

How to Enable SafeSearch

<https://campus.barracuda.com/doc/39819700/>

SafeSearch mode prevents a web search engine from displaying objectionable thumbnail images in search results; only filtered thumbnails are displayed in the search results. You can enable SafeSearch with the **Safe Browsing** feature on the **BLOCK/ACCEPT > Content Filter** page. This will limit search results to filtered thumbnails in Yahoo, Bing, Google, YouTube and other applications that return video and photo thumbnail search results.

Since Google and some other search engines always use HTTPS, Barracuda recommends enabling the SSL Inspection feature when using Safe Search for searching YouTube videos and other web content. To enable SSL Inspection, you must have:

- A Barracuda Web Security Gateway 410 running version 7.1 or above: see [How to Configure SSL Inspection Version 7.1](#), OR
- A Barracuda Web Security Gateway 310 or above running version 12.0 or above: see [How to Configure SSL Inspection Version 12 and Above](#)

How to Enable SafeSearch for All Users

1. Enable **SSL Inspection** if you want to enforce Safe Search over HTTPS, which is recommended.
 1. Barracuda Web Security Gateway 610 and higher: Enable **SSL Inspection** on the **ADVANCED > SSL Inspection** page and install a secure certificate in all client browsers.
 2. Barracuda Web Security Gateway 410 running 7.1 and higher: Enable **SSL Inspection** on the **BLOCK/ACCEPT > Configuration** page and install a secure certificate in all client browsers.
2. Go to the **BLOCK/ACCEPT > Content Filter** page. At the top of the page next to **Policy** on the right, select either **Authenticated** or **Unauthenticated**.
3. In the **Safe Browsing** section, select the category/search engine for which you want to enable Safe Search. If you were previously using the **YouTube For Schools** feature, see [How to Restrict YouTube Content On Your Network](#).
4. Click **Save**.

With the Barracuda Web Security Gateway version 9 and above, when **YouTube SafeSearch** is enabled, the user can only browse YouTube as a guest, and not as a logged in user. This means that private videos will not be visible, nor can videos be uploaded. The user can, however, log into Google or Gmail as usual.

If you **Enable** SafeSearch, it will limit the thumbnails returned in search results for images and videos for ALL **Authenticated** or **Unauthenticated** users, depending on which **Policy** you choose per the steps above. If you want to limit SafeSearch to certain users or group(s) of users, you should **Disable** SafeSearch on the **BLOCK/ACCEPT > Configuration** page and

create one or more Exceptions for those users. The following example illustrates the process to do that.

Use Case: Safe Browsing for Students

To limit SafeSearch to a specific group of users, such as students, for example, but allow appearance of all thumbnail images in search results for teachers and staff, create an exception using the *Enable* action, like this example:

1. Enable **SSL Inspection** if you want to enforce SafeSearch over HTTPS.
 1. Barracuda Web Security Gateway 610 and higher: Enable **SSL Inspection** on the **ADVANCED > SSL Inspection** page and install a secure certificate in all client browsers.
 2. Barracuda Web Security Gateway 410 running 7.1 and higher: Enable **SSL Inspection** on the **BLOCK/ACCEPT > Configuration** page and install a secure certificate in all client browsers.
2. On the **USERS/GROUPS > Local Groups** page, create a new group called **Students**.
3. On the **USERS/GROUPS > New Users** page, add the students' usernames on the Barracuda Web Security Gateway to the **Students** group, following instructions in the online help for that page.
4. On the **BLOCK/ACCEPT > Content Filter** page, in the table under **Safe Browsing** , select **Disable** for each search engine listed in the table, or click the [All](#) link.
5. On the **BLOCK/ACCEPT > Exceptions** page, create the policy:
 1. For **Applies To**, select **Local Group**, and then in the next drop-down, select **Students**.
 2. Select the **Exception Type** as **Content Filter**.
 3. For **Content Type**, scroll down and select **Safe Browsing**.
 4. Select the **Enable** action (it may be automatically selected) above.
 5. Click the **Add** button to see the exception added to the **List of Exceptions** table on the page.

© Barracuda Networks Inc., 2022 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.