Exemption Policies

https://campus.barracuda.com/doc/93201098/

Use this page to create exemptions for certain web traffic, destination servers, or processes from filtering by the BCS agent with your BCS Plus subscription.

Exempting Specific Application Traffic: Barracuda Content Shield intercepts TCP traffic on ports 80/443 in order to provide security and to enforce browsing policy. It does this by means of a forced HTTP/S proxy, which examines the outgoing connection and traffic, and then redirects it to the intended host. Outgoing traffic on those ports that doesn't conform to the protocol specification, such as non-standard connection options or message payloads, are not supported by the proxy. For example, certain applications may communicate over TCP port 443, but exchange data in their own proprietary format.

At the current time, Barracuda Content Shield does not support such products directly, but allows an administrator to exempt such application traffic from policy enforcement.

## Exempt All Microsoft Application Traffic

Enable this feature if you want to exempt all Microsoft application traffic such as Microsoft 365, Skype, or Teams, from filtering by the BCS agent.

Define All Process Exemptions

To exempt one or more processes from scanning or filtering on the endpoint machine, enter executable names or the full path of a process in the **PROCESS EXEMPTIONS** text box. When specifying the path of an executable/process, make sure to use the drive letter/path or process/application name. **Entries are case sensitive.**
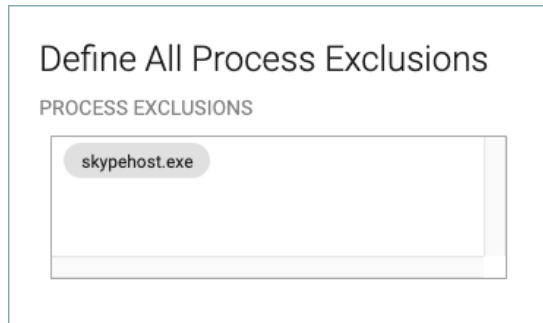
Example 1.

These entries exempt explorer.exe and c:\Desktop\Excel.exe from scanning on the endpoint:
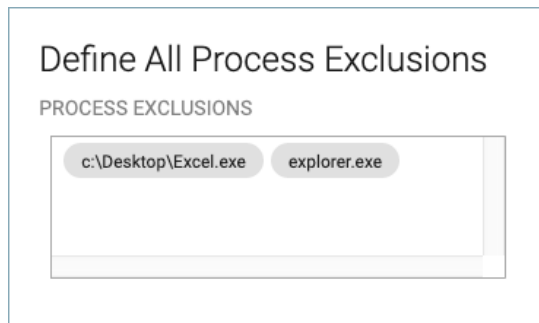
Example 2.

Say you created a block domain rule for Skype.com on the **Advanced Filtering** page. When the user accesses Skype.com in their browser on the endpoint, it will be blocked. When the user tries to log into the Skype app, that will also be blocked since it sends requests to Skype.com – or related URLs – which are blocked because of the Advanced Filtering policy.

If you want to allow the user to log into Skype using the app, but not via the browser, use the Process Exclusion feature to exempt skypehost.exe from the block policy. Skype.com can still be blocked on the browser, but logging into the Skype app would be successful.

To edit or remove an exclusion you created, click on the process to select it and delete it.

Exempt Destination Network Servers

Best practice: If there are specific local networks that you do not want the BCS agent to filter (for example, printers, VPN), add them here.

Exempt Destination Network Servers

Exclude all Network IPs/ranges or hostnames from filtering by the BCS agent. Use CIDR notation for Network IP ranges. Example: 198.61.2.1/32 or *.barracuda.com

NETWORK EXEMPTIONS

198.35.20.112/32   *.barracuda.com   barracuda.com
auth.atlasssian.com   *.auth.atlassian.com   test.com
wexlerinsurance-my.sharepoint.com   wexlerinsurance-files.sharepoint.com
1.1.1.1   *.results-cx.com   *.yahoo.com

In the **Exempt Destination Network Servers** text box, enter each IP address or hostname to certain destination servers you want to bypass filtering by the BCS agent. For example, exempt applications like Cisco Anyconnect. Use CIDR notation – for example, 192.168.100.0/24 represents an IP address of 192.168.100.0 with a subnet mask of 255.255.255.0.

 Note that you can create network exemptions, and you can specify top level domains, like barracuda.com, or *.barracuda.com, for example. So you have the option to block all subdomains with *.barracuda.com (or any set of subdomains) and top level domains when necessary.

Figures

1. ExcludeExplAndExcel.png
2. ExcludeSkypehost.png
3. ExemptDestServers.png