CLOUDFLARE
AREA 1 SECURITY

Portal Single Sign-on (SSO)

Deployment and Configuration Guide with Azure

SSO Overview

For added security and convenience, Cloudflare Area 1 offers support for SAML based single sign-on (SSO) logins to our portal. This feature is centrally configured by your organization and compatible with all SAML based SSO providers. Organizations will be able to choose between having users access the Area 1 security data with a username and password + two-factor authentication (2FA) code, or having them use an SSO provider, such as one login or okta, to access the portal.

SAML Configuration Options:

1. Identity Provider SAML
2. SP-Initiated SAML

All Area 1 SAML Setup:

1. The first step, if you don't have one already, is to select and set up an SSO provider (such as Onelogin or Okta) which will manage the user interface and settings for your organization. Any software that supports SAML will work (this is not an endorsement for any SSO provider).
2. You can turn on the feature in the Area 1 portal from the SSO settings page: https://horizon.area1security.com/settings/single-sign-on

Version: 1.3

3. SSO enforcement

None

Admin

Non-admin Only

    a. **None** - Each user can choose between SSO or Username, Password + 2FA (recommended setting while testing SSO).
    b. **Admin** - This setting will force only Admin to use SSO only. The exception is that the user who enables this setting will still be able to login using Username, Password + 2FA. This is a backup so that your organization does not get locked out of the portal in emergencies.
    c. **Non-Admin Only** - this option will require that all “Read only” and “Read & Write” users use SSO to access the portal. Admins will still have the option to use either SSO or Username, Password + 2FA.

4. **SAML SSO Domain** - This is the domain that points to the SSO provider.

5. **METADATA XML** - You will need to copy and paste the SAML XML Metadata settings from your provider into Area 1. These settings (and even their exact text descriptions) are in different locations depending on your SSO provider.
   Please contact your SOO provider or Area 1 support for assistance with this step if you run into any issues.

6. **Identity Provider SAML Setup -** Area 1’s service today supports only IdP-Initiated (Identity Provider) SAML 2.0. The values to be configured in the IdP setup are as follows:

Identity Provider SAML Setup:

Area 1’s service today supports only IdP-Initiated (Identity Provider) SAML 2.0. The values to be configured in the IdP setup are as follows:

SAML Consumer URL: https://horizon.area1security.com/api/users/saml

A customer parameter must also be added to the SAML assertion.

Parameter: email

Value = Email of user. Should match the email the user has already had created in the Area 1 portal

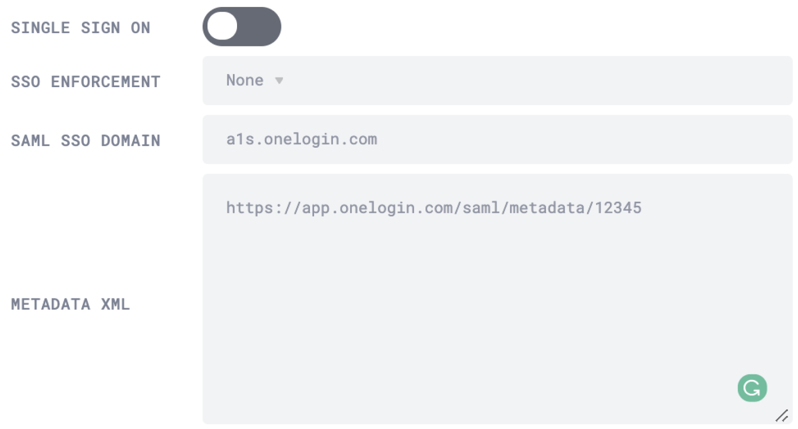
Once you have the above configured and the SAML icon created download the metafile.

Copy and paste it into the box “METADATA XML”

To test - On the landing page of your SAML solution. Locate the ICON you have created

for SSO login with Area 1 Security.

*user must already have an account with Area 1’s portal.



