Username of the contact as configured in the user’s Amtelco Secure Messages App and in the user’s Contact Settings in the Amtelco Secure Messages Admin Web.

Station

The Station field is used to indicate which ASM Web Service to use on systems that have more than one ASM Web Service. It must match a Station Number configured for one of the MSM Connections in the System Setup pages of IS Supervisor.

Enter the Station Number of the ASM Web Service used by this contact.

Field

The Field menu contains a list of Master Fields that have a Data Type of Contact Secure Messaging ID. If any fields are listed, the Username assigned to this Contact Method can be displayed in one of those fields.

To display the Username in a directory field, select the name of the appropriate field.

◉ Legacy Mode

The Legacy Mode option is displayed when a Secure Messaging Contact Method created on an older version of IS Supervisor is edited. For newer Contact Methods, this option is not displayed.

In Legacy Mode, when a message is sent to an Amtelco Secure Messages user who has more than one Amtelco Secure Messages account, the message can be sent to the account with the lowest Group ID number or to an account with a specific Group ID.

To send messages to the user's account that has the lowest Group ID, select the Legacy Mode option.

More information about Group IDs is provided in the *Amtelco Secure Messages Admin Web Guide*.

◉ Specific Group

The Specific Group option is displayed when a Secure Messaging Contact Method created on an older version of IS Supervisor is selected. For newer Contact Methods, this option is not displayed but is selected by default.

In Specific Group mode, when a message is sent to an Amtelco Secure Messages user who has more than one Amtelco Secure Messages account, the message can be sent to the account with the lowest Group ID number or to an account with a specific Group ID.

To send messages to an Amtelco Secure Messages account that has a specific Group ID, select the Specific Group option.

Group

The Group field is displayed when a Contact Secure Messaging ID field set to Specific Group mode is selected. The Group indicates the Group ID of the Amtelco Secure Messages account to message using this Contact Method.

Type or use the up arrow ▲ or down arrow ▼ buttons to select the Group ID of the Amtelco Secure Messages account.

More information about Group IDs is provided in the *Amtelco Secure Messages Admin Web Guide*.

Order

The Order field determines which Contact Method is displayed first in the IS Directory when more than one of the same type of Contact Method is displayed. The Order field is also used with the IS Transformer feature to uniquely identify each Contact Method during an import.

Type a number or select a number with the up arrow or down arrow buttons to indicate the order that this Contact Method should be displayed in the IS Directory.

Web Visible

The Web Visible field determines if this Contact Method can be accessed from the miTeamWeb and IS Web applications other than through User Settings or My Settings.

If you would like new Contact Methods entered into this Contact field to be accessible from miTeamWeb and the IS Web by default, select "True."

OR

If you would like new Contact Methods entered into this Contact field to not be accessible from miTeamWeb and the IS Web by default, select "False."

Note: If a listing is associated with an Agent ID, people logging into miTeamWeb or the IS Web with that Agent ID are able to access the listing's Contact Methods through the User Settings or My Settings page, even if Web Visible is set to "False."

When you have finished setting the Contact Method properties, click the Save button to save the settings and close the Secure Message Contact Editor window.

OR

Click the Cancel button to discard your changes and close the Secure Message Contact Editor window.

Saving Your Entries

After you have finished entering or editing Contact Method information, click the Apply button to save your entries.

OR

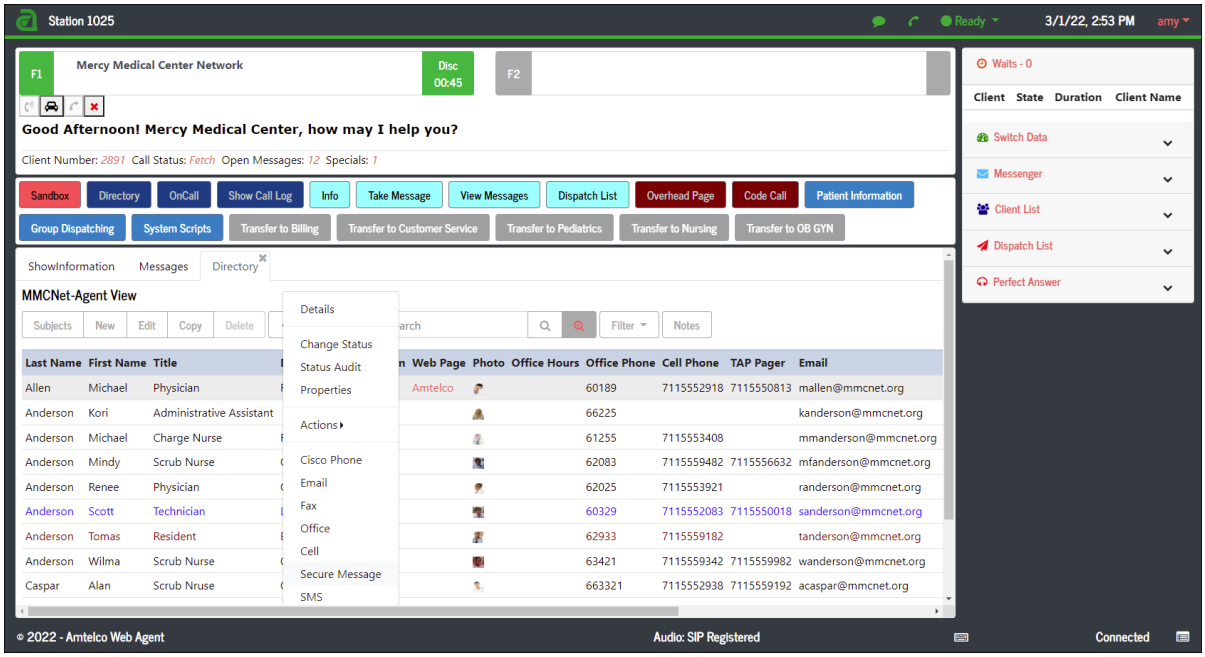
Click the OK button to save your entries and close the Listing Properties pane.

OR

Click the Cancel button to discard your changes and close the Listing Properties pane.

Sending a Secure Message from Web Agent

Secure Messaging Contact Methods can be used to send secure messages from the IS Directory or an IS OnCall schedule in the Web Agent application.



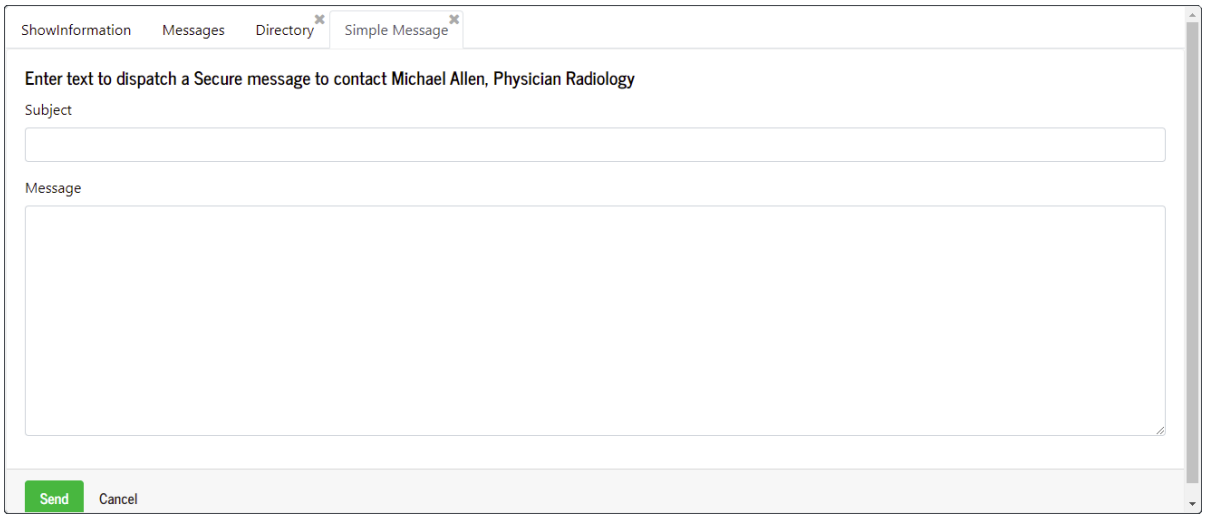
To send a secure message, right-click the listing or resource that you want to contact.

A context menu is displayed.

Click the Contact Name of a Secure Messaging Contact Method.

A simple message script is displayed.

The simple message script contains a Subject field, a Message field, a send button, and a Cancel button.



Subject

Type your message subject in the Subject field.

Message

Type your message in the Message field.

To send the message, click Send.

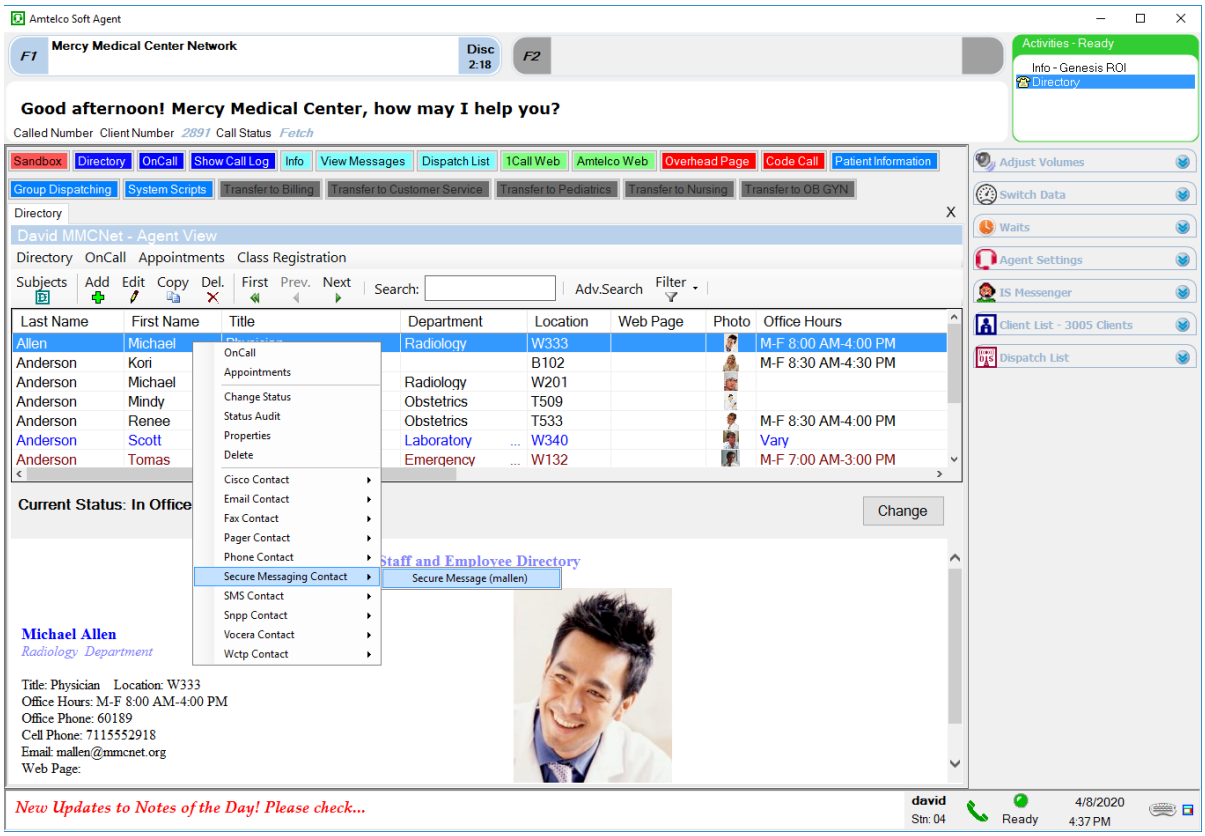
OR

To discard the message, click Cancel.

Secure Messages also can be sent from Intelligent Message scripts using the Contact Dispatch and Contact Send Secure Message response elements. More information about response elements is provided in the “Response Element Library” section of the *Intelligent Series Supervisor Reference Guide*.

Sending a Secure Message from Soft Agent

Secure Messaging Contact Methods can be used to send secure messages from the IS Directory or an IS OnCall schedule in the Soft Agent application.



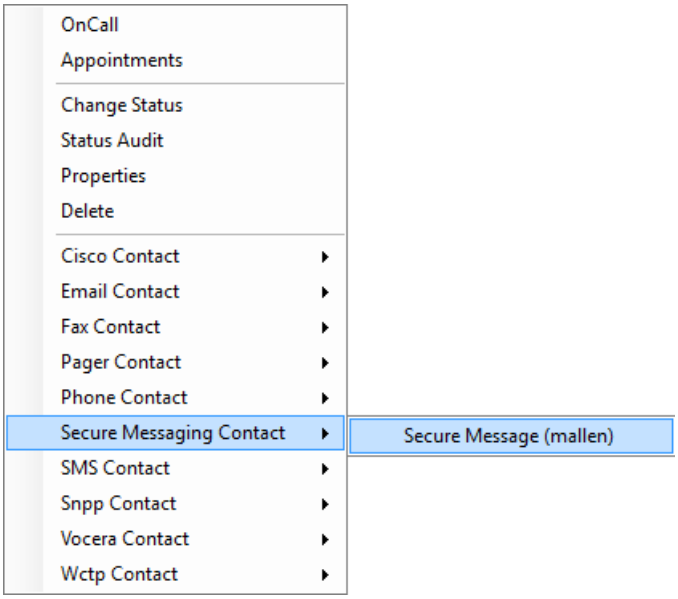
To send a secure message, right-click the listing or resource that you want to contact.

