



Barracuda Cloud Control



User's Guide

Version 2.x

Copyright Notice

Copyright © 2004-2012, Barracuda Networks, Inc., 3175 S. Winchester Blvd, Campbell, CA 95008 USA

www.barracuda.com

v2.0.13.x-120208-04-0424sk

All rights reserved. Use of this product and this manual is subject to license. Information in this document is subject to change without notice.

Trademarks

Barracuda Cloud Control is a trademark of Barracuda Networks, Inc. All other brand and product names mentioned in this document are registered trademarks or trademarks of their respective holders.

Chapter 1 – Getting Started	5
Overview	6
Concepts	6
Management Contexts	6
Cloud Control Context.	6
Group Context.	7
Product Context	8
Exceptions.	8
Contacting Technical Support.	8
Chapter 2 – Managing Products and Groups	9
Cloud Control Administration	10
Managing Products	11
Supported Products	11
Connecting and Disconnecting Devices.	11
The Product Tree	11
The Unit Health Pane	11
Product Context	12
Interpreting Device Statistics	13
Groups	13
Synchronizing Settings Across a Group.	13
Settings Not Configurable in the Group Context	13
Dealing With Exceptions	14
Exception Triangle	14
Exception Circle	14
Creating Groups.	15
Use Case Scenarios	15
Scenario: Opening a Support Tunnel on Multiple Devices	15
Scenario: Synchronizing Firmware and Energize Updates	16
Scenario: Using a Mixed Mode Deployment	16
Scenario: Applying Policies Across Multiple Barracuda Web Filters	16
Scenario: Aggregating Reports Across Multiple Products.	17
Scenario: Synchronizing Security Policies Across Products	18
Index	19

Chapter 1

Getting Started

This chapter provides an overview of Barracuda Cloud Control and important concepts, and gets you started connecting devices and understanding the web interface.

<i>Overview</i>	6
<i>Concepts</i>	6
<i>Contacting Technical Support</i>	8

Overview

Barracuda Cloud Control is a comprehensive cloud-based service that enables administrators to monitor and configure multiple Barracuda Networks products from a single console. With Barracuda Cloud Control, you can check the health of all connected devices, run reports that are generated by gathering data from all the devices, and assign roles with varied permissions to different types of users.

The powerful web interface of Barracuda Cloud Control provides for convenient configuration and management of multiple Barracuda Networks device settings, while providing a view of each device web interface for individual configuration or reporting. No need to install software or deploy hardware.

View key statistics by device type at a glance on the [Status](#) page of the web interface, or drill down into the individual web interface for each connected device for more detail.

This guide walks you through initial Barracuda Cloud Control configuration, providing concepts and examples to understand how best to manage Barracuda Networks products through Barracuda Cloud Control according to your organization's deployment needs and security policies.

Concepts

Understanding these concepts enables you to take full advantage of Barracuda Cloud Control features for configuring and synchronizing settings on individual or groups of Barracuda Networks products.

Management Contexts

There are three 'contexts' you use to administer products connected to Barracuda Cloud Control. These contexts include:

- The *Cloud Control* context; for managing Barracuda Cloud Control configuration;
- The *Product* context; for managing an individual Barracuda Networks product using the product web interface;
- The *Group* context; for managing a group of the same type of Barracuda Networks products with one web interface, or for grouping products by company, location, or department.

These contexts are described briefly below. The chapter, *Managing Products and Groups*, beginning on page *page 9*, covers using each context in detail including examples.

Cloud Control Context

When you log into Barracuda Cloud Control, you first see the Cloud Control *context*—on the **CLOUD CONTROL > Status** page—which displays a snapshot of product traffic statistics for the connected Barracuda Networks product(s).

The Cloud Control pane on the left displays either a list of individual products connected to Barracuda Cloud Control, or groups of products which you create. The center pane provides an interface for managing your account and for connecting products, as well as a snapshot of product traffic statistics for all connected products. The Unit Health pane on the right includes a performance overview, connectivity, firmware, and subscription status for each individual product organized by product type.

