Single Sign-On Authentication for Blackbaud Award Management

Updated: 8/09/2022

Contents

User Account Maintenance

An attribute of each user's account in Blackbaud Award Management or Stewardship Management is a unique user ID corresponding to an attribute available through your SSO system and available in your student information system, e.g., Banner PIDM, Datatel Colleague ID, or PeopleSoft Employee ID. This information should be enough to uniquely identify users logging into the system.

Once the integration is established, users who authenticate via SSO will go through the traditional means for your campus for functions such as password recovery or changing their password. Should a user update his or her credentials, Blackbaud will work immediately with the new credentials as our system relies on your SSO server to handle all user authentication.

Additionally, once a user exists in Blackbaud Award Management or Stewardship Management with a specific user ID, that user ID cannot change. Other user attributes such as name and email address may change, however, the user ID must remain the same.

SSO Integration Accompanied with an Import of Student Information

We highly recommend our clients take advantage of our student information import API alongside the SSO integration. This provides the ideal user experience to both administrators and students. These two integrations work in concert based on an immutable and unique identifier.   When an applicant signs into Blackbaud Award Management or Stewardship Management via SSO, the SSO server passes Blackbaud a unique identifier. Blackbaud Award Management and Stewardship Management then uses this unique identifier to look up the student's information in the import file. In other words, the unique identifier passed from your SSO server is the key to marry that user up to his data in the import file. The unique identifier may be the same as the username for an applicant only if that identifier will never change. Please refer to the Blackbaud Award Management Data Import Process document for more information.

Please note that the unique identifier returned by your SSO server must match exactly to the unique identifier in the import file, down to the casing of text. For instance, if your SSO server returns a unique identifier for a user of "N12345" when she logs in and that corresponding user's import record is associated to the unique identifier "n12345", the records will not be matched. Blackbaud would not consider "N12345" to match "n12345".

Password Storage

The only SSO user passwords Blackbaud ever needs are the passwords for test accounts. These are used during implementation to verify that the SSO configuration is set up correctly. These passwords are also used whenever system maintenance is performed which requires a testing of proper SSO authentication. These test accounts can be completely bare bones; they need only allow Blackbaud connect and authenticate the sample account.

Linking to Blackbaud Award Management or Stewardship Management from Your SSO Portal

Some clients wish to include a link inside their SSO portal to pass users directly into Blackbaud already authenticated. If you wish to do this, please use the URL below. Please note that you will need to replace **client_subdomain** with your Blackbaud Award Management or Stewardship Management subdomain.

SAML Example:

https://bigstate.academicworks.com/saml.init / https://**client_subdomain**.academicworks.com/saml/init

Shibboleth Example:

https://bigstate.academicworks.com/secure / https://**client_subdomain**.academicworks.com/secure

Whitelist IP Addresses

Some institution's IT policies dictate that you must have a specific set of IP addresses to add to your firewall's outbound traffic whitelist. If this is the case for your institution, please whitelist the IP addresses below. If you wish to specify a port, all traffic for the import process should be over HTTPS and port 443.

54.85.254.104
54.88.71.228
54.173.102.180
54.174.140.185
54.175.197.190
54.175.217.111

Single Logout

Currently, Blackbaud Award Management and Stewardship Management do not support Single Logout (SLO). There are considerable technical and user experience issues with SLO. Blackbaud recommends that our clients implement SSO session timeouts, and that clients consider adding language to their SSO portal and Blackbaud site encouraging users to log out of both Blackbaud Award Management and their SSO portal. Blackbaud automatically logs out any user after 30 minutes of inactivity.

This is mainly in response to the fact that the Shibboleth 2 IdP does not support SLO. You can read more about this from the maintainers of Shibboleth here: https://wiki.shibboleth.net/confluence/display/CONCEPT/SLOIssues.

We do, however, support redirecting users to a url upon logging out of Blackbaud Award Management and Stewardship Management. If you would like to use this feature, please provide the sign out redirect URL in your configurations.

SAML SSO

Authentication Between Systems

When a client implements SAML SSO for Blackbaud Award Management or Stewardship Management, scholarship administrators and applicants will be authenticated using their SSO credentials. This is accomplished using SAML 2.0 (Secure Access Markup Language), which allows two disparate systems to create and exchange authentication and authorization information using an XML framework thus minimizing the need for your campus users to re-enter their credentials when accessing Blackbaud Award Management or Stewardship Management.

Note: Blackbaud supports the SAML 2.0 protocol, which is not backwards compatible with SAML 1.x.

In a SAML SSO transaction, an authenticated campus user is seamlessly signed in to Blackbaud Award Management and Stewardship Management without re-submitting his credentials. In this type of transaction, the campus is the SAML authority and makes an authentication statement, which declares the user's UID (unique identifier) and how he was authenticated. If the relaying party (called an assertion consumer service in SAML

SSO transactions) chooses to trust the campus system, the user is seamlessly signed into the service provider using the user's UID contained in the statement. If a user is not currently logged into your SSO portal, Blackbaud Award Management or Stewardship Management will direct the user to your SSO portal to authenticate before gaining access to the system.

Once Blackbaud has connected to your SSO server and securely validated the user, we search for the user's UID provided by your SSO portal as the external key into our table of users. Blackbaud uses this UID as a lookup key to the user account in Blackbaud Award Management or Stewardship Management database to determine which user is logging in and what that user's appropriate permission level should be. If this is the user's first time to attempt to log into Blackbaud Award Management or Stewardship Management, we will create a new user account for that user. The default role in the system is that of an applicant. For a new user to have administrative privileges, another administrative user will need to bestow those additional privileges on the new user.