A context menu is displayed.

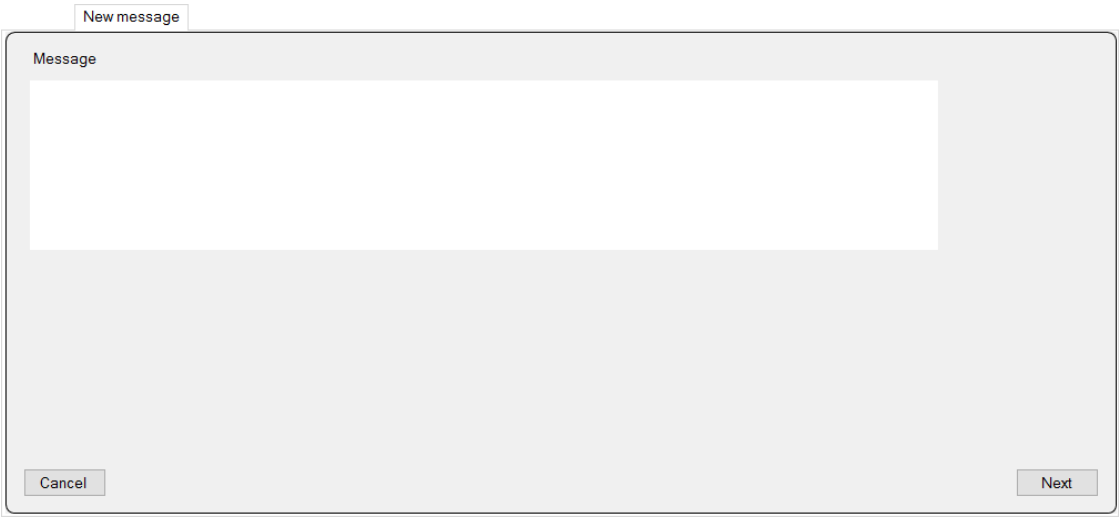
Point to "Secure Messaging Contact" to display a pop-out menu of the listing's Secure Messaging Contact Methods.

Click the name of a Secure Messaging Contact Method.

A simple message script is displayed.



The simple message script contains a Message field, a Cancel button, and a Next button.



Message

Type your message in the Message field.

To send the message, click the Next button.

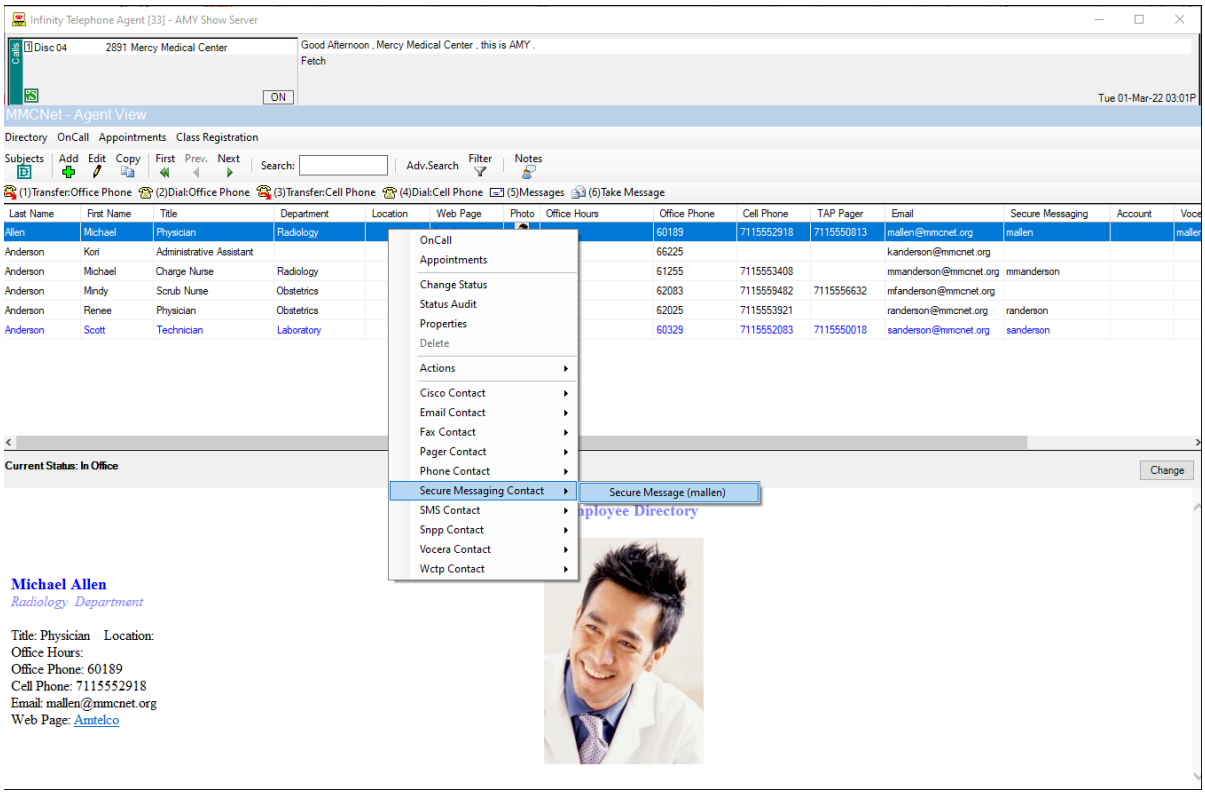
OR

To discard the message, click the Cancel button.

Secure Messages also can be sent from Intelligent Message scripts using the Contact Dispatch and Contact Send Secure Message response elements. More information about response elements is provided in the “Response Element Library” section of the *Intelligent Series Supervisor Reference Guide*.

Sending a Secure Message from Infinity Telephone Agent

Secure Messaging Contact Methods can be used to send secure messages from the IS Directory or an IS OnCall schedule in the Infinity Telephone Agent application.



To send a secure message, right-click the listing or resource that you want to contact.

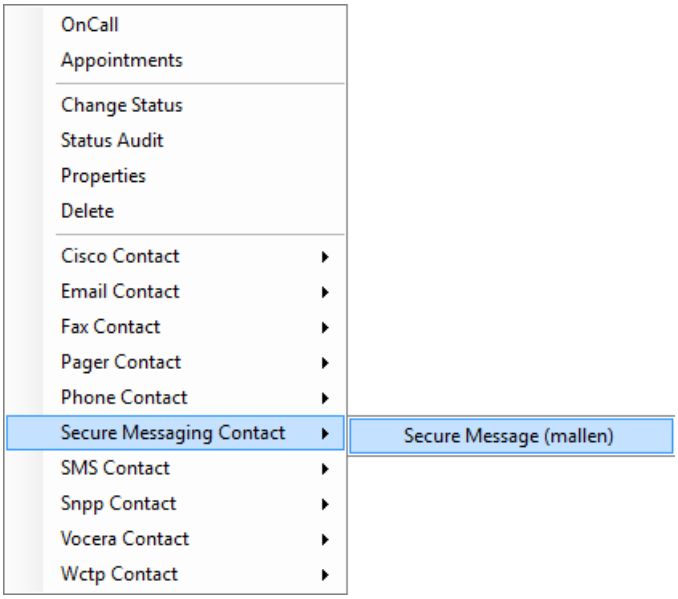
A context menu is displayed.

Point to "Secure Messaging Contact" to display a pop-out menu of the listing's Secure Messaging Contact Methods.

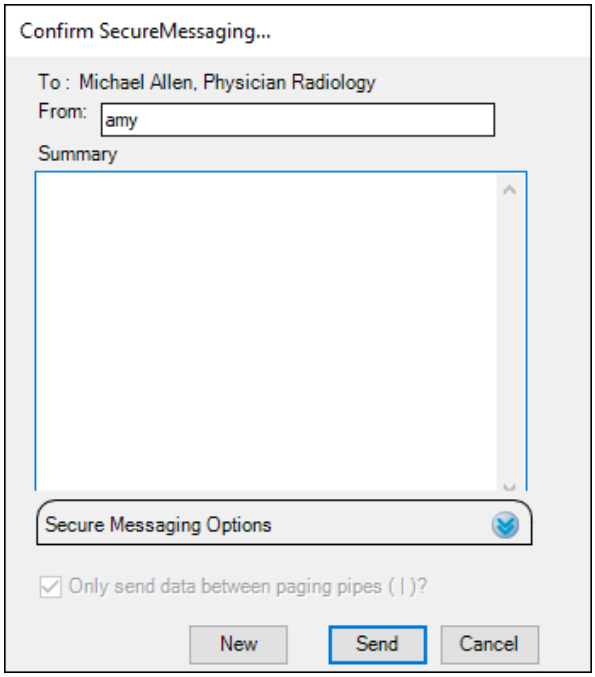
Click the name of a Secure Messaging Contact Method.

The Confirm SecureMessaging pop-up window is displayed.

The Confirm SecureMessaging window contains a From field, a Summary field, Secure Messaging



Options, and New, Send, and Cancel button.



If the Confirm SecureMessaging pop-up window is displayed, click the New button to start a new message.

Summary

Type your message in the Summary field.

To send the message, click Send.

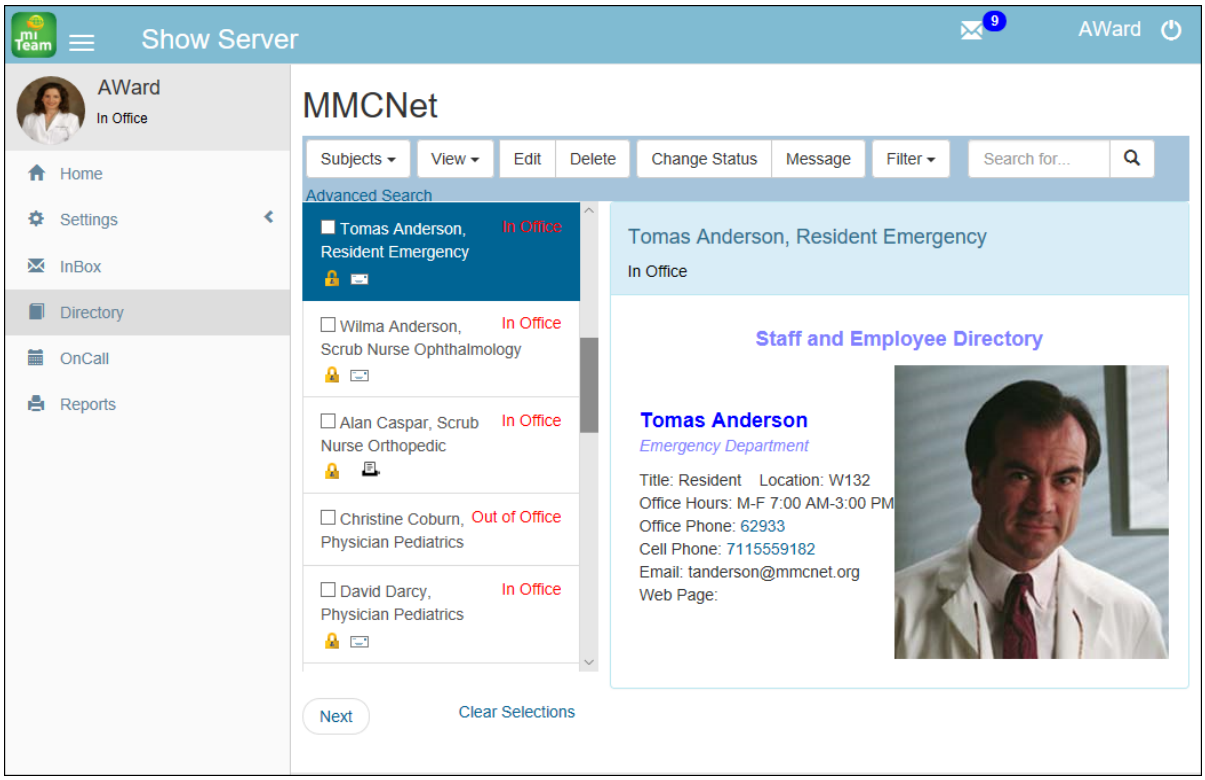
OR

To discard the message, click Cancel.

Secure Messages also can be sent from Intelligent Message scripts using the Contact Dispatch and Contact Send Secure Message response elements. More information about response elements is provided in the "Response Element Library" section of the *Intelligent Series Supervisor Reference Guide*.

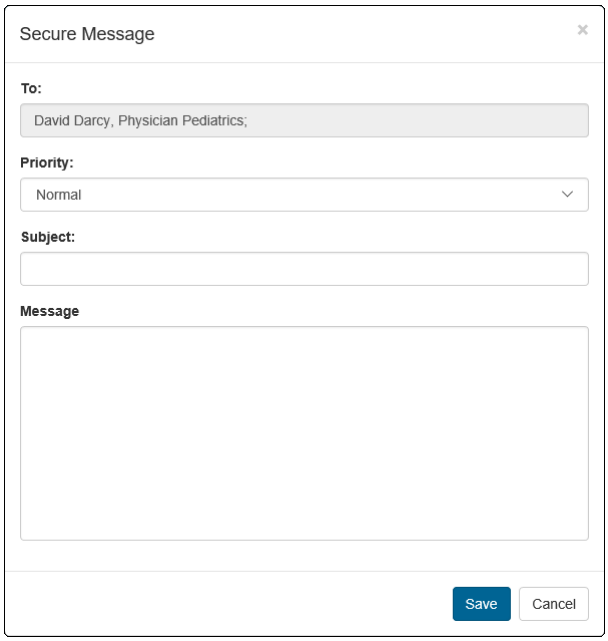
Sending a Secure Message from miTeamWeb or IS Web

In the miTeamWeb and IS Web applications, Secure Messaging Contact Methods can be activated by clicking the Secure Message icon in one of the Directory or OnCall widgets and pages.



