



## CacheFlow Appliance Release Notes

Software Version:	3.3.x	
Current Release:	3.3.2.1	30 January 2014
Document Revision:	3.5	30 January 2014

### Important Notes

**Before using the software, it is recommended that you read:**

- ▣ CacheFlow Appliance Release Notes
- ▣ The “CacheFlow Appliance 500 Series Quick Start Guide” or the “CacheFlow Appliance 5000 Series Quick Start Guide”

### Product Documentation

Access the product documentation and product MIBs on BlueTouch Online:

<https://bto.bluecoat.com/cacheflow>

### Support

Frequently asked questions and more information about this release can be found in the Knowledge Base: <https://kb.bluecoat.com>

Direct support questions regarding this release to: <https://bto.bluecoat.com>

### Supported Platforms

**IMPORTANT:** This software is only supported on CF500-KX and CF5000-MX appliances.

## Supported Upgrade Path

The CacheFlow appliance must be running at least CacheFlow 2.2.1.1 or greater before upgrading to CacheFlow 3.x.

The 2.x to 3.x software upgrade must be performed in conjunction with the CF5000-CX to CF5000-MX upgrade. Contact Blue Coat to purchase the CF5000-CX to CF5000-MX hardware upgrade kit.

The hardware and software upgrade must follow the exact steps specified in the “Hardware Maintenance & Upgrade Guide”. Failure to follow the exact steps may result in an unstable and unusable system.

## GUI Requirements

The GUI is available through a browser. The following browsers are supported: IE7 or greater and Firefox 3.5 or greater.

To run the GUI you must have the following enabled in your browser:

- ▣ JavaScript
- ▣ Cookies

We recommend that you use a minimum resolution of 1280 x 800 on your display for the optimal GUI experience.

## Licensing Requirements

There is no license required for the base CacheFlow Appliance running with the CachePulse™ service.

Blue Coat WebFilter™ is available for a free trial by simply enabling it on box.

## Release Note Directory

These release notes present information for each 3.3.x release. Each section provides feature descriptions, fixes and known issues.

- ▣ [Version 3.3.2.1, Build 132442 on page 4](#)
- ▣ [Version 3.3.1.2, Build 111363 on page 6](#)
- ▣ [Version 3.3.1.1, Build 109212 on page 7](#)

## Version 3.3.2.1, build 132442

*Release Date: 30 January 2014*

*Supported Platforms: CF500-KX, CF5000-MX*

### Version 3.3.2.1 Contents

- ▣ New Features in 3.3.2.1
- ▣ Changes in 3.3.2.1
- ▣ Fixes in 3.3.2.1
- ▣ Known Issues in 3.3.2.1

### New Features in 3.3.2.1

CacheFlow 3.3.2.1 introduces support for the CF5000-MX platform with the CacheFlow 3.3.x codebase.

### Changes in 3.3.2.1

Toshiba 2TB disks (MG03SCA200) and Seagate 2TB disks (ST2000NM0023) are now supported for the CF500-KX platform (B#189202).

SmartFilter content filtering now includes support for URLs categorized with up to 45 user-defined categories. Previously, URLs mapping onto a user-defined category would be categorized as None (B#189756).

### Fixes in 3.3.2.1

Fixed error code 0x4003A restart that occurred under certain traffic patterns (B#185313, SR 2-547340084, SR 2-568065862).

Setting the MTU on an LACP aggregate interface persisted the configuration change, but had no effect on the actual MTU used by the underlying interfaces. Changing the MTU on an aggregate interface is now fully supported (B#186089, SR 2-554572521).

Resolved issues with `test http get` command returning errors for some websites (B#188210, SR 2-577488592).

Creating a PCAP filter for an IPv6 address will no longer fail with an error indicating 'resolved to multiple addresses' (B#189869, SR 2-595822971).

Certain commands which are common to all content filter services were incorrectly disabled for the SmartFilter and local database services. The common commands are now available to all providers (B#189464, SR 2-591805964).

A CacheGroup manager now supports using a control-key sequence to terminate an inline command. Using the sequence previously resulted in an error-causing update that required a full-configuration reset on the member. (B#189052, SR 2-585116581).

A warning message will no longer appear as a result of configuring multiple "Grant Administrator Rights" rules in the GUI (B#185158, SR 2-545155332).

The SNMP sysName OID will now return the current appliance name. Previously, appliance name changes were only visible to SNMP after a system restart (B#191016, SR 2-610555762, SR 2-785517502).

Fixed restart issue caused by high packet rates (B#193796, SR 2-682621745).

Fixed a resource leak caused by an upstream server alternating between providing cacheable and non-cacheable responses to the same URL at different times (B#194866, SR 2-678435871).

