

How to Use the Barracuda Content Shield Suite for Windows

<https://campus.barracuda.com/doc/79468430/>


- For endpoint computers using Firefox, Barracuda Content Shield (BCS) Suite requires Firefox 68.0 or later. For information about getting and installing the BCS suite, see [How to Manage Deployment of the Barracuda Content Shield Suite for Windows](#).

The Barracuda Content Shield (BCS) Suite for Windows includes two components:

- Web Filtering Component (WFC) – Applies policies you create on the **Advanced Filtering** page to endpoint web traffic, which take precedence over rules configured on the **DNS Filtering** page.
- [Malware Prevention Component \(MPC\)](#) – Scans files on the endpoint for malware both at initial installation and as the user accesses files. For Windows Terminal Server deployments, any files quarantined will appear as such to all users. **Note that, with version 2.1 and later, the MPC agent is not installed by default; you must elect to install it** (see [How to Manage Deployment of the Barracuda Content Shield Suite for Windows](#)). Available for Windows. ***The Malware Prevention feature (MPC) was no longer sold as part of BCS Plus after December 21, 2021.***

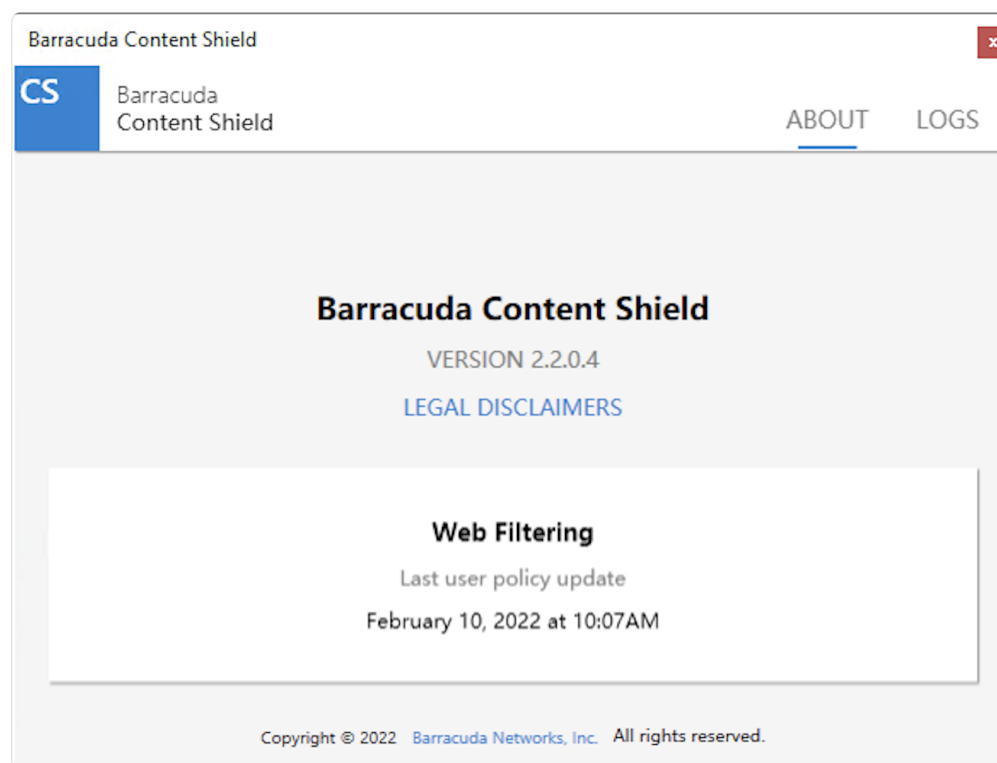
Best Practice: If you are using the BCS agent with a DNS proxy solution, do the following for local domains:

In the **DEFINE ALL LOCAL DOMAINS** section of the **Agent Settings** page, enter local domains in the **LOCAL DOMAINS** text box. The BCS agent will resolve the domains configured here using the DNS Server configured on the endpoints.

The BCS suite user interface is displayed on the Windows endpoint machine when the user clicks the shield icon  in the system tray. If you have installed both the MPC and WFC components, the **About** screen will display tiles for each. By default, only the WFC component is installed; however, you can choose to install the MPC as well if you select a custom installation. The timestamps in the Malware Prevention and Web Filtering tiles reflect the most recent policy update received for that feature.



If you only installed the WFC component, the **About** screen will show only the **Web Filtering** tile.



The **Status** screen of the BCS suite user interface displays information about malicious or suspicious

files that are detected and quarantined by the Malware Protection feature of BCS Plus.

If you disable **Malware Prevention** on the **Threat Policy** page:

- The MPC is disabled and threat policies are not applied on the client machines. Web Filtering will still apply to web traffic per policy.
- The *scan and deliver* behavior will be disabled. See **Scan and Delivery of Downloaded Files** below.

