

How to Configure an Outlook Web Access Web Forward

<https://campus.barracuda.com/doc/48660727/>

To give your end users direct access to their corporate email resources, configure an Outlook Web Access / Outlook Web App (OWA) resource. The SSL VPN offers preconfigured web forward templates for Outlook Web Access 2003, 2007, 2010, and 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.

Before you begin

Enable and configure SSL VPN on the firewall. For more information, see [How to Enable SSL VPN and CudaLaunch](#).

Configure an Outlook Web Access web forward (OWA)

1. Go to the **VPN > SSL VPN** page and click the **Resources** tab.
2. In the **Web Forwards** section, click **Add Web Forward**.
3. In the **Add Web Forward** window, set **Enable** to **Yes**.
4. (optional) Click **Browse** to upload a PNG file for the web portal, less than 30 kB and not larger than 80x80 pixels.
5. Select the **OWA** template matching your Exchange server from the **Web Forward Template** drop-down list. A pop-up window appears, asking for the server name.
6. Enter the FQDN, hostname, or IP address for your Microsoft Exchange server, and click **OK**.



What is the hostname of the exchange server?

mail.myexchange.com

Cancel

OK

7. (OWA 2003 only) Enter the Single Sign-On (SSO) domain for your Exchange server, and click **OK**.
8. In the **Name** field, enter the visible name for the web forward. This is the name displayed for the user in the web portals and CudaLaunch.

Add Web Forward ?

Enable: ☒ Yes ☐ No

Icon:
PNG File, less than 30kB and not bigger than 80x80 pixel.

Name:

Web Forward Template:

Root URL:

Launch Path:

9. (optional) In the **Allowed Hosts** list, add all servers that must be proxied by the SSL VPN when accessing this web forward. Enter **Name**, **Root URL**, and **Launch Path** in the **Allowed Hosts** section, and click +.
10. (optional) To restrict access to the web forward by user group, remove the * entry in the **Allowed User Groups** list. Enter the user groups that can access the web forward, and click + after each entry. If no groups are added, the web forward cannot be accessed. Use question marks (?) and asterisks (*) as wildcard characters.
11. (optional) In the **Single Sign On** section, change the session attribute for user attributes to enable SSO if your OWA username and password differ from the session username and password. For more information on how to create user attributes, see [How to Use and Create Attributes](#).
12. Click **Save**.

Figures

1. web_fwd_owa_01.png
2. web_fwd_owa_02.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.