To send a secure message, click the Secure Message icon next to the Listing Description of the listing or resource that you want to contact.

The Secure Message window is displayed.



Priority

The message priority can be set to either Normal, High, or Low. The default for message priority is Normal.

- **To mark a message as urgent, click the Priority menu and select "High."**
- **To mark a message as low priority, click the Priority menu and select "Low."**

Subject

Below the Priority menu is the Subject field.

Type the desired subject into the Subject field.

Message

Type your message into the Message field.

If you are using miTeamWeb, click the Save button to send the message.

OR

If you are using IS Web, click the Send button to send the message.

More information about the miTeamWeb application is provided in the *miTeamWeb User Guide*.

More information about the IS Web application is provided in the "Directory" and "OnCall" sections of the *IS Web User Guide*.

Configuring Protected Dialing through Genesis

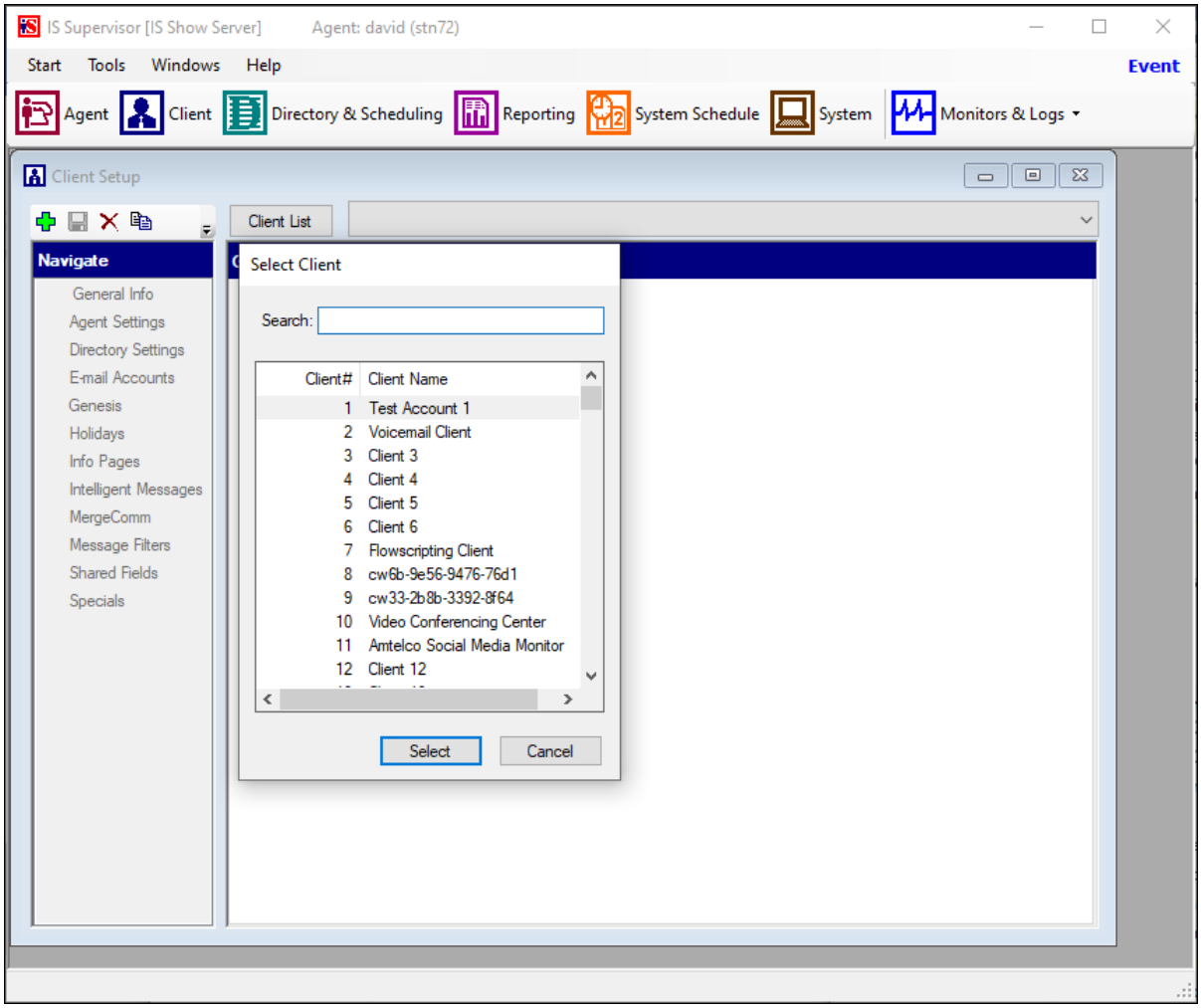
The optional Protected Dialing feature allows phone calls placed from the Amtelco Secure Messages app to be routed through Genesis, enabling users to keep their personal device's phone number private and to display their call center or organization's phone number.

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.

In order to use the Protected Dialing feature, an Intelligent Series (IS) Client must be configured for a Direct Inward Dialing (DID) number and the Protected Dialing behavior in the IS Supervisor application.

Click the Client icon  on the IS Supervisor Toolbar.

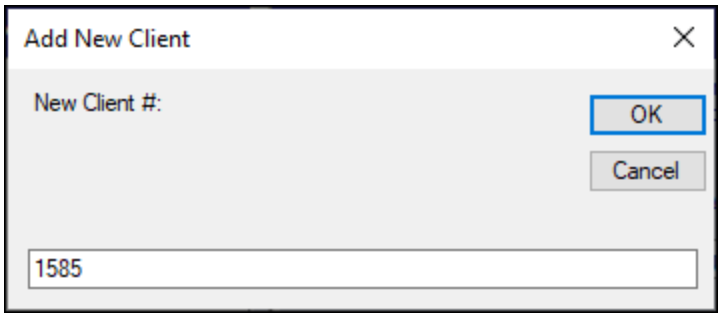
The Select Client window is displayed.



Click the Cancel button to close the Select Client window.

Click the Add icon ✚ in the Client Setup Toolbar.

The Add New Client window is displayed.



New Client

Each Client must have a unique Client Number. This Client Number can be the client's phone number or another unique identifier.

Enter the client's phone number or another unique number that will identify this Client, and then click the OK button.

The General Info settings for the new Client are displayed.

Client Name

The Client Name is a text name used to identify the Client to the agents and supervisors.

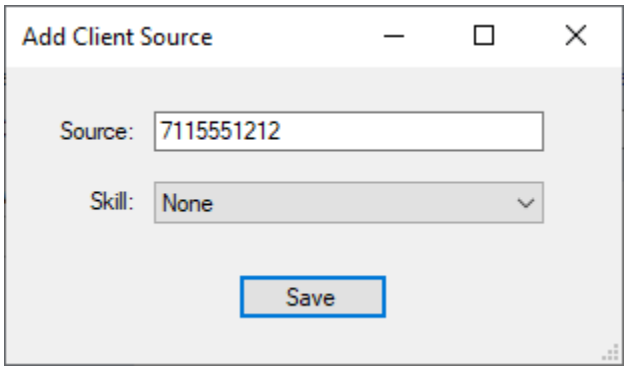
Enter a name for the Client.

Sources

The Sources setting is available on systems that have one or more Web Agent or Soft Agent licenses. Sources are the port numbers on which calls come into the Web Agent and Soft Agent applications for this Client. Each Client should have one or more unique source numbers so that the Intelligent Series server knows which calls to route to that Client.

To add a source number, click the Add icon.

The Add New Source window appears.



Source

Type the source number that you want to assign to this Client. Then click the OK button.

The source number is added to the menu of sources.

Skill

The Skill menu is used to select an ACD Skill to assign to calls that come in from this source. Since calls that come into this source will not be handled by an operator, Skill should be set to "None."

Select "None."

Click the Save button.

DID Limit

The DID (Direct Inward Dialing) Limit on the General Info page puts a limit on the number of live calls that can be in the system for this Client at one time. IS will return a busy signal for any calls for this Client that exceed the DID Limit. The ideal DID Limit will depend on the number of trunks on your system and how many trunks you need to leave free for other types of calls.

Enter the number of live calls to allow in the system for this Client.

To save changes that you made to the Client, click the Save icon in the Client Setup Toolbar.

Protected Dialing Behavior

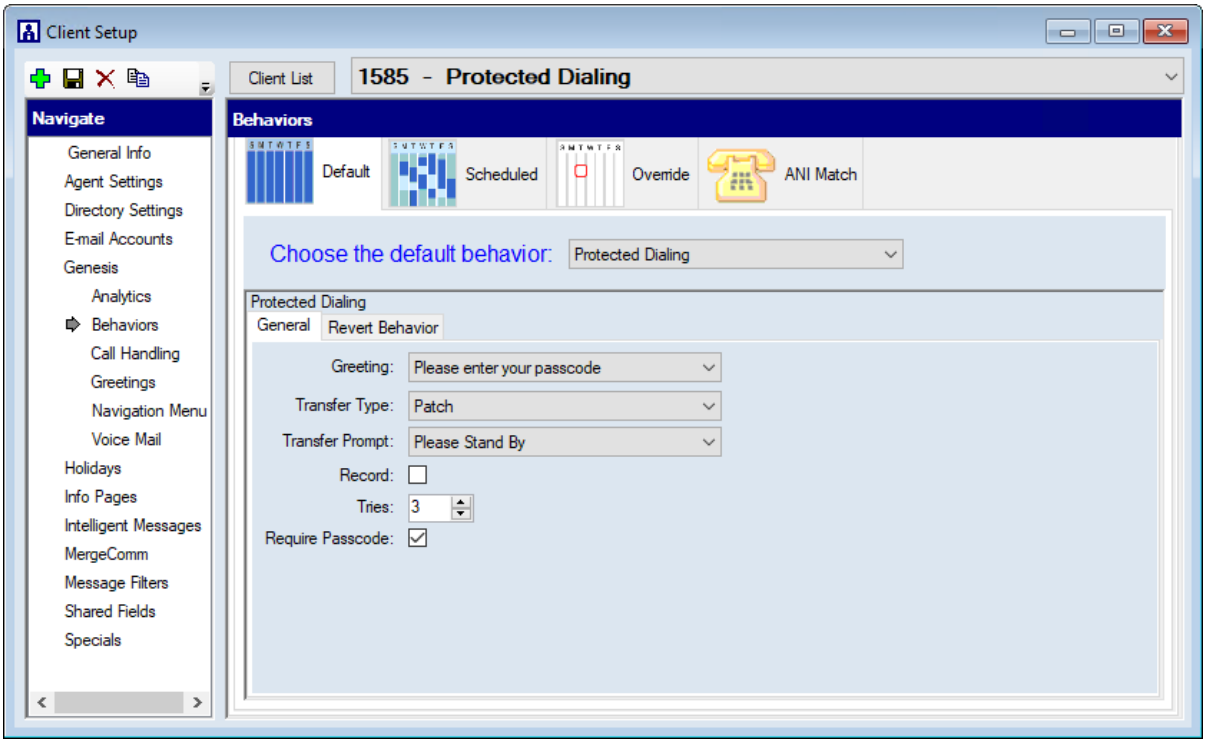
When users call into a Client with the Protected Dialing behavior, IS prompts the caller to enter a phone number and then transfers the call to the entered phone number. IS changes the Automated Number Identification (ANI) information to the Client's Caller Name and Caller ID phone number programmed under the Outbound tab on the Genesis Call Handling page. This behavior can be configured to require a password to be entered before asking for a phone number.

To open the Behaviors page, follow these steps:

On the Client Setup Navigation Menu, click the Genesis hyperlink.

Click the Behaviors hyperlink.

The Behaviors page is displayed.



The Behavior settings are divided into tabs for default behavior, scheduled behaviors, override behaviors, and ANI Match behavior.

Click the Default tab if it is not already selected.

Choose the Default Behavior

Click the menu and select the "Protected Dialing" behavior.

The Protected Dialing Behavior settings are displayed.

Greeting

If the "Require Passcode" check box is selected, a recorded greeting can be played. The greeting should prompt the caller to enter the passcode.

If you will be using the "Require Passcode" option, select the name of the greeting that will prompt the callers to enter the passcode.

OR

Select "Silence" to skip playing a passcode prompt.

Greetings can be recorded and saved to IS from the Greetings page.

Transfer Type

The Transfer Type property determines the type of transfer that is performed.

- If the Transfer Type is set to "Blind," the caller is transferred to the phone number and the call is removed from Genesis. After the transfer, the trunk is available for other calls.
- If the Transfer Type is set to "Patch," the caller is connected to the phone number and the call remains in Genesis. With this Transfer Type, the trunk remains in use for the entire duration of the call, which prevents the trunk from being used for other calls.

Select the type of transfer to perform.

Transfer Prompt

A prompt can be played to the caller before the call is transferred.