NOTE: If the administrator has DISABLED the Malware Prevention setting under the account's **Threat Policy** page, scanning of files will be deferred indefinitely, or until the feature is re-enabled. The end user can check the state of this feature by hovering their mouse over the timestamp within the Malware Prevention tile on the BCS suite user interface **About** screen. The tooltip will display either *ACTIVE* or *DISABLED*.

Scan and Delivery of Downloaded Files

The WFC scans files (executables, archives, documents, etc.) that the user attempts to download. When a user navigates to a website and clicks the download link for some software, the agent downloads the file for internal scanning before delivery to the user. If the file is determined to be malicious:

- The file is blocked, and the full file path to the file is displayed on the [THREAT LOGS](#) page.
- The user is served a block page indicating that a threat has been found and the file has been blocked.



Scanning Files

The MPC will conduct a full scan of the local file system when the software is first installed, and then again after every reboot. Subsequent scans only evaluate files that have either been added or changed since the previous scan, allowing the process to complete in less time. Newly introduced files will be scanned when downloaded as described above.

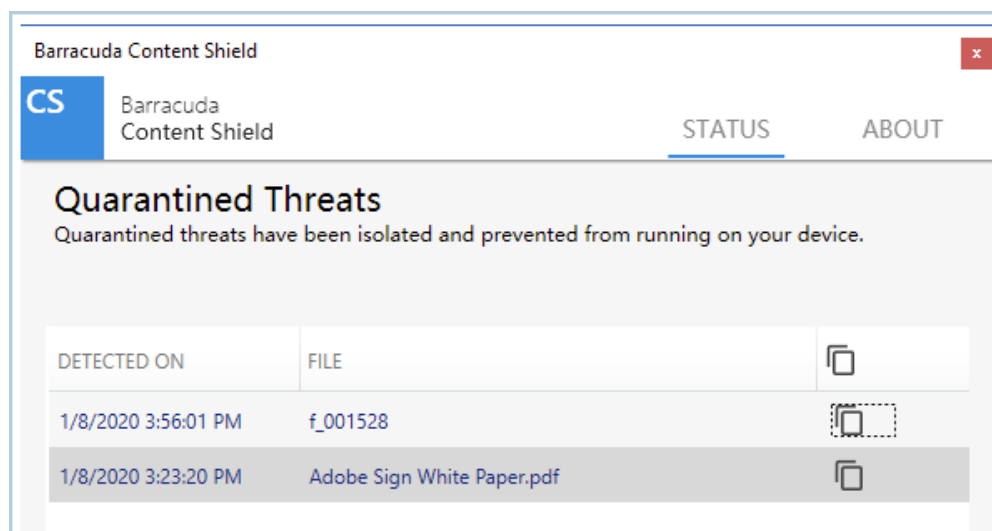
Note that the MPC does not support scanning RDS User Profile Disks on Windows Server systems.

Quarantined Threats

When the MPC detects a suspicious or malicious file on disk, the file is quarantined and a notification is displayed in the lower right-hand corner of the user's display. Additionally, the BCS suite icon in the system tray will change to reflect that one or more threats have been detected:

The threat icon  is displayed until the end user has accessed the BCS suite user interface **Status** screen, thereby acknowledging receipt of the threat notification(s). The icon will then revert back to the normal state .

The initial state of the **Status** screen, with no threats having yet been detected, displays a large green shield outline with a check mark inside. After a threat is detected and quarantined, an entry is added to a table displayed on the **Status** screen. The table then lists the DETECTED ON date & time, the FILE name, and a clipboard icon. Hovering your mouse over an entry will display a tooltip containing the full path to the location the quarantined file was removed from. Clicking on the clipboard icon will copy attribute details for the file into the system's clipboard, from where it can be copied and, for example, mailed to the system admin.







The clipboard contents for the first entry as shown will look something like this:

```

Verdict : VIRUS - Known malware
File Name : f_001528
Mime Type : application/x-gzip
File Size : 33576 bytes
SHA-256 : 9ba41d51fbabdb9fcaa7e9e34581d153d8f901a2ce9e364f60162ca278743813
SHA-1 : 86419ba79b0a0ba924f6e6e349ad078aa8fb6f80
MD5 : 55b8e6059da09b4e50cbe105e4a090a3
QID : d6731f0f-38e2-a24f-a9e1-b52f00ec44f5
Detected : 1/8/2020 3:56:01 PM
Full Path :
C:\Users\ismith\AppData\Local\Google\Chrome\User Data\Default\Cache\f_001528
  
```

Note that only the administrator can remove files from quarantine.

