

Dashboard for Barracuda Content Shield Plus

<https://campus.barracuda.com/doc/79466243/>

This article applies to *Barracuda Content Shield (BCS) Plus* subscriptions. For *Barracuda Content Shield (BCS)* subscriptions, see [Dashboard for Barracuda Content Shield DNS Filtering](#).

The statistics displayed on this dashboard indicate what kind of activity is being blocked for your clients. Tune your policies as needed on the **Advanced Filtering** page, as described in [How to Configure Advanced Filtering Policies](#).

For remote users, see:

- [Barracuda Content Shield Agent for Endpoints](#)
- [How to Get and Configure Barracuda Chromebook Security for BCS](#)

Graphs of Threats Blocked and Other Endpoint Metrics

At the bottom of each graph, select **Last 24 hours**, **Last 7 days**, or **Last 30 days**:

- **Threat Summary** - Total number of threats blocked, including threats identified via website downloads of malware.
- **Threats Blocked** - Graph of number of threats blocked by hour or by day.
- **Encrypted Traffic** - Graph showing number of HTTPS and HTTP requests.
- **TLS Versions** - Number of requests on endpoints and corresponding TLS versions in use.
- **Applications** - Shows type of browser used on endpoints and number of requests.
- **Top 5 Endpoints Encountering Threats** - Table listing Endpoint Names, Usernames, Threats (number), the date and time of the Last Threat, and Barracuda Content Shield (BCS) Suite Versions.
 - Click **Download CSV** for a .csv file.
 - Click **View All** to see the Threat Logs page listing details for the blocked files for the selected endpoint.

The right pane of the page displays:

- **Subscriptions** by Type, Number of Licenses, and Expiration date
- **Blocked Supercategories** and the **Top Blocked Categories** tabs. Click on either tab to view the **Count** and **Trend** of number of requests blocked by category or supercategory.
- Adjust the time frame for the **Blocked Supercategories** and the **Top Blocked Categories** tabs: At the bottom of the right pane, select **Last 24 hours**, **Last 7 days**, or **Last 14 days**.
- Create and view reports: click **View Report** at the bottom of the right pane to go to the Reports page. See [Reports](#) for details.

Navigation from the Dashboard

The following screens are available from the Dashboard page left navigation pane. Click on the page name for more details about features.

- [DNS Filtering](#) - Create, review or delete preset or customized filtering policies by categories of domains.
- [Advanced Filtering](#) - Use this page to create, review or delete preset or customized filtering policies for a particular user or group. Policies can be based on either categories or domains.
- [Web Filtering Logs](#) - View the allowed and blocked traffic logs.
- [Threat Policy](#) - Select actions to take with harmful files, specify file types to scan, allow or block password-protected or encrypted files, whether to scan removable drives, and to exclude specific paths or files from scanning.
- [Quarantine](#) - Table listing suspicious files quarantined by the service if **Action For Suspicious Files** is set to *Quarantine* on the **Threat Policy** page.
- [Threat Logs](#) - Table of threats identified by the service, including Date, User, Endpoint Name, Path, Filename, and Scan Determination (*Suspicious, Malicious or Encrypted*).
- [Reports](#) - Create or schedule reports on Blocked Categories or Blocked Supercategories.
- [Endpoints](#) - A record of the threats seen and the BCS Suite version installed on the endpoint.
- [Alerts](#) - Create notifications to specific recipients based on a selected event (Notification Type).
- [Downloads](#) - Download a copy of the Barracuda Content Shield software to install on endpoints.
- [Users](#) - Configure LDAP / AD for associating users and/or groups with the service for authentication and applying policies. Or manually configure users locally to the service.
- [Account Settings](#) - Upload a custom logo to display on reports and on blocked pages displayed to end users. Configure Syslogs, Look up a domain by category, or re-categorize a domain.
- [Block Page](#) - Use this page to customize the message in the block page the user sees when a website is blocked due to configured policy.
- [Agent Settings](#) - Configure **Allow Agent Removal** (Tamper Proof feature), agent updates, Max CPU usage allowed on endpoints, and option for agent to resolve specified domains using the DNS Server configured on the endpoints.
- [Exemption Policies](#) - Configure exemptions to filtering by the BCS agent, such as processes or destination network servers

Note on Blocked HTTPS Sites

Blocked HTTPS sites show an *invalid certificate* error in the popup block page the first time the website is accessed. However, per the example below, the user just needs to click **Proceed to <website>** at the bottom of the popup to continue.

← → ↻ ⚠ Not secure | https://gambling.com



Your connection is not private

Attackers might be trying to steal your information from **gambling.com** (for example, passwords, messages, or credit cards). [Learn more](#)

NET::ERR_CERT_AUTHORITY_INVALID

☐ Automatically send some [system information and page content](#) to Google to help detect dangerous apps and sites. [Privacy policy](#)

HIDE ADVANCED

Back to safety

This server could not prove that it is **gambling.com**; its security certificate is not trusted by your computer's operating system. This may be caused by a misconfiguration or an attacker intercepting your connection.

[Proceed to gambling.com \(unsafe\)](#)

Figures

1. CertError.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.