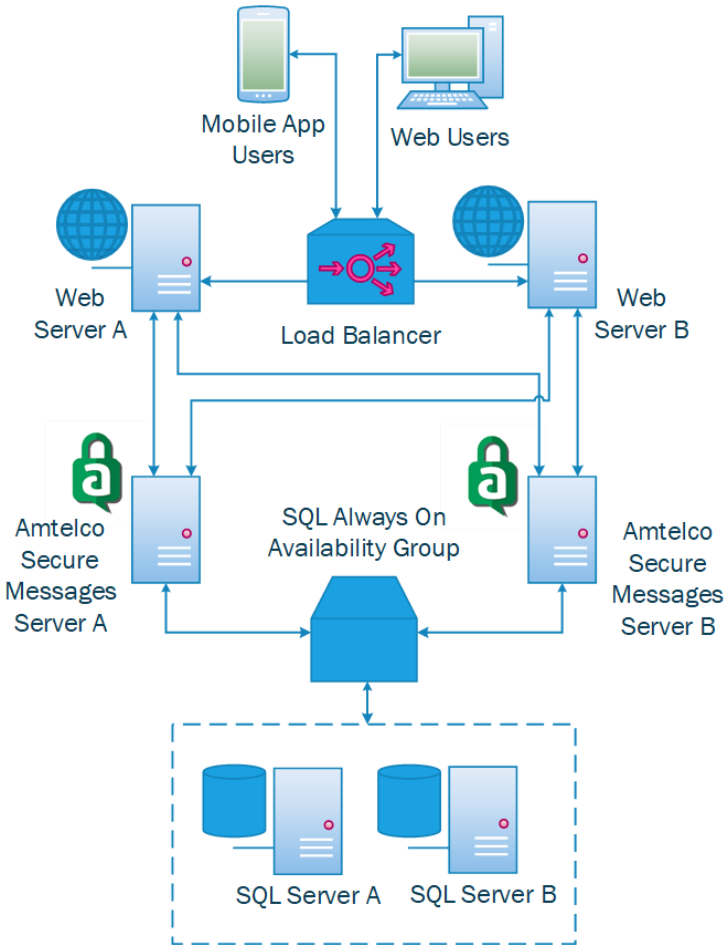
R&D Software Department
4800 Curtin Drive, McFarland, WI USA 53558
www.amtelco.com

Amtelco Secure Messages High Availability



Connect your Amtelco Secure Messages (ASM) system to multiple servers in a cloud-based or on-site solution instead of the standard one server system with Amtelco's High Availability solution. The optional High Availability feature allows Amtelco Secure Messages to be configured for multiple ASM servers and web servers, with automated failover from one server to another when a server goes down.

The active/active configuration can provide continuous uptime during some server upgrades of the Amtelco Secure Messages system and prevents downtime due to a single server failure. Maintenance can be performed on one server while the other servers continue to run. In an active/active configuration, the servers are all active and running concurrently, unlike an active/passive configuration in which the secondary server is inactive until something happens to the primary server.

High Availability Components

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

- Second application server running 64-bit Microsoft Windows Server 2016 or later with Microsoft .NET Framework 4.7.2
    - ASM Service
    - ASM Configuration Application
    - ASM Notification Service
- File share location for thread archive if not using Amazon for storage
- Customer-provided High Availability solution for the Web server
    - Network Load Balancer
    - Sticky sessions enabled
- Customer-provided High Availability solution for the SQL database server
    - SQL Always On Availability Groups

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

High Availability Setup Steps

ASM High Availability is configured by performing the following steps:

- Configure loading balancing and enable sticky sessions on the Web servers.
- Configure SQL Always On availability for the SQL database servers.
- Configure the ASM Service on the additional server just like the initial server. It will need its own IP address but should point to the same database. The additional server should have its own ASM Notification Service installed.
- The thread archive path (if not archiving to Amazon) should be set up on a file share. Otherwise, archives could end up being split between the servers, making it harder to find archived messages.
- ASM Web Service and Amtelco Secure Messages Admin Web need to be configured to use the additional server. This is done by adding the new server (formatted as server:port) to the comma separated list of servers in the Servers key in the web.config file.
- Configure the events for "Inactive server" to be notified if a server is down, and "Unlicensed server" to be notified if an unlicensed server is running.

