Securing Your Brainshark Content

Table of Contents

Securing Your Brainshark Content

Overview	Corporate privacy and content security are the top concerns of businesses today. Securing corporate assets is a fundamental objective for every IT department. Content authors want to ensure that their internal corporate presentations, educational materials and product information are accessible only by those with appropriate permissions. To properly discuss content security, this document reviews the following topics: • Administration Presentation Settings • Brainshark fundamentals for private/public presentations • The Brainshark URL syntax and how it can be used to capture viewer information • Advanced techniques for providing Brainshark security • Brainshark User profile creation
Company Administrator Settings	In the **Presentation Security** section of ***Administration***, you can choose settings that span presentations across the company.
Login Required	Choosing "Yes" allows the authors to choose whether a login is required in order to view a presentation. Setting a presentation's initial settings for new presentations as **Private** or **Public** can be set here as well.
Presentation Expiration	These options allow you to set all presentations to expire after being active for a certain number of days, and notifying certain users before they expire.
Presentation Copy	Setting Presentation Copy to "**Yes**" allows other people to copy an author's presentation. The second option allows the author to override the company setting.
Active on Upload	If "Active on Upload" is set to "**Yes**," all presentations will be available to view as soon as the upload is complete.

Hide Content

Hide Content removes the content from searches in the Content Portal and Sales Accelerator. You can also give authors the ability to override this.

Brainshark Fundamentals

The Primary Principle

The primary principle for securing Brainshark content is to ***make presentations Private***. This document discusses other methods, but all require content to be considered Private to ensure its security.

Brainshark content (presentations) may be considered as Public or Private.

- Public presentations can be viewed by anyone with access to the presentation link (URL).
- Private presentations require a viewer to login prior to viewing. The viewer, therefore, must have a valid Brainshark user profile.
- Brainshark Content Authors may set a presentation to Public or Private through the 'Require User ID and Password to view presentation' option. This option is found on the Security tab while editing a presentation.
  - This can also be set at the company level in Presentation Security of Administration.
- All Brainshark Learning Courses are automatically set to Private.

Brainshark Presentation URL Basics

It's important to understand the syntax of the Brainshark presentation URL. The basics are discussed in this section. In later sections the URL will be augmented to collect viewer information.

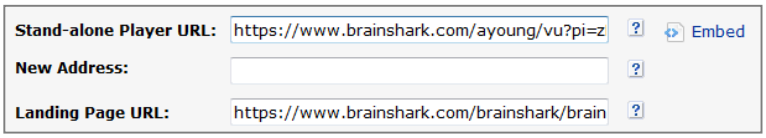
When a Brainshark author creates a Presentation or Learning course, Brainshark immediately assigns a presentation id (PID) and formulates the Brainshark URL. This URL can be entered into a browser, posted on a web page or embedded within an email. Viewers following the URL will be shown the presentation (if the presentation is marked Public) or will be asked for their Brainshark user credentials (if the presentation is marked as Private).

The Brainshark stand-alone player URL takes the following syntax:
https://www.brainshark.com/{**company_name**}/vu?pi={**PID**}

- {**company_name**} is the Brainshark name for your site
- **PID***:* presentation id assigned by Brainshark

NOTE: As mentioned above, if the presentation referenced within the URL is Private, viewers will be prompted to enter their Brainshark credentials. For view tracking purposes, the viewer is known. If the presentation is public, however, the presentation would prompt for a Guestbook or augment the URL to 'silently' pass Guestbook information into Brainshark. The Guestbook columns must be selected within the reports to show the viewer's information.

The URLs are found on the Presentation Properties tab while editing the Brainshark presentation.



Identifying Presentation Viewers

Private Content

When your Brainshark content is secure (private), the viewer is immediately identified since he or she is required to log in to Brainshark. All Viewing Reports identify the logged in user within the Viewer Info column.

Extending the scenario to Public presentations, viewers may be identified by:

- Adding a Guestbook to collect viewer information.
  - Refer to *Capturing Viewing Data with a Guestbook* document.
- Augmenting the Brainshark URL to 'silently' pass Guestbook information to Brainshark
  - Refer to *Pre-filling Guestbook Data* document.

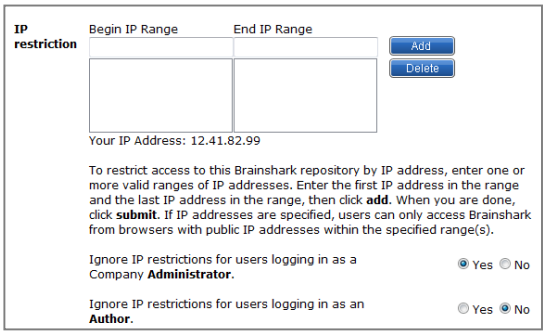
Advanced Security Methods

Overview

Beyond creating Private Brainshark presentations, Brainshark provides several methods to enhance a more site-wide security environment.