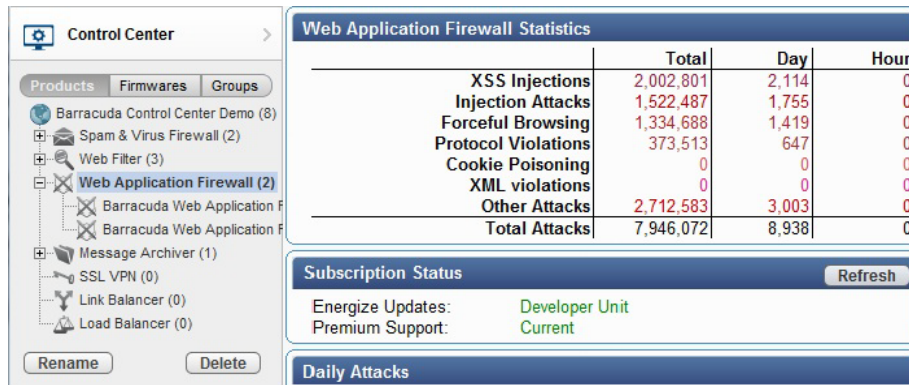
Once you click on an individual product, either in the product tree in the Cloud Control pane or in the Unit Health pane, you leave the ‘Cloud Control context’ and drill-down into the product type web interface. The product web interface displays activity for an individual product if you only have one of that type connected. If you have multiple of one product type connected, the settings and statistics for all products of that type display in one web interface.

Group Context

Grouping Barracuda Networks products enables you to manage settings and apply policies across multiple Barracuda Networks products of the same type from one web interface. You can also use “grouping” to organized your Barracuda Networks products by location, company, department, etc., and you can include products of different types. Grouping happens in one of two ways:

1. **By default, Barracuda Cloud Control groups Barracuda Networks products by product type.** For example, if you have two or more Barracuda Web Application Firewalls connected to Barracuda Cloud Control, they are automatically grouped as such. You can then click on that product type in the Cloud Control pane and see one web interface with aggregated statistics and settings for all of the devices within that group. See *Figure 1.1* below. From the web interface, you can set policies for all of the products in the group at the same time since they are the same product type. This group context also enables reporting on aggregated statistics across a group.

Figure 1.1: Click on a product type to see aggregated statistics for all products of that type



2. You can *create* a grouping of two or more products. When you click on that group in the Cloud Control pane, aggregated statistics display on the **Status** page for each product type in the group.

Additional reasons to manage products in the group context include:

- If you have many devices in one or more locations, managing them with a central console enables you to easily track firmware versions across products and keep them up-to-date.
- Grouping devices by location helps you keep track of where each device is physically located in case it needs service. As long as the unit is joined to Barracuda Cloud Control, you do not need to look up the admin password to configure or update the product.
- Grouping devices of the *same* type enables viewing ‘exceptions’ in which values for the same setting differ across the devices.
- Grouping either devices of the *same* type or of *different* types provides a performance and traffic statistic snapshot on the **CLOUD CONTROL > Status** page for each device in the group. Statistics are aggregated for devices of the same type. For example, if you have several Barracuda Networks products in your London office and several in your New York office, click on that group to quickly view the traffic and performance statistics.

For more details about working with groups, see *Groups*, page 15.

Product Context

If you have only one of any Barracuda Networks product type connected to Barracuda Cloud Control, when you click on that product link in the Cloud Control pane or in the Unit Health pane, the web interface for that individual device displays. From the product web interface, you manage the individual settings just as you would if you logged into the device directly.

Exceptions

When you have more than one of a Barracuda Networks product type connected to Barracuda Cloud Control, and you view the settings of all of them as a group (with one web interface as described above), a yellow **Exception** (⚠) icon displays if the value of the setting is not the same on all devices in the group. When you hover the mouse over the icon, Barracuda Cloud Control clearly indicates what the values for that setting are on each device, so that you can change the settings if desired. See *Dealing With Exceptions*, page 15 for more information and examples.

Contacting Technical Support

To contact Barracuda Networks Technical Support:

- By phone: call 1-408-342-5400, or if you are in the United States, (888) Anti-Spam, or (888) 268-4772
- By email: use support@barracuda.com
- Online: visit <http://www.barracuda.com/support> and click on the **Support Case Creation** link.

