

## How to Configure Web Monitoring in Barracuda SecureEdge

<https://campus.barracuda.com/doc/100370345/>

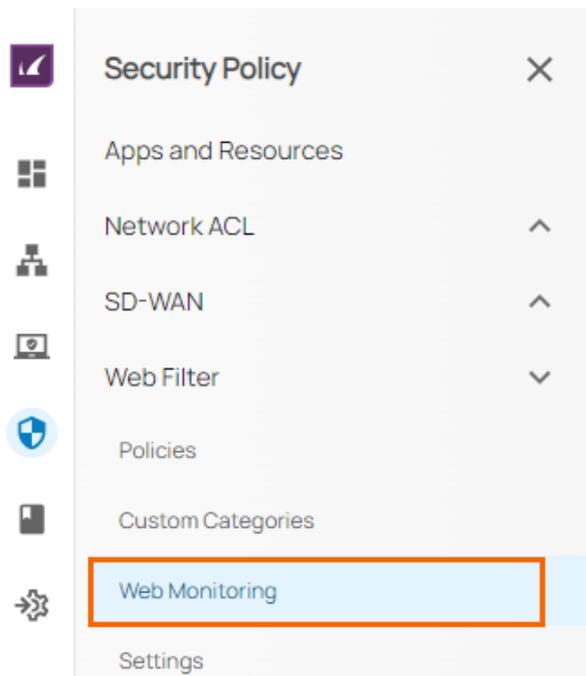
The Barracuda SecureEdge Manager allows you to configure Web Monitoring policies, so that suspicious keywords can be detected in search engines such as Google, Yahoo, Bing, DuckDuckGo, and YouTube. You can select both keywords and keyword categories to be monitored for a specific workspace. The SecureEdge Cloud UI provides a default list for the following categories: Adult/Pornography, Cyber Bullying/Profanity, Weapons and Violence, and Terrorism. In addition, users can specify their own keywords that they want to detect. The default categories can be selected via a check box, and a new list of user-defined keywords can be created and added to the monitoring list. By default, Web Monitoring is disabled.

When enabling Web Monitoring on Barracuda SecureEdge, SSL Security Inspection must be enabled and configured.

To enforce Web Monitoring via the SecureEdge Agent, you must configure a Zero Trust Access (ZTA) policy for search engines that Barracuda SecureEdge supports.

### Enable Web Monitoring

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to enable Web Monitoring for.
3. Go to **Security Policy**.
4. Expand the **Web Filter** menu on the left and select **Web Monitoring**.

