

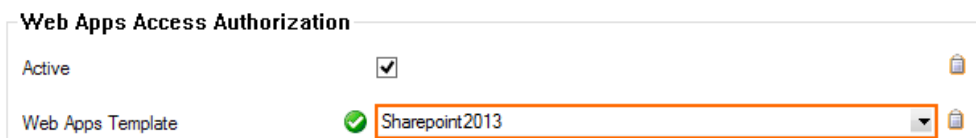
How to Configure a SharePoint Web App

<https://campus.barracuda.com/doc/79462831/>

The Barracuda CloudGen Firewall SSL VPN offers preconfigured templates for Microsoft SharePoint 2010 and 2013. The template automatically fills in all necessary web app parameters and configures Single Sign-On using the session username and password. If the user must use a different password or user to sign in, create user attributes to replace the session attributes.

Configure a SharePoint Web App

1. Go to **CONFIGURATION > Configuration Tree > Box > Assigned Services > VPN-Service > SSL-VPN**.
2. In the left menu, select **Web Apps**.
3. Click **Lock**.
4. In the **Proxied Web Apps** section, click **+** to add a web app to the list.
5. Enter a **Name** for the web app and click **OK**. The **Proxied Web Apps** window opens.
6. Select the **SharePoint** template matching your SharePoint server from the **Web Apps Template** dropdown. The **Enter Name** window opens.



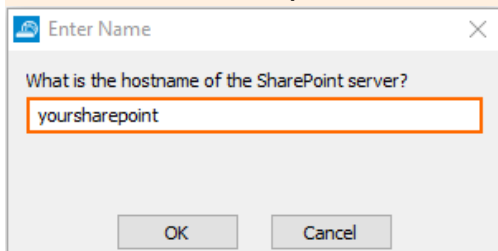
Web Apps Access Authorization

Active

Web Apps Template Sharepoint2013

7. Enter the non-qualified hostname of your Microsoft SharePoint server and click **OK**. E.g., yoursharepoint

Do not enter an FQDN for the SharePoint server.




Enter Name

What is the hostname of the SharePoint server?

yoursharepoint

OK Cancel

8. Enter the Single Sign-On (SSO) domain for your SharePoint server and click **OK**.



Enter Name

What domain is used for SSO?

yourdomain.com

OK Cancel

9. Enter the **Visible Name**. This is the name used in the desktop and mobile portal for this web app.
10. (optional) Check **Must be Healthy** if the user has to pass a health check before launching the web app. This setting requires a configured NAC client on a Windows device and policy server.

For more information, see [Access Control Service](#).

11. (optional) To restrict access to the web app by user group, replace the * entry in the **Allowed User Groups** list. Click + to add new user group.
12. (optional) Click **Ex/Import** to upload a custom icon.
13. (optional) To use user attributes to sign in, replace the session attributes in the **HTTP Authorization Headers** section with user attributes. For more information on how to create user attributes, see [How to Use and Create Attributes](#).
14. (optional) To make this resource only available when enabled by a super user,
 - Expand the **Configuration Mode** menu on the left, and select **Switch to Advanced View**.
 - Scroll down to the **Dynamic Access** section.
 - Select the **Dynamic App** checkbox.
 - Allow super users to enable, disable, or time-enable the resource.
 - Select the **Allow Maximum/Minimum Time** checkboxes and restrict the maximum and minimum amount of time this resource can be time-enabled for.
15. Click **OK**.
16. Click **Send Changes** and **Activate**.

Figures

1. sharepoint01.png
2. sharepoint02.png
3. owa03.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.