Configuring Web Server Load Balancing and Sticky Sessions

It is the customer's responsibility to implement a High Availability solution for the web server, if one does not already exist. Make sure to configure loading balancing and enable sticky sessions for the two Web servers.

Configuring SQL Server Always On Availability

It is the customer's responsibility to implement a High Availability solution for the SQL server, if one does not already exist. Amtelco recommends SQL Always On availability for the SQL database servers.

Configuring a Second Secure Messages Server

For High Availability of Amtelco Secure Messages services, a second Secure Messages server is needed to handle secure messaging at times when the first Secure Messages server is unavailable.

To configure the second Secure Messages Server, follow these steps:

1. **Install the ASM Service on the second Secure Messages server.**
2. **Install the ASM Notification Service on the second Secure Messages server.**
3. **Configure the ASM Service using the same settings as the first Secure Messages server, except point it to the ASM Notification Service on the second server.**
4. **Configure the ASM Notification Service using the second server's IP address and port.**

Changing the Thread Archive Path

For High Availability of Amtelco Secure Messages services, the thread archive path on both 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.

To change the Thread Archive Path on your Secure Messages server, open the ASM Server Configuration application on one of your ASM Servers.

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

The Server and Customers nodes are displayed.

Click the Customers node.

Select the Customer ID.

Click the Maintenance tab.

The Maintenance Properties are displayed.

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 your desired archive location on Amazon or on a file share.

The account that runs the ASM Service must have permission to read and write to the selected archive location.

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.

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

Repeat these steps on your second ASM Server to set the Thread Archive Path to the same Amazon or file share location.

Adding a Second Server to the ASM Web Service

The second Secure Messages Server needs to be added to the appSettings section of the web.config file for the ASM Web Service.

In the appSettings section of the web.config file for the ASM Web Service, 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 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 Secure Messages server.

