Garantir

GaraSign SAML Configuration

Version 1.24.0

Table of Contents

Preface

Document Information

Title	GaraSign SAML Configuration
Product Version	1.24.0
Release Date	January 9, 2024

Trademarks

Disclaimer

Garantir makes no representations or warranties with respect to the contents of this document and specifically disclaims any implied warranties of merchantability or fitness for any particular purpose. Furthermore, Garantir reserves the right to revise this publication and to make changes from time to time in the content hereof without the obligation upon Garantir to notify any person or organization of any such revisions or changes.

We have attempted to make these documents complete, accurate, and useful, but we cannot guarantee them to be without error or otherwise perfect. When we discover errors or omissions, or they are brought to our attention, we endeavor to correct them in succeeding releases of the product.

Please send any constructive comments on the contents of this document to the following email address: support@garantir.io

Overview

This document describes how to configure SAML authentication for administrators of GaraSign.

Intended Audience

All products produced by Garantir are designed to be installed, configured, operated, and maintained by personnel with the necessary knowledge, skill, training, and qualifications to safely perform their duties. This document is intended for personnel responsible for reviewing GaraSign's architecture and assessing its security. It is assumed that the readers of this document and the users of its content have a strong understanding of:

- Security concepts including, but not limited to, authentication, authorization, digital signatures, logging, separation of duties, and preventative/detective controls
- Computer networking
- Cryptographic Tokens (e.g., hardware security modules)
- GaraSign's architecture (see the GaraSign architecture document for details)

Document Conventions

This document uses the following convention to alert you to important information.

Warnings

To help reduce the chance of data loss or corruption, this document provides warnings inside a red box with a warning icon, as shown below:

> ⚠ **Warning**: Always exercise caution when performing security-related duties.

Identity Provider Configuration

Prior to configuring SAML in GaraSign, the SAML application must first be registered with the Identity Provider (IdP) and the IdP metadata XML file must be downloaded. Instructions on how to configure SAML for various IdPs is out of scope for this document, but links to some commonly used IdPs are provided below for convenience:

1. Azure Entra ID SAML Configuration
2. Okta SAML Configuration
3. Google SAML Configuration
4. Duo SAML Configuration

Note: Since the IdP metadata XML file is a prerequisite for GaraSign, you may be required to temporarily put bogus values for the SAML URLs for your GaraSign instance. Once SAML is configured in GaraSign you will be able to download the SP metadata file and import it into your IdP's SAML configuration.

