Mutare Voice™ Configuration for SAML with Azure AD

Mutare Voice (SAM) can be configured to use SAML2 authentication with various identity providers. This document outlines how to configure Mutare Voice to use SAML2 with Azure Active Directory.

What You Need to Begin

You will need the following information to begin:

1. Full URL to the Mutare Voice. For the examples below, the URL is https://a-dev-sam.mutare.com
2. Admin access to the Azure AD server
3. Your token signing certificate
4. Your SAML Login URL
5. Your SAML Logout URL

Mutare Voice Configuration

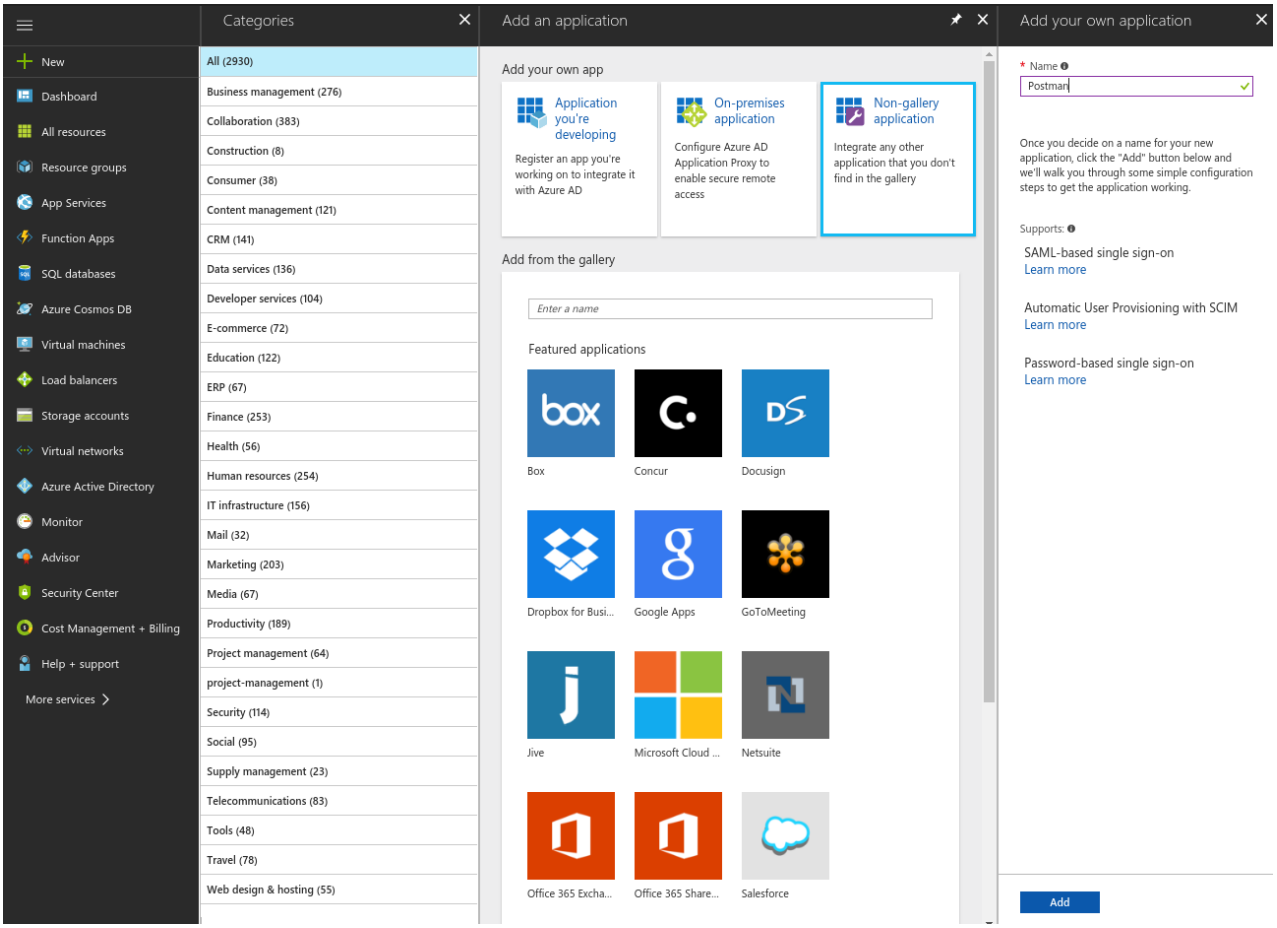
Configure the following settings in the System Settings in Mutare Voice. Please complete this section and return to your project manager:

SAML Configuration in Mutare Voice	Customer Information
Provide SAMLLogin – This is the URL to the client's Azure login. *e.g. https://login.microsoftonline.com/b2bbb9f1-5008-4dca-a49a-aed72a7bf3c8/saml2*	
Provide SAMLLogout - This is the URL to the client's Azure logout *e.g. https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0*	
Provide your Azure Token Signing Certificate. *i.e. C:\SAM\Certificates\SSO.cer*	
SAMLIdentifier – This is the URL to Mutare Voice. *i e.g. https://a-dev-sam.mutare.com*	*Mutare to provide based on pre-install document.*

Customer Initials:

Azure AD Configuration

Navigate to the Azure portal, Azure Active Directory, Enterprise Applications, and select “Add New Application” of type Non-gallery application. Enter name of app and press Add.

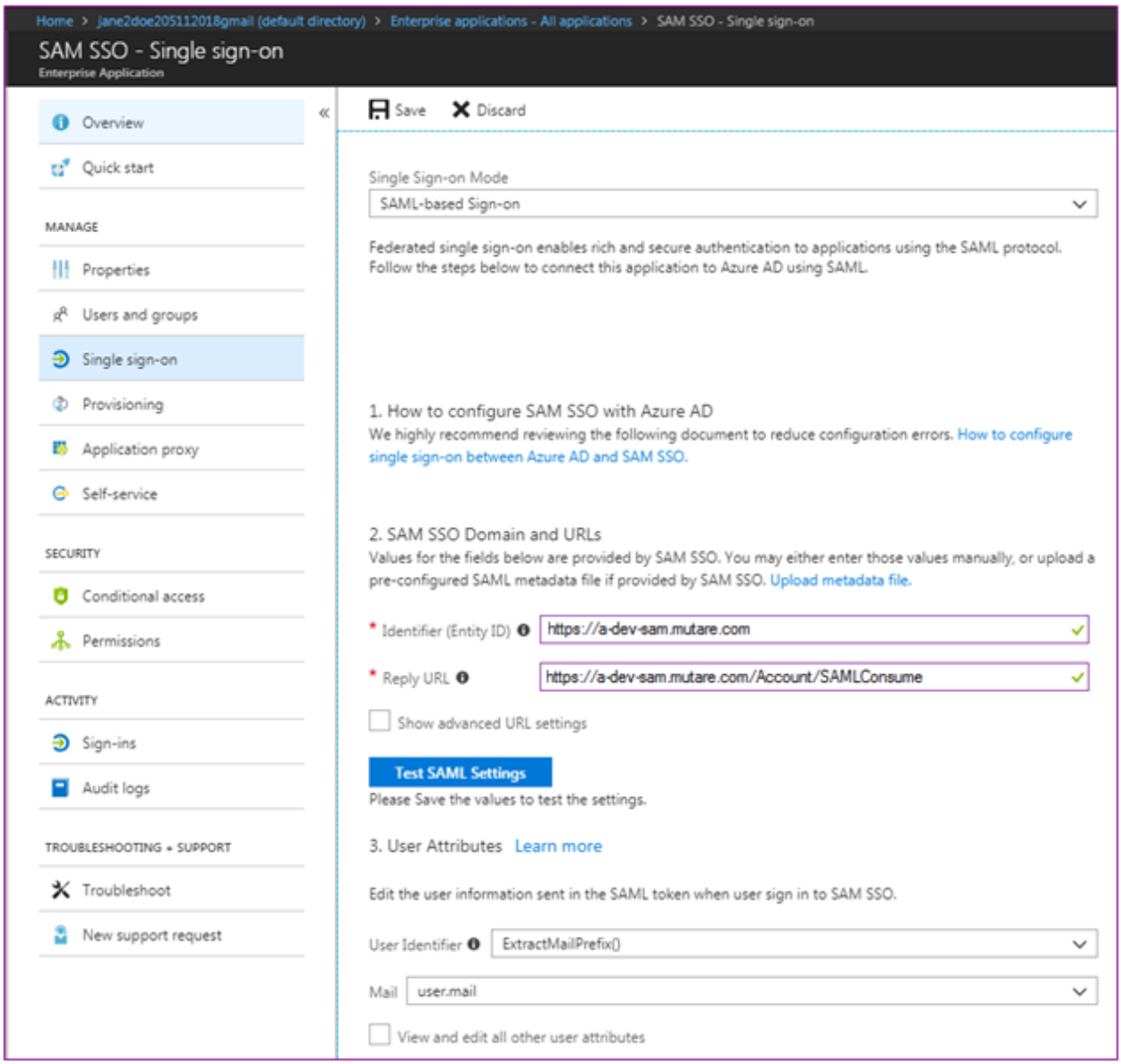


Customer Initials:

Ensure Users and groups are properly configured.

Navigate to Single sign-on. Follow the settings below:

- SAML-based Sign-on = Single Sign-on Mode
- Identifier = the Mutare Voice website URL
- Reply URL = the Mutare Voice website URL plus /Account/SAMLConsume
  NOTE: This is case sensitive. The screenshot below is incorrect.
- User Attributes User Identifier = ExtractMailPrefix(), Mail = user.mail
- Download the Certificate (Raw), we will need this.
- Navigate to the Configure Mutare Voice SSO, we will need the SAML Sign-on Service URL and the Sign-out URL.



Customer Initials:

4. SAML Signing Certificate Learn more

Manage the certificate used by Azure AD to sign SAML tokens issued to SAM SSO.

App Federation Metadata Url https://login.microsoftonline.com/b2bbb9f1-5008-4dca-a49a-aed7...

STATUS	EXPIRATION	THUMBPRINT	DOWNLOAD
Active	5/11/2021	ABBB68328ED681A34F3C143D4787ED77F888A1C6	Certificate (Base64) Certificate (Raw) Metadata XML

Create new certificate

Show advanced certificate signing settings Learn more