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

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" />
```

Adding a Second Server to the ASM Admin Web

The second Secure Messages server needs to be added to the appSettings section of the web.config file for the ASM Admin Web application.

In the appSettings section of the web.config file for the ASM Admin Web, 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 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 Secure Messages server.

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

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

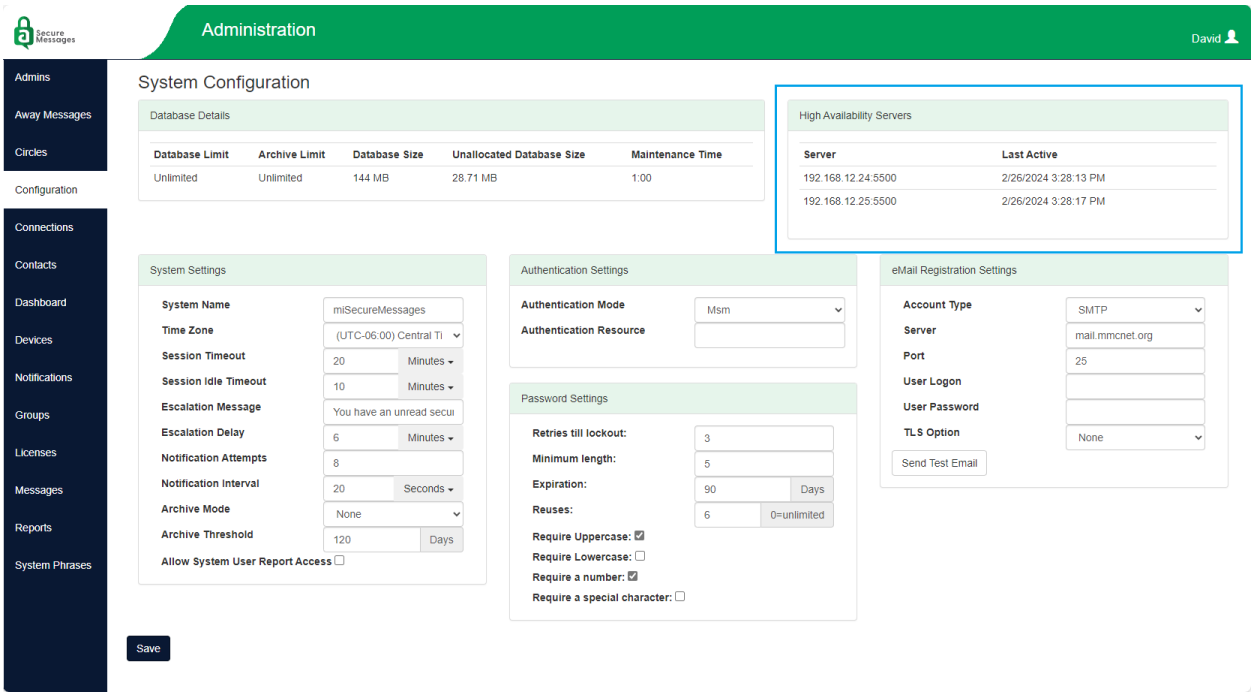
Remove this line of code:

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

The High Availability Servers pane on the System Configuration page of the ASM Admin Web displays information about the servers added to the Servers key in the ASM Admin Web's web.config file.

To check that the server was added successfully, log into the ASM Admin Web application.

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



High Availability Servers

The High Availability Servers pane displays the following information about the servers added to the Servers key in your ASM Admin Web's web.config file.

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

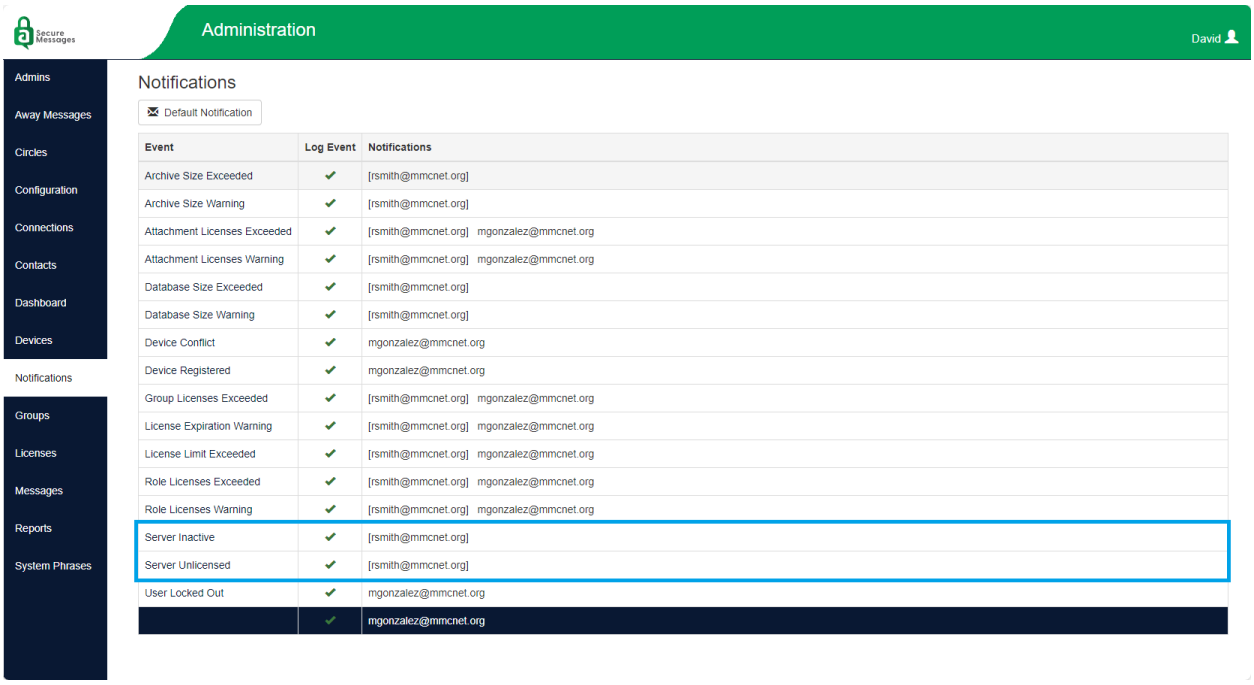
Note: Having servers listed in the High Availability Servers pane does not guarantee that your system is configured for automated failover. Contact Amtelco for more information about configuring your Amtelco Secure Messages system for High Availability.

Configuring High Availability Event Notifications

The Notifications page in the ASM Admin Web is used to configure e-mail notifications for specific Amtelco Secure Messages system events. Each type of event can be configured to trigger an e-mail notification to one or more e-mail addresses.

To configure event notifications, log into the ASM Admin Web application.

Click the Notifications command on the ASM Admin Web navigation menu to access the Notifications page.



Two events are related to the High Availability feature: the Server Inactive event and the Server Unlicensed event.

Server Inactive

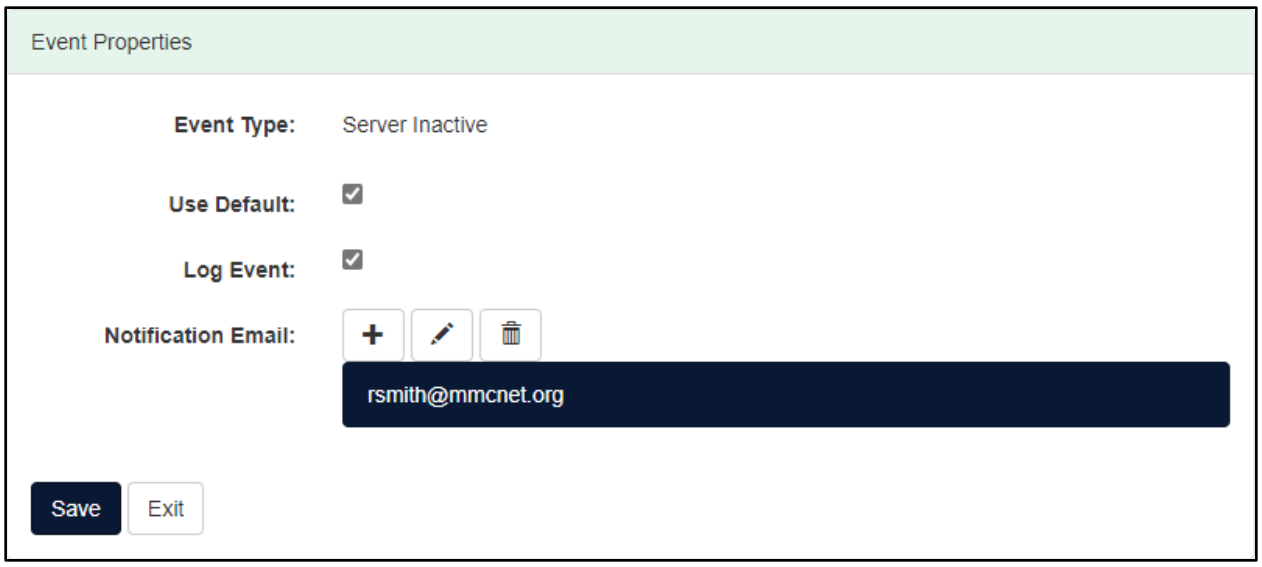
The Server Inactive event is used with the High Availability feature. The Server Inactive event sends a notification when the Last Active date and time for an ASM server is more than 10 minutes old, provided there is another ASM server still active to send the notification. If both servers are down, or if the High Availability Feature is not configured, the Server Inactive event will not be able to send a notification.