SINGLE SIGN ON

SSO ENFORCEMENT: None ▾

SAML SSO DOMAIN: a1s.onelogin.com

METADATA XML: https://app.onelogin.com/saml/metadata/12345

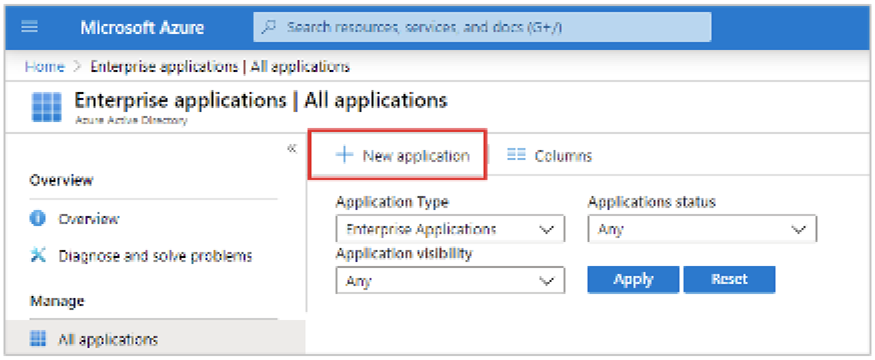
Azure Active Directory:

Azure Active Directory Configuration

This will walk you through the steps for configuring a Non-Gallery Enterprise Application within Azure Active Directory to establish SAML SSO with Area 1 Security Portal.

1. Login to Azure portal and open **Enterprise Applications**.

2. Click on **+ New Application** to create a new application.

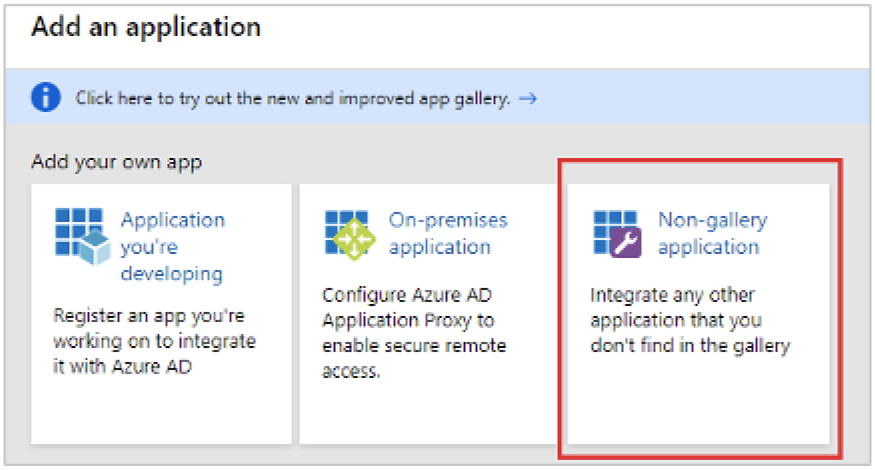

Microsoft Azure
Search resources, services, and docs (G+/)
Home > Enterprise applications | All applications
Enterprise applications | All applications
Azure Active Directory
«
+ New application
Columns
Overview
Overview
Diagnose and solve problems
Manage
All applications
Apply
Reset

Application Type: Enterprise Applications

Applications status: Any

Application visibility: Any

3. Select **Non-gallery application**.



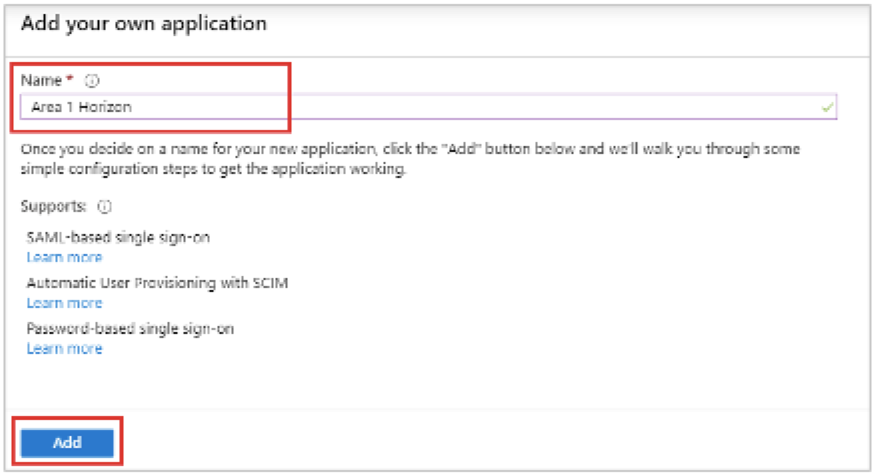
Click here to try out the new and improved app gallery. →