Note: Your IdP server should be configured for SP-initiated Single Sign-On to allow users to initiate authentication either from your SSO portal or from Blackbaud Award Management or Stewardship Management. This is the best practice configuration for services not managed by campus IT resources, and it is strongly recommended to not use IdP-initiated Single Sign-On.

Configuring SAML in your Award Management System

When you are ready to begin the configurations, you can enter them directly into your Award Management System. To access the system, please contact us, and we will be able to provide an account for you.

Once you have access to the site, the configuration page can be found under the ***Site-Authentication-SAML SSO Setup*** menu. When configuring SAML SSO for use with Blackbaud Award Management and Stewardship Management, we need the following pieces of information:

1. What is the IdP metadata URL for your SSO system? If you're not able to provide a metadata URL, please provide the target URL for your SSO service.
2. What is the Name Identifier Format for the unique identifier Blackbaud will be using? The possible Name Identifier Format values are:
    a. urn:oasis:names:tc:SAML:1.1:nameid-format:unspecified (default value)
    b. urn:oasis:names:tc:SAML:1.1:nameid-format:emailAddress
    c. urn:oasis:names:tc:SAML:2.0:nameid-format:persistent
    d. urn:oasis:names:tc:SAML:2.0:nameid-format:transient

    Please keep in mind that the value of the Name ID should correspond to the UID that will be used to uniquely identify staff and students, and will be provided to Blackbaud via the student import file.
3. What is the UID attribute Name? This attribute should appear in the AttributeStatement portion of your SAML response and should have the same value as the Name Identifier Format.
4. What is the email attribute Name? This attribute appears in the AttributeStatement portion of your SAML response.
5. If you are unable to provide metadata, please provide a PEM encoded certificate for your SSO server.
6. If you would like to redirect users to a specific URL upon logging out of Blackbaud, please provide the URL.

7. If possible, please provide credentials for a test account to us. The test account does not need to be a real user, however, must contain the unique attributes that you'll be passing over (unique ID and email address).

Once you have provided the configuration details within the system, please contact us, and we can begin testing the authentication process.

Shibboleth SSO

Authentication Between Systems

When a client implements federated SSO authentication via Shibboleth for Blackbaud Award Management or Stewardship Management, scholarship administrators and applicants will be authenticated using their SSO credentials. This is accomplished using Shibboleth 2.x for institutions who are members of the InCommon Federation, which allows two disparate systems to create and exchange authentication and authorization information using an XML framework thus minimizing the need for your campus users to re-enter their credentials when accessing Blackbaud Award Management or Stewardship Management.

In the Shibboleth SSO transaction, an authenticated campus user is seamlessly signed in to Blackbaud Award Management and Stewardship Management without re-submitting his credentials. In this type of transaction, the campus is the IdP (Identity Provider) and makes an authentication statement, which declares the user's UID (unique identifier) and how he was authenticated. If the relaying party (called an SP or Service Provider) chooses to trust the campus system, the user is seamlessly signed into the service provider using the user's UID contained in the statement. If a user is not currently logged into your SSO portal, Blackbaud Award Management or Stewardship Management will direct the user to your SSO portal to authenticate before gaining access to the system.

Once Blackbaud has connected to your SSO server and securely validated the user, we search for the user's UID provided by your SSO portal as the external key into our table of users. Blackbaud uses this UID as a lookup key to the user account in Blackbaud Award Management or Stewardship Management database to determine which user is logging in and what that user's appropriate permission level should be. If this is the user's first time to attempt to log into Blackbaud Award Management or Stewardship Management, we will create a new user account for that user. The default role in the system is that of an applicant. For a new user to have administrative privileges, another administrative user will need to bestow those additional privileges on the new user.

Note: Your IdP server should be configured for SP-initiated Single Sign-On to allow users to initiate authentication either from your SSO portal or from Blackbaud Award Management or Stewardship Management. This is the best practice configuration for services not managed by campus IT resources, and it is strongly recommended to not use IdP-initiated Single Sign-On.

Configuring Shibboleth in your Award Management System

When you are ready to begin the configurations, you can enter them directly into your Award Management System. To access the system, please contact us, and we will be able to provide an account for you.

Once you have access to the site, the configuration page can be found under the ***Site-Authentication-Shibboleth SSO Setup*** menu. When configuring Shibboleth SSO for use with Blackbaud Award Management and Stewardship Management, we need the following pieces of information:

1. Please provide your EntityID.

2. Please release the attribute that corresponds to the unique identifier that will be used to uniquely identify staff and students that will also be present in the import file containing student information that you will be sending to us. Please provide us both the OID and SAML 2.0 name for the UID attribute.

3. Please release the attribute that corresponds to the user’s email address. We will use this email address temporarily in the case where a student logs into the system before their information appears in the student import file. Please provide us both the OID and SAML 2.0 name for the email attribute.

4. Please provide us with credentials for a test account that will allow us to mimic logging in as a student or staff member.

5. If you would like to redirect users to a specific URL upon logging out of Award Management, please provide the URL.

As soon you have provided the configuration information, please contact us, and we will request our metadata for your Blackbaud site be published. When we receive approval from InCommon, we will let you know that our metadata is ready to be consumed. Once we have received all this information and completed the steps mentioned previously, we can begin testing the integration.

Once configured, our EntityID will adhere to the following format where **client_subdomain** represents your Award Management subdomain, which can be found on the Shibboleth configuration page:

https://**client_subdomain**.academicworks.com/shibboleth-sp