Server Unlicensed

The Server Unlicensed event is used with the High Availability feature. The Server Unlicensed event sends a notification when an ASM Server is started up and there are not enough High Availability licenses available. The unlicensed server will run in Degraded Mode, meaning it won't process requests from the Amtelco Secure Messages apps.

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

The Event Properties pane is displayed.



Event Type

The name of the event is displayed.

☑ Use Default

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

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

☑ Log Event

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

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

Notification Email

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

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

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

The settings on the Email Notification Entry pane are the same as the settings on the Default Email Notification pane.

Configure the To, From, Subject, Server, Port, Login, Password, Use TLS, and Encrypted settings as appropriate for this type of system event notification.

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

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

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

The Event Properties pane is displayed.

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

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

Requirements:

- Amtelco Secure Messages Server version 6.8 or later
- Android OS 7.0 or later with a cellular data plan and a Google account
- Amtelco Secure Messages Android App 6.8 or later
- Apple iOS 12.0 or later with a Business Use data plan
- Amtelco Secure Messages Apple App 6.8 or later
- Apple watchOS 5.0 or later
- Apple Watch Series 3 or later
- Second application server running 64-bit Microsoft Windows Server 2016 or later with Microsoft .NET Framework 4.7.2
    - ASM Service
    - ASM Configuration Application
    - ASM Notification Service
- File share location for thread archive if not using Amazon for storage
- Customer-provided High Availability solution for the Web server
    - Network Load Balancer
    - Sticky sessions enabled
- Customer-provided High Availability solution for the SQL database server
    - SQL Always On Availability Groups

Browser Compatibility:

Amtelco Secure Messages web applications are tested with the latest release of the following browsers.

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