- **Select "None" to skip playing a transfer prompt.**
- **Select "Hold For" to have Genesis play, "Please hold for.".**
- **Select "Please Stand By" to have Genesis play, "Please stand by."**
- **Select "Transfer Op" to have Genesis play, "Please hold while your call is being transferred."**

☑ Record

The Record option records the calls and stores the recordings in the IS Call Log.

To record calls placed using the Protected Dialing behavior, select the "Record" check box.

Tries

When the caller is prompted, "Please enter a phone number followed by the pound key," the Tries setting determines the number of times a caller can attempt to enter digits.

After the prompt plays, the caller has three seconds to enter valid digits. If the caller enters invalid digits or takes longer than three seconds to enter digits, one try expires and the prompt, "Please try again," is played. If the number of times a caller fails to enter valid digits exceeds the Tries value, the Revert Behavior is performed.

Enter the number of times to allow a caller to attempt to enter valid digits.

☑ Require Passcode

The Require Passcode check box, when selected, requires the caller to enter the password specified in the Protected Dialing Passcode field. If a greeting is selected in the Greeting field, the greeting is played first, and then Genesis listens for the caller to enter digits. If the incorrect passcode is entered, the Revert Behavior is performed.

The Protected Dialing Passcode field is located on the Voice Mail page of Client Setup under the General tab.

Select this check box to play the Greeting and require callers to enter the Protected Dialing passcode.
OR
Clear this check box to skip the Greeting and not require a passcode.

Revert Behavior

The Revert Behavior tab is used to specify which behavior a call reverts to if the caller enters the wrong passcode or exceeds the number of tries to enter a phone number.

Behavior

The Behavior setting determines the call behavior that is performed if the caller enters the wrong passcode or exceeds the number of tries to enter a phone number.

More information about behaviors is provided in the "Behaviors" section of the *Intelligent Series Supervisor Reference Guide*.

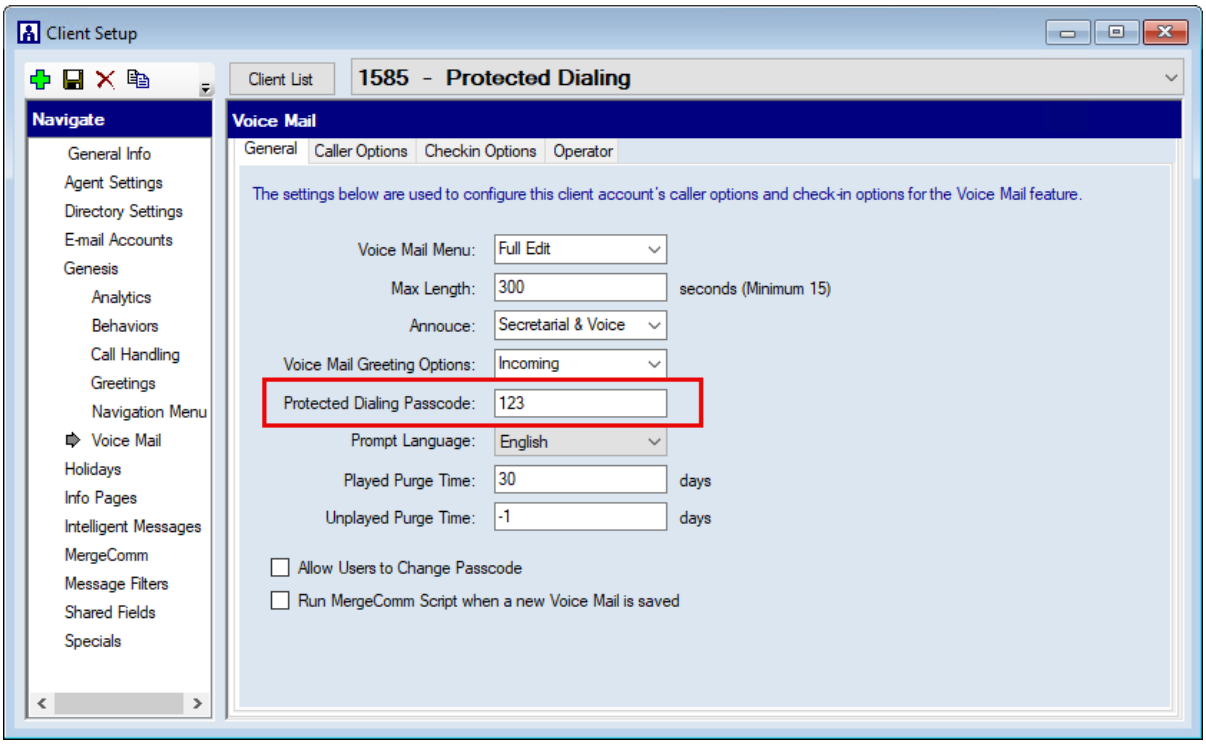
When you have finished configuring the Protected Dialing Behavior settings, click the Save icon in the Client Setup Toolbar.

Protected Dialing Passcode

If you selected the Require Passcode check box, the Protected Dialing Passcode field must be configured on the Voice Mail page of Client Setup under the General tab.

On the Client Setup Navigation Menu, click the Voice Mail hyperlink.

The General page is displayed.



Protected Dialing Passcode

The Passcode field is used to specify the passcode that callers must provide in order to use the Protected Dialing feature.

Note: The Protected Dialing Passcode must be unique for each IS Client. The passcode that the Protected Dialing behavior receives determines which IS Client is billed for the call and what Caller ID is presented.

If you are using the "Require Passcode" feature, type the passcode that callers will be required to enter.

Adding Protected Dialing to a Group

Protected Dialing is enabled for individual Groups in the ASM Admin Web.

Log into the ASM Admin Web.

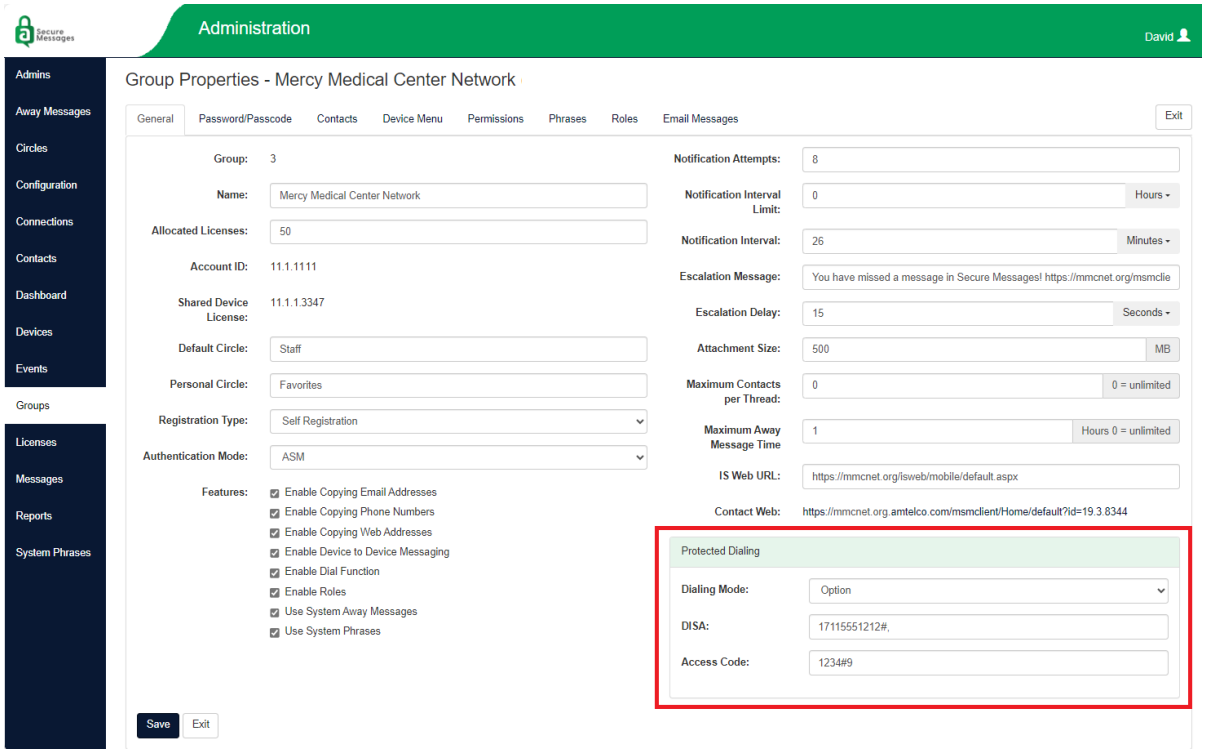
The Dashboard page is displayed. The ASM Admin Web Navigation Menu is displayed on the left side of the page.

Click the Groups command in the navigation menu.

The Groups page is displayed.

Click the Edit hyperlink in the same row as the name of the group that you want to configure to use Protected Dialing.

The Group Properties are displayed.



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.

Dialing Mode

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

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.

Select Dialing Mode that you want to use (DISA or Option).

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.

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 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.

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 or Option

DISA#: 17115551212#,

Access Code: 1234#9

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

Configuring Role-Based Messaging

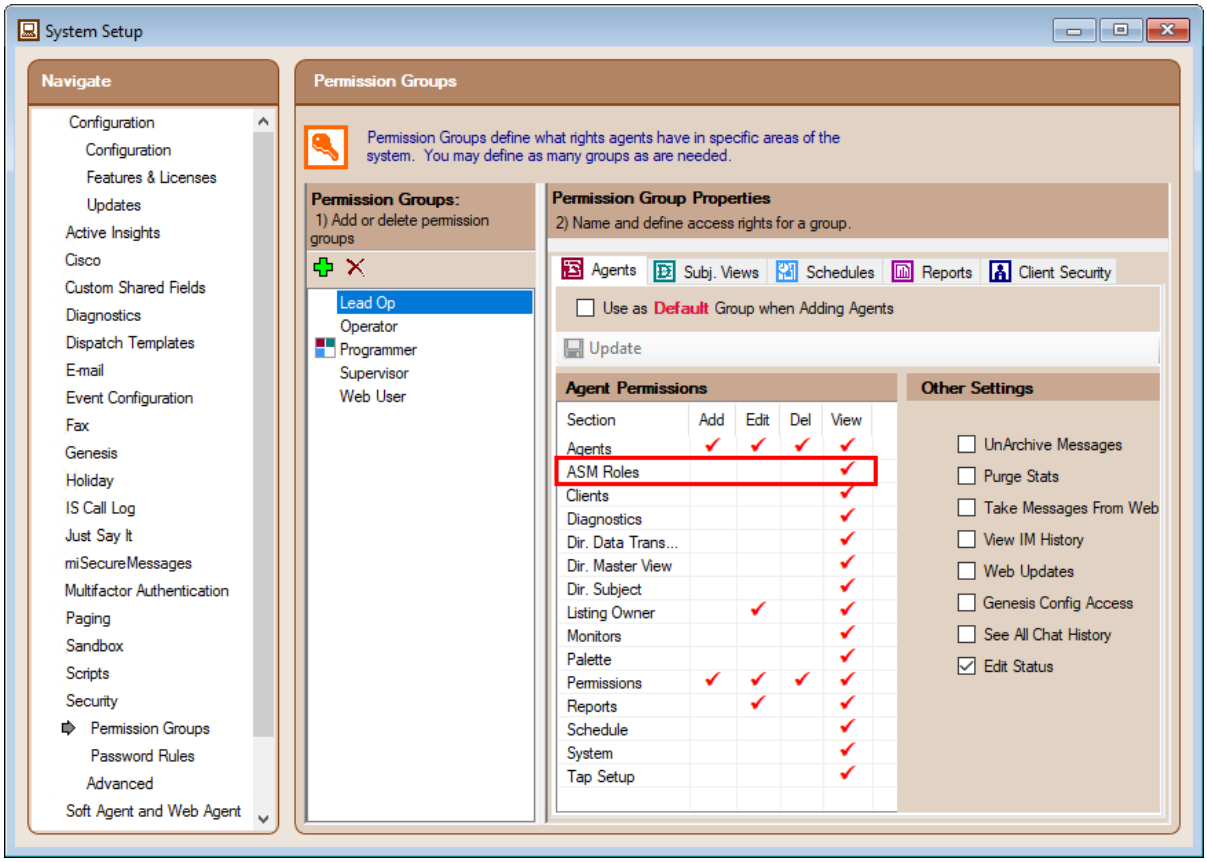
The optional Role-Based Messaging feature connects Amtelco Secure Messages roles to Intelligent Series (IS) OnCall schedules. With Role-Based Messaging, Amtelco Secure Messages users can retrieve assigned resources and Amtelco Secure Messages roles for on-call schedules, and can choose to send secure messages to a role or to individual contacts. Messages send to a role stay with the role instead of the user, allowing contact who cover that role in a later shift to follow up on those messages.

Several new settings have been added to Directory Setup that are used to connect Amtelco Secure Messages to IS on-call schedules for Role-Based Messaging.

Note: Role-Based Messaging requires Intelligent Series (IS) Server version 5.7 or later, IS Supervisor 5.7.8867.01 or later, the Role-Based Messaging feature, and the IS Directory OnCall feature.

Assigning Permissions for ASM Roles

The ASM Roles permission has been added to the Agent Permissions in the Security pages in System Setup. The ASM Roles property controls access to the Roles subtab under the Secure Messages tab in the Directory Setup Subject Properties.



To access Agent Permissions, click the Security hyperlink in the System Setup Navigation Menu.

