How to Configure Single Sign-On (SSO)

https://campus.barracuda.com/doc/41092545/

Required Product Model and Version

This article applies to the Barracuda Load Balancer ADC 540 and above, version 5.1 and above.

On the Barracuda Load Balancer ADC, you can configure Single Sign-On (SSO) to let end users access multiple applications across different web servers protected by the Barracuda Load Balancer ADC, without requiring them to reauthenticate. Successfully authenticated users with proper access privileges are given an SSO User Session Cookie, authenticating them for a period of time. If the login fails, the authentication request is rejected.

The Barracuda Load Balancer ADC supports both single domain and multi-domain SSO.

Prerequisite

Verify that an authentication service and an authorization policy have been created for the services of your web applications.

For instructions, see How to Configure Authentication and Access Control (AAA).

Single Domain SSO

Single domain SSO takes place within a single domain. For example, `bc.com` hosts several restricted websites on several hosts. You can configure single sign-on for this domain, so that authenticated users can access all or a subset of the restricted resources by authenticating once.

When a user logs out of a domain, the Barracuda Load Balancer ADC removes the user session cookie from the browser by expiring it, so that the user is automatically logged out of other corresponding domains. For example, a user is logged into `host1.bc.com` , `host2.bc.com` , and `host3.bc.com` using `bc.com` as the cookie domain. When the user logs out of `host1.bc.com` , the user session cookie is removed from the browser and the user is automatically logged out of `host2.bc.com` and `host3.bc.com` .

Configure Single Domain SSO

In the authentication policy for the service, specify the SSO domain.

1. Go to the **ACCESS CONTROL > Authentication** page.
2. Click **Edit** next to the policy.
3. In the **Edit Authentication Policy** window, ensure that the policy is enabled and that an authentication service has been selected for the service.
4. In the **Session-Cookie Domain** field, enter the domain name of the service (e.g., `bc.com`) .
5. In the **Idle Timeout** field, enter the maximum length of time that a user can remain idle in the domain before being logged out automatically.
6. Click **Save**.

Multi-domain SSO

With multi-domain SSO, your users are authenticated for multiple domains after logging into one domain. When you configure multi-domain SSO, you must designate a master domain with one or more slave domains. The master domain acts as a centralized authentication server that authenticates the users and transfers the SSO User Session Cookie to the slave domains.

Users must be initially authenticated by the master domain. If a user tries to access the master domain before a slave domain, the user is prompted to provide login credentials. If a user tries to visit a slave domain before the master domain, the user is redirected to the master service URL for authentication and prompted to provide login credentials. After being successfully authenticated and authorized, the user is granted access to the master domain and slave domains.

For example, `www.abc.com` is the master domain and `www.xyz.com` is the slave domain. If a user first tries to access `www.abc.com`, the user is prompted to provide login credentials. If the user first tries to access `www.xyz.com` , the user is redirected to `www.abc.com` for authentication and prompted to provide login credentials. After being successfully authenticated and authorized, the user receives SSO User Session Cookies to access both domains.

When users log out of a domain, they are not automatically logged out of all domains; they must manually log out of each domain.

Configure Multi-Domain SSO

To set up multi-domain SSO, configure the authentication policies for the services of your master and slave domains. You must also create an authorization policy for the master domain.

Step 1. Configure the Master and Slave Domains

Complete the following steps for the services of your master and slave domains.

1. Go to the **ACCESS CONTROL > Authentication** page.
2. Click **Edit** next to the policy.

3. In the **Edit Authentication Policy** window, ensure that the policy is enabled and that an authentication service has been selected for the service.
4. In the **Single Sign On** section, specify if the domain is the master or a slave.
    - If the domain is the master, set **Master Service** to **Yes** and enter its URL path in the **Master Service URL** field. The URL must be a virtual URL (internal URL). For example: `/ncsso.process`
    - If the domain is a slave, set **Master Service** to **No** and enter the URL of the master domain in the **Master Service URL** field. In the master service URL, you must specify the protocol, host, master domain, and URL path. For example: `http://www.abc.com/ncsso.process`
5. Click **Save**.

Step 2. Create an Authorization Policy for the Master Service

Create an authorization policy with the URL of the master service.

1. Go to the **ACCESS CONTROL > Authorization** page.
2. In the **Add Authorization Policy** section:
    1. From the **Service** list, select the service.
    2. Enter a name for the policy.
    3. Set the **Status** to **Off**.
    4. In the **URL Match** field, enter the URL of the master service. For example: `/ncsso.process`
    5. Specify the host and any other expressions that must be matched in the requests.
    6. Specify the **Login Method**. If you want to create a custom login or challenge page, select **HTML Form**.

        > If you are using a custom challenge page, it does not support the **HTTP Basic Authentication** login method.
3. Click **Add**. The authorization policy appears in the **Existing Authorization Policies** section.
4. Next to the policy, click **Edit**.
5. In the **Edit Authorization Policy** window, specify if you want to allow or deny the request to all authenticated users or only specific users and groups.
6. Click **Save**.