Application you're developing: Register an app you're working on to integrate it with Azure AD

On-premises application: Configure Azure AD Application Proxy to enable secure remote access.

Non-gallery application: Integrate any other application that you don't find in the gallery

4. Name the application and then click **Add** at the bottom of the screen.



Add your own application

Name * ⓘ

Area 1 Horizon

Once you decide on a name for your new application, click the "Add" button below and we'll walk you through some simple configuration steps to get the application working.

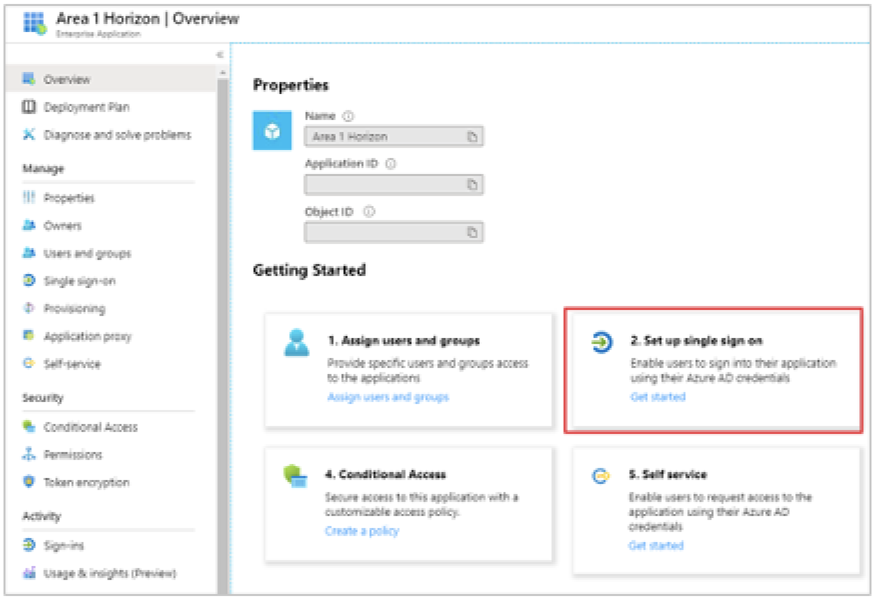
Supports: ⓘ

SAML-based single sign-on
Learn more

Automatic User Provisioning with SCIM
Learn more

Password-based single sign-on
Learn more

5. On the application Overview page, click on **2. Set up Single Sign On**.



Properties

Name ⓘ

Area 1 Horizon

Application ID ⓘ

Object ID ⓘ

Getting Started

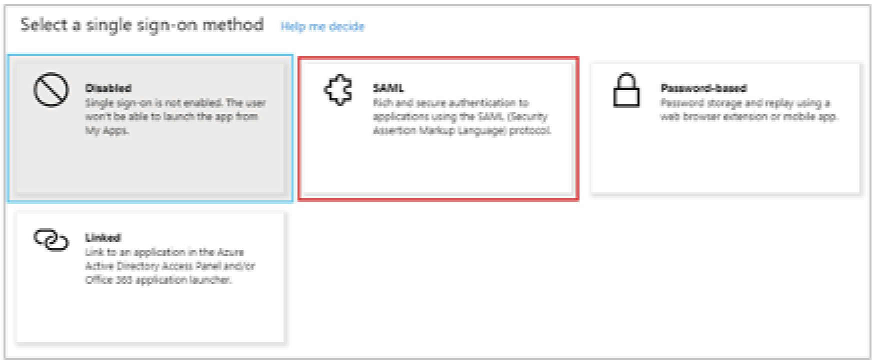
1. Assign users and groups
Provide specific users and groups access to the applications
Assign users and groups