There is also a Barracuda Networks Support Forum available where users can post and answer other users' questions. Register and log in at <http://forum.barracuda.com>.

Managing Products and Groups

This chapter illustrates using the Barracuda Cloud Control features to manage your devices in either a group context or individually.

<i>Cloud Control Administration</i>	10
<i>Managing Products</i>	11
<i>Interpreting Device Statistics</i>	13
<i>Groups</i>	13
<i>Use Case Scenarios</i>	15

Cloud Control Administration

When you log into Barracuda Cloud Control, the Barracuda Cloud Control *context* and the **CLOUD CONTROL > Status** page of Barracuda Cloud Control web interface display. In this context you view a summary of all devices connected to your Barracuda Cloud Control. Any Barracuda Networks products you have already connected is listed on the left Products pane. The central portion of the page displays aggregated performance and traffic statistics for all connected devices.

For all devices of the same type, the **CLOUD CONTROL > Status** page shows a graph and corresponding table listing statistics aggregated across all devices over the past 30 days. For example, if you connect multiple Barracuda Web Application Firewalls, the **CLOUD CONTROL > Status** page shows a graph and corresponding table listing detected attacks, totaled by attack type (XSS Injections, Injection Attacks, Cookie Poisoning, etc.), over the past hour, 24 hour period, and grand total since the last system reset. If you connect multiple Barracuda Web Filters, a table and graph display total Spyware downloads, Virus Downloads, Policy (number of threats blocked by your configured policies), etc. aggregated across your connected Barracuda Web Filters.

If you have various different Barracuda Networks products connected to your Barracuda Cloud Control, a separate set of statistics displays for each device on the **CLOUD CONTROL > Status** page. This is useful for having a ‘snapshot’ of activity on all of your Barracuda Networks products on one page.

On the right of the page the Unit Health pane summarizes performance statistics for each system by device type.

From the **CLOUD CONTROL** tab:

- The **Connect Products** page gives instructions for adding Barracuda Networks products to the Barracuda Cloud Control.
- The **My Account** page enables setting Time Zone, Account Notification Email Address, Account Name and Account Preferred Time Zone (the default time zone used to display statistics and report data).
- The **User Management** page lists users including roles, status (Active, Inactive), Administrator actions, and time zone.
- The **Audit Log** page lists login activity.

From the product context or group context, you can always return to the Cloud Control context by clicking the Cloud Control icon in the left pane as shown below.

Figure 2.1: Return to the Cloud Control context by clicking the right arrow.



Managing Products

Supported Products

Currently Barracuda Cloud Control supports the following Barracuda Networks products:

- Barracuda Spam & Virus Firewall
- Barracuda Web Filter
- Barracuda Web Application Firewall
- Barracuda Message Archiver
- Barracuda SSL VPN
- Barracuda Link Balancer
- Barracuda Load Balancer
- All Barracuda Networks VM versions of the above products

Connecting and Disconnecting Devices

If a Barracuda Networks product no longer appears in the product tree, contact your administrator and have them reconnect the product to Barracuda Cloud Control.

The Product Tree

You should see all Barracuda Networks products connected to Barracuda Cloud Control listed in the product tree in the Barracuda Cloud Control pane on the left side of the web interface. In the left pane, your Barracuda Networks products are listed by product type (Barracuda Message Archiver, Barracuda Web Filter, etc.) under **Products**. If you click on **Groups**, your Barracuda Networks products are listed by groups you have defined, or you can create new groups as described below. A group can contain one or more devices that may be of the same or different product type. If you click on **Firmwares**, your Barracuda Networks products display by firmware version.

The Unit Health Pane

Click on the **Cloud Control** link above the product tree in the left pane to return to the Cloud Control *context*, where you can see the Unit Health pane on the right side of the screen. The Unit Health pane indicates, for each of the connected Barracuda Networks products, a general status for performance statistics. **Expand** (☞) icon on the right side of the pane to expand the detailed list of performance statistics for each device. This list varies among product types.