IP Restrictions

- Brainshark Administrators can restrict site access by specifying a set of IP Address ranges. When these IP Ranges are entered, Brainshark viewers can access Brainshark only from browsers with public IP addresses within the specified range(s).
- Administrators can access The IP Restrictions feature through:
  My Applications > Administration > Manage Company > Advanced Options > Restricting Site Access



Single Sign-On

Brainshark's Single Sign-on (SSO) implementation allows users who have already logged in to their corporate web site or network to access to their Brainshark site or Private presentations without the need to re-login to Brainshark.

Brainshark communicates with the client's corporate identity provider, using the industry-standard SAML 2.0 protocol, to authenticate the user's credentials.

Various SSO configuration options include: auto-creation of new user accounts in Brainshark, auto-association of existing Brainshark user accounts and exposure of a direct Brainshark log-in for those users 'off the corporate network'.

NOTE: SSO is an optional feature. Contact your Sales Representative for more information. Refer to the SSO section of this document for more detailed information.

Login and Go

Brainshark offers an alternative approach through its Login-and-Go function to accommodate client environments that do not support SSO.

Login-and-Go is accessed through a special Brainshark URL that identifies the user and the Brainshark destination. The users are identified by either their username/password or through a unique identifier. The destination may be a Brainshark presentation, the Brainshark Content Portal or the Brainshark Learning Locker. The Login-and-Go function does what its name implies – it logs the user into Brainshark and goes to the destination page specified.

Refer to the Login and Go section of this document for more detailed information.

> ***NOTE***: Login-and-Go requires that Brainshark user accounts pre-exist. Login-and-Go does not create users (as with SSO).
>
> Refer to the Use Case Examples detailed in this document's Appendix.

Creating Brainshark User Profiles (Accounts)

Overview

The creation of secure content (Private presentations or Learning courses/curriculums) requires the presence of Brainshark user accounts. The accounts provide user credentials, rights and viewing permissions. This section reviews the various methods to properly create the user accounts.

Brainshark Administrator

User profile or account creation and maintenance is a fundamental responsibility of the Brainshark Administrator. For instructions and procedures on this topic, refer to the *Administration Quick Reference Guide* document.

Self-Registration

It is sometimes appropriate to allow new users to create their own Brainshark user accounts based upon completing a self-registration form. For instructions and procedures regarding user self-registration, refer to the *Self Registration* document.

Single Sign-On	Client environments supporting SSO authentication may take advantage of the SSO configuration option to create new user accounts as they are authenticated into Brainshark. Refer to the SSO information in the Appendix of this document.
Brainshark Web Services APIs	Brainshark provides a robust set of Web Services APIs (both SOAP and REST) to create user accounts programmatically. Contact your sales representative for more detail.
Batch Upload	Brainshark provides a stand-alone application that allows clients to create and modify user accounts. Refer to the *Guide to Preparing a Bulk User Upload* document.

Single Sign-On

Benefits	Single Sign-On ensures fast, secure account creation and user authentication. Brainshark's Single Sign-On (SSO) feature enables administrators to control access to Brainshark without the hassle of managing and maintaining a separate user account. For users, it provides streamlined access to Brainshark without having to log in separately.
Enhanced Security	With Software-as-a-Service (SaaS) applications, maintaining control over logins and permissions can be challenging. Brainshark's SSO feature supports the most common security protocols used by identity providers. Administrators can limit employee access to a specific set of applications, and easily terminate that access to all systems at once when the employee leaves the company.
Compliance	Brainshark's SSO feature supports even the most rigidly enforced security requirements from IT departments.

Reduced Help Desk Costs

One of the most prevalent IT Help Desk incident types is users forgetting their password or having login difficulties. By enabling users to log in to Brainshark (and other applications) through a single sign-on process, you'll dramatically reduce this type of incident.

Increased User Adoption Rate

Creating and managing user accounts can be a very cumbersome process – to the point of inhibiting an application's widespread rollout. With features to auto-associate and auto-create users, you can expand Brainshark access with ease.

