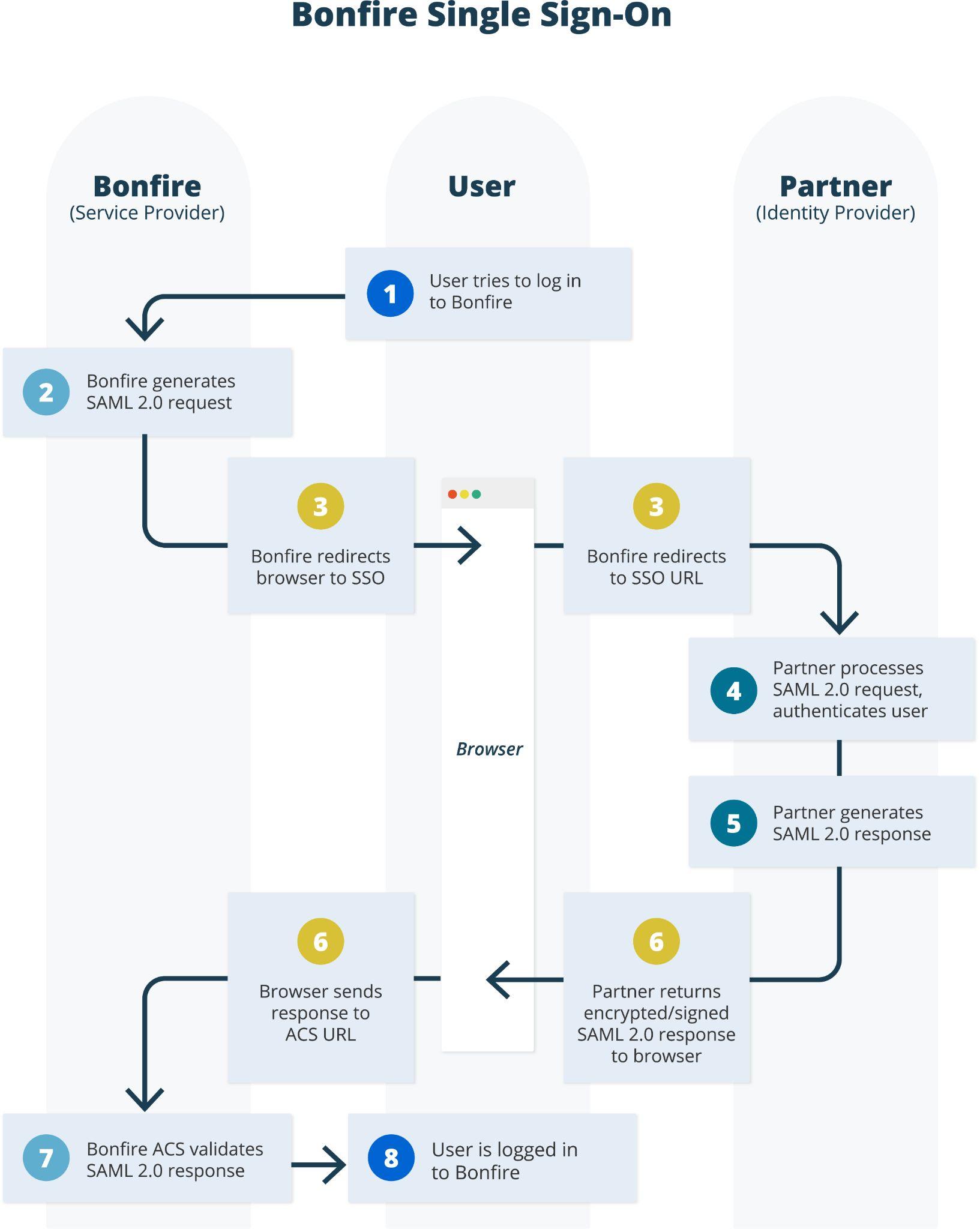
A close up of a logo

Description automatically generated

Azure AD - Bonfire Single Sign-On Setup

Bonfire Single Sign-On (SSO) is based on the [SAML 2.0 protocol](https://www.oasis-open.org/committees/tc_home.php?wg_abbrev=security#samlv20). This is how it works:

  
*Figure 1: Logging in to Bonfire using Single Sign-On*

# **Getting Started:**

Your organization will be assigned a testing environment to ensure your production portal is not impacted as we work through your unique configurations. The portal you have been assigned is **[Assigned Portal Name.** Please click the link below to expose the SAML Metadata**.**

|  |
| --- |
| [**https://sso5.bonfirehub.com/saml/metadata**](https://sso5.bonfirehub.com/saml/metadata) |

**Interpreting the Metadata**

**NOTE: The metadata will be unique to your SSO Environment Assignment.**

The testing environment will look like the .xml in the screenshot below:

Graphical user interface, text, application, email

Description automatically generated

There is important information you will need to configure on your Azure AD Application. We have highlighted the information below:

**entityID**

Graphical user interface, text, application, email

Description automatically generated

**SingleLogOutService**

Graphical user interface, text, application

Description automatically generated

**AssertionConsumerService**

Graphical user interface, application

Description automatically generated with medium confidence

**NOTE: The metadata will be unique to your SSO Environment Assignment.**

**Steps for setting up Azure AD**:

**Step 1**: Create the Application.

To create the application navigate to your Azure AD>Enterprise Applications - Name the application Bonfire

Graphical user interface, text, application

Description automatically generated

**Step 2**: Select Single Sign On

Graphical user interface, application, Word

Description automatically generated

**Step 3**: Edit Basic SAML configuration

This is where Bonfire’s SAML Metadata is configured.