2. Set up single sign on
Enable users to sign into their application using their Azure AD credentials
Get started

4. Conditional Access
Secure access to this application with a customizable access policy.
Create a policy

5. Self service
Enable users to request access to the application using their Azure AD credentials
Get started

6. Select **SAML** as your single sign-on method



Select a single sign-on method Help me decide

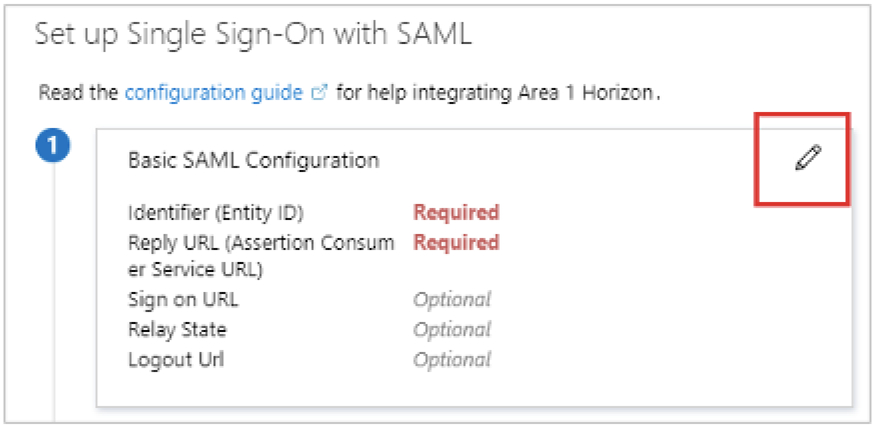
Disabled
Single sign-on is not enabled. The user won't be able to launch the app from My Apps.

SAML
Rich and secure authentication to applications using the SAML (Security Assertion Markup Language) protocol.

Password-based
Password storage and replay using a web browser extension or mobile app.

Linked
Link to an application in the Azure Active Directory Access Panel and/or Office 365 application launcher.

7. Edit **Basic SAML Configuration**.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating Area 1 Horizon.

1 Basic SAML Configuration

Identifier (Entity ID)	Required
Reply URL (Assertion Consumer Service URL)	Required
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

8. Update the **Identifier (Entity ID)** and **Reply URL (Assertion Consumer Service URL)** fields as follows, then **Save** and exit the Basic SAML Configuration screen.

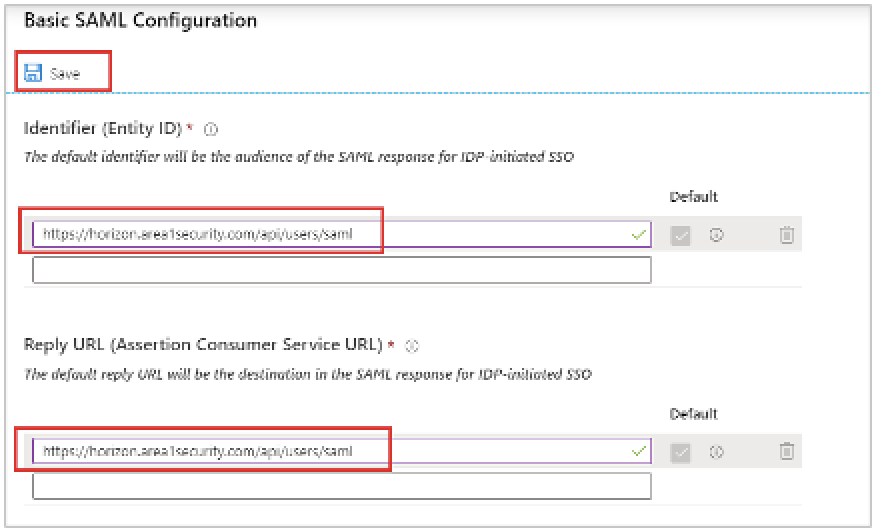
Identifier (Entity ID): https://horizon.area1security.com

