

How to Configure Single Sign On for Proxied Web Apps

<https://campus.barracuda.com/doc/73719115/>

Proxied web apps can be configured to automatically log in the SSL VPN user with the username and password used to log in to the SSL VPN portal, or user attributes that can be filled in by the end user. The following authentication methods are supported:

- **HTTP authentication**
- **Form based authentication**

HTTP Authentication

HTTP authentication is a basic method for authenticating users. An HTTP header is inserted into the HTML page, and the browser then queries the user for a username and password. HTTP authentication is supported in three variants: basic, digest, and NTLM authentication. The authentication type is automatically detected by the Barracuda CloudGen Firewall. To automatically log into web apps using HTTP authentication, you can use static user credentials or user attributes. User attributes can either be the session username or password, or custom values that are configurable by the end user.

Form Based Authentication

Form based authentication is used when the login credentials are entered on a HTML page. Open the source of the page and look at the HTML code in between the `</form>` and `</form>` tags. The Barracuda CloudGen Firewall can automatically log users into web apps. The form-based authentication type is determined by the HTML source of the login page.

POST

POST is the most common form submission type. Set the type to POST if the *method* attribute is set to POST. If the form contains unique or random hidden `<input>` elements, use JavaScript instead of POST as the form type. To find out which elements must be filled in, inspect the form submission process with a tool such as HTTPWatch or Fiddler. Create a **Form Parameter** for every parameter submitted by the form. When using POST, set the **Launch path** to the destination of the *action* attribute of the `<form>` element. E.g., `/somedir/index2.html` in the example below.

HTML Form

```
<form action="/somedir/index2.html" name="testform" method="POST" >  
<input type="text" name="name">
```

```
<input type="password" name="password ">
<input type="checkbox" name="rememberme">
  <input type="submit" value="Submit">
</form>
```

HTTP Watch

URL	Status	Domain
POST index2.html	200 OK	10.0.91.40

Headers	Post	Response	HTML	Cache
Parameters		application/x-www-form-urlencoded	Do not sort	
name dadf password sdfsd secret 666				
Source				
name=dadf&password+=sdfsdf&secret=666				

Web Resource Configuration

To use the custom attributes username and password, create the following two **Form Parameter** entries in the web resource configuration:

```
name=${user:AnUserAttribute}

password=${user:AnUserAttribute}
secret="666"
```

JavaScript

Forms using random or unique hidden input elements must use the JavaScript authentication type. After waiting for a configurable amount of time to make sure the page has finished loading, the Barracuda CloudGen Firewall injects a small JavaScript script into the HTML page. This script fills in the parameters specified in the web resource configuration. Create a form parameter for every entry the user has to interact with when logging in, including the submit button.

POST Form Example

HTML Form

```
<form action="index2.html" name="testform" method="POST" >
<input type="text" name="name">
<input type="password" name="password ">
<input type="hidden" name="UID" value="12345678901234567899012738230123123">
<input type="submit" name="submit" value="doLogin">
</form>
```

HTTP Watch

URL	Status	Domain
POST index2.html	200 OK	10.0.91.40

Headers	Post	Response	HTML	Cache
Parameters		application/x-www-form-urlencoded	Do not sort	
name dadf				
password sdfsd				
secret 666				
Source				
name=dadf&password+=sdfsdf&secret=666				

Web resource configuration

To use the session username and password, create the following two form parameter entries in the web resource configuration:

```
name=${session:username}
password=${session:password}
submit="doLogin"
```

GET

Set the form type to GET if the **method** attribute of the **form** element in the HTML source is set to GET. Determine which form parameters you must fill in to complete a successful login by looking at the parameters appended to the URL after you have logged in. These form parameters are then replaced by either session/custom User Attributes or static user credentials.

GET Form Example

HTML Form

```
<form action="index.php" name="testform" method="GET" >
<input type="text" name="name">
```

```
<input type="password" name="password ">  
<input type="hidden" name="secret" value="666">  
<input type="submit" value="Submit">  
</form>
```

URL

Entering "John" results in the following rule

```
/test/index.php?name=John&destination=Rome&secret=666&submit=Submit
```

Web Resource Configuration

To use the session username and password, create the following two form parameter entries in the web app configuration:

```
name=${session.username}  
password=${session.password}
```

Before You Begin

Configure a Web Resource. For more information, see [How to Configure a Generic Proxied Web App](#).

Step 1. Determine the Authentication Type

Analyze the HTML source to determine the form type (POST, GET or JavaScript).

