
How to Configure a Microsoft SharePoint Web Forward

<https://campus.barracuda.com/doc/39813237/>

When you create a Web Forward for SharePoint 2013 on the Barracuda SSL VPN, use the SharePoint 2013 Web Forward template. To get SharePoint working through a proxy, you must also add **Alternate Access Mappings** to tell SharePoint to expect requests that were made to other hosts (namely, the Barracuda SSL VPN).

Using SharePoint 2007 and 2010

- When using SharePoint 2010, the end user must disable the **Trusted Documents** setting to allow the editing of documents on a SharePoint 2010 server using Office 2010.
- When using SharePoint 2007, be aware that the SharePoint 2007 template only allows site navigation, limited editing of the SharePoint site, and the uploading and downloading of documents.

Step 1. Configure the SharePoint server

On the SharePoint server, add alternate access mappings. Then restart the IIS server.

Step 1.1 Add alternate access mappings

1. Go to the SharePoint 2013 Central Administration console (this might be set up on *your SharePoint server*:1317). If it is not available, log into the system that IIS is running on and go to **Start > SharePoint 2013 Central Administration**.
2. On the **Central Administration** page, click **Configure alternate access mappings** in the **System Settings** section.
3. Click **Edit Public URLs**.
4. From the **Alternate Access Mapping Collection** list, select **SharePoint - 80**.
5. Add the following entries:
 - **Default:** `http://your SharePoint server`
 - **Intranet:** `http://your fully qualified SharePoint server`
 - **Internet:** `http://your fully qualified Barracuda SSL VPN`
 - **Extranet:** `https://your fully qualified Barracuda SSL VPN`

Step 1.2 Restart the IIS server

1. Go to **Start > Internet Information Services (IIS) Manager**.
2. In the left pane, click **SHAREPOINT**.
3. In the right pane under **Manage Server**, click **Restart**.

Step 2. Create the Web Forward for SharePoint

Configure the Web Forward with the information for the SharePoint server, and add policies for the users and groups who are allowed to use it.

1. Log into the [SSL VPN web interface](#).
2. In the upper right, verify that you have selected the correct user database.
3. Go to the **Manage System > RESOURCES > Web Forwards** page.
4. In the **Create Web Forward** section, configure these settings:
 - **User Database** - Select the database that the users reside in.
 - **Name** - Enter a name to help end users identify the Web Forward. For example, SharePoint.
 - **Web Forward Category** - Select the **Portals** check box, and then select **SharePoint 2013**.
 - **Hostname** - Enter the hostname or IP address of the server that you want to connect to.
 - **Domain** - Enter the domain that the SharePoint server belongs to.
5. From the **Available Policies** list, add the policies that you want to apply to the Web Forward.
6. To add the Web Forward to the default Resource Category, enable **Add to My Favorites**.
7. Click **Add**.

The SharePoint 2013 Web Forward appears in the **Web Forwards** section.

Step 3. Launch the Web Forward

Add a resource category to the Web Forward to make it available to users on their **My Resources** page.

1. In the **Web Forwards** section, click **Edit** next to the Web Forward entry.
2. In the **Edit Web Forward** window, scroll to the **Resource Categories** section, and add the available categories that you want to apply to the Web Forward.
3. If you want the Web Forward to automatically launch whenever users log into the Barracuda SSL VPN, scroll to the **Details** section and enable **Auto-Launch**.
4. Click **Save**.

© 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.