Reply URL (Assertion Consumer Service URL): https://horizon.area1security.com/api/users/saml

Sign-On URL: *Blank*

Relay State: *Blank*

Logout Url: *Blank*



Basic SAML Configuration

Identifier (Entity ID) *

The default identifier will be the audience of the SAML response for IDP-initiated SSO

Default

https://horizon.area1security.com/api/users/saml

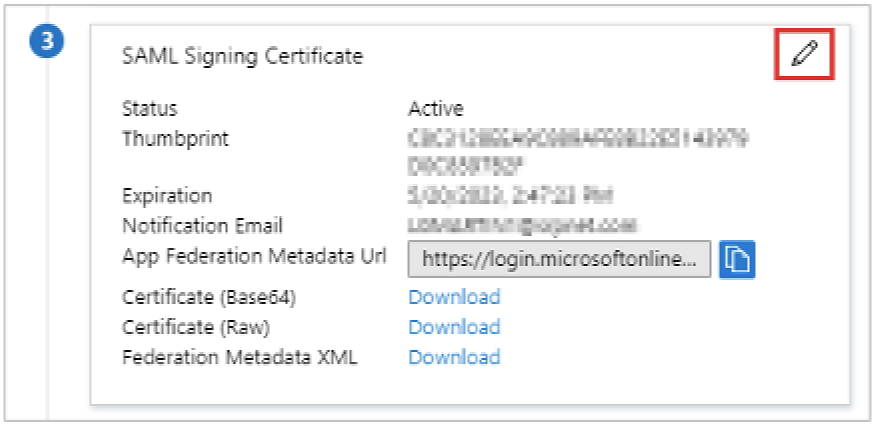
Reply URL (Assertion Consumer Service URL) *

The default reply URL will be the destination in the SAML response for IDP-initiated SSO

Default

https://horizon.area1security.com/api/users/saml

9. Edit **SAML Signing Certificate**.



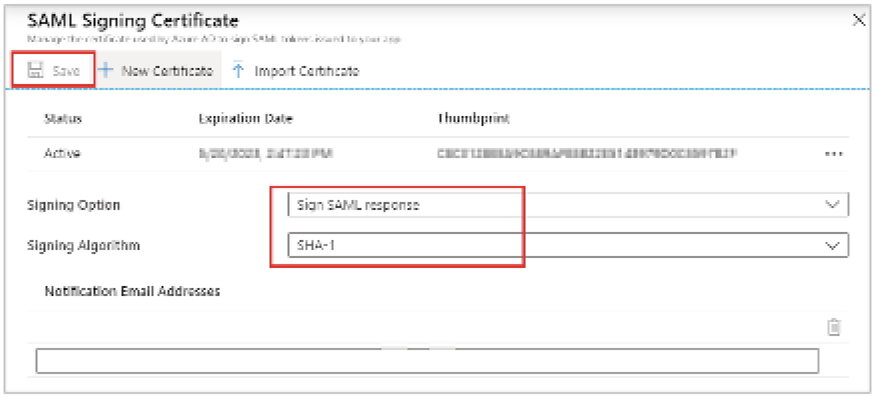
SAML Signing Certificate

Status	Active
Thumbprint	[redacted]
Expiration	[redacted]
Notification Email	[redacted]
App Federation Metadata Url	https://login.microsoftonline...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

10. Update **Signing Option** and **Signing Algorithm** as follows, then **Save** and exit the SAML Signing Certificate screen.

Signing Option: Sign SAML response

Signing Algorithm: SHA-1



SAML Signing Certificate

Manage the certificate used by Azure AD to sign SAML tokens issued to your app

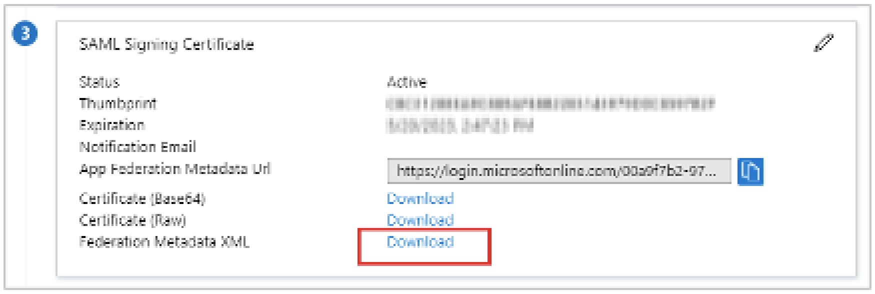
Status	Expiration Date	Thumbprint
Active	[redacted]	[redacted]

Signing Option: Sign SAML response

Signing Algorithm: SHA-1

Notification Email Addresses

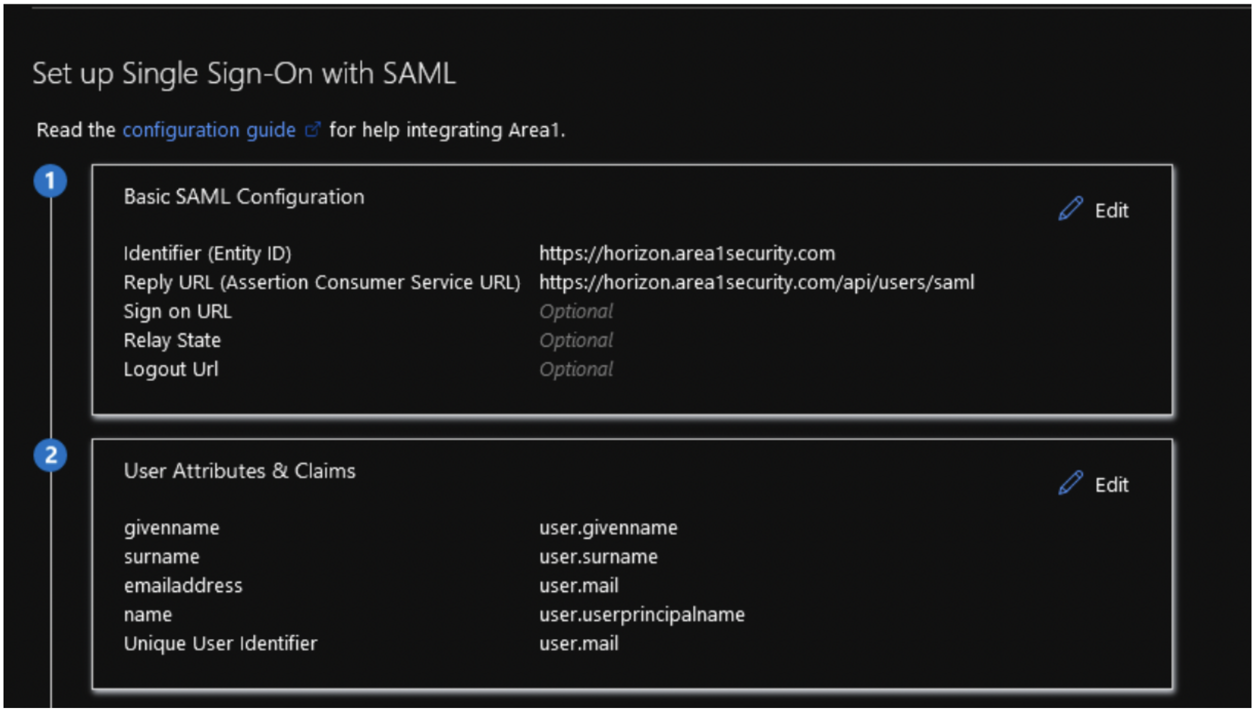
11. Download the **Federation Metadata XML** as you will need it for the SSO Configuration within the Area 1 Portal.



SAML Signing Certificate

Status	Active
Thumbprint	[redacted]
Expiration	[redacted]
Notification Email	
App Federation Metadata Url	https://login.microsoftonline.com/00a9f7b2-97...
Certificate (Base64)	Download
Certificate (Raw)	Download
Federation Metadata XML	Download

12. This completes the Enterprise application SAML configuration. The configuration should look similar to the screenshot below.



Set up Single Sign-On with SAML

Read the configuration guide for help integrating Area1.

1 Basic SAML Configuration

Identifier (Entity ID)	https://horizon.area1security.com
Reply URL (Assertion Consumer Service URL)	https://horizon.area1security.com/api/users/saml
Sign on URL	*Optional*
Relay State	*Optional*
Logout Url	*Optional*

2 User Attributes & Claims

givenname	user.givenname
surname	user.surname
emailaddress	user.mail
name	user.userprincipalname
Unique User Identifier	user.mail

PLEASE NOTE: Now that the application configuration is complete, update **User Assignments** and **Application Properties** as needed to ensure that authorized personnel are able to access the new application from their Apps Catalog. Additionally, you may choose to update the application Logo image file or the privacy policy URL.

Area 1 Portal Configuration with Azure:

This section will provide guidance on completing the SSO configuration within the Area 1 Portal using the information from the Azure AD application created in the previous section.

1. Login to Area 1 Portal.
2. Navigate to **Settings > SSO**.
3. Update SSO settings as follows and verify the configuration looks similar to the configuration below.

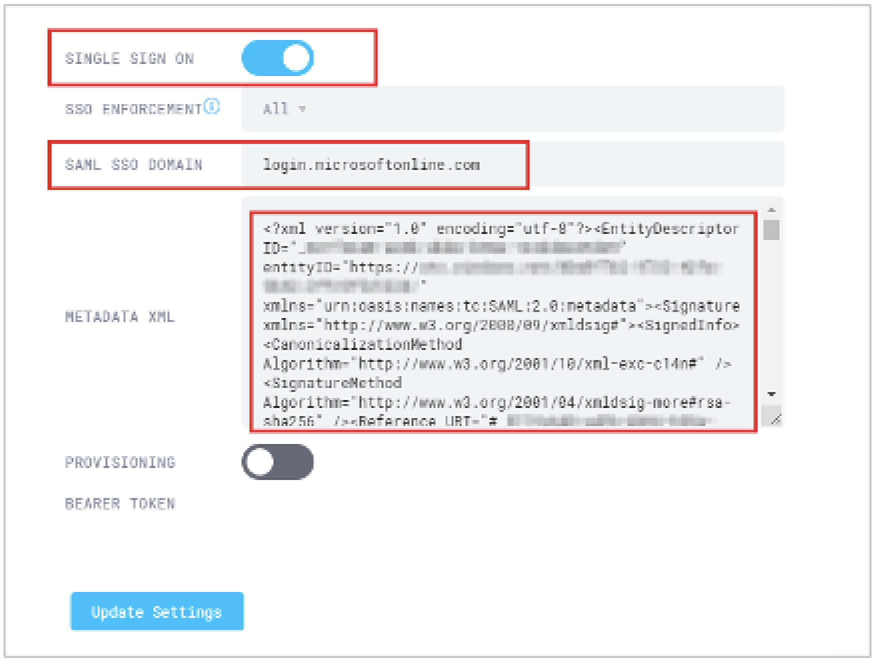
Single Sign-On: Enabled

SSO Enforcement: *Configure to the desired setting based on your organization's policy*

SAML SSO Domain: login.microsoftonline.com

Metadata XML*: *Paste contents of previously downloaded Metadata XML file from Azure AD*

> ***To obtain Metadata XML file contents, open in Text Editor program and copy all of the text. Ensure there are no leading carriage returns or spaces when you copy the text. The copied text should begin with**
>
> <?xml version="1.0" encoding="utf-8"?><EntityDescriptor ID="_*<yourDescriptorID>*" entityID="https://*<yourEntityID>* " xmlns="urn:oasis:names:tc:SAML:2.0:metadata">...



SINGLE SIGN ON	●
SSO ENFORCEMENT	All ▾
SAML SSO DOMAIN	login.microsoftonline.com
METADATA XML	
PROVISIONING	○
BEARER TOKEN	

```
<?xml version="1.0" encoding="utf-8"?><EntityDescriptor
ID="_[redacted]"
entityID="https://[redacted]
[redacted]"
xmlns="urn:oasis:names:tc:SAML:2.0:metadata"><Signature
xmlns="http://www.w3.org/2000/09/xmldsig#"><SignedInfo>
<CanonicalizationMethod
Algorithm="http://www.w3.org/2001/10/xml-exc-c14n#" />
<SignatureMethod
Algorithm="http://www.w3.org/2001/04/xmldsig-more#rsa-
sha256" /><Reference URI="#[redacted]
```

4. Click **Update Settings** to save configuration.

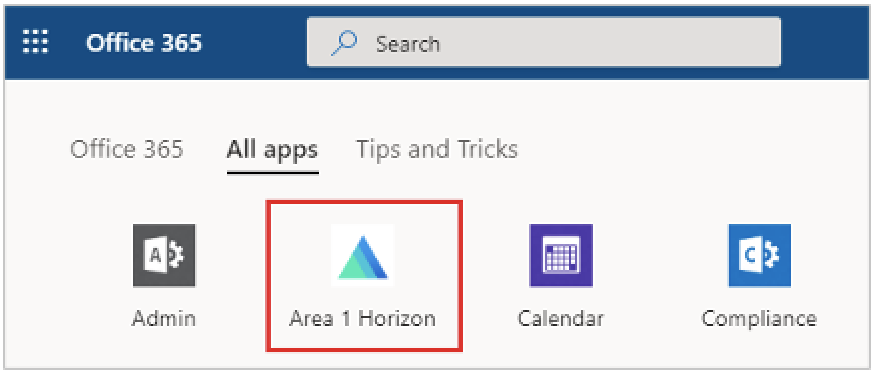
Test SSO Configuration:

After you have completed both the Azure AD Enterprise Application configuration along with Area 1's Portal SSO configuration, it is time to test your access.

Important: Verify the **User Assignments** and **Application Properties** of your new Azure AD application have been updated accordingly to ensure that authorized personnel are able to access the new application from their Office 365/Azure Apps Catalog page. Application logos and privacy policy URL can also be updated as needed.

For this example, the Area 1 Horizon application's logo has been updated.

1. Login to your Office 365 portal (portal.office.com).
2. Click on **All Apps**. Navigate to **Settings > SSO**.
3. Locate the **Area 1 Horizon** application (or whichever name you gave your application) and click on it to initiate your SSO login with Area 1's Portal.



4. If configured correctly, you should be signed in to the Area 1 Portal and redirected to the dashboard.

Troubleshooting:

- Verify the user exists in Area 1's Portal.
- Verify Identifier and Reply URLs in Azure AD.
- Verify SAML response is being signed (**not** SAML assertion) and algorithm set to SHA-1.
- Verify SAML SSO Domain is set correctly in Area 1 Portal SSO settings.
- Verify name ID identifier is set to Email Address

If the configuration is correct, but issues persist, please submit the ticket to Area 1 Support with the following SAML tracer logs:

1. add this 'saml tracer' extension to your browser: https://chrome.google.com/webstore/detail/saml-tracer/mpdajninpobndbfcldcmbpnnbhibjmch?hl=en
2. Open up the extension
3. Try connecting to Area 1 through SSO
4. Copy the response you see on saml tracer (or download the json file) and send it Area 1 support.