Figure 2.2: General status for each connected device



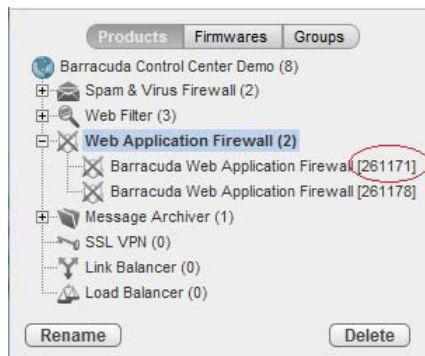
Legend for the Unit Health pane is as follows:

- Connectivity: Green indicates device is connected, red indicates device is not connected
- Firmware:
 - Green indicates current release
 - Yellow indicates that a new minor release is available for download
 - Red indicates that a new major release is available for download
- Health: General indicator of device performance statistics
- Storage: Green indicates that there are no storage issues.
- Subscription: Green indicates that Energize Updates, Instant Replacement (where applicable), and Premium Support (where applicable) are current for the device, and red indicates that one or more of these subscription items is either expired or not yet activated

Product Context

When you click on a particular device in the product tree or the Unit Health pane, Barracuda Cloud Control displays the unique statistics and settings for that device with the same web interface you would see if you logged directly into the web interface of that device outside of Barracuda Cloud Control. For example, to view the individual web interface of Barracuda Web Application Firewall serial# 261171, click on that device in the product tree:

Figure 2.3: Click on the individual device to see that device's web interface.



The product web interface displays settings for that device ONLY. For the selected product, you can view and change all settings available from within Barracuda Cloud Control; note that some settings are *not* available from within Barracuda Cloud Control and must be configured from logging into the device directly from your browser. Pages or settings not available from within the Barracuda Cloud Control are grayed out.

Interpreting Device Statistics

The **CLOUD CONTROL > Status** page provides an overview of the performance and health of all of the Barracuda Networks devices connected to Barracuda Cloud Control. In this view, the same traffic and performance statistics available in the **BASIC > Status** page for your other Barracuda Networks products display. Where there are multiple products of the same type, the statistics are aggregated in one section of the page. To view the traffic and performance statistics of a single device, click on the device name in the product tree or in the Unit Health pane. For details on interpreting the statistics, see the Administrator's Guide for that product at <http://www.barracuda.com/documentation>

Groups

Synchronizing Settings Across a Group

Applying policies across a group of same-type Barracuda products is perhaps the most powerful feature of the group context. For example, if you have several Barracuda Web Application Firewalls grouped and you want to enable *Encrypted Cookie Security Mode* on all of the devices, you would do the following:

1. Click on the group link for those products in the product tree.
2. Navigate to the **BASIC > Default Security** page and click on *Encrypted* for **Cookie Security Mode**, the **Save Changes**. This setting synchronizes across all devices.
3. To change the value of a setting on just one of the devices, from the product tree, click on the device itself within the group. You'll see the individual product web interface, where you can navigate to the appropriate page and change the setting as needed. Doing so causes a yellow **Exception** (⚠) icon to appear in the Group context web interface as described below.

Settings Not Configurable in the Group Context

Some features must be configured on each individual device within a group. Examples include IP Address, Quarantine settings on the Spam & Virus Firewall, Services on the Barracuda Web Application Firewall, and Default Host Name on various product types. Note that some tabs or pages of the web interface (in the group context) for a product may be grayed out (unavailable) for this reason, or because the features on that tab or page are not supported in the group context.

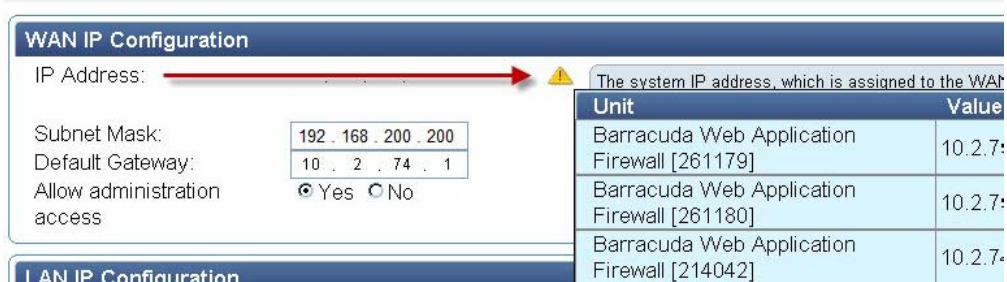
Dealing With Exceptions

Exception Triangle

When using the group context to view the settings on all devices of one type, if you see the yellow **Exception** (⚠) icon next to the setting, this means that for a particular setting, the *values* of that setting differ across the devices in the group. You can hover the mouse over the setting to see a text box or table displaying the actual value of the setting on each device.