If the Permission Groups page is not displayed, click the Permission Groups hyperlink.

Programmers who are responsible for setting up and managing roles used for the optional Role-Based Messaging feature need Add, Edit, Delete, and View permission to ASM Roles. To assign View permission to ASM Roles, follow these steps:

1. **Select a Permission Group in the Permission Groups list and then click the Client Agents tab.**

   The Agents settings for the selected Permission Group are displayed.

2. **Select the check box at the intersection of the View column and the ASM Roles row.**

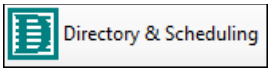
   A red checkmark is displayed in the clicked checkbox.

3. **To save your changes, click the Update icon on the Agents Toolbar.**

Repeat these steps for each Permission Group that needs to set up or manage Secure Messaging roles.

Connecting Amtelco Secure Messages to an IS Directory Subject

The Secure Messages tab has been added to the Subject Properties in Directory Setup. The settings under the Secure Messages tab are used to connect an Amtelco Secure Messages station and group to an IS Directory Subject to be used for Role-Based Messaging.

To open the IS Directory, click the Directory & Scheduling icon 

on the IS Supervisor Toolbar.

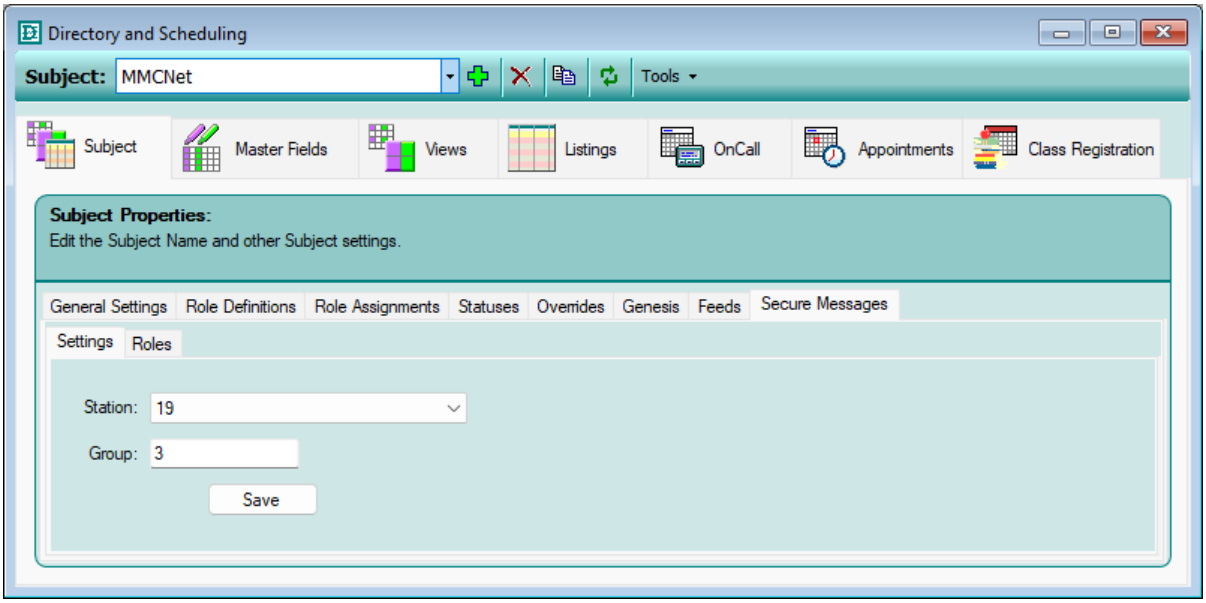
The Directory and Scheduling window is displayed.

To select a Subject, open the Subject menu and select the desired directory Subject.

The General Settings for the selected subject are displayed.

Click the Secure Messages tab.

The Settings and Roles subtabs are displayed. The Settings subtab is selected by default.



The settings under the Settings subtab are used to connect an ASM station and group to an IS Directory Subject to be used for Role-Based Messaging.

Station

The Station menu is used to select the Station Number of the ASM Web Service that you want to connect to this IS Directory Subject. It must match a Station Number configured for one of the MSM Connections in the System Setup pages of IS Supervisor.

Select the Station Number of the ASM Web Service that you want to connect to this IS Directory Subject for Role-Based Messaging.

Group

The Group field is used to specify the unique group number of the ASM group that you want to connect to this IS Directory Subject. The group number can be found on the Group Properties page of the Amtelco Secure Messages Admin Web.

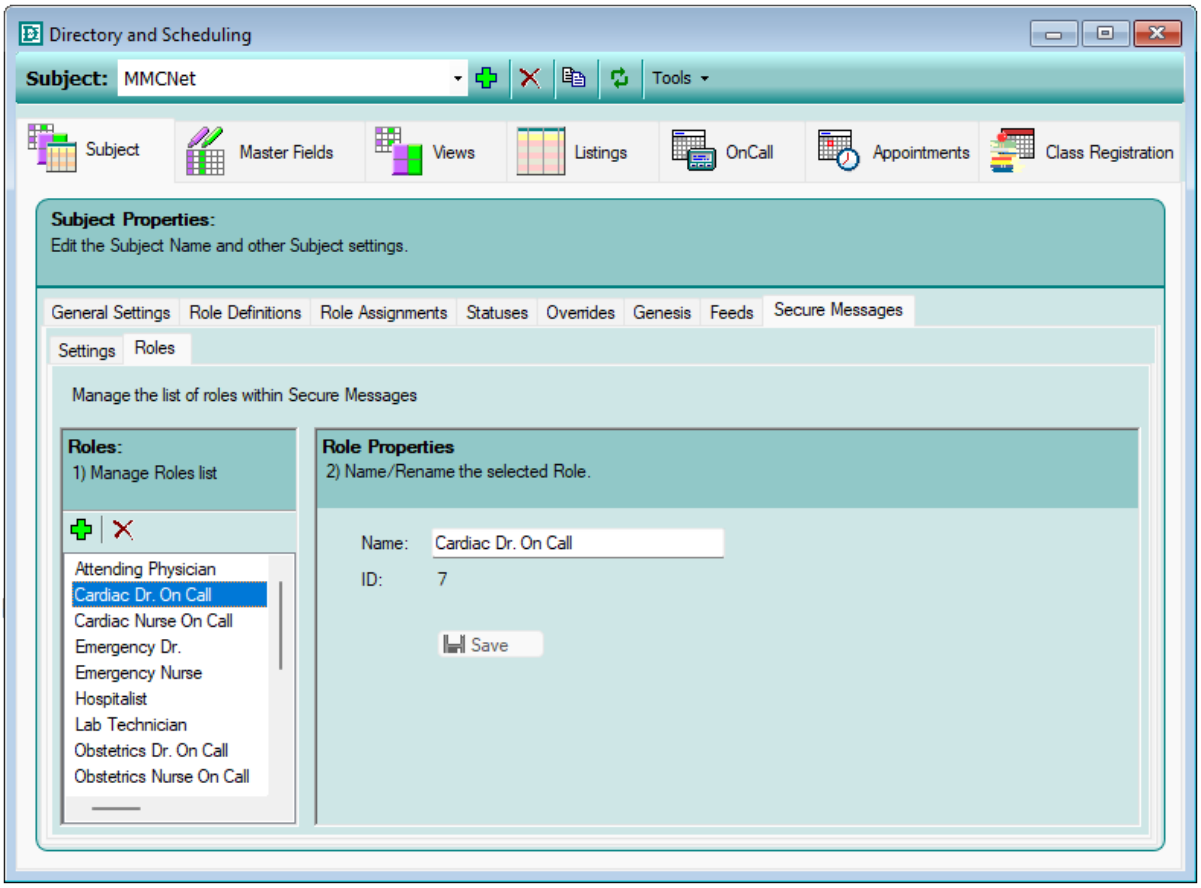
Enter the group number of the ASM group that you want to connect to this IS Directory Subject for Role-Based Messaging.

Saving Your Entries

When you have finished making changes to the settings, click the Save button.

Adding Secure Messages Roles to an IS Directory Subject

The settings under the Roles subtab are used to create, edit, and delete roles that are used with the optional Role-Based Messaging feature for the Amtelco Secure Messages Group and Station configured under the Settings subtab.



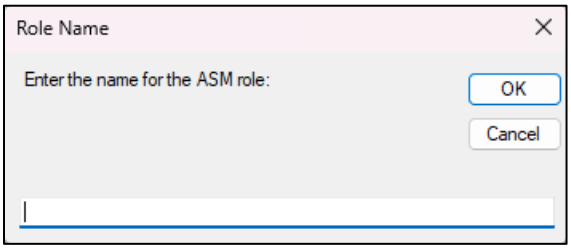
Click the Roles subtab.

The Roles and Role Properties panes are displayed.

Adding Roles

To add a role, click the Add icon.

The Role Name window is displayed with a blank Name field.



Enter a unique name for the role and then click the OK button.

Editing Roles

To edit a role, click the name of the role in the Roles List. The Role Properties for the selected role are displayed.

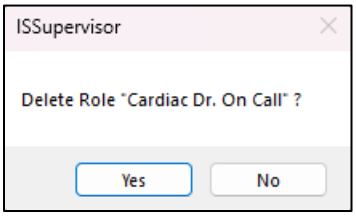
Name

The Name field is used to enter a unique name for the role.

Click the Save button to save your changes.

Removing Roles

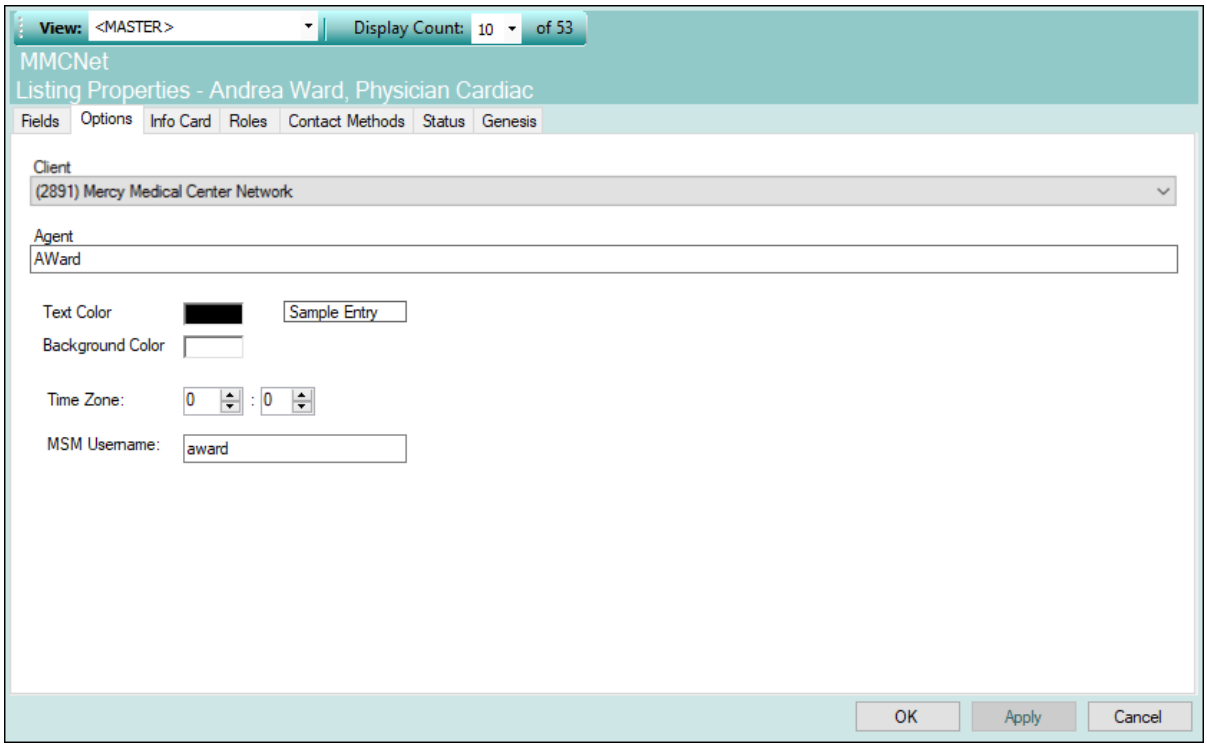
To remove a role, click the role that you want to remove and then click the Delete icon. A dialog box is displayed to confirm the delete request.



If you are sure you would like to delete the role, click the Yes button.

Connecting a Listing to an Amtelco Secure Messages Username

The MSM Username setting is used to link an IS Directory listing to an Amtelco Secure Messages user. The setting is located under the Options tab in Listing Properties.



To edit a listing in the directory, select the Master View or another View for which Edit rights have been assigned to the fields that you need to edit.

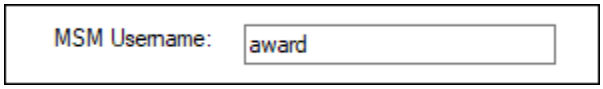
Select the listing in the menu of listing Descriptions or the table of listing fields and then click the Edit icon.

All viewable fields for the selected View are displayed in the Listing Properties pane.

Click the Options tab.

The Options settings are displayed. The Options settings are used to configure the Client, Agent, Listing Color, and Time Zone settings for a directory listing.

