Web Categorization Upgrade for Barracuda Web Security Gateway 15.x

https://campus.barracuda.com/doc/90441547/

If you have upgraded your Barracuda Web Security Gateway to version 15.x, Barracuda Networks recommends upgrading your web categorization engine to WCS 3.0 to access the latest web categorization, which includes many more and finer grained categories than WCS 2.0. You can then apply finer grained policies (including SSL Inspection) to user browsing and produce more granular reports on domains visited. There are significant benefits of upgrading to WCS 3.0, and there are caveats you should be aware of before upgrading. **Barracuda Networks recommends reading this article completely before moving to WCS 3.0.**

> Important: If you upgrade to WCS 3.0 and create new policies and exceptions, and then revert back to WCS 2.0, all of the data collected when you were running WCS 3.0 will be inaccessible unless you upgrade back to WCS 3.0.

Benefits of upgrading to WCS 3.0

- Over twice as many categories of domains than available with WCS 2.0
- Allows for much finer grained policies for web browsing

Caveats of upgrading to WCS 3.0

1. Mapping of WCS 2.0 categories to WCS 3.0 categories is not 1:1, so some policies will shift.
2. Most policies and exceptions are converted based on WCS 3.0 categorization.
3. All content filter rules are disabled, including rules created for **Saved Custom Categories** on the **BLOCK/ACCEPT > Content Filter** page. These rules must be recreated per the new categorization of domains in WCS 3.0.
   1. Review the updated custom categories and ensure that they are correct, based on your policy needs. Note that *custom categories* that were created on the **BLOCK/ACCEPT > Custom Categories** page with WCS 2.0 are preserved and converted based on the new categorization in WCS 3.0.
   2. Enable the content filtering rules.
4. Browsing statistics – including Dashboard displays – are cleared after upgrading to WCS 3.0. For example:
   1. On the **Dashboard** page, in the **Most Recently Blocked Requests** section, category names in the **Last Blocked** column are cleared and replaced by new data captured with WCS 3.0 running.

2. On the **Dashboard** page, **Top Blocked Categories - By Request** and **Top Blocked Categories - By Bandwith** data is cleared and replaced by new data captured with WCS 3.0 running.

5. Report data based on WCS 2.0 is no longer visible after upgrading to WCS 3.0; however, if you revert to WCS 2.0, that report data will again be visible. Scheduled reports that filter on categories from WCS 2.0 are disabled after upgrading to WCS 3.0.
    1. Review the updated categories.
    2. Re-enable scheduled reports.
6. Categories selected on the **ADVANCED > SSL Inspection** page in the **Inspected Categories** section are converted to WCS 3.0.

How to upgrade to WCS 3.0

This procedure assumes you have already upgraded your Barracuda Web Security Gateway to version 15.0 or above.

1. Barracuda Networks recommends making a backup of your configuration on the **ADVANCED > Backups** page.
2. Make a list of your policies and exceptions.
3. Go to the **ADVANCED > Configuration** page and set **WCS version** to *3*.
4. Go the **BLOCK/ACCEPT> Content Filter** page and create new policies that are based on the updated categories and custom categories.

Mapping WCS 2.0 to WCS 3.0

Some categories defined in [WCS 2.0](#) have been split into several more granular categories that cover the same kinds of websites in WCS 3.0. In those cases, your policies remain the same, but are now more granular. Some examples of these are shown in the table.

Example 1. WCS 2.0 category *Entertainment*, which was under the supercategory *Leisure*, becomes a WCS 3.0 supercategory. In WCS 3.0, the *Entertainment* supercategory now includes the list of categories as shown in the **New Categorization Policy in WCS 3.0** column. So if you blocked *Entertainment* in your category policy using WCS 2.0, you are now blocking all sites in that list of categories (supercategory) as well.

Example 2. WCS 2.0 category *Adult Content*, which was under the supercategory *Propriety*, becomes a WCS 3.0 supercategory. In WCS 3.0, the *Adult Material* supercategory now includes the list of categories as shown in the **New Categorization Policy in WCS 3.0** column. So if you blocked *Adult Content* in your category policy using WCS 2.0, you are now blocking all sites in that list of categories (supercategory) as well.

Example 3. The *Spyware* category under the *Security* supercategory is expanded into multiple categories in WCS 3.0: *BOT Phone Home*, *Spyware,* and *Keyloggers.*

WCS 2.0 Supercategory	WCS 2.0 Category	Description	WCS 3.0 Supercategory	WCS 3.0 Categories
Leisure	Entertainment	Sites providing information on theater arts, movies, concerts, tv, radio, and other amusements, or about celebrities of those venues.	Entertainment	*Art and Cultural Events, Dining or Gourmet, Downloads, Entertainer or Celebrity, Games,* etc. See Web Use Categories 3.0 for the complete list under the supercategory *Entertainment*.
Propriety	Adult Content	Sites containing sexually explicit content in an image-based or textual form. Any other form of adult/sexually-oriented material is also listed here.	Adult Material	Adult Magazines or News, Adult Porn, Nudity, Fetish, Dating, etc. See Web Use Categories 3.0 for the complete list under the supercategory *Adult Material*.
Security	Spyware	Sites that are accessed from spam message clicks, which distribute programs to gather user information, or covertly send information to third party sites.	Security	BOT Phone Home, Spyware, Keyloggers

How to revert back to WCS 2.0

Note that if you revert from WCS 3.0 back to WCS 2.0, any new configuration changes you made after switching to WCS 3.0 will be no longer exist after reverting back to WCS 2.0. Any new reporting data that was generated during the time the Barracuda Web Security Gateway was using WCS 3.0 will also no longer be visible.

1. Go to the **ADVANCED > Configuration** page and set **WCS version** to *2*.

2. Verify that your content filtering policies are as they were originally created with WCS version 2.0.