GaraSign Configuration

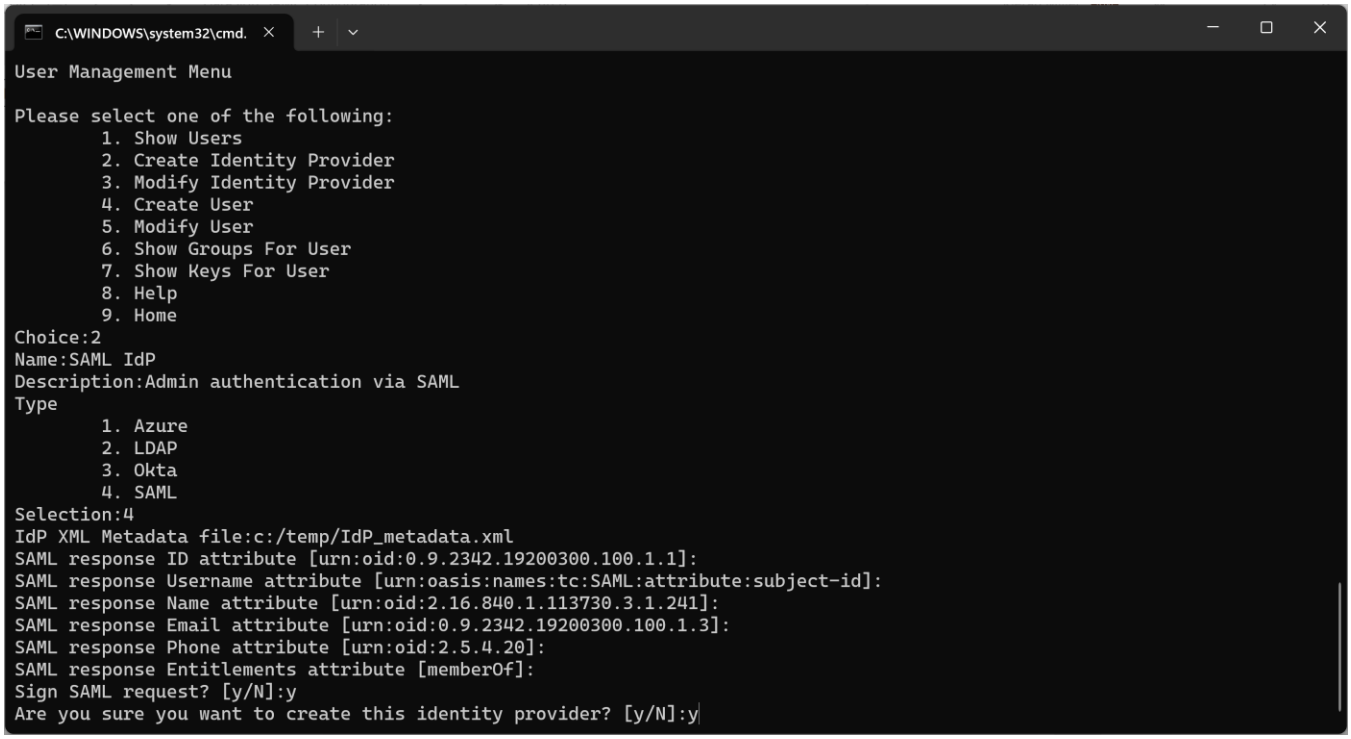
Once you have downloaded the IdP metadata XML file, you can link the IdP to GaraSign. As of this release, the preferred method to do this is via the Admin Command Line Interface (CLI), although initial beta support has been added to the web admin portal as well.

Admin CLI

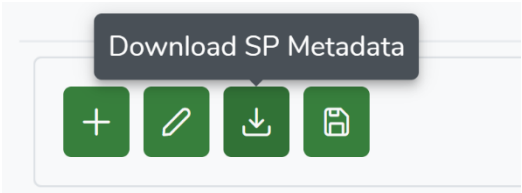
To configure SAML authentication for GaraSign administrators via the Admin CLI, execute the following steps:

1. Login to the Admin CLI
2. Choose *User Management*
3. Choose *Create Identity Provider*
4. Provide a Name
5. If desired, provide a Description
6. Choose *SAML* as the Type
7. Provide the full path (including filename) to the downloaded IdP metadata XML file
8. Enter the SAML response ID attribute (i.e., the unique identifier attribute for the user from the SAML response)
9. Enter the SAML response Username attribute (i.e., the username attribute for the user from the SAML response)
10. Enter the SAML response Name attribute (i.e., the name attribute for the user from the SAML response)
11. Enter the SAML response Email attribute (i.e., the email attribute for the user from the SAML response)
12. Enter the SAML response Phone attribute (i.e., the phone attribute for the user from the SAML response)