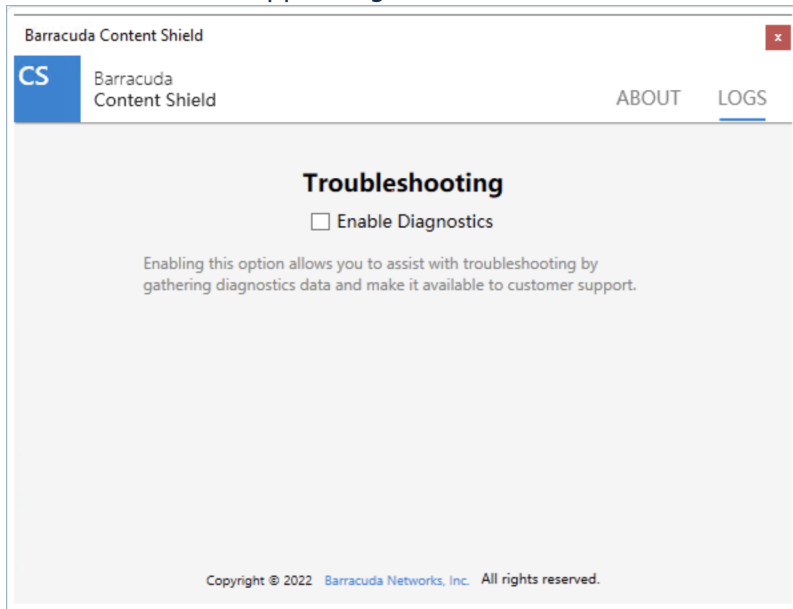
System Tray Icons and Notifications / Errors

Task Tray Icon Appearance	Meaning
	When a threat is detected and a file is quarantined. Click on the icon to see the Status screen. If the agent loses connection with the BCS service before you click the icon, then the  icon will display until you click on it.
	The endpoint machine cannot communicate with Barracuda Content Shield, and/or the on-access scanner is not running. File scanning can still take place using local settings, but the MPC is not being triggered to scan when a user accesses a file. This can happen if the MPC was uninstalled and then re-installed without rebooting. Try rebooting the machine.
	The Barracuda Content Shield service is not available, or there is no Internet connection. On-access scanning will still apply, but only with cached results. If a threat has been detected but the threat task tray icon has not been clicked and BCS cannot connect, this icon supersedes the threat icon in the task tray.

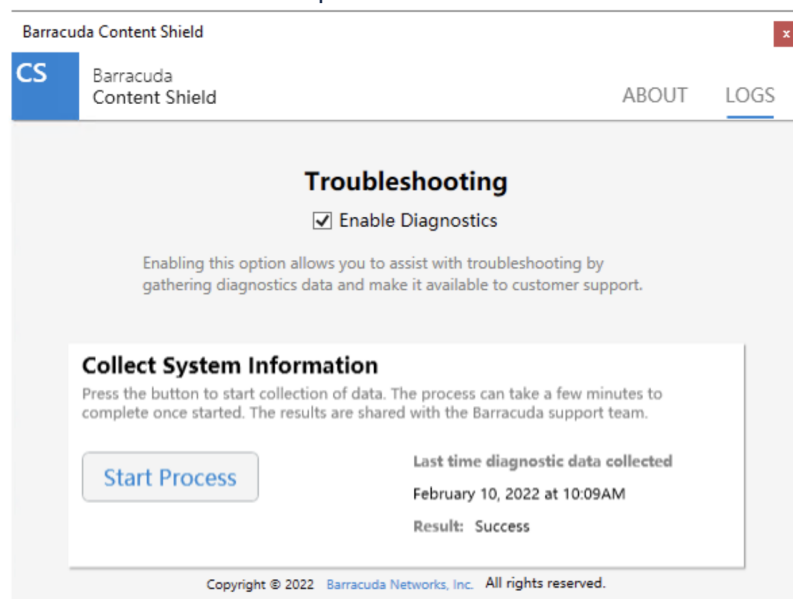
Support Diagnostics

The administrator can enable the user to collect log diagnostic data on the endpoint and send it to Barracuda Networks Support (*this feature available for Windows only*). To enable this, go to the **Agent Settings** page and set **Allow Log Collection** to **ON**. The user will then see a **LOGS** tab in the upper right in the BCS Agent UI after the next successful configuration sync on the endpoint. For the user to collect and send support log data:

1. The user clicks the **LOGS** tab, and then checks **Enable Diagnostics** on the Troubleshooting screen to enable support log collection:



2. Next, the user can trigger log collection by clicking **Start Process**. Log collection can take several minutes to complete.



3. After log collection has completed, the last diagnostics collection date and the Result (e.g. "Success") are displayed to the right of **Start Process**.
Note: This functionality is blocked for 5 minutes after the log collection is triggered in order to maintain system performance.
4. The log data is sent from the agent to Barracuda Networks Support.