Step 2. (optional) Define User Attributes

If you need to use different login credentials from the SSL VPN portal username and password, or additional user configurable parameters to complete the login, create User Attributes. User Attributes are filled in by the end user in the desktop or mobile portal of the SSL VPN service.

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > SSL-VPN**.

2. In the left menu, select **User Attributes**.
3. Click **Lock**.
4. Click **+** to add an **User Attribute**.
5. Configure the following settings for each User Attribute:
 - **Format** - Select the type of User Attribute. Possible values are: **Text, Number, Checkbox, Password** and **TextArea**.
 - **Label** - Enter the name visible to the end-user.
 - **Description** - Enter a description of the attribute.
 - **Default Value** - If the attribute should be set to default value, enter the value here.
 - **Category** - Enter a category name. User attributes will be grouped by category in the mobile and desktop portal.
 - **Weight** - Enter a value. Attributes are sorted within a category by this number.
 - **Validator** - Enter a regular expression to validate the input.
 - 4 digits PIN number**
[0-9]{4}
 - URL**
(https?:\\\/\\\/)?(\\[da-z\\.-]+)\\.([a-z\\.]{2,6})(\\\/\\w \\.-]*)*\\\/?
 - IPv4 address**
(?:(:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)\\.){3}(?:25[0-5]|2[0-4][0-9]|[01]?[0-9][0-9]?)
6. Click **OK**.
7. Click **Send Changes** and **Activate**.

Step 3. Add Authentication Configuration to a Web App

Add authentication information to a web app to automatically log the user in to the web application using the session user credentials or custom user attributes.

FORM Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, select **Web Apps**.
3. Click **Lock**.
4. Double-click on a web app. The configuration windows opens.
5. (POST authentication only) Change the **Launch Path** to the path set in the **action** attribute of the from element. E.g., /somedir/index.php if the form element is form
action="/somedir/index.php" name="testform" method="POST"
6. Set the **Authentication Type** to **HTTP** or **FORM**.
7. Set the **Form Type** to **GET, POST** or **JavaScript**.
8. (JavaScript only) Enter the **Form Name**. E.g., testform if the form element is form
action="/somedir/index.php" name="testform" method="POST"
9. (JavaScript only) Enter the **Timeout(s)** in seconds. This is the amount of the time the Barracuda

CloudGen Firewall waits before injecting the JavaScript code into the page. Default: 5 sec

10. Enter the **Form Parameters**.

- POST and GET **Form Type** - Add an entry for every <input> element in the login form.
- JavaScript **Form Type** - Add entries for the <input> elements the user enters data into.

Form Parameter Examples

```
<form action="index.php" name="testform" method="GET" >
<input type="text" name="name">
<input type="password" name="password ">
<input type="checkbox" name="rememberme " value="on">
<input type="hidden" name="secret" value="666">
<input type="submit" value="Submit">
</form>
```

Necessary form parameters for POST/GET From Type

```
name=${session.username}
password=${session.password}
rememberme="on"
secret="666"
```

Necessary form parameters for JavaScript From Type

```
name=${session.username}
password=${session.password}
```

11. Click **OK**.
12. Click **Send Changes** and **Activate**.

HTTP Authentication

1. Go to **CONFIGURATION > Configuration Tree > Box > Virtual Servers > your virtual server > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, select **Web Apps**.
3. Click **Lock**.
4. Double-click on a web app. The configuration windows opens.
5. (POST authentication only) Change the **Launch Path** to the path set in the **action** attribute of the from element. E.g., /somedir/index.php if the form element is <form action="/somedir/index.php" name="testform" method="GET">
6. Set the **Authentication Type** to **HTTP**.
7. Enter the **Username**. You can enter static content E.g., johndoe or use an Attribute E.g., \${userAttribute.SpecialUser} or \${session.username}.
8. Enter the **Password**. You can enter static content E.g., johndoe or use an Attribute E.g., \${userAttribute.SpecialUser} or \${session.username}.
9. Click **OK**.
10. Click **Send Changes** and **Activate**.

Figures

1. POST_Firebug_Example.png
2. POST_Firebug_Example.png

© Barracuda Networks Inc., 2019 The information contained within this document is confidential and proprietary to Barracuda Networks Inc. No portion of this document may be copied, distributed, publicized or used for other than internal documentary purposes without the written consent of an official representative of Barracuda Networks Inc. All specifications are subject to change without notice. Barracuda Networks Inc. assumes no responsibility for any inaccuracies in this document. Barracuda Networks Inc. reserves the right to change, modify, transfer, or otherwise revise this publication without notice.