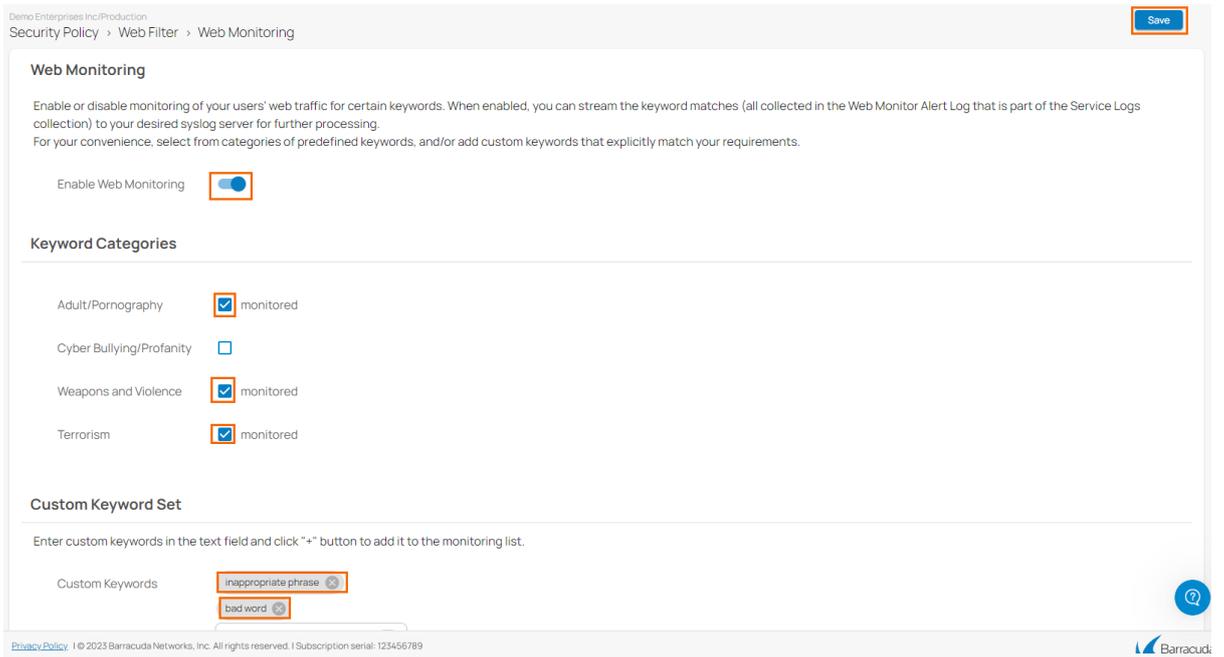


5. The **Web Monitoring** page opens. Specify values for the following:

- **Enable Web Monitoring** – Click to enable/disable. By default, Web Monitoring is disabled.

When **Web Monitoring** enabled, specify the following:

- In the **Web Monitoring** section, you can select predefined keywords for the following categories:
  - **Adult/Pornography** – Click to select/clear the box.
  - **Cyber Bullying/Profanity** – Click to select/clear the box.
  - **Weapons and Violence** – Click to select/clear the box.
  - **Terrorism** – Click to select/clear the box.
- In the **Custom Keyword Set** section, specify the following:
  - **Custom Keywords** – Enter custom keywords and click **+** to add more keywords to the monitoring list. To remove custom keywords, click **x**. Note that the maximum length per custom keyword is 128, and valid custom keyword values are as follows:
    - Uppercase letters: A-Z.
    - Lowercase letters: a-z.
    - Numbers: 0-9.
    - Symbols: [.,-]
    - Spaces.

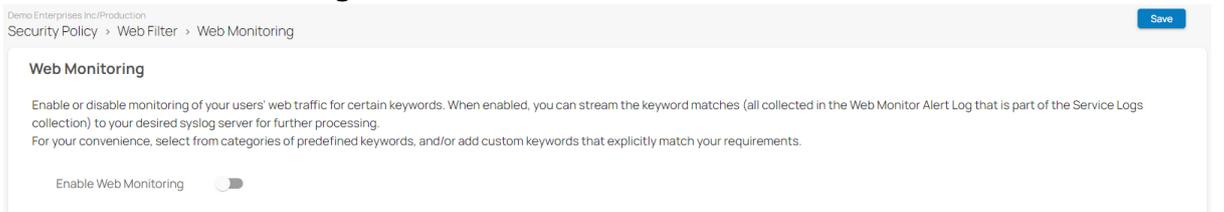


6. Click **Save**.

The Web Monitoring configuration is saved. With respect to a selected workspace: if you search for content matching predefined categories or custom keywords on your appliance, these searches are reported in the Web Monitor Alert log, which is part of the Service Logs collection. You can stream these logs to your desired syslog server for further processing. In addition, you can also verify that changes to the Web Monitoring policies are audited, and that notifications are sent. For more information, see [How to Configure Syslog Streaming in SecureEdge](#).

## Disable Web Monitoring

1. Go to <https://se.barracudanetworks.com> and log in with your existing Barracuda Cloud Control account.
2. In the left menu, click the **Tenants/Workspaces** icon and select the workspace you want to disable Web Monitoring for.
3. Go to **Security Policy**.
4. Expand the **Web Filter** menu on the left and select **Web Monitoring**.
5. The **Web Monitoring** page opens. Specify values for the following:
  - o **Enable Web Monitoring** – Click to disable.



6. Click **Save**.

After the configuration is saved, the workspace that was previously enabled for Web Monitoring will be disabled. Searches for content that matches previous Web Monitoring settings on a box will not be reported.

## Figures

1. GotoWebMonitoring.png
2. WebMonitoring-9.0.1.png
3. WebMonitoring-disable.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.