As shown in *Figure 2.4*, if you hover the mouse over the icon, Barracuda Cloud Control displays the value of that setting for each product in the group. In this example, each Barracuda Web Application Firewall in the group has a different value for the **IP Address**, each of which displays in a pop-up table when you hover the mouse over the icon.

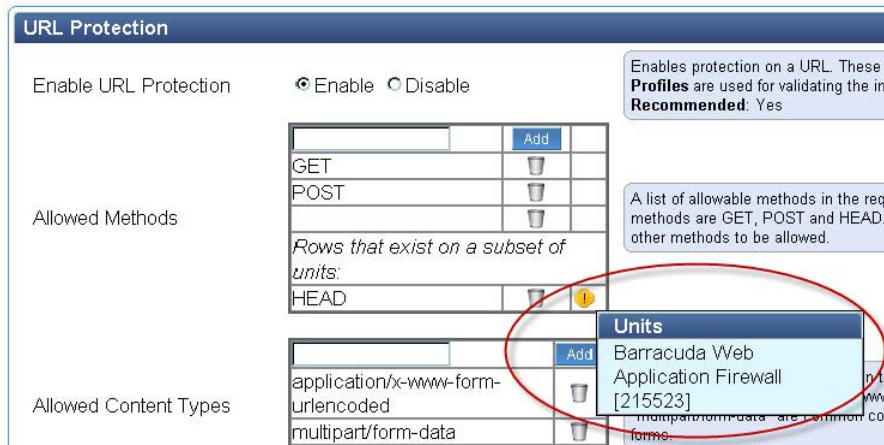
Figure 2.4: Exception triangle indicates different values for settings on products of same type



Exception Circle

A round yellow **Exception** (⚠) icon next to a setting indicates that the setting is unique to that device and is not shared or aggregated. For example, suppose you have multiple Barracuda Web Application Firewalls and you have configured the GET and POST **Allowed Methods** for each device on the **Security Policies > URL Protection** page. Additionally, you have configured the HEAD **Allowed Method** for only one of the devices, so the icon displays next to the HEAD **Allowed Method** indicating that *this* value is additional and unique to a particular device. Hover the mouse over the icon and a pop-up text box displays the device serial number as shown in *Figure 2.5*.

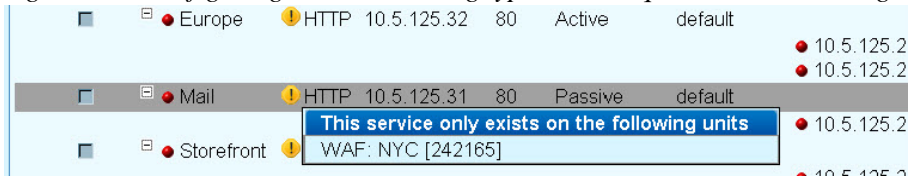
Figure 2.5: Exception circle indicates a setting unique to one device in a group



In another example, if you have multiple Barracuda Web Application Firewalls in a group, you might configure an **HTTP Service** from the **BASIC > Services** page on all devices, but give each Service a unique name. The exception circle, as shown below in *Figure 2.6*, indicates that the Service is unique

to the device by **Name**, even though it is the same actual Service type (**HTTP**) as the Services on the other devices. If an **HTTP** service with the same **Name** was configured on each of the devices, you would see one entry for the Service and no exception circle.