Graphical user interface, text, application, email

Description automatically generated

Input the following information:

|  |  |
| --- | --- |
| **Azure Field** | **Bonfire Metadata Value** |
| Identifier (Entity ID) | **entityID (e.g** https://sso.bonfirehub.com/saml/metadata) |
| Reply URL (Assertion Consumer Service URL) | **AssertionConsumerService (e.g** https://sso.bonfirehub.com/saml/acs) |
| Logout URL | SingleLo**goutService** (**e.g** https://sso.bonfirehub.com/saml/sls) |

**NOTE: The metadata will be unique to your SSO Environment Assignment. Refer to Interpreting the Metadata in the above section of this document**

A screenshot of a computer

Description automatically generated with medium confidence

**Step 4**: Configure your Attributes & Claims

Click edit within Attributes & Claims

**Graphical user interface, text, application

Description automatically generated**

**Unique Identifer (NAME ID)**

The first configuration required is Unique User Identifier (Name ID). This must be set as **UNSPECIFIED**

A picture containing application

Description automatically generated

Once saved, configure the following claims

**User.Mail**

Name: **urn:oid:0.9.2342.19200300.100.1.3**

Namespace: Leave Blank

Source: Attribute

Source Attribute: user.mail

Background pattern

Description automatically generated with medium confidence

**Users.Surname**

Name: **urn:oid:2.5.4.4**

Namespace: Leave Blank

Source: Attribute

Source Attribute: user.surname

Background pattern

Description automatically generated

**Users.Givenname**

Name: **urn:oid:2.5.4.42**

Namespace: Blank

Source: Attribute

Source Attribute: user.givenname

Background pattern

Description automatically generated

**User Settings**

Through AzureAD, organizations will have two options for assigning users to the application:

1. **PREFERED -** Assignment Not required – This will allow any user active in your IdP to authenticate through Azure. Bonfire will then check the user in our system and authenticate accordingly. If User is not present in Bonfire, they will receive an unauthorized error message and be blocked from access Bonfire. Subsequently, if an employee is not in your IdP and is in Bonfire, they will be blocked from authenticating.
2. Assignment to Application – This will require Procurement Teams in frequently send IT requests for access as Evaluation Committees are created for each Project. Configuring your SSO in this way will require an internal processes be set for these requests. Each user will be added to the Users & Groups Menu.

To adjust this setting, navigate to the SAML Properties and set assignment required

A screenshot of a computer

Description automatically generated with medium confidence

# 

# **Exporting/Sending your Federation metadata**

In order for the integration to be tested, Bonfire’s SSO Integrations Team must configure our equivalent of the integration. To do this, we must receive your federatation metadata. This can be found by navigating the SAML Signing Certificate. You will have two options for sending the data:

1. Copy the App Federation Metadata URL and email it to Bonfire’s SSO Integration Contact
2. Download the .XML file and email it to Bonfire’s SSO Integration Contact

# Graphical user interface, application, Teams Description automatically generated

# **Testing**

To test your settings, you will first need to be invited into the SSO Portal by Bonfire’s SSO Integration Team. Once invited, navigate to the assigned SSO portal and attempt logging in. If successful, you will be able to view the following Screen:

Graphical user interface, text, application, email

Description automatically generated

In the event of an error, please provide screenshots of the error messaging to Bonfire’s SSO Integration Team for further troubleshooting.

# **Troubleshooting:**

You may receive a number of error messages when attempting to log into Bonfire. We have included several common errors below with their resolutions:

|  |  |
| --- | --- |
| **Error Message** | **Resolution** |
| * Signature validation failed. | * Certificate is invalid or configured incorrectly. Ensure you have configured your Basic SAML Configuration to point to correct portal urls |
| * Invalid issuer in the Assertion\/Response (expected 'URL', got 'OTHER\_URL') | Wrong SamlIdpEntityId, confirm Basic SAML Configurations are configured to the correct portal url |
| * Missing mail claim urn:oid:0.9.2342.19200300.100.1.3 | * Claims are misconfigured, check Claims and Attributes and ensure you have input the correct information |
| * NameID not found in the assertion of the Response | Claims misconfiguration around NameID not pointing to email, or missing. Review Claims and Attributes |
| * No user found with email | IdP authenticated user who doesn't have an account in Bonfire. Confirm user has been invited into Bonfire |

# **Configurations for Production**

Upon successful testing in our SSO sandbox environment, you can update your SSO configuration to point towards the production environment. The basic SAML configuration will need to be updated. Your Production URL is:

|  |
| --- |
| [**https://waukeshacounty.bonfirehub.com/saml/metadata**](https://waukeshacounty.bonfirehub.com/saml/metadata) |

The following values will need to be updated:

|  |  |
| --- | --- |
| **Azure Field** | **Bonfire Metadata Value** |
| Identifier (Entity ID) | **entityID** |
| Reply URL (Assertion Consumer Service URL) | **AssertionConsumerService** |
| Logout URL | **SingleLogoutService** |

# **Testing in Production**

The final test will occur in production, once invited, navigate to the Production portal and attempt logging in.