MSM Username



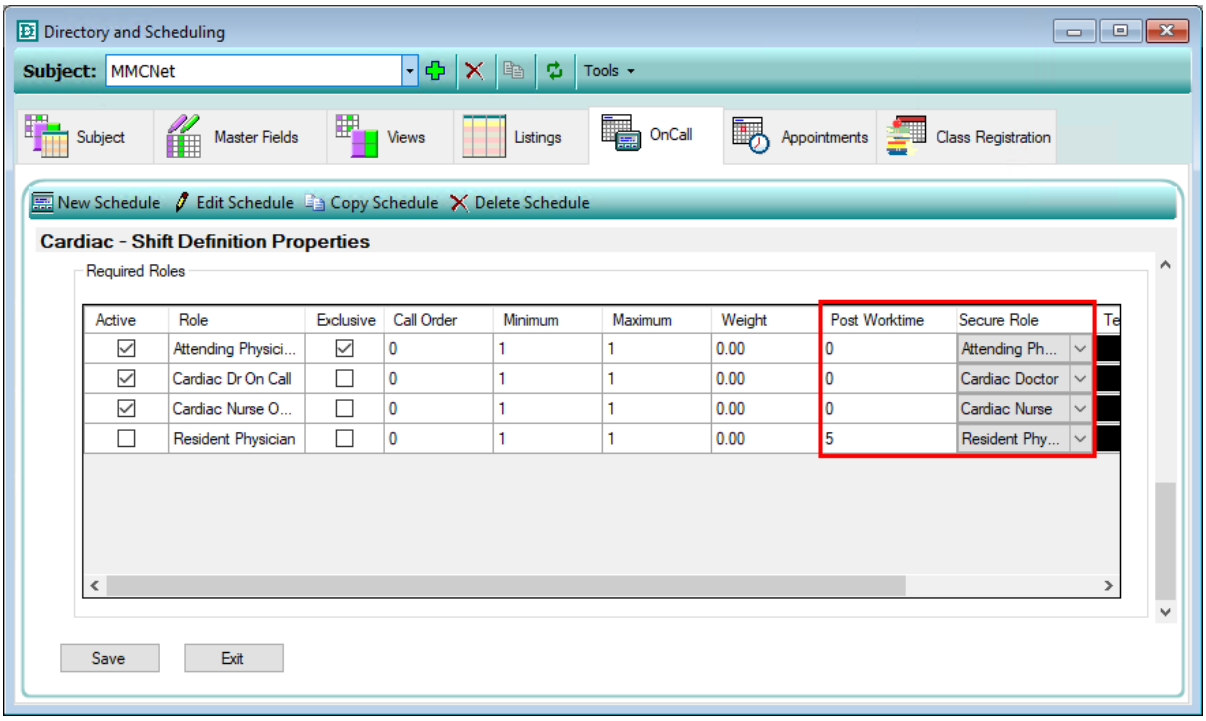
The MSM Username setting is used to link the listing to an Amtelco Secure Messages (ASM) user for use with the optional Role-Based Messaging (RBM) feature. This setting is only used with Role-Based Messaging and is separate from the Secure Messaging Contact Methods created under the Contact Methods tab.

Enter the username of the ASM user you would like to link to the listing for use with Role-Based Messaging.

Click the OK button to save your changes.

Connecting an OnCall Schedule to Amtelco Secure Messages

The Secure Role and Post Work Time columns of the Required Roles Table in the Shift Definition Properties are used to link on-call shifts to Amtelco Secure Messages roles.



Post Worktime

The Post Worktime column is displayed if a Station is programmed under the Secure Messages Settings, enabling the optional Role-Based Messaging (RBM) feature for this Directory Subject. The Post Worktime value is used to assign the number of minutes contacts filling this role have access to messages sent to the role after their shift has ended.

If you are using Role-Based Messaging for this schedule, type the number of minutes contacts filling this role should have access to messages sent to this role after their shift has ended.

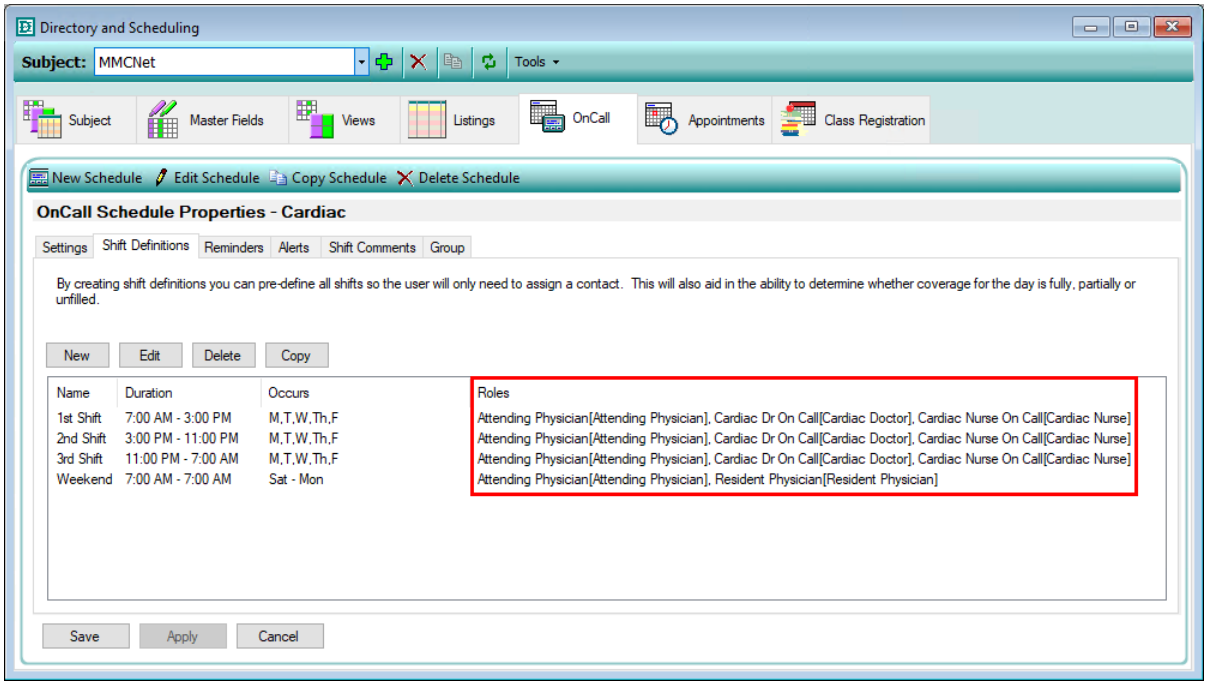
Secure Role

The Secure Role column is displayed if a Station is programmed under the Secure Messages Settings, enabling the optional Role-Based Messaging (RBM) feature for this Directory Subject. The Secure Role column displays the Amtelco Secure Messages (ASM) roles assigned to the IS OnCall roles for the shift.

To assign an ASM role to this IS OnCall role, select the desired ASM role from the menu.

When you have finished setting the Shift Definition Properties, click the Save button to save the Shift Definition.

The Shift Definitions tab in the OnCall Schedule Properties displays the Amtelco Secure Messages roles that have been assigned to each shift. The Amtelco Secure Messages roles are displayed under the Roles column in brackets following the IS roles for that shift.



Adding Amtelco Secure Messages to Infinity

Amtelco Secure Messages can be integrated into the Infinity automated call distribution and unified messaging system using a dedicated Amtelco Secure Messages login, a default account, a route number, and two special dial-string codes. If you have an Infinity system and want to use it to send secure messages, follow the instructions in this section.

The Amtelco Secure Messages Login

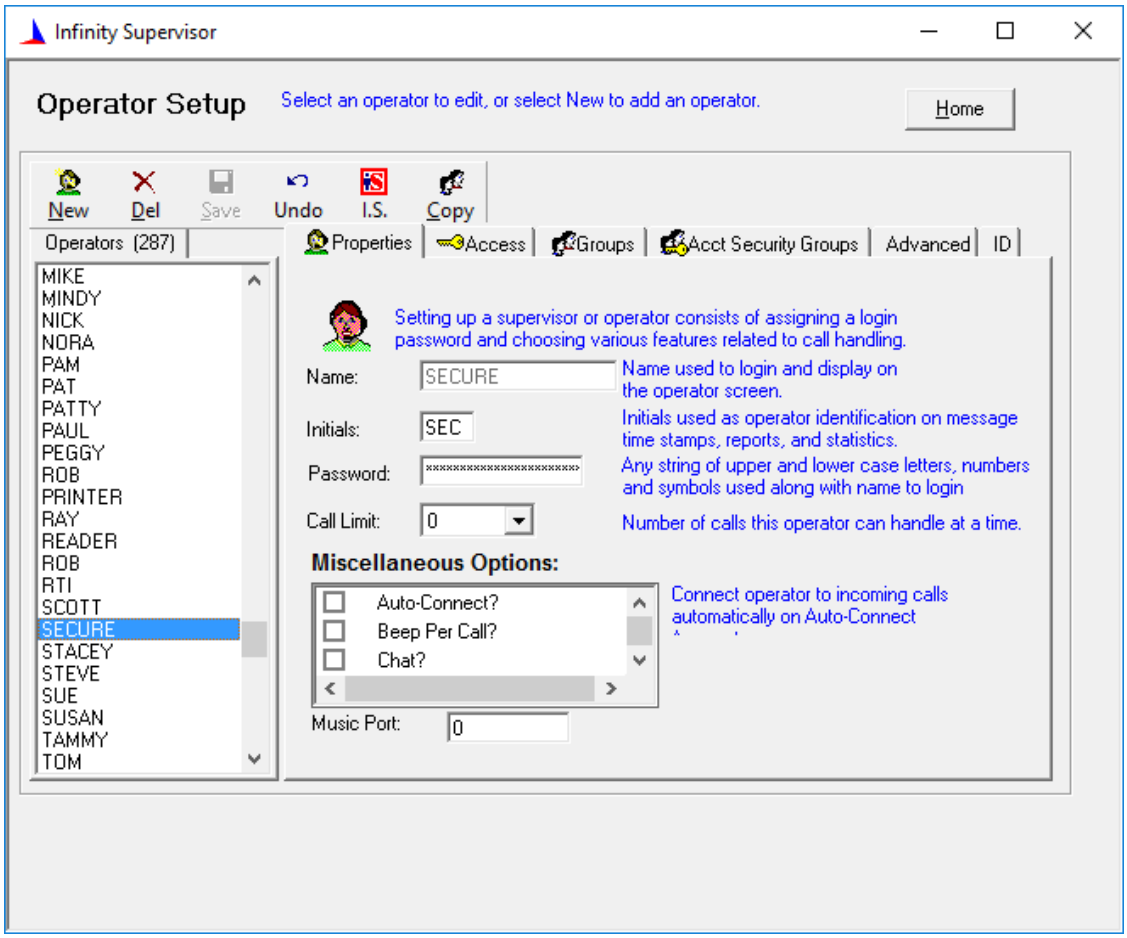
The ASM Service requires one dedicated Infinity login and password to communicate with the Infinity Server. This login should be a login that is only used by the ASM Service and is not used by any operators or other Infinity features. The login must be assigned the “Secure Messages” Station Type.

Open the Infinity Supervisor application.

Click the Operator icon to open the Operator Setup page.

Click the New button on the Operator Setup toolbar to create a new operator.

The Properties tab is displayed.



Properties Tab

The settings under the Properties tab are used to create a login name, initials, and a password to identify an operator to the Infinity applications. They are also used to set a call limit and enable operator options.

Name

The ASM Service requires its own login name to access Infinity. The login name can be up to eight characters long and can be comprised of letters, numbers, or a mixture of both.

Enter a login name for the ASM Service to use to access Infinity.

The login name must match the Login specified for the Infinity Server connection in the ASM Admin Web on the Connections page.

Instructions for configuring the Connections page are provided in this document under the topic “Installing and Configuring the Amtelco Secure Messages Admin Web.”

Initials

Initials are used to identify the ASM Service statistically when there is not room for a login name. Assign the ASM Service a unique set of initials that is not in use by any operator or service. The entry accepts up to three characters: letters, numbers, or a mixture of both.

Enter unique initials to identify the ASM Service.

Password

A password is used to protect your system and data from unauthorized use. The entry accepts up to 32 characters and can include uppercase and lowercase letters, symbols, and numbers. Entering zero (0) in the Password entry effectively disables the password.

Enter a password for ASM Service to use.

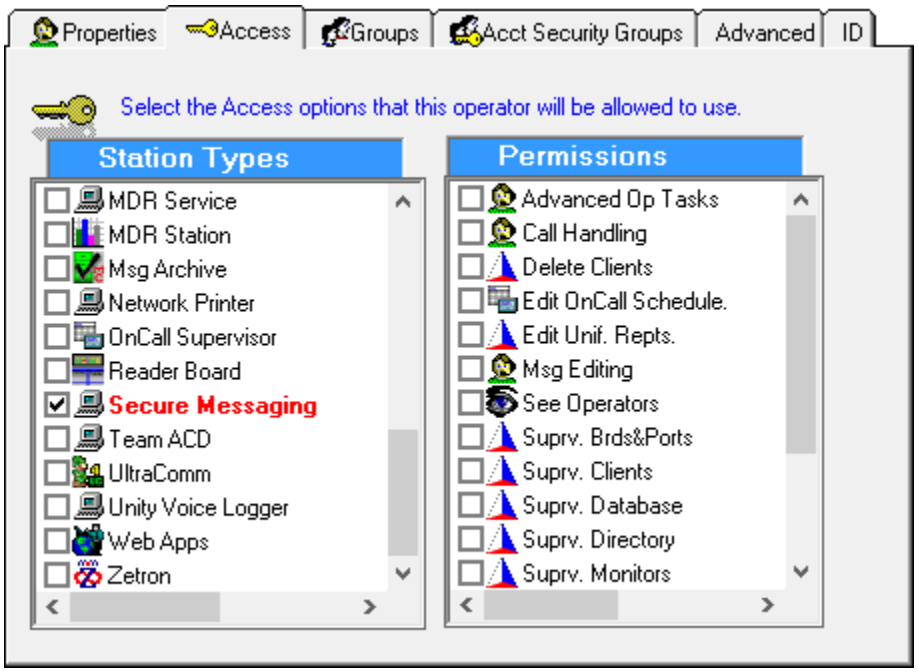
The password must match the password specified for the Infinity Server connection in the ASM Admin Web on the Connections page.