Figure 2.6: Configuring the same setting type with unique names across a group



Creating Groups

If you want to create a group of a ‘mix’ of different types of Barracuda products:

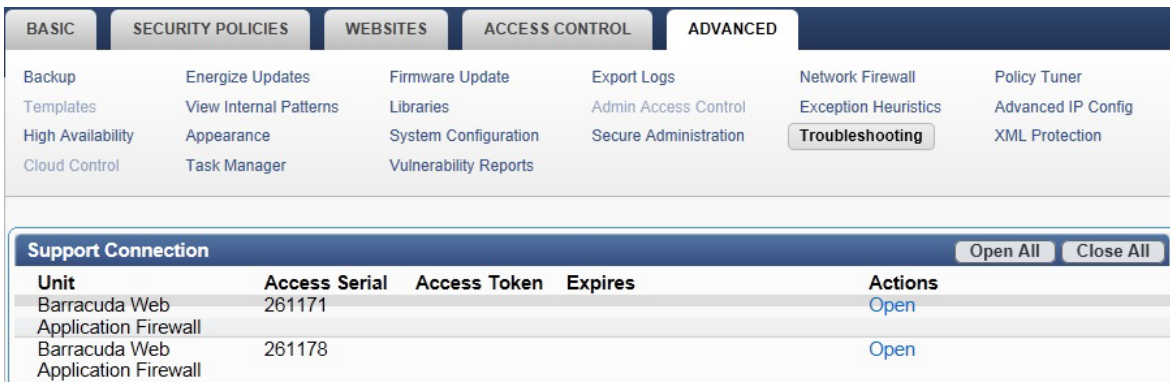
1. From the Cloud Control left pane, click **Groups**, click **Add**, and enter a name for the group of devices. For example, if you want to group all of the Barracuda Web Filters by location, for your Paris office you might call your group *ParisWF*. If you want to group multiple types of Barracuda Networks products that serve the Marketing department, you could name the group *MarketingVarious*, indicating that there is more than one type of product in the group.
2. Next, click on each device you want to add and drag it to the group name. The screen refreshes and that device is added to the group. You can use the **Rename** and **Delete** buttons at the bottom of the pane to manage groups. Note that deleting a group does NOT disconnect the devices in the group from Barracuda Cloud Control, it just removes the grouping.

Use Case Scenarios

Scenario: Opening a Support Tunnel on Multiple Devices

With Barracuda Cloud Control, you can troubleshoot problem devices in a remote location by opening a support tunnel on one or more of your Barracuda Networks products at the same time. Barracuda Networks Technical Support can then assist you with any of the devices connected to Barracuda Cloud Control. Using the Barracuda Web Application Firewall as an example, you click on the Message Archiver group, and click **ADVANCED > Troubleshooting**.

Figure 2.7: Barracuda Message Archiver: Opening a Support Tunnel



Each Barracuda Web Application Firewall is listed by serial number. If the **Actions** column shows *Open*, there is not a support tunnel currently open to the device. Click *Open* to open a support tunnel. You can then click *Close* at any time to close the support tunnel.

Scenario: Synchronizing Firmware and Energize Updates

Barracuda Cloud Control provides a fast and convenient method of keeping track of firmware versions running on all of your Barracuda Networks products. Click the **Firmwares** button in the Cloud Control left pane, and expand the product tree. The firmware version displays as a folder. Expand the firmware version folder to view all devices currently on that firmware version.

To change the firmware version of a device, click on the device name, and click on the **ADVANCED > Energize Updates** page. Click the **Update** button to update the device to latest firmware release, or **Revert** to downgrade to the previous version.

Scenario: Using a Mixed Mode Deployment

You must use Barracuda Cloud Control to view and manage mixed mode deployments such as the Cloud Protection Layer component of the Barracuda Spam & Virus Firewall. Click the plus symbol (+) next to the Barracuda Spam & Virus Firewall in the product tree, then click on the **Cloud Protection Layer** link to access the web interface. A subset of the pages and features offered by the Barracuda Spam & Virus Firewall that **ONLY** apply to the Cloud Protection Layer displays.

Unlike the Barracuda Spam & Virus Firewall, the Cloud Protection Layer captures the message body for email messages blocked due to Rate Control, Barracuda Reputation, and other IP analysis filtering.

Note that the aggregated statistics do **NOT** combine data from the Cloud Protection Layer and the Barracuda Spam & Virus Firewall, as the two products perform different filtering functions. Barracuda Cloud Control shows separate traffic statistics for each component on the Cloud Control context page.

Settings you see in the Cloud Protection Layer web interface are unique for that component and are not shared across other devices or services.

Scenario: Applying Policies Across Multiple Barracuda Web Filters

As an administrator of Barracuda Web Filters for a university, you may have two groups of devices; one group for faculty and staff and another group for students. You want to *allow* Skype and Yahoo IM internally for faculty and staff, but not for students.

To configure: Click on the Barracuda Web Filter group assigned to faculty and staff. From the web interface, you would set *Allow* for those applications on the **BLOCK/ACCEPT > Applications** page.

For the Barracuda Web Filters filtering student traffic, you want to block those applications, but allow Gogetalk. Click on the Barracuda Web Filter group assigned to faculty and staff. From the **BLOCK/ACCEPT > Applications** page you can configure these settings for the student group.

Additionally, your IT department may want to push Microsoft updates to the students' PCs, so, in the **Updates** section of the **BLOCK/ACCEPT > Applications** page, you might set **Microsoft Updates** to *Block*. However, the faculty and staff have admin rights to their PCs - you'd set this value to *Allow* on that group.

Scenario: Aggregating Reports Across Multiple Products

Suppose you have connected three Barracuda Web Filters to Barracuda Cloud Control and you want to run a report aggregating a list of users by bandwidth across all three devices. You assume all three devices are up and running. Run the report by clicking on the group of Barracuda Web Filters from the Cloud Control pane. Select the **Users by Bandwidth** report from the **BASIC > Reports** page.

As shown in *Figure 2.8* below, for the Barracuda Web Filters listed at the top of the report, an aggregated list of users shows in the table below the graph, sorted by the user with the most bandwidth used for the report time frame shown at the top. For more details about reports, see the Barracuda Web Filter online help on the **BASIC > Reports** page.

Problem: In the report below, you can see by the highlighted devices that two of the Barracuda Web Filters have data included in the report, but one of the three devices, SN 121153, was unreachable by Barracuda Cloud Control. This is an alert that there might be a power outage or network issue where that device is located.

Solution: Try logging into the web interface directly for the Barracuda Web Filter SN 121153. If you can, then you can use the troubleshooting features on the **ADVANCED > Troubleshooting** page for that device. Or you can open a support tunnel from the same page and call Barracuda Technical Support if necessary. If you cannot log in directly from the web interface, you might need to check on the physical device.

Figure 2.8: Data aggregated across multiple Barracuda Web Filters

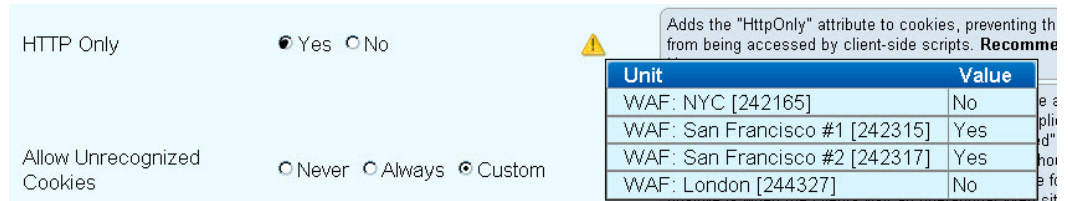


Scenario: Synchronizing Security Policies Across Products

You have four Barracuda Web Application Firewalls serving three locations: New York, San Francisco, and London. Your master Security Policies database dictates that all devices should have the **Http Only** attribute set to *Yes* for cookies, preventing the cookie from being accessed by client-side scripts.

To Configure: Click on the group of Barracuda Web Application Firewalls from the Cloud Control pane and check the **SECURITY POLICIES > Cookie Security** page. An exception triangle for this setting may display, as shown below, if the devices are not in sync for this setting. Hover the mouse over the setting to view the values for **Http Only** on each device in the pop-up table:

Figure 2.9: Exception shows different values for a setting across a group of devices



The screenshot shows the 'HTTP Only' setting with radio buttons for 'Yes' (selected) and 'No'. A yellow warning triangle is present next to the setting. A tooltip table shows the following data:

Unit	Value
WAF: NYC [242165]	No
WAF: San Francisco #1 [242315]	Yes
WAF: San Francisco #2 [242317]	Yes
WAF: London [244327]	No

Resolving an Exception: To resolve the issue, you'll click on the NYC and London Web Application Firewalls, successively, in the product tree, and change the settings to match those of the two San Francisco systems. Once you save those settings, the exception triangle will no longer appear next to the setting when viewed in the Group context.

Index

A

- Actions
 - Open All/Close All 16
- Activation 12
- Administering Barracuda Cloud Control 10
- Aggregated reports 7, 17
- Aggregated statistics 7
- Allowed Method 14
- Audit Log 10

B

- Barracuda Cloud Control
 - Administering 10
 - Concepts 6
 - Features 6, 7, 13
 - Overview 5
- Barracuda Networks products
 - Grouping 7, 8, 11, 15
 - Supported devices 11

C

- Centralizing product management 7
- Cloud Control
 - Administration 10
 - Connecting devices 10
 - Context 6, 10, 11
 - Pane 6, 7, 8, 11, 17, 18
 - Status 6, 7, 10, 13
- Cloud Protection Layer 16
- Configure multiple products 6
- Connecting devices 10
- Connectivity 12

D

- Data aggregation example 17
- Deleting groups 15
- Deployment, mixed mode 16
- Device
 - Connecting 10
- Device management, centralizing 7
- Device statistics 13
- Device status 6, 7, 13, 17
- Devices, opening a support tunnel 15
- Disconnecting devices 11

E

- Energize Updates 12, 16
- Examples 15, 16, 17
- Exceptions 7, 8, 13, 14, 18
 - Resolving 18
- Expand performance statistics by device 11
- Expand product types 7, 11, 16

F

- Features of Barracuda Cloud Control 6, 7, 13
- Firmware 12
 - Synchronizing updates on same products 16
 - Version 6, 7, 11, 16

G

- Green indicator 12
- Group context 6, 7
- Grouping products 6, 7, 8, 11, 13, 14, 15
- Groups
 - Creating 13, 15
 - Rename or delete 15
 - Settings not configurable across a group 13
 - Synchronizing settings 13

H

- HEAD 14
- Health 6, 7, 8, 11, 12, 13
- Host Name, default 13
- HTTP Service 14

I

- Indicators, Unit Health legend 12
- Instant Replacement 12
- IP Address 13, 14

M

- Management contexts 6
- Mixed mode deployment 16
- My Account 10

P

- Premium Support 12
- Product context 6, 8
- Product tree 11
- Product types 8
 - Aggregating reports across multiple 17
 - Grouping multiple product types 15
- Products, grouping 11, 15
 - Exceptions 14
- Products, managing 11
- Products, supported devices 11

R

- Red indicator 12
- Renaming a group 15
- Reports 17
 - Aggregated 7
 - Aggregating across multiple products 17
 - Statistics 6, 7, 12, 13
 - Unit Health 6, 7, 11, 12, 13

S

- Scenarios 15, 16, 17
- Security Policies 14
- Security policies 18
- Services 14
- Settings
 - Groups 13
 - Updating device settings 13
- Statistics 7, 12, 13
 - Aggregated 7
 - Traffic 6
- Statistics, interpreting 13
- Status 13, 17
 - Product traffic 6, 7, 13
- Storage 12
- Subscription 12
- Support Case Creation 8
- Support Tunnel, opening on multiple devices 15
- Support, contacting 8
- Supported Barracuda Networks products 11
- Supported products 11
- Synchronizing Security Policies across products 18

T

- Technical support, contacting 8
- Traffic statistics 6
- Troubleshooting 17
 - Device is disconnected 11
 - Exception circle displays 14
 - Exception triangle displays 13, 14
 - How do I delete a group? 15
 - How do I determine the firmware version? 16
 - Opening a support tunnel 15
 - Remote devices 15
 - Settings are grayed out 13
 - Synchronizing security policies across products 18
 - Unit Health legend 12

U

- Unit Health 7, 8, 11, 12, 13
- Unreachable devices 17
- URL Protection 14
- Use Case Scenarios 15
- Use case scenarios 15, 16, 17
- User Management 10
- Using the Cloud Protection Layer 16

W

- Web interface 6, 7, 11, 12, 13, 16, 17

Y

- Yellow indicator 12