Supported Security Protocols

Brainshark provides optimum control over logins and permissions through its support of the most common security protocols used by identity providers. Almost all SSO implementations utilize SAML (Security Assertion Markup Language), an XML standard for exchanging authentication data between an identity provider (i.e., an SSO partner that vouches for the identity of a user) and a service provider (i.e., an SSO partner that provides services to an end user like Brainshark). Brainshark supports the dominant protocols for "federated identity": SAML 2.0 (issued in 2005 based on the work of the Liberty Alliance – another consortium of business and government entities) and WS-Federation (used by Microsoft Active Directory through Microsoft ADFS, or Active Directory Federated Services).
It enables administrators to limit user access to a specific set of applications. When an employee leaves your company, you can easily terminate his or her access to all systems to which they logged in.

The SAML Assertion: Data Requirements

As stated above, the SAML assertion is expected to contain two sets of data:

A unique and persistent user identifier. This is the primary means for identifying users with Brainshark and should be contained within the first element of the SAML Subject (NameID). See the highlighted area below:

```
<saml:Subject>
    <saml:NameID>{Unique_User_ID}</saml:NameID>
    <saml:SubjectConfirmation
      Method="urn:oasis:names:tc:SAML:2.0:cm:bearer">
      <saml:SubjectConfirmationData
        NotOnOrAfter="2011-05-06T21:38:46Z"
        Recipient="https://sso.brainshark.com/sp/ACS.saml2" />
    </saml:SubjectConfirmation>
  </saml:Subject>
```

Error! No text of specified style in document.*continued*

Attributes with new Brainshark User information. The customer must inform Brainshark what Attributes will be used to contain the user's First Name, Last Name and Email Address. See highlighted areas below:

```
<saml:Attribute
      Name="FirstName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
      <saml:AttributeValue xmlns:q2="http://www.w3.org/2001/XMLSc
hema"
        p7:type="q2:string" xmlns:p7="http://www.w3.org/2001/XMLSch
ema-instance">Arnie</saml:AttributeValue>     <saml:Attribute
      Name="LastName"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
      <saml:AttributeValue xmlns:q4="http://www.w3.org/2001/XMLSc
hema"
        p7:type="q4:string" xmlns:p7="http://www.w3.org/2001/XMLSch
ema-instance">Young</saml:AttributeValue>
    </saml:Attribute>
    <saml:Attribute
      Name="Email"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
  <saml:AttributeValue xmlns:q5="http://www.w3.org/2001/XMLSchem
a"
        p7:type="q5:string" xmlns:p7="http://www.w3.org/2001/XMLSch
ema-instance">ayoung@brainshark.com</saml:AttributeValue>
    </saml:Attribute>

 <saml:Attribute
      Name="Username"
      NameFormat="urn:oasis:names:tc:SAML:2.0:attrname-
format:basic">
      <saml:AttributeValue xmlns:q5="http://www.w3.org/2001/XMLSc
hema"
        p7:type="q5:string" xmlns:p7="http://www.w3.org/2001/XMLSch
ema-instance">ayoung@brainshark.com</saml:AttributeValue>
    </saml:Attribute>
```

Login and Go

Overview

The Brainshark Login-and-Go utility allows an external application to:

- Identify existing Brainshark Users and log them into their Brainshark site
- Launch either a Brainshark presentation or a Brainshark Application page (Private Portal or Learning Locker)

This document illustrates several end-user scenarios and how to best apply Login-and-Go.

The Primary Assumptions

The Brainshark Login-and-Go utility is ideally suited for workflows where users access Brainshark presentation links (or the link to the Brainshark customer site) after logging into a corporate portal or network. The Login-and-Go URLs replace the direct (standard) Brainshark presentation URLs to allow for user identification.

The Login-and-Go URL contains a number of query strings that require their values be dynamically populated by the program 'calling' the utility. The assumption is that the calling program knows the value of these parameters (e.g., user credentials) and can properly populate the URL as needed.

Calling Login-and-Go

The Login-and-Go utility may be called from a web page or application and takes the following form:

http://www.brainshark.com/brainshark/public/login/loginandgo.asp?query_strings

where the Query Strings are detailed in the following table:

Query String	Notes
UID	**User ID**: The username of an existing Brainshark user-account; programmatically placed into the URL. Must be matched with the corresponding PWD (password) query string.
PWD	**Password:** The password of an existing Brainshark user-account; programmatically placed into the URL. Must be matched with the corresponding UID (username) query string.
UCI	**Unique Company Identifier**: A field in the Brainshark User Account that contains a unique value among users within the customer's Brainshark site. Used in conjunction with CID (company id) to substitute for UID / PWD.
CID	**Company ID:** The client's Brainshark site ID; a fixed value supplied by the Brainshark Administrator
DEST	**URL-encoded Destination:** Where to 'take' the user once logged in. It may represent a presentation URL, the URL to the Private Portal or the URL to the Learning Locker