Instructions for configuring the Connections page are provided in this document under the topic “Installing and Configuring the Amtelco Secure Messages Admin Web.”

Access Tab

The settings under the Access tab are used to grant the selected operator permissions and access to specific station types.

Click the Access tab to set the Access Station Type for this login.



☑ Secure Messaging

The Secure Messaging Station Type is required for the Amtelco Secure Messages login.

Select the check box labeled "Secure Messaging."

The Amtelco Secure Messages login is the only login that requires the "Secure Messaging" station type. The Amtelco Secure Messages login does not need any other Station Types or Permissions.

Saving Your Entries

Click the Save button on the Operator Setup toolbar to save the settings for the Amtelco Secure Messages login.

Click the Home button to exit Operator Setup.

The Amtelco Secure Messages Default Account

The Infinity Server is displayed as a contact in the Contact List in the Amtelco Secure Messages apps and in the Amtelco Secure Messages Contact Web. The Default Account setting indicates which Infinity client account will accept new secure messages sent to the Infinity contact.

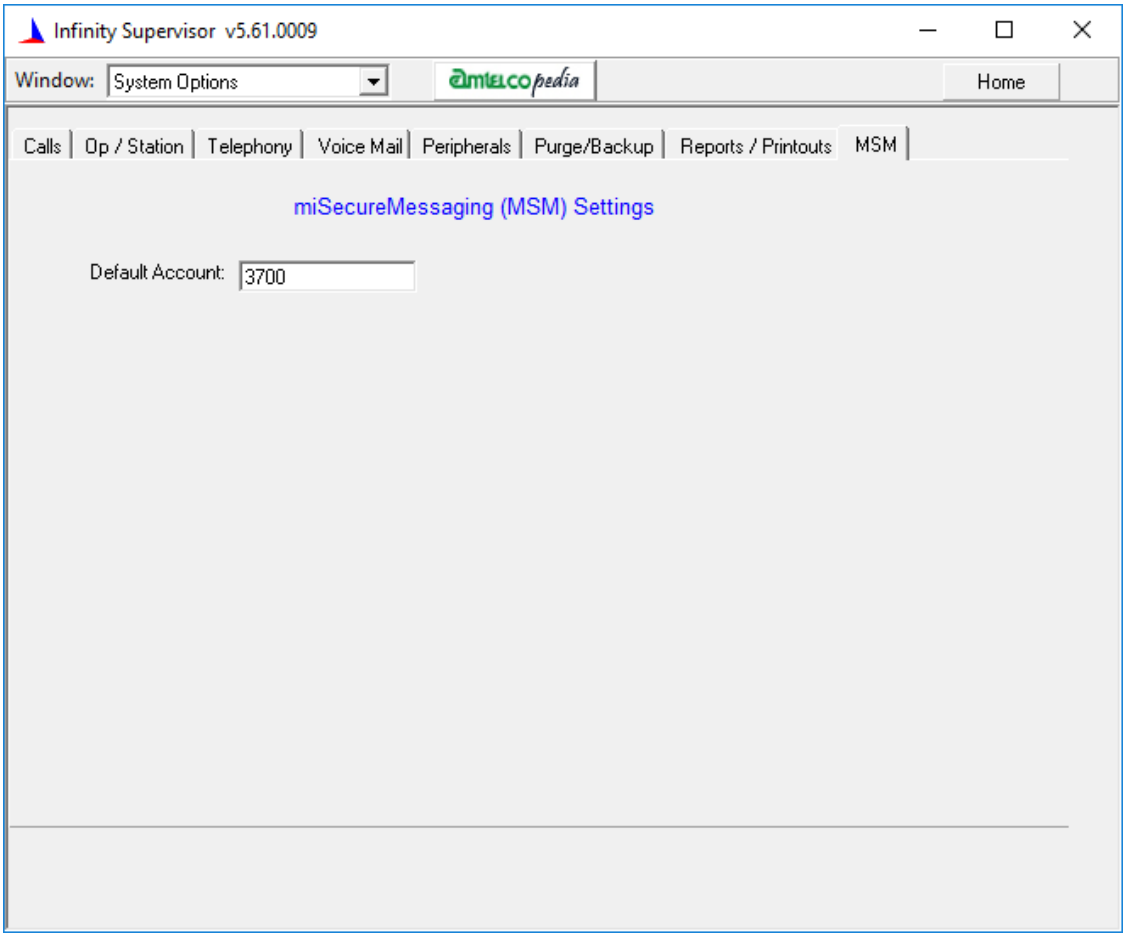
Click the System Settings icon on the Infinity Supervisor Home page to open the System Settings pages.

Open the Window menu and select "System Options."

The System Options page is displayed.

Click the MSM tab.

The MSM page is displayed.



Default Account

When an unsolicited secure message comes into Infinity, the message is sent to the Default Account specified on the MSM page.

Enter the Infinity client account number that should receive unsolicited secure messages sent to the Infinity Server.

Amtelco Secure Messages Dial Strings

Amtelco Secure Messages dial strings can be programmed in either of the following two formats:

.*RouteNumber***R.."***FromNumber***"."***FromName***"."***Username***"..512L**

.*RouteNumber***R.."***FromNumber***"."***FromName***"."***Username***"..768L**

Each of the segments of these dial strings are explained in the following table.

Segment	Description
.*RouteNumber***R**	This segment indicates the route number. Replace *RouteNumber* with the Route number specified in the ASM Admin Web, Connections page, Infinity Server, Route. **Note:** The route number must match the route number entered in the Infinity Server connection settings in the ASM Admin Web. Instructions for configuring the Connections page are provided in this document under the topic "Installing and Configuring the Amtelco Secure Messages Admin Web."
.	This period is a required and indicates and unused segment of the dial string.
."*FromNumber***"**	This segment is the optional "From" phone number that will be sent with messages. Replace *FromNumber* with the phone number you want to display in Amtelco Secure Messages. If you do not want to include a "From" phone number, exclude the number and the quotation marks, but do not exclude the period.
."*FromName***"**	This segment is the "From" name that will be sent with messages. Replace *FromName* with the name of your company or service.
."*Username***"**	A contact's username can be used to send a secure message to all of a contact's devices that are registered with the Amtelco Secure Messages app. Replace *Username* with the username of the contact as configured in the user's Amtelco Secure Messages app and in the user's Contact Settings in the ASM Admin Web. Substitute the plus sign (**+**) for any periods in the username. **Note:** The username may not include spaces, accent marks (as used in languages like French and Spanish), nor any of these special characters: " **[€ £ ¥ + ,**
.	This period is a required and indicates and unused segment of the dial string.
.512L or **.768L**	This segment is the filter code. The filter code determines what action Infinity takes if no reply is received before the Confirmation Time expires.

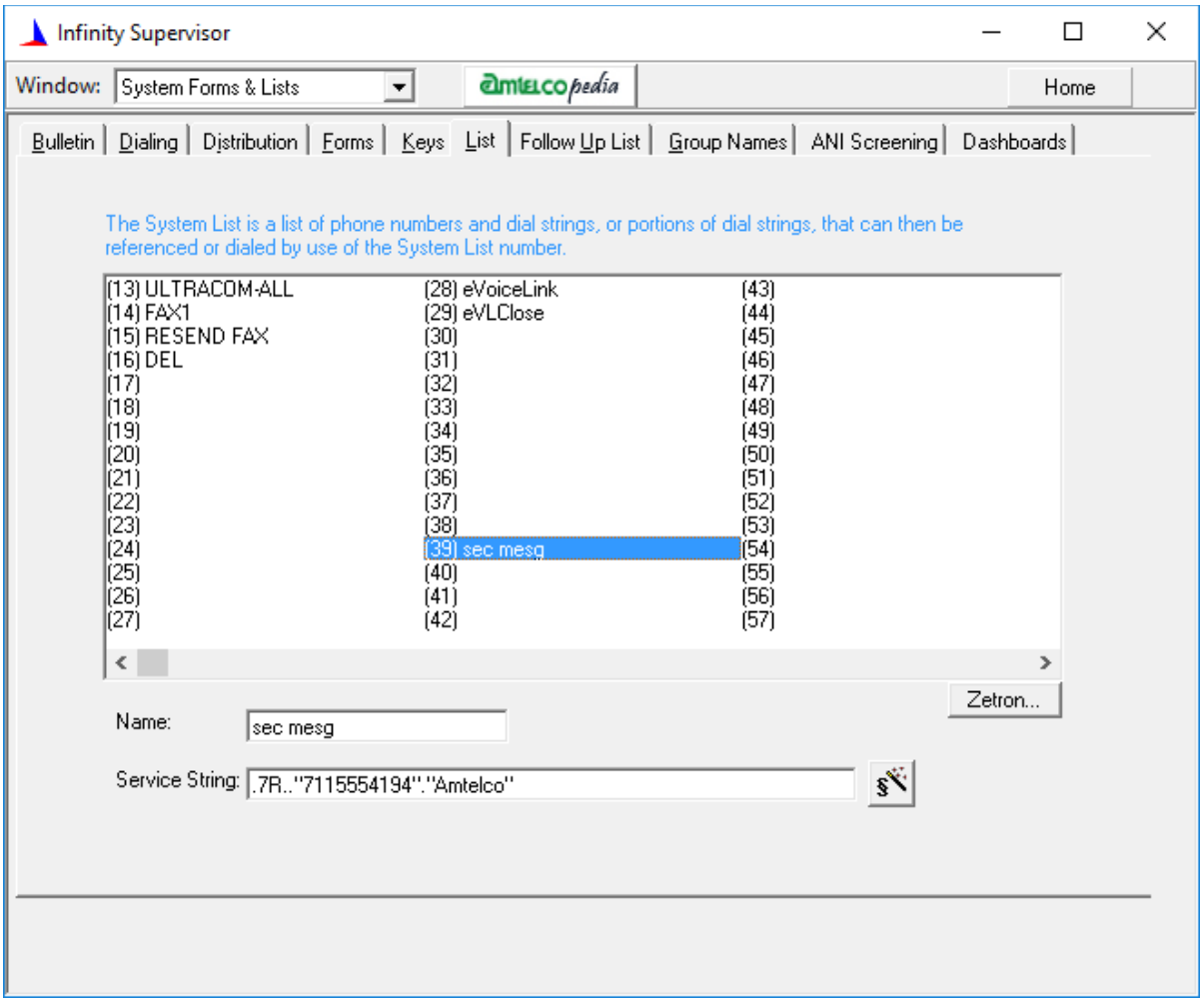
Segment	Description
	• If filter code **.512L** is used, no action is taken if no reply is received. • If filter code **.768L** is used, the account is presented to operators using the client account's Call Distribution Tables and displays "No Reply" if no reply is received before the Confirmation Time expires. The Confirmation Time setting is located on the Paging Management page of Infinity Client Setup under the heading "Alpha-Page and SMS Confirmation." To access the Confirmation Time setting, select a client account to edit. Select "Paging Management" from the Page menu. Then, click the Secure Messages tab.

The first part of the dial string can be stored in a System Service List as shown in the following illustrations.