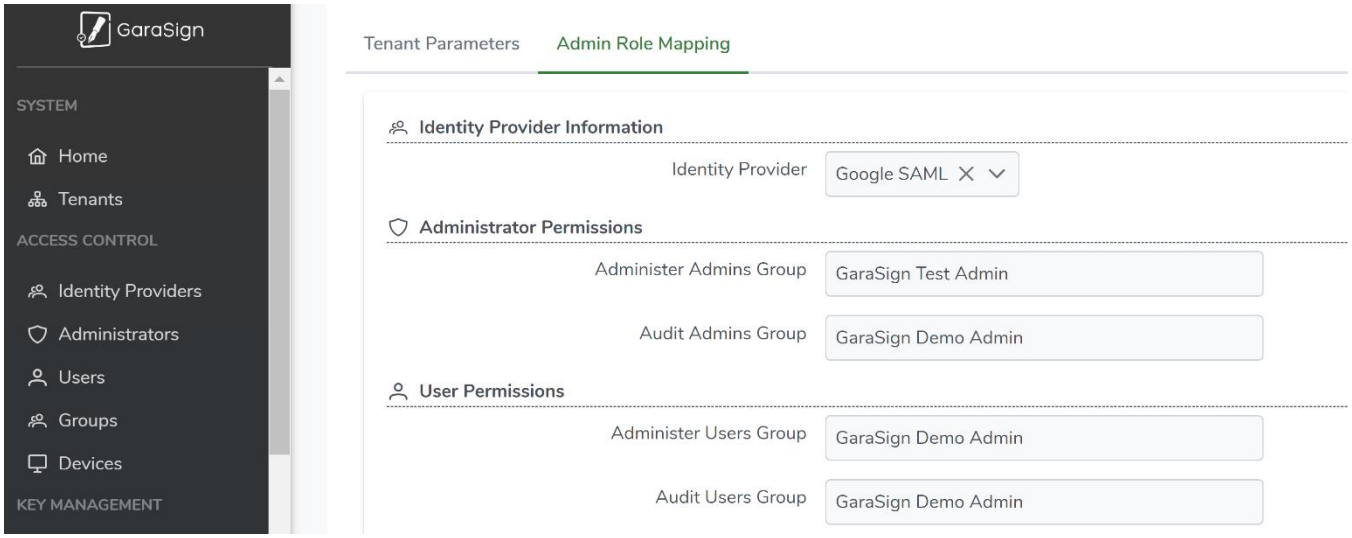
13. Enter the SAML response Entitlements attribute (i.e., the group memberships attribute for the user from the SAML response)
14. Choose whether you want the SAML response to be signed
15. Enter *Y* to confirm creation of the SAML Identity Provider in GaraSign



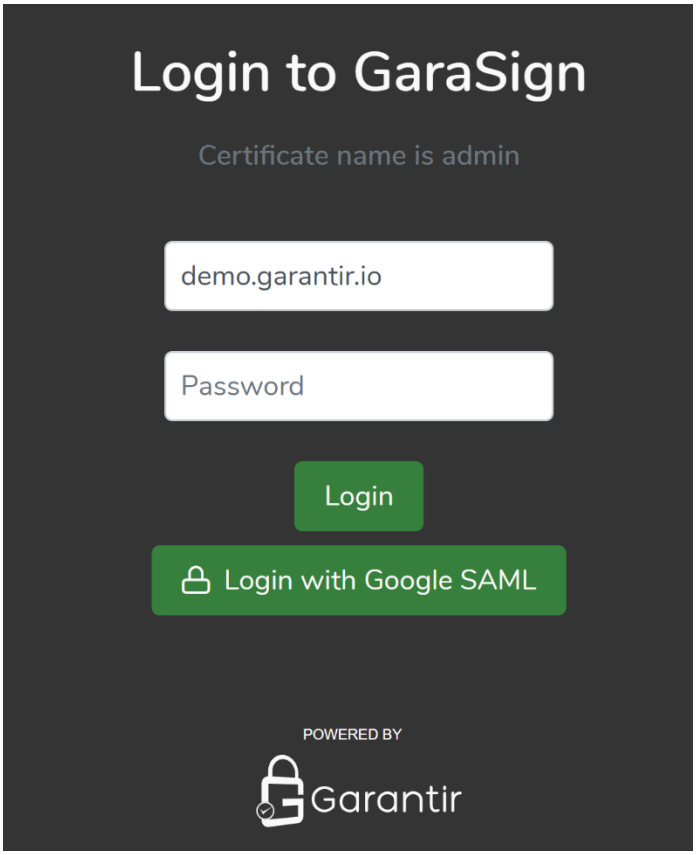
16. Login to the GaraSign web admin portal via your browser
17. Navigate to Identity Providers via the left-hand navigation
18. Select the newly created SAML Identity Provider
19. Click the Download button to download the SP metadata XML file



20. Import the SP metadata XML file into your Identity Provider's configuration
21. Back on the GaraSign web admin portal, navigate to Tenants via the left-hand navigation
22. Edit the desired tenant
23. Click on Admin Role Mapping
24. In the Identity Provider dropdown, select the newly created SAML IdP
25. For each desired role, map the appropriate group from the IdP
26. Save the changes



27. Logout of the GaraSign web admin portal and you should now be able to authenticate via SAML



Web Admin GUI

Documentation for performing these steps via the web admin portal is not currently provided as this is not yet the preferred approach. Please consult with your Garantir professional services representative if you would like to try configuring SAML via the browser.