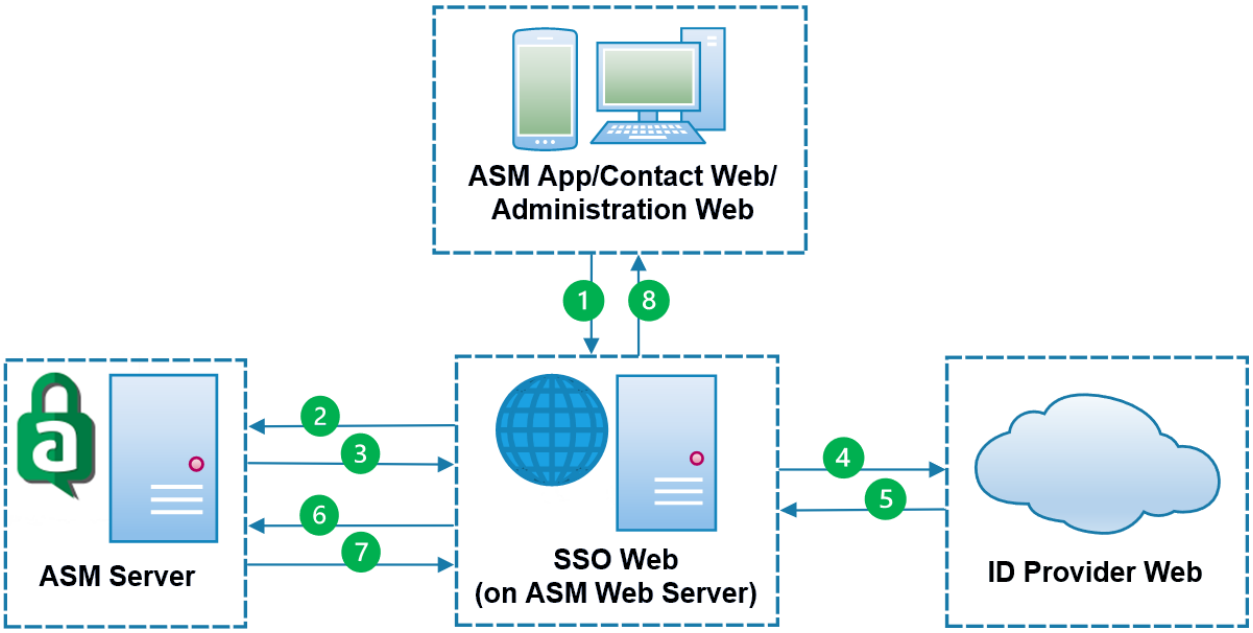
R&D Software Department
4800 Curtin Drive, McFarland, WI USA 53558
www.amtelco.com

Amtelco Secure Messages Single Sign-On

The optional Amtelco Secure Messages (ASM) Single Sign-On feature enables ASM contact usernames and ASM Administration Web admin login names to be configured to use a Single Sign-On (SSO) Identity Provider to keep track of passwords and to perform authentication. SSO authentication requires a third-party SSO Identity Provider. Amtelco has tested Amtelco Secure Messages with the following SSO Identity Providers:

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

Amtelco Secure Messages Single Sign-On Process



1. The client directs the web view to the SSO web.
2. The SSO web does pre-authentication validation with the ASM server.
3. The result of the pre-authentication validation is sent to the SSO web.
4. The SSO web redirects to your organization's ID provider web.
5. Your organization's ID provider web returns SAML assertion.
6. The SSO web does post-authentication validation with the ASM server.
7. The result of the post-authentication validation is sent to the ASM server.
8. The SSO result is returned to the client.

Single Sign-On Components

In order to use SSO authentication, the following components are required in addition to the standard Amtelco Secure Messages components.

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

*It is up to your organization to maintain and renew your security certificates.

Installing the ASM Assertion Consumer Web Service

The ASM Assertion Consumer Web service needs to be installed on your web server to act as the service provider for Single Sign-On authentication. Contact Amtelco Field Engineering for assistance with performing the following steps:

1. On your web server, create a folder named ASMSSO in C:\inetpub\wwwroot.
2. Extract the SSOWeb.zip file to the C:\inetpub\wwwroot\ASMSSO.
3. Create a Logs subfolder in C:\inetpub\logs\logfiles\ASMSSO.

