Qualtrics Single Sign-On Specification

Version 3/19/2018

Table of Contents

Introduction

Single sign-on (SSO) allows a third-party to authenticate a user for the Qualtrics System. The Qualtrics System supports three basic types of SSO authentication: CAS, LDAP, and SAML/Shibboleth. Each type requires the third-party to have a type specific server (e.g., CAS SSO authentication relies on the third-party having a CAS server).

Implementation Considerations

Qualtrics offers several options for providing users of an organization a Qualtrics account based on their needs and usage. When considering implementation of a SSO solution, the following information is important in determining how SSO is configured for the organization:

Qualtrics has not been used by the organization prior to SSO integration

Implementing a SSO solution for a new organization is considerably simpler than for an established organization. Once implemented, users are created automatically upon initial login. If a small number of user accounts existed previously (for demo or testing purposes), these accounts can be migrated manually by Qualtrics.

Qualtrics has been used by the organization prior to SSO integration

If user accounts have already been established in Qualtrics for an organization, those accounts can be restructured in order to use SSO authentication. Existing users have login credentials for Qualtrics that may not match the SSO provider's credentials. For organizations in which Qualtrics user accounts already exist, Qualtrics provides the option to migrate users through the following process:

1. The user arrives at the Qualtrics login page (e.g., mybrand.qualtrics.com).
2. The user authenticates using the SSO authentication method configured for the organization.
3. Once the user has authenticated using SSO, they are redirected back to Qualtrics.
4. Qualtrics determines based on the user ID passed back through SSO whether the user exists in Qualtrics.
5. If the user ID is in use by an account in Qualtrics, the user is logged directly into their account.
6. If the user ID is not in use by an account in Qualtrics, the user is presented the following options:
    a. "I do not have a Qualtrics account."
        i. Users without an account in the organization's brand should use this option.
        ii. If the account exists outside of the organization's brand, the user will need to select "Contact Support" on https://www.qualtrics.com/support to request that their account be transferred into the organization's brand via a User Move.
        iii. Users will log in via the SSO portal with their organization's credentials moving forward.
    b. "I already have a Qualtrics account."
        i. Users with an account in the organization's brand should use this option.
        ii. If this option is selected, the user is presented with a form to authenticate using their existing Qualtrics username and password. Upon successful authentication, the user's account username is updated to have the user ID value being passed on authentication for the user.
        iii. Users will log in via the SSO portal with their organization's credentials moving forward.

Configurable Options

SSO implementation with Qualtrics has several configurable options, all of which are listed below for reference:

1. User Type Mapping
    a. If enabled, this will automatically assign users to a User Type upon login based on an attribute passed in authentication.
        i. This can be applied on first login or on each login attempt.
        ii. Access to Qualtrics can be set based on this mapping. If users do not pass an attribute value laid out in mapping, they will not be able to access the system.
    b. If disabled, users will be assigned to the Default User Type upon login. Any updates to the user's account will have to be done manually.

2. Division Mapping
    a. If enabled, this will automatically assign users to a Division upon login based on an attribute passed in authentication.
        i. This can be applied on first login or on each login attempt.
    b. If disabled, users will not be assigned to a Division upon login. Users will need to be manually assigned to Divisions.

3. Group Mapping
    a. If enabled, this will automatically assign users to a Group upon login based on an attribute passed in authentication.
        i. This can be applied on first login or on each login attempt.
    b. If disabled, users will not be assigned to a group upon login. Users will need to be manually assigned to Groups.

4. Create New Users
    a. If enabled, this will create new users in the Qualtrics system upon successful authentication.
        i. It is possible to trigger a notification email upon account creation.
    b. If disabled, this will only allow access to users that are already in the Qualtrics system. New users must be created manually.

5. Restrict Login to Domain
    a. If enabled, users will be required to access Qualtrics via your branded Qualtrics login portal. This means that all users must authenticate through SSO to gain access to the system.
    b. If disabled, users can access their accounts outside of SSO on the general Qualtrics login portal. This assumes that they know their Qualtrics username and password.

6. Logout Redirection
    a. If enabled, users will be redirected to a specified web page upon logout.
        i. To end the login session for the user and prevent login without credentials, the specified web page must delete cookies.
    b. If disabled, users will be redirected to the login portal.

CAS Introduction

Central Authentication Service (CAS) provides enterprise single sign-on service and is supported by the JA-SIG CAS. More information about CAS can be found at their website, http://www.ja-sig.org/products/cas/. The Qualtrics System can act as a CAS client, allowing the user to authenticate via CAS and login to the Qualtrics system.

CAS Setup Process for a Third-Party

To setup CAS SSO, it is assumed that the third-party has a working CAS server using the CAS 2.0 protocol or newer. The following configuration parameters must also be provided:

1. At minimum, the following parameters are required:
    1. CAS server hostname
    2. CAS server port
    3. URI to the CAS system on the host
2. If a version of CAS that supports SAML 1.1 is used, the following configuration parameters are capable of being consumed:
    1. Attribute containing the user's first name (e.g. firstname)
    2. Attribute containing the user's last name (e.g. sn)
    3. Attribute containing the user's email address (e.g. mail)
    4. Attribute used for User Type mapping
    5. Attribute used for Division mapping
    6. Attribute used for Group mapping

Once the above information is provided, Qualtrics can arrange to set up CAS integration with the third-party.

LDAP Introduction

LDAP (Lightweight Directory Access Protocol) is a directory service against which a third-party can authenticate. The Qualtrics System can be set up to automatically authenticate against an LDAP server when a user logs in to the Qualtrics System.

LDAP Setup Process for a Third-Party

To setup a LDAP integration, it is assumed that the third-party has a working LDAPv3 server. The following configuration parameters must also be provided:

1. At minimum, the following parameters are required:
    a. LDAP server hostname
    b. LDAP server port
    c. Base Distinguished Name (DN) (e.g. o=organization)
    d. Authentication filter parameters (e.g. uid=%username%)
2. The following configuration parameters are optional:
    a. Bind DN
        i. Must use if your LDAP server does not allow unauthenticated search.
    b. Bind Password
        i. Must use if your LDAP server does not allow unauthenticated search.
    c. Attribute containing the user's first name (e.g. firstname)
    d. Attribute containing the user's last name (e.g. sn)
    e. Attribute containing the user's email address (e.g. mail)
    f. Attribute used for User Type mapping
    g. Attribute used for Division mapping
    h. Attribute used for Group mapping

Once the above information is provided, Qualtrics can arrange to set up a LDAP integration with the third-party.

SAML/Shibboleth Introduction

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between security domains; that is, between an identity provider (a producer of assertions) and a service provider (a consumer of assertions). The Qualtrics System can be set up to automatically authenticate through a third-party identity provider using SAML when a user logs in to the Qualtrics System.

SAML/Shibboleth Setup Process for a Third-Party

To set up a SAML integration, it is assumed that the third-party has a working SAML 2.0 or Shibboleth 2.0 implementation. The following configuration parameters must also be provided:

1. Identity Provider Metadata in XML
    a. Please see https://openidp.feide.no/simplesaml/saml2/idp/metadata.php for an example.
    b. At minimum, the following elements are required:
        i. EntityDescriptor
        ii. KeyDescriptor
        iii. SingleSignOnService
            1. We support both HTTP Post or HTTP Redirect bindings.
        iv. Attribute containing the user's unique username or ID
    c. The following configuration parameters are optional:
        i. Attribute containing the user's first name (ex. firstname)
        ii. Attribute containing the user's last name (ex. sn)
        iii. Attribute containing the user's email address (ex. mail)
        iv. Attribute used for User Type mapping
        v. Attribute used for Division mapping
        vi. Attribute used for Group mapping

Once the above information is provided, Qualtrics can arrange to set up a Shibboleth/SAML integration with the third-party.

Qualtrics supports two workflows for SAML/Shibboleth exchanges: service provider-initiated and identity provider-initiated. The more common of the two is a service provider-initiated exchange. The identity provider-initiated exchange is primarily used when users authenticate on an internal network. Below are the anticipated workflows:

Service Provider-Initiated

1. The user arrives at the Qualtrics login page.
2. An authentication request is sent to the third-party identity provider and the user is redirected to the third-party login portal.
3. The user authenticates and a SAML response is returned to Qualtrics.
    a. Please see https://survey.qualtrics.com/ControlPanel/File.php?F=F_e5TrbCBvzJk2VKZ for an example.
    b. At minimum, the following elements are required:
        i. Issuer
        ii. Signature
        iii. Status
        iv. Subject

        1. Must contain NameID.
    v. AttributeStatement
        1. Must have an Attribute containing the user’s unique username or ID.
4. Qualtrics grants/denies access based on the SAML response and attribute statement.

Identity Provider-Initiated

1. The users authenticate through a portal on the local network.
2. An HTTP request is sent to the Qualtrics assertion consumer service with a SAML Response.
    a. Please see https://survey.qualtrics.com/ControlPanel/File.php?F=F_e5TrbCBvzJk2VKZ for an example.
    b. At minimum, the following elements are required:
        i. Issuer
        ii. Assertion Signature
        iii. Status
        iv. Subject
            1. Must contain NameID.
        v. AttributeStatement
            1. Must have an Attribute containing the user’s unique username or ID.
3. Qualtrics grants/denies access based on the SAML response and attribute statement.