

## How to Configure an Outlook Web Access Web App

<https://campus.barracuda.com/doc/53248539/>

The Barracuda NextGen Firewall F-Series SSL VPN offers preconfigured web app templates for Outlook Web Access 2003 to 2013. By default the session username and password is used to authenticate on the Outlook Web Access portal. If the user must use a different password or user to sign in, create user attributes to replace the session attributes.

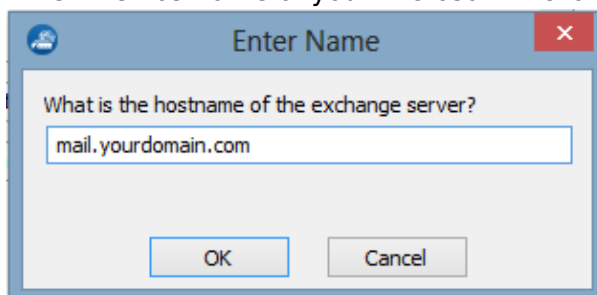
### Configure an Outlook Web Access Web App (OWA)

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. 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 **OWA** template matching your Exchange server from the **Web Resource Template** dropdown.



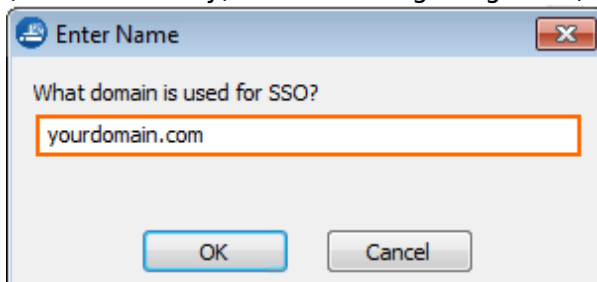
The screenshot shows the 'Web Apps Access Authorization' configuration window. The 'Active' checkbox is checked. The 'Web Apps Template' dropdown menu is open, showing 'OWA\_2003' selected. There are icons for help and save on the right side.

7. Enter the hostname of your Microsoft Exchange server and click **OK**.



The screenshot shows an 'Enter Name' dialog box with the title 'Enter Name'. The text inside asks 'What is the hostname of the exchange server?'. A text input field contains 'mail.yourdomain.com'. There are 'OK' and 'Cancel' buttons at the bottom.

8. (OWA 2003 only) Enter the Single Sign On (SSO) domain for your Exchange server and click **OK**.



The screenshot shows an 'Enter Name' dialog box with the title 'Enter Name'. The text inside asks 'What domain is used for SSO?'. A text input field contains 'yourdomain.com'. There are 'OK' and 'Cancel' buttons at the bottom.

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 username and password entries with user attributes. For more information on how to create user attributes, see [How to Use and Create Attributes](#).
14. Click **OK**.
15. Click **Send Changes** and **Activate**.

## Figures

1. owa01.png
2. owa02.png
3. owa03.png

© Barracuda Networks Inc., 2024 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.