Uploading Certificates

The Service Provider certificate and Identity Provider certificates should be uploaded to the Microsoft Management Console (MMC) Certificate Store in the Personal/Certificates folder.

The Thumbprint for each certificate can be found by double-clicking on the certificate in the Certificate store and then selecting Details, Thumbprint. Set the appropriate thumbprint for each provider under their section.

The IIS_IUSRS group must have full control over the Service Provider Certificate. In the Certificate Store, right-click the certificate, select All Tasks and Manage Private Keys, and add the IIS_IUSRS group to give them full control.

Configuring SAML

Once the ASM Assertion Consumer Web service is installed and the certificates are uploaded, the Security Assertion Markup Language (SAML) file must be configured to establish the ASM Assertion Consumer Web as a service provider and your Single Sign-On Server as the identity provider. Contact Amtelco Field Engineering for assistance with making the following changes to the Saml.config file:

In the Server Provider Section:

1. Set the ServiceProvider Name to the URL (Uniform Resource Locator) of your web server.
2. Set the AssertionConsumerServiceURL to the URL of the ASM Assertion Consumer Web service on your web server.
3. Reference the Server Provider certificate thumbprint.

In the Partner Identity Provider Section:

4. Set the PartnerIdentityProvider Name to the URL of your Single Sign-On Identity Provider.
5. Set the Description to identify your SSO provider (for example, “Azure Login” or “ADFS Login”).
6. Set the SignAuthnRequest to “True.”
7. Set the SingleSignOnServiceUrl to the URL of your SSO Identify Provider.
8. Reference the Identity Provider certificate thumbprint.

Editing the Web.Config File

Some changes need to be made to your web server’s web.config file in order to implement Single Sign-On. Contact Amtelco Field Engineering for assistance with making changes to the web.config file.

In the <appSettings> section of the web.config file, add the following keys:

```
<add key="license" value="LicenseKey" />
```

Replace *LicenseKey* with your Amtelco Secure Messages license key provided by Amtelco.

```
<add key="servers" 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.

```
<add key="ShowResults" value="true" />
```

```
<add key="useOptions" value="Value" />
```

Replace “*Value*” with “false” if you are using Azure for your SSO Provider and “true” if you are using ADFS.

