How to Configure Single Sign-On for Web Forwards

https://campus.barracuda.com/doc/48660737/

Configure single sign-on (SSO) to automatically log the SSL VPN user in to a web-based service when accessing a web forward. As login credentials, you can use either the session username and password, or custom user attributes. User attributes are entered by the end user the first time the web resource is launched. Websites using one of 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 NextGen Firewall X-Series. To automatically log into web forwards 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 X-Series Firewall can automatically log users into web forwards. The form-based authentication type is determined by the HTML source of the login page.

POST

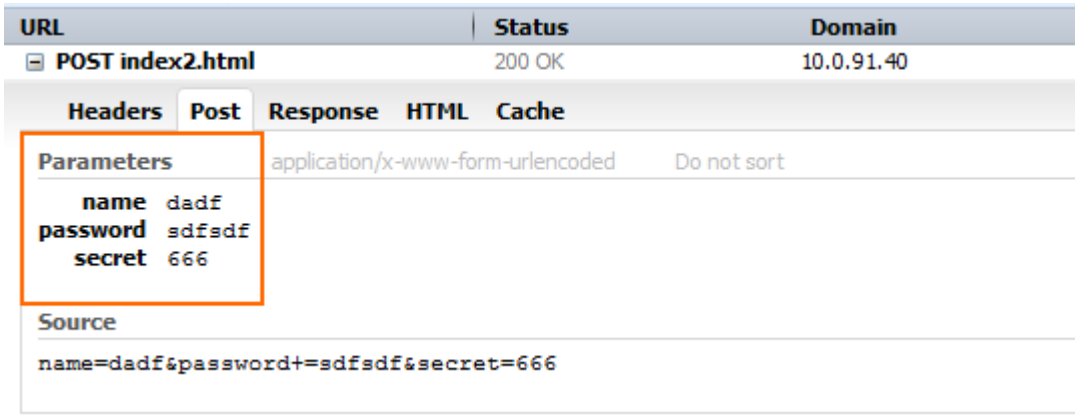
POST is the most common form submission type. Set the type to POST if the *method* attribute is set to POST. If the form contains unique or random hidden <input> elements, use JavaScript instead of POST as the form type. To find out which elements must be filled in, inspect the form submission process 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.

POST Form Example

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



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

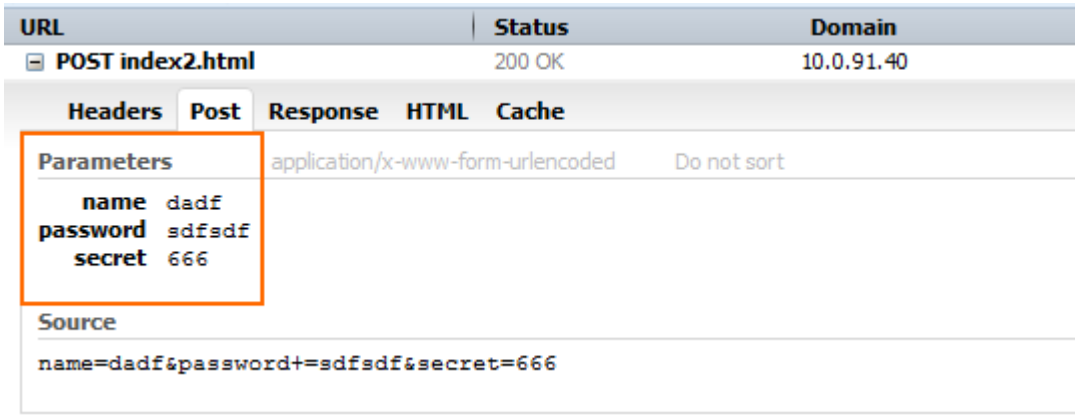
Forms using random or unique hidden input elements must use the JavaScript authentication type. After waiting for a configurable amount of time to make sure the page has finished loading, the X-Series Firewall injects a small JavaScript script into the HTML page. This script fills in the parameters specified 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



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 resource configuration:

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

Before you begin

Configure a web resource. For more information, see How to Configure a Generic Web Forward.

Step 1. Authentication type

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

Step 2. (Optional) Define user attributes

Create 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. User attributes are filled in by the end user in the web portal of the SSL VPN service.

1. Go to the **VPN > SSL VPN** page and click the **Resources** tab.
2. Under the **Applications** section, click **Show Advanced Options**. The **User Attributes** section appears.
3. Click **Add User Attribute**.
4. Configure the following settings for each user attribute:
   - **Format** – Select the type of user attribute. Possible values are: **Text**, **Number**, and **Password**.
   - **Name** – Enter the name of the user attribute.
   - **Label** – Enter the name visible to the end user.
   - **Description** – Enter a description of the attribute.
   - **Default** – 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 web portal.
   - **Weight** – Enter a value. Attributes are sorted within a category according to their weight.
   - **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]?)`
2. Click **Save**.

Step 3. Add authentication configuration to a web forward

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

FORM authentication

1. Go to the **VPN > SSL VPN** page and click the **Resources** tab.
2. Edit a generic web forward.
3. (POST authentication only) Change the **Launch Path** to the path set in the **action** attribute of the form element. E.g., `/somedir/index.php` if the form element is `<form action="/somedir/index.php" name="testform" method="POST" >`
4. Set the **Authentication Type** to **HTTP** or **FORM**.
5. Set the **Form Type** to **GET, POST** or **JavaScript**.
6. (JavaScript only) Enter the **Form Name**. E.g., `testform` if the form element is `<form`

`action="/somedir/index.php" name="testform" method="POST">`

7. (JavaScript only) Enter the **Timeout(s)** in seconds. This is the amount of the time the firewall waits before injecting the JavaScript code into the page. Default: 5 sec.
8. Enter the **Form Parameters** and click **+** to add an entry.
   - 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}
9. Click **Save.**

HTTP authentication

1. Go to the **VPN > SSL VPN** page and click the **Resources** tab.
2. Edit a generic web forward.
3. (POST authentication only) Change the **Launch Path** to the path set in the **action** attribute of the form element. E.g., `/somedir/index.php` if the form element is `<form action="/somedir/index.php" name="testform" method="GET">`
4. Set the **Authentication Type** to **HTTP Authorization Headers**.
5. Enter the **Username**. You can enter static content E.g., `johndoe` or use an Attribute E.g., `${userAttribute.SpecialUser}` or `${session.username}.`
6. Enter the **Password**. You can enter static content E.g., `johndoe` or use an Attribute E.g., `${userAttribute.SpecialUser}` or `${session.username}.`
7. Click **Save**.

Figures

1. POST_Firebug_Example.png
2. POST_Firebug_Example.png