* Notification Email jane2doe205112018@gmail.com

5. SAM SSO Configuration

SAM SSO must be configured to use Azure AD as a SAML identity provider. Click below to view instructions on how to do this.

Configure SAM SSO

Customer Initials:

Configure SAM SSO for single sign on

For users to be able to sign in using their organization account, SAM SSO must be manually configured to use your Azure Active Directory as a SAML identity provider. SAM SSO cannot prompt or otherwise allow users to sign in using Azure Active Directory if it has not been configured to do so.

To configure SAM SSO for single sign-on:

1. Review the process for configuring SAML identity providers in SAM SSO. To determine the correct process, view the documentation for SAM SSO or contact your SAM SSO representative for more information.
2. **Note:** Some guidance on how to configure SAM SSO can be found on Azure.com, and we are in the process of migrating the application-specific steps to this guide. The older article on how to configure SAM SSO can be found here, where only the steps related to uploading the Azure AD files and URLs to SAM SSO need to be followed.
3. During this process, you will be prompted to provide files and URLs that correspond to Azure Active Directory. When prompted, use the files and URLs shown below:
    - **SAML Single Sign-On Service URL:** https://login.microsoftonline.com/b2bbb9f1-5008-4dca-a49a-aed72a7bf3c8/saml2
    - **SAML Entity ID:** https://sts.windows.net/b2bbb9f1-5008-4dca-a49a-aed72a7bf3c8/
    - **Sign-Out URL:** https://login.microsoftonline.com/common/wsfederation?wa=wsignout1.0
    - SAML Signing Certificate - Base64 encoded
    - SAML Signing Certificate - Raw
    - SAML XML Metadata
4. Once this information has been provided and configured in SAM SSO, SAM SSO will begin to require or otherwise allow users to sign in using your instance of Azure Active Directory.

Customer Initials: