Brandwatch

# SAML SSO
# Integration Guide

## Introduction

The Brandwatch SAML SSO integration makes it possible to access the Brandwatch application by authenticating your users with SAML instead of using Brandwatch login credentials.

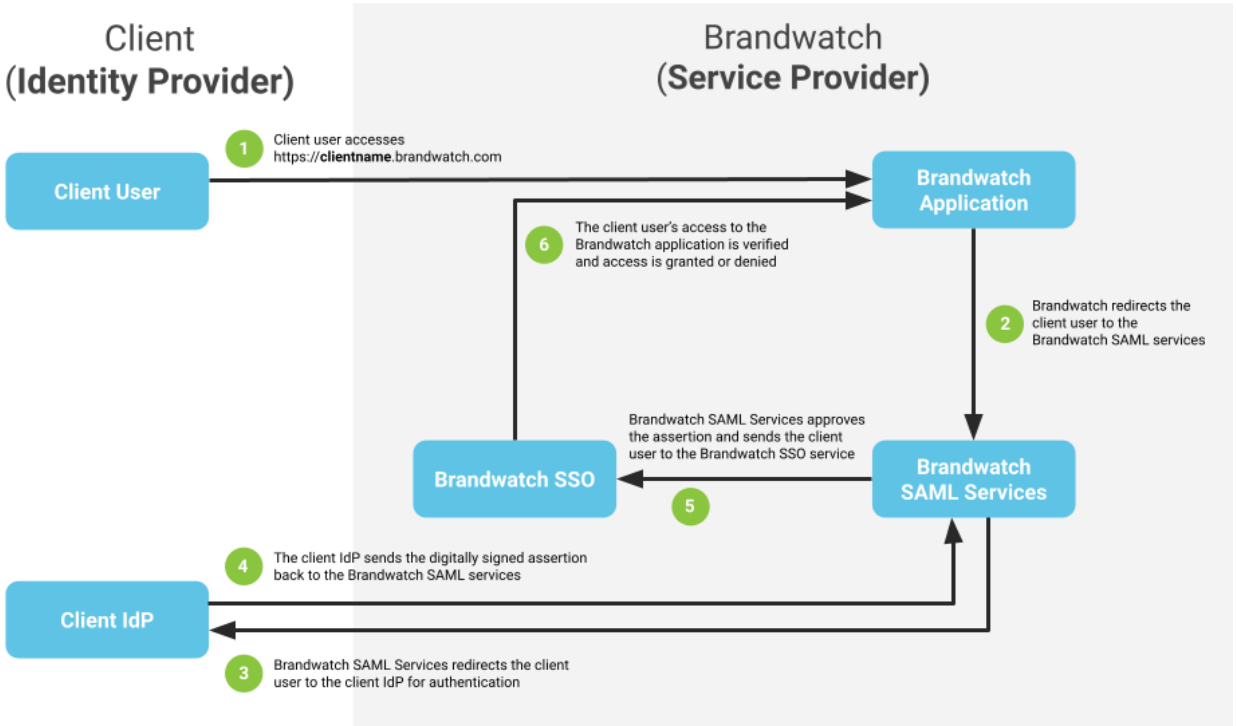
We implement SAML 2.0 using a widely-deployed federated identity solution. As a result, the large majority of identity providers (IdPs) are compatible.

This guide provides an overview of our SAML SSO integration along with the options available. We'll need you to confirm your choices in the requirements form that accompanies this guide.

The setup process is also explained so you know what to expect from us ahead of time.

## An overview of the Brandwatch SAML SSO integration

The diagram below illustrates how our SAML SSO integration works:



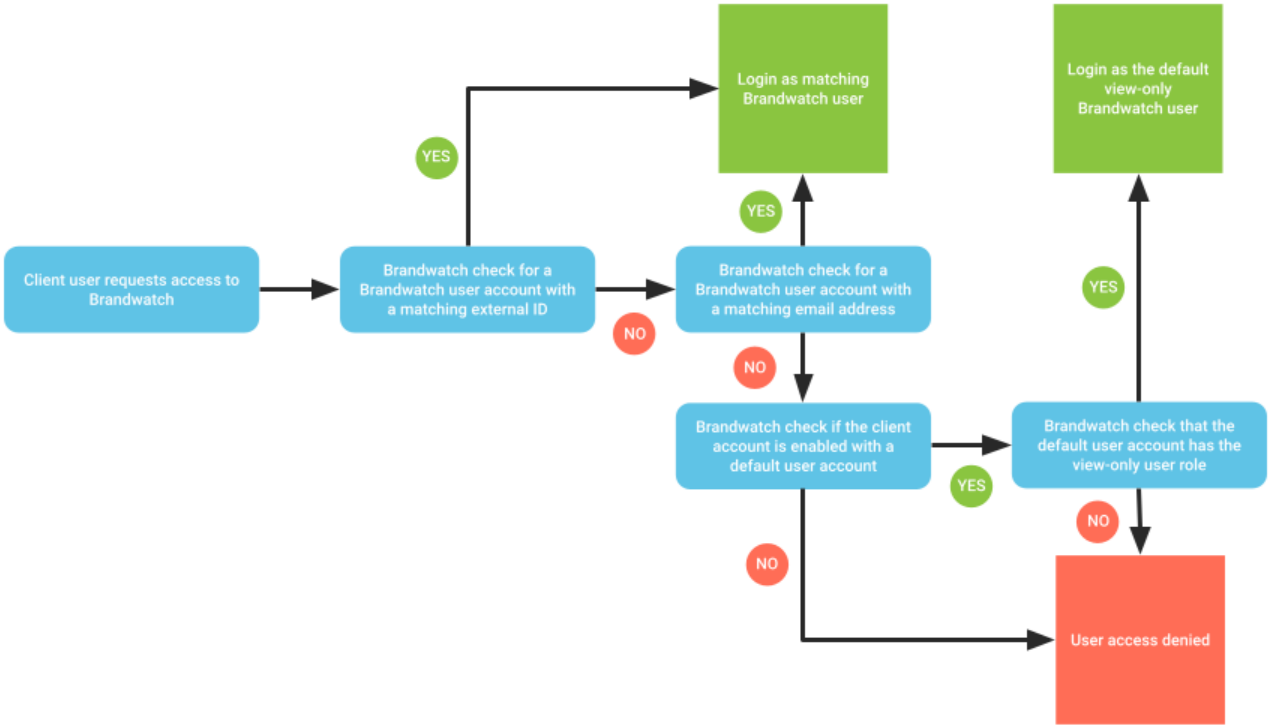
## Access to the Brandwatch application with SAML

In order to create a mechanism for alerting the Brandwatch system to authenticate a user with SAML, we will create a dedicated subdomain for you to use to access the Brandwatch application.

This generally takes the format **clientname**.brandwatch.com and users accessing this will be redirected to your client identity provider login page to log in with their client user credentials before then being taken through to the Brandwatch application.

## Mapping client user accounts to Brandwatch user accounts

When a client user requests permission to access the Brandwatch application through your dedicated Brandwatch subdomain, we will use the process illustrated in the flowchart below to understand how we should handle the request:




Individual client user accounts can be mapped to individual Brandwatch user accounts by either:

- **email address**; or
- a unique, **external ID** (such as an Employee ID)

**Brandwatch does not automatically provision new user accounts**. This approach requires a Brandwatch admin user to create a corresponding Brandwatch user account for each client user account and each Brandwatch user created will contribute to your Brandwatch account's user limit.

### Default user

If you have multiple staff that require view-only access to the Brandwatch application, the client user accounts for these staff can be matched and authenticated against a **single** view-only Brandwatch user account (known as the **default user**) where:

- a default, view-only Brandwatch user account is requested and set up as part of your Brandwatch SAML SSO integration
- the client user accounts do not have corresponding Brandwatch user accounts that match either their external ID or email address

The default user will generally take the format of **defaultuser**@yourdomain.com and will consume **one** user from your Brandwatch account's user limit.

The view-only default user allows the customer and Brandwatch to prevent untrackable changes being made to setup and data within the Brandwatch application.

### Access control for the default user

When a default user is enabled as part of your SAML SSO integration, it is possible to specify which client user accounts should be granted access to authenticate as the default user by using SAML attributes.

For example, you can specify that a SAML attribute for a user should be set to something specific, such as ***department = marketing*** in order to access the Brandwatch application as the default user.

In these instances if the client user account cannot be matched against a corresponding Brandwatch user account by email address or external ID and the client user account does not include the required SAML attribute, their attempt to gain access to the Brandwatch application will be denied.

## Update and sync Brandwatch user account information upon login

When a client user makes changes to certain account information, it is possible to automatically update and sync the account information for the corresponding Brandwatch user when they log into Brandwatch with SAML.

It is possible to update and sync the following Brandwatch user account information upon login:

- First Name
- Last Name
- Department
- Job Title
- External ID (this is a free text option)

In order to do this, Brandwatch needs to map each chosen item from the list to the corresponding SAML attribute that you will be providing in the metadata of your SAML assertion.

You'll need to confirm the name of the corresponding SAML attribute for each chosen item in your requirements form.

**User email addresses are not editable in Brandwatch**. If employee email addresses are likely to change, we suggest that you authenticate users with another unique data field.

## Enforce SAML authentication to Brandwatch

It is possible to enforce SAML authentication by preventing the use of Brandwatch usernames and passwords to access the Brandwatch application.

It is also possible to enforce SAML authentication for specific user-roles only. For example, you may wish to enforce SAML authentication for all users with the exception of admins who may choose to use either SAML authentication or Brandwatch credentials.

As the Brandwatch SAML SSO integration is not compatible with Brandwatch Reviews or our APIs, the user-role restriction is a common choice for customers with access to these additional products.

## Limitations

Our current SAML solution officially works for Brandwatch Consumer Research, Audiences, Vizia, Buzzsumo, MyBrandwatch and other administration areas. It does not currently support Brandwatch Reviews, or our APIs.

Please note that the following is not possible with our SAML SSO integration:

- Just-in-time (JIT) creation of new Brandwatch user accounts
- Automatic sync of client user account lists to Brandwatch user account lists
- Deletion of Brandwatch user accounts
- Changes to Brandwatch user account email addresses

- Single sign-out (other than our standard user inactivity timeout)

## Timeframes

Upon receipt of a completed requirements form and assignment to an Engineer, the implementation of a SAML SSO integration generally takes between 2-4 weeks and includes:

- Exchange of metadata files
- Creation of your dedicated Brandwatch subdomain and Staging environment
- Implementation of the Brandwatch-side setup for Staging and Production environments
- Stage and Production testing
- Production deployment

## Customer requirements form

After reading this guide, please fill in the SAML SSO Requirements Form and return to your Brandwatch representative at your earliest convenience.

Should you have any questions, please contact our Customer Support team.

In the form we'll also need you to provide the details for your technical contact. This is the person that will be carrying out your client-side implementation.

If we have any questions regarding your completed requirements form once we have received it, our Customer Support team will be in touch. Otherwise we'll be in touch to confirm once your integration is waiting to be assigned to an Engineer.

## Setup process

The setup process generally involves no more than a few email exchanges as follows:

- As soon as one of our Engineers is available to begin the implementation of your SAML SSO integration, they will email your Customer Success Manager and the technical contact you specified in your requirements form to introduce themselves and exchange metadata files for both Staging and Production environments.

- Once we've received your metadata files, we'll carry out the Brandwatch-side implementation for the Staging environment. We'll then be in touch when we are ready for you to test with your dedicated Staging environment and subdomain.

  We'll set up a test user for your technical contact and provide instructions for the creation of additional users. We'll then await your confirmation before proceeding further.

- Once we've received your confirmation of successful Stage testing, we'll verify on our side and then proceed with the implementation for the Production environment.

  We'll be in touch when this is ready for you to test on your dedicated Brandwatch subdomain using any of your existing Brandwatch user accounts. Again, we'll await your confirmation before proceeding further.

- Once we've received your confirmation of successful testing on the Production environment, we'll then await your approval to deploy your SAML SSO integration to your Brandwatch account and confirm once the deployment is complete.

  From this point, your Brandwatch SAML SSO integration will be live and you should direct your staff to access the Brandwatch application from your dedicated Brandwatch subdomain.