```
<add key="PartnerIdentityProvider" value="IdentityProviderURL" />
```

Replace *IndentityProviderURL* with the URL from your SSO Identity Provider setup.

ADFS/Azure Setup

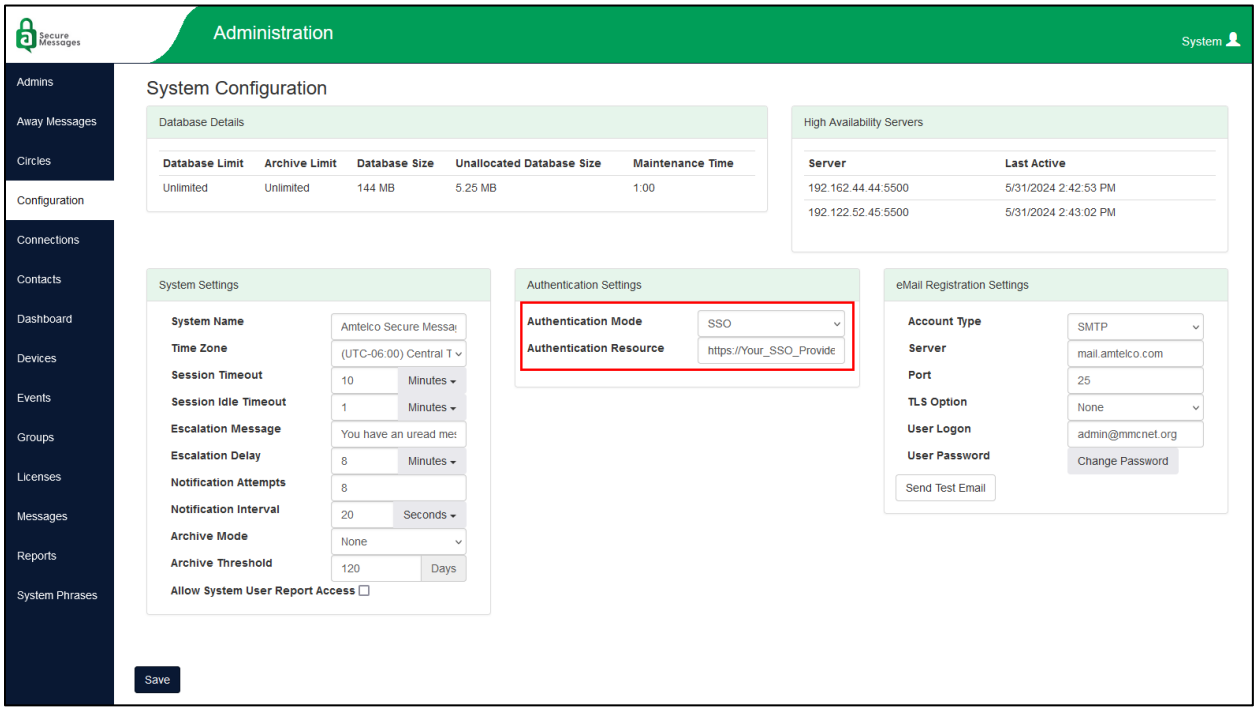
Each Single Sign-On provider has their own process for setup. Contact your SSO provider for instructions on how to configure their application.

Configuring Single Sign-On for Administrators

The SSO settings for admin login names are located on the System Configuration screen of the ASM Administration Web.

Log into the ASM Administration Web application.

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



Administration Settings

The Administration Settings are settings that determine how administrators can log into the ASM Administration Web.

Authentication Mode

ASM Administration Web administrator login names can be configured for one of two authentication modes: ASM (Amtelco Secure Messages) and SSO (Single Sign-On).

Select "SSO" to use a Single Sign-On Identity Provider to keep track of passwords and perform authentication.

Authentication Resource

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

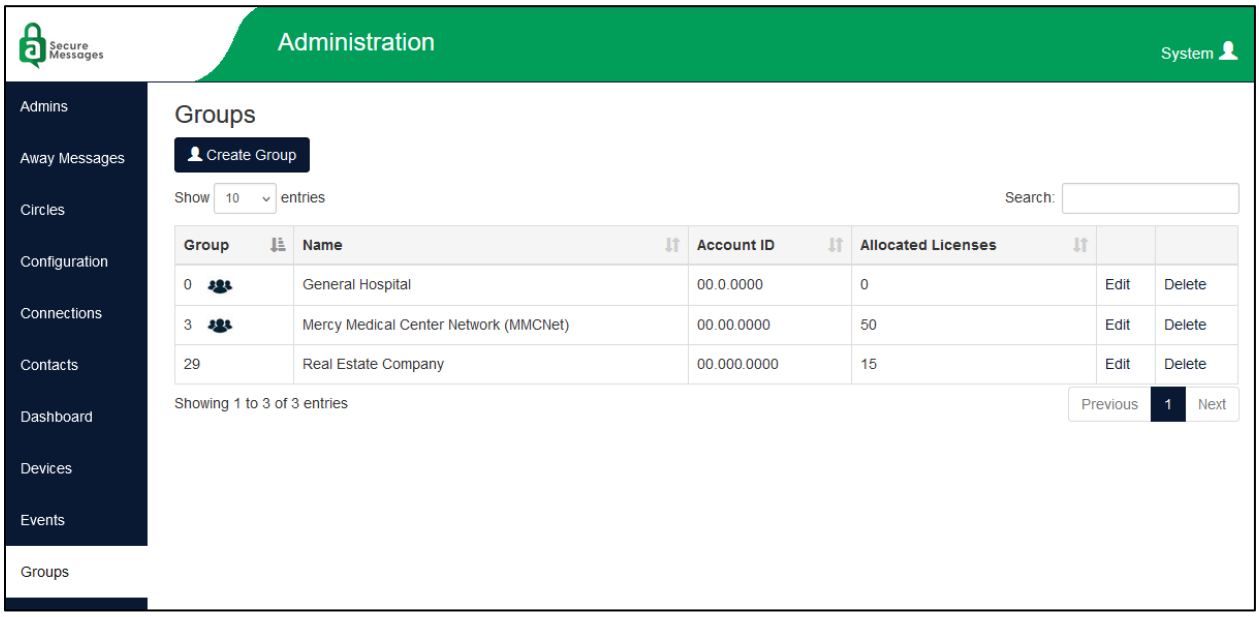
Enter the URL specified by your Single Sign-On Identity Provider.

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

Configuring Single Sign-On for Groups

The SSO settings for Groups are located under the General tab on the Group Properties screen in the ASM Administration Web.

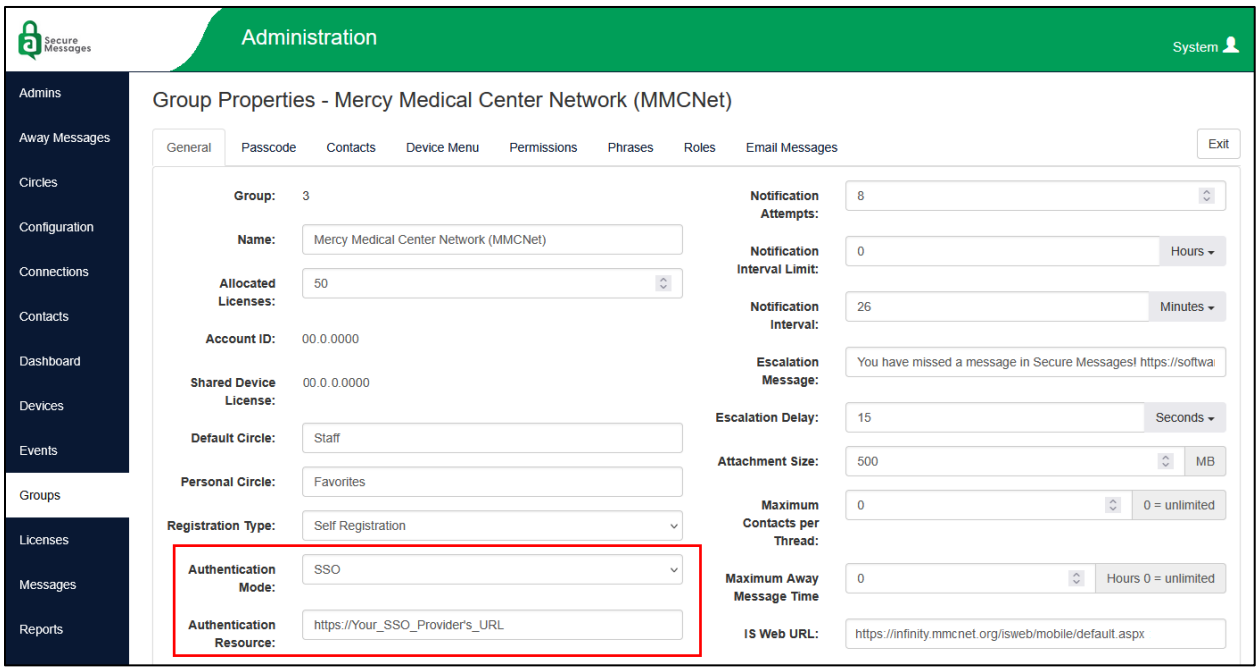
Click the Groups command on the navigation menu to access the Groups page.



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

The group authentication settings are located under the General tab.

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



Authentication Mode

The Authentication Mode setting determines how contacts in this group can log into Amtelco Secure Messages apps and the Contact Web. Each Amtelco Secure Messages group can be configured for one of two authentication modes: ASM (Amtelco Secure Messages) and SSO (Single Sign-On).

Note: Contacts are identified by username, not e-mail address.

Select "SSO" to use a Single Sign-On Identity Provider to keep track of passwords and perform authentication.

Authentication Resource

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

Enter the URL specified by your Single Sign-On Identity Provider.

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

Repeat these steps for each group that you want to use Single Sign-On.

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

*It is up to your organization to maintain and renew your security certificates.

Browser Compatibility:

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

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

Amtelco Part Number: 232MP323