How to Uninstall the Barracuda Content Shield Suite

The Barracuda Content Shield employs a Tamper Proof feature that prevents end users from uninstalling this software. However, the administrator can choose to bypass this feature using the **Allow Agent Removal** option on the **AGENT SETTINGS** page:

1. Set **Allow Agent Removal** to *On*
2. Enter an **Agent Password**, which must be entered at the endpoint in order to bypass the Tamper Proof feature and allow the software to be uninstalled.

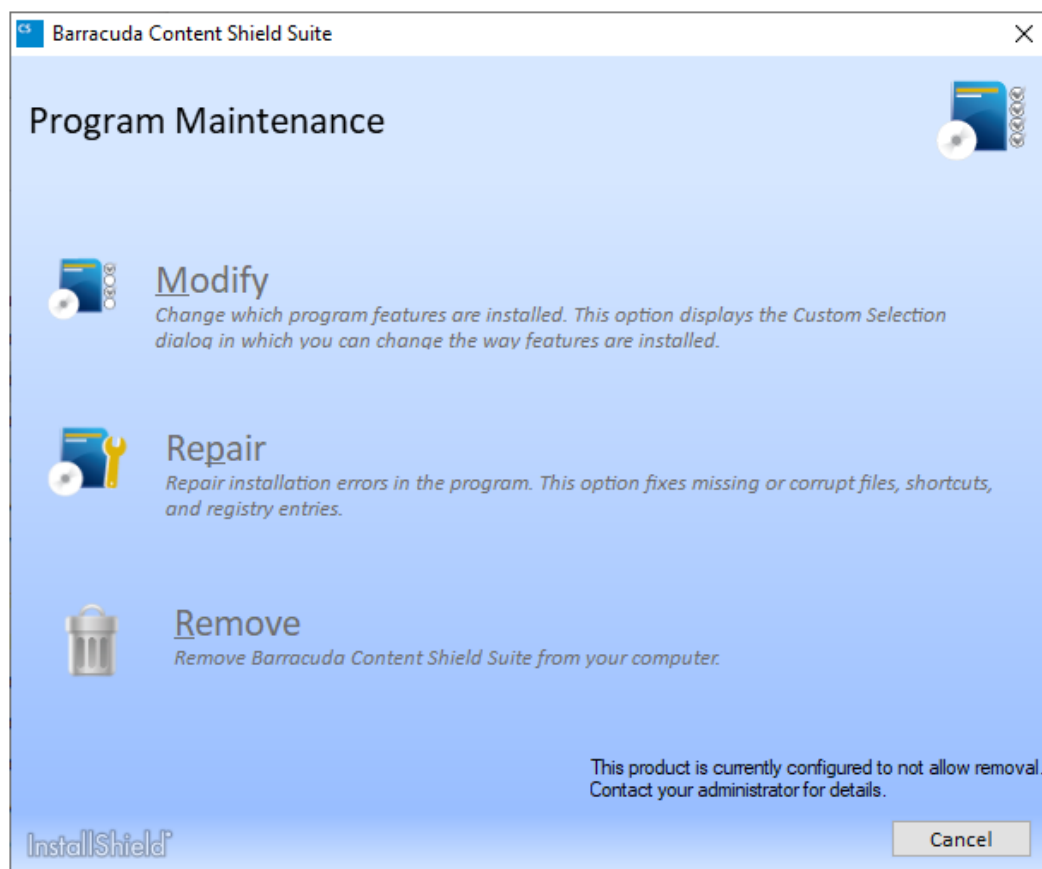
Notes about the Tamper Proof Feature:

- Changes made to features on the **AGENT SETTINGS** page are propagated to endpoint machines when they receive their next policy update (roughly every 15 minutes).
- In the example screenshot below, the text *This product is currently configured to not allow removal* displayed above the **Cancel** button indicates that Tamper Proof is NOT bypassed, as the **Allow Agent Removal** toggle is set to *Off* (on the **AGENT SETTINGS** page).

After the Agent Settings have been properly configured, the software can be uninstalled in either of two ways;

1. Launch the BarracudaContentShieldSetup-#####.exe installer and select *Remove*, and enter the **Agent Password** when prompted.
2. Access the Windows Control Panel and select the Programs and Features option. Highlight the BCS suite entry, then click on **Uninstall**. When prompted, enter the **Agent Password**.

When the uninstall completes you will be prompted to reboot the computer.



Figures

1. idle.jpg
2. BCS Suite main screen.png
3. AgentWindowsSplash2.2.0.4.png
4. Threat.PNG
5. eps-agent-idle.png
6. BSC Suite Quar Threats.png
7. threatdetailsx.png
8. Threat.PNG
9. CriticalError.PNG
10. Warning.PNG
11. CriticalError.PNG
12. Troubleshooting1.png
13. DiagnosticsComplete.png
14. UninstallGUI.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.