The System Service List contains the first portion of the string in either of these formats:

.*RouteNumber***R.."***FromNumber***"."***FromName***"**

.*RouteNumber***R..."***FromName***"**


Infinity Supervisor
Window: System Forms & Lists
Amtelcopedia
Home
Bulletin
Dialing
Distribution
Forms
Keys
List
Follow Up List
Group Names
ANI Screening
Dashboards
The System List is a list of phone numbers and dial strings, or portions of dial strings, that can then be referenced or dialed by use of the System List number.
(13) ULTRACOM-ALL
(14) FAX1
(15) RESEND FAX
(16) DEL
(17)
(18)
(19)
(20)
(21)
(22)
(23)
(24)
(25)
(26)
(27)
(28) eVoiceLink
(29) eVLClose
(30)
(31)
(32)
(33)
(34)
(35)
(36)
(37)
(38)
(39) sec mesg
(40)
(41)
(42)
(43)
(44)
(45)
(46)
(47)
(48)
(49)
(50)
(51)
(52)
(53)
(54)
(55)
(56)
(57)
Zetron...
Name:
sec mesg
Service String:
.7R..''7115554194''.''Amtelco''

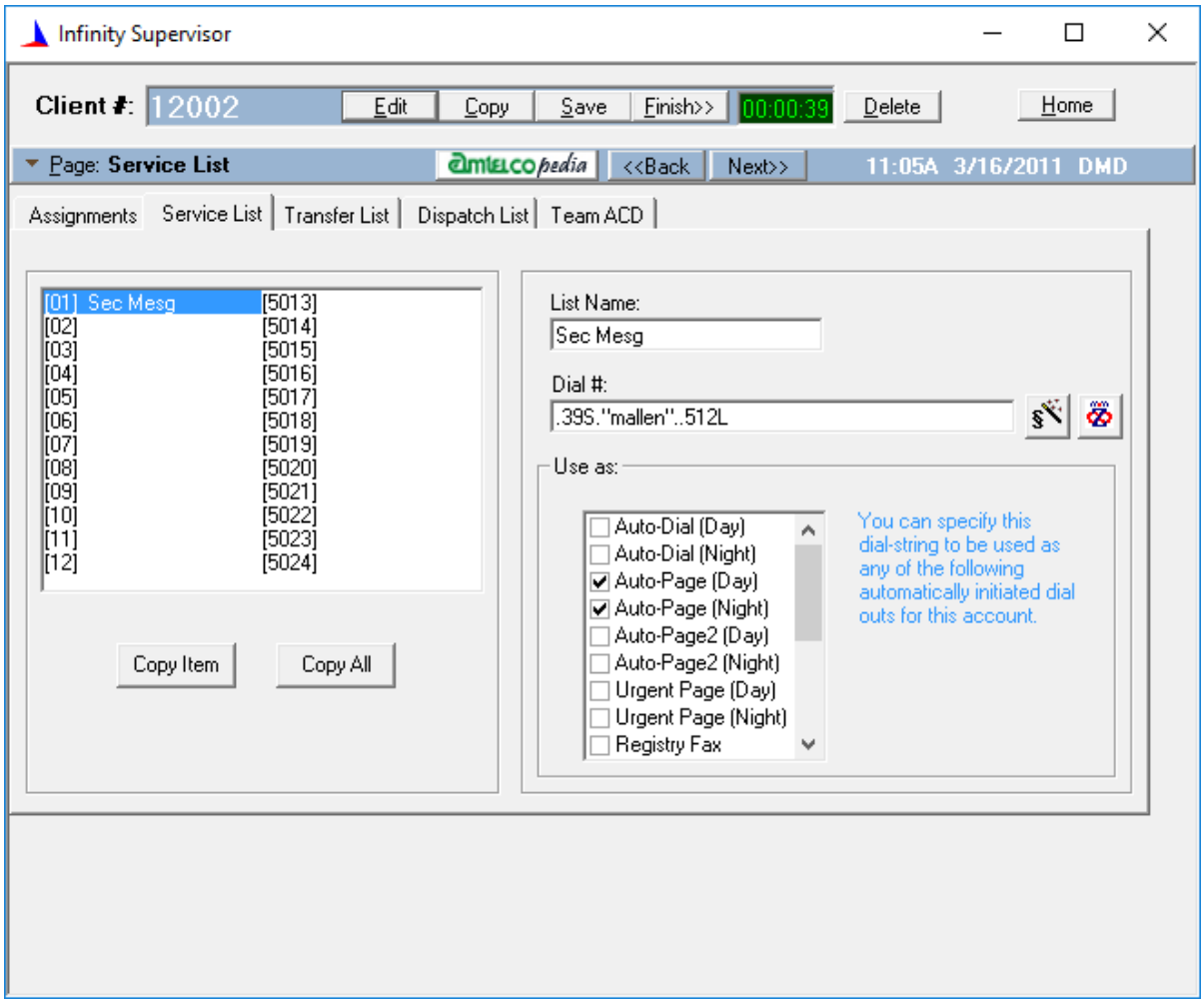
The client account contains a reference to the service list and the last portion of the string in either of these formats:

.*SystemListNumber***S."***Username***"..512L**

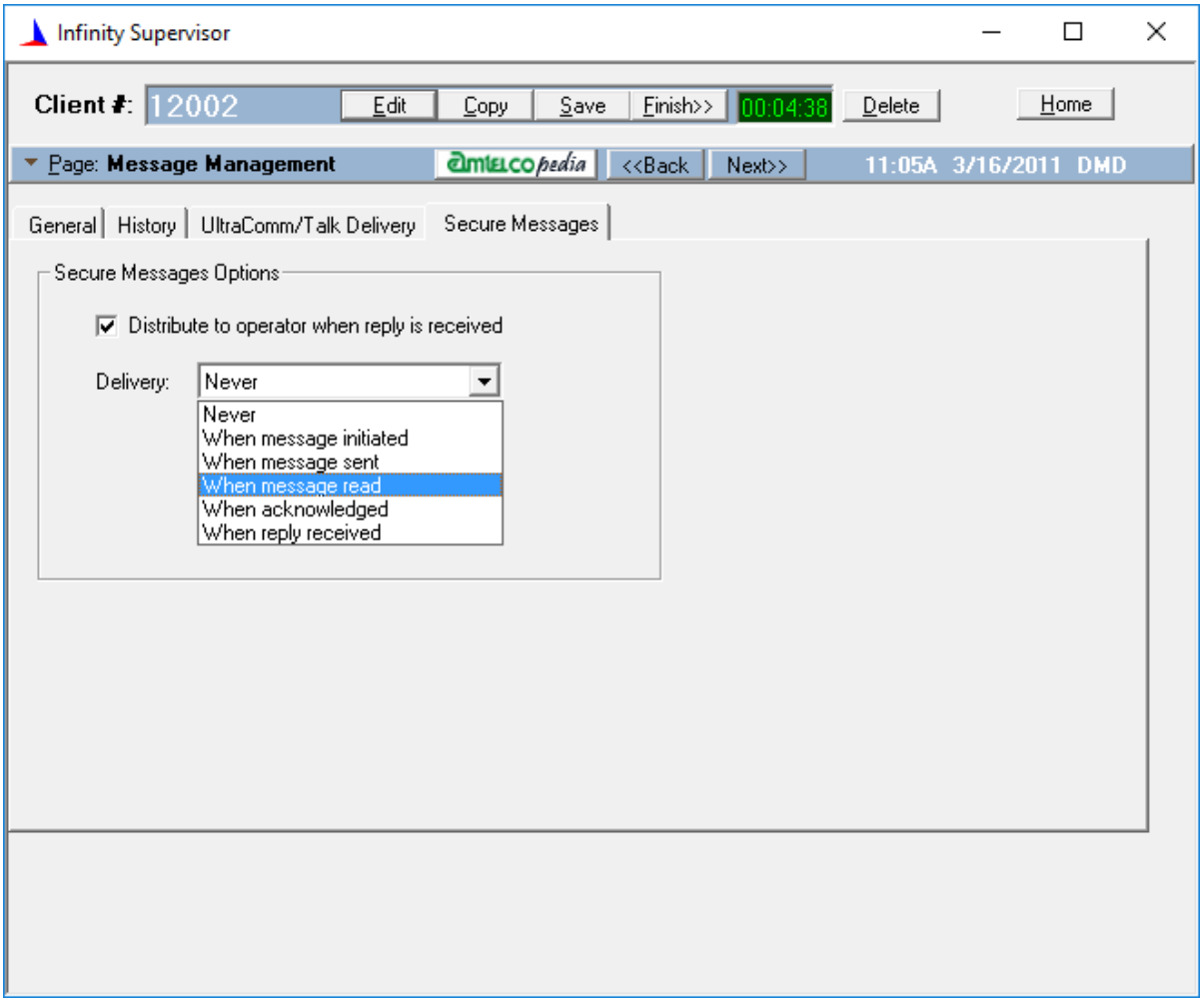
.*SystemListNumber***S."***Username***"..768L**

Segments are as listed in the previous table with the addition of the following segment.

Segment	Description
.*SystemListNumber***S**	This segment indicates which System Service List contains the missing portion of the dial string. Replace *SystemListNumber* with the System Service List number.



Client Message Management



Secure Messages Options for each client account are located on the Message Management page of Client Setup in Infinity Supervisor.

To access the Secure Messages Options, select a client account to edit.

Select "Message Management" from the Page menu.

Then, click the Secure Messages tab.

The Secure Messages Options for the selected client account are displayed.

☑ Distribute to operator when reply is received

This option can be set to distribute the message to a console operator when a reply is received.

- If this check box is selected, replies to secure messages will be noted in the Infinity message history and will be distributed to operators using the client account's Call Distribution Tables.
- If this check box is cleared, replies to secure messages will be noted in the Infinity message history but not distributed to operators.

Delivery

The Delivery setting is used to indicate when a message should be marked as “Delivered.” These setting options are:

- **Never:** The message is not automatically marked “Delivered.”
- **When message initiated:** The message is marked “Delivered” as soon as the job is initiated.
- **When message sent:** The message is marked “Delivered” when it is delivered to the user’s inbox.
- **When message read:** The message is marked “Delivered” when it is opened by the recipient.
- **When marked completed:** The message is marked “Delivered” when the recipient marks the message “Completed.”
- **When reply received:** The message is marked “Delivered” when a reply is received and matched with the message.

Configuring Protected Dialing through Infinity

The Protected Dialing feature allows 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. 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.

Documentation Change Log

Software Version	Document Section	Changes	Published Date
Amtelco Secure Messages 7.0.0	All	Changed “miSecureMessages” to “Amtelco Secure Messages” and changed “MSM” to “ASM.”	11/22/2024
Amtelco Secure Messages 7.0.0	All	Changed “MSM Administration Web” to “Amtelco Secure Messages Admin Web.”	11/22/2024
Amtelco Secure Messages 7.0.0	Introduction	Added the IS ASM Web API and the ASM IS Web API to the system diagrams. Changed “Messages sent from IS or Infinity are processed…” to “Messages initiated from the IS Server are sent to the ASM Notification Service using two Web Application Program Interfaces (Web APIs), one connected to the ASM Service and one connected to the IS Server. Messages sent from Infinity are processed…”	11/22/2024
Amtelco Secure Messages 7.0.0	Components	Added ASM IS Web API and IS ASM Web API.	11/22/2024
Amtelco Secure Messages 7.0.0	Additional High Availability Components	Updated diagram.	11/22/2024
Amtelco Secure Messages 7.0.0	Creating and Configuring the ASM SQL Database	Removed reference to 6.8 and instructions for setting up memory optimized tables.	11/22/2024
Amtelco Secure Messages 7.0.0	Configuring Customer Data	Updated screenshot. In connection strings, changed “SecureMessaging” to “ASM_*CustomerID*” and added “Replace *CustomerID* with your Amtelco Secure Messages customer ID provided by Amtelco.”	11/22/2024

Software Version	Document Section	Changes	Published Date
Amtelco Secure Messages 7.0.0	Configuring the ASM Notification Service	Added instructions for connecting to more than one ASM Service.	11/22/2024
Amtelco Secure Messages 7.0.0	Adding Secure Messaging to the IS Directory	Updated screenshots. Added information about the "OnCall Schedule, Appointments, or Class Registration" check box needed for Role-Based Messaging.	11/22/2024
Amtelco Secure Messages 7.0.0	Adding Amtelco Secure Messages to Infinity	Renamed from "Adding miSecureMessages to Infinity."	11/22/2024
Amtelco Secure Messages Admin Web *7.0.8892.2*	Configuring the Amtelco Secure Messages Admin Web	Renamed from "Configuring the MSM Administration Web." Updated screenshots.	11/22/2024
Amtelco Secure Messages Admin Web *7.0.8892.2*	Adding Protected Dialing to a Group	Added the word "optional." Updated screenshot. Changed "Genesis Dialing" to "Protected Dialing." Changed "Genesis DISA#" to "DISA#." Changed "Genesis Code" to "Access Code."	11/22/2024
Amtelco Secure Messages Android App 7.0.5.0	Configuring the Amtelco Secure Messages Android App	Renamed from "Configuring the miSecureMessages Android App." Updated screenshots.	11/22/2024
Amtelco Secure Messages Apple App 7.0.5.0	Configuring the Amtelco Secure Messages Apple App	Renamed from "Configuring the miSecureMessages Apple App." Updated screenshots.	11/22/2024
Amtelco Secure Messages Apple App 7.0.5.0	Configuring the Amtelco Secure Messages Apple Watch App	Renamed from "Configuring the miSecureMessages Apple Watch App." Updated screenshots.	11/22/2024

Software Version	Document Section	Changes	Published Date
Amtelco Secure Messages Contact Web 7.0.8641.4	Logging into the Amtelco Secure Messages Contact Web	Renamed from "Logging into the miSecureMessages Contact Web." Updated screenshots.	11/22/2024
IS Supervisor 5.7.8867.01	Configuring Role-Based Messaging	Added section.	11/22/2024
IS Supervisor 5.7.8445.3	Adding Amtelco Secure Messages to IS	Renamed from "Adding miSecureMessages to IS."	11/22/2024
IS Supervisor 5.7.8445.3	Configuring Unsolicited Client Settings	Updated screenshots. Added Configuration and Connections screens to instructions.	11/22/2024
IS Supervisor 5.7.8445.3	Configuring Connections to ASM Web Services	Added section.	11/22/2024
IS Supervisor 5.7.8445.3	Configuring Event Notifications	Updated description of Station under MSM Notification Properties.	11/22/2024
IS Supervisor 5.7.8445.3	Adding Fields to a View	Updated description of Station under "Contact Secure Messaging ID Fields" and under "Secure Message Contact Editor."	11/22/2024
N/A	Configuring the Amtelco Secure Messages Admin Web	Added Connections section.	11/22/2024
N/A	Configuring Protected Dialing through Genesis	Added the word "optional." Changed instructions to include the pound sign (#). Updated the example to include the pound sign (#) after the DISA.	11/22/2024

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