Destination	URL	URL Encoded
Brainshark Presentation (standard)	/brainshark/vu/view.asp?pi={PID}	%2Fbrainshark%2Fvu%2Fview.asp%3Fpi%3D{PID}
Brainshark Private Content Portal	/brainshark/brainshark.net/portal/home.aspx	%2Fbrainshark%2Fbrainshark.net%2Fportal%2Fhome.aspx
Brainshark Learning Locker	/brainshark/learning/MyLearning.asp?ca=4	%2Fbrainshark%2Flearning%2FMyLearning.asp%3Fca%3D4

Use Case Examples

Example 1

A client web site posts links to private Brainshark presentations. The web site requires that the individual users' login to the web site to gain access to the presentation links. The web site has access to the Brainshark username/passwords of existing accounts. The Brainshark business user wants the content to remain 'private' and to track views by individual.

In this use case, the Brainshark Administrator would communicate with the web developer providing the PIDs for the presentation URLs to be posted. The users within Brainshark may have been created with a bulk upload process or through the Brainshark API – so their login credentials are known to the web developer.

Calling Login-and-Go with the UID, PWD, CID and DEST as shown below would be the most appropriate call. As stated above, the UID and PWD would be provided programmatically.

http://www.brainshark.com/brainshark/public/login/loginandgo.asp?uid=guest&pwd=guest&cid=9022&dest=%2Fbrainshark%2Fvu%2Fview.asp%3Fpi%3DzEhzNU2RYzFSDz0%20%20

Example 2

A client web site posts links to private Brainshark presentations. The web site requires that the individual users' login to the web site to gain access to the presentation links. The Brainshark user accounts were created to contain a Unique Company Identifier for each user. This UCI value may be placed into the user's Brainshark User Profile manually or through the Bulk Upload process. The Brainshark business user wants the content to remain 'private' and to track views by individual.

By using the UCI for each user, the web developer does not need to expose the username / password of the individual user being logged in. Instead, only the UCI and CID are used to identify the user.

http://www.brainshark.com/brainshark/public/login/loginandgo.asp?uci=123&cid=9022&dest=%2Fbrainshark%2Fvu%2Fview.asp%3Fpi%3DzEhzNU2RYzFSDz0%20%20

The UCI would be provided programmatically.

In this example, the combination of UCI=ay123 and CID=9022 identify the Unique Company Identifier and the company site. The DEST argument remains the same. The result remains tracking by individual.

Example 2A

If individual user accounts do not exist within Brainshark, it may be more appropriate to create a single 'mock' Brainshark user containing a UCI. Using the URL in Example 2 (above) with the same UCI for each call would result in the same mock user being logged into Brainshark and viewing the presentation.

The only view tracking would be against the 'mock' user in Brainshark.

Example 3

Building on Example 2A, if the client desires to still identify the viewers but not have individual accounts for them within Brainshark, the approach would be:

- Create a 'mock' user in Brainshark with their UCI set
- Modify the DEST URL to call the Brainshark presentation and include silent Guestbook values to be passed to Brainshark

Guestbook Query Strings that may be added are:

&fn	First name
&ln	Last name
&em	E-mail address
&cn	Company name
&dp	Department
&ti	Title
&bp	Business Phone
&c1	Custom field 1
&c2	Custom field 2
&c3	Custom field 3
&c4	Custom field 4
&c5	Custom field 5
&c6	Custom field 6
&c7	Custom field 7
&c8	Custom field 8
&c9	Custom field 9
&c0	Custom field 10

The sample below shows the passing of the viewer's first name, last name and email address. These values would be programmatically modified on the URL.

http://www.brainshark.com/brainshark/public/login/loginandgo.asp?uci=123&cid=9022&dest=%2Fbrainshark%2Fvu%2Fview.asp%3Fpi%3DzEhzNU2RYzFSDz0%26fn%3DArnie%26ln%3DYoung%26em%3Dayoung%40brainshark.com

Example 4

Using any of the previous examples, the client may decide to change the DEST (destination) to show the Private Content Portal or the Learning Locker (Learning application) instead of going directly to a presentation. The table on Page 1 shows the proper DEST URLs.

Logging in and going directly to the Private Content Portal:

http://www.brainshark.com/brainshark/public/login/loginandgo.asp?uci=123&cid=9022&dest=%2Fbrainshark%2Fbrainshark.net%2Fportal%2Fhome.aspx

Logging in and going directly to the Learning Locker:

http://www.brainshark.com/brainshark/public/login/loginandgo.asp?uci=123&cid=9022&dest=%2Fbrainshark%2Flearning%2FMyLearning.asp%3Fca%3D4