For the CF500-KX model, removed the unused "Warning Threshold - Low" for Disk Count health, as a disk count of less than four is always immediately Critical (B#182673).

Fixed a compact flash file system error that may have resulted in a "no bootable image" error after an upgrade. This fix required updating the starter to version 2.5.114862 and will require an additional restart of the system during upgrade (B#189337).

### Known Issues in 3.3.2.1

Changing the MTU of an aggregate interface which is processing traffic may result in an uncontrolled restart. Stopping traffic on the component interfaces is recommended (B#195025).

If the MTU size on an aggregate link has been changed to something other than the default of 1500, the `show interface` command incorrectly shows the MTU size for its constituent interfaces as 1500. This is a display problem only and the constituents are in fact running the same MTU size as the aggregate (B#195026).

While proxying traffic under moderate resource load, the appliance may bypass/drop some traffic due to overload (according to the configured overload handling option, and corresponding entries appear in the event log indicating the number of bypassed/dropped connections). Running additional disk-intensive activities such as writing access logs or performing content-filter updates seems to exacerbate this behaviour. If the amount of bypassed/dropped traffic becomes unacceptable, it is recommended to either disable access logging, restrict content filter update times, reduce the traffic load to the appliance, or some combination of these actions (B#182986).

Connecting the CacheFlow to a 100Mbit switch in half-duplex mode is not supported (B#144719).

Some browsers, including Firefox version 10.0.2, may report an error when attempting to install complex policy with a large number of rules. If you encounter this issue, try an alternative browser (B#174478).

## Version 3.3.1.2, build 111363

*Release Date: 30 April 2013*

*Supported Platform: CF500-KX*

### Version 3.3.1.2 Contents

- ▣ Changes in 3.3.1.2
- ▣ Fixes in 3.3.1.2
- ▣ Known Issues in 3.3.1.2

### Changes in 3.3.1.2

Having the caching subsystem performance incorporated into the system resource load resulted in high resource load values which did not usefully reflect the state of the system. The caching subsystem load has been given its own metric. A sustained system cache load above 100% indicates that bandwidth savings may be compromised. Please refer to the Capacity Monitoring section of the CacheFlow Online Documentation for more information (B#186321).

The `show capacity resource-load` command has been deprecated and replaced with `show capacity load` which also includes the new Cache Load statistic (B#187568).

### Fixes in 3.3.1.2

Having an access log on the appliance which has a name consisting of a single character no longer prevents the policy UI create rule wizard from launching (B#187937).

### Known Issues in 3.3.1.2

While proxying traffic under moderate resource load, the appliance may bypass/drop some traffic due to overload (according to the configured overload handling option, and corresponding entries appear in the event log indicating the number of bypassed/dropped connections). Running additional disk-intensive activities such as writing access logs or performing content-filter updates seems to exacerbate this behaviour. If the amount of bypassed/dropped traffic becomes unacceptable, it is recommended to either disable access logging, restrict content filter update times, reduce the traffic load to the appliance, or some combination of these actions (B#182986).

Connecting the CacheFlow to a 100Mbit switch in half-duplex mode is not supported (B#144719).

Some browsers, including Firefox version 10.0.2, may report an error when attempting to install complex policy with a large number of rules. If you encounter this issue, try an alternative browser (B#174478).

## Version 3.3.1.1, build 109212

*Release Date: 15 March 2013*

*Supported Platform: CF500-KX*

### Version 3.3.1.1 Contents

- ▣ New Features in 3.3.1.1
- ▣ Known Issues in 3.3.1.1

### New Features in 3.3.1.1

CacheFlow 3.3.1.1 introduces support for the CF500-KX platform.

### Known Issues in 3.3.1.1

The inclusion of disk load in the resource load metric has resulted in resource load spikes (B#186321).

While proxying traffic under moderate resource load, the appliance may bypass/drop some traffic due to overload (according to the configured overload handling option, and corresponding entries appear in the event log indicating the number of bypassed/dropped connections). Running additional disk-intensive activities such as writing access logs or performing content-filter updates seems to exacerbate this behaviour. If the amount of bypassed/dropped traffic becomes unacceptable, it is recommended to either disable access logging, restrict content filter update times, reduce the traffic load to the appliance, or some combination of these actions (B#182986).

Connecting the CacheFlow to a 100Mbit switch in half-duplex mode is not supported (B#144719).

Some browsers, including Firefox version 10.0.2, may report an error when attempting to install complex policy with a large number of rules. If you encounter this issue, try an alternative browser (B#174478).

Copyright© 1999-2014 Blue Coat Systems, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of Blue Coat Systems, Inc. All right, title and interest in and to the Software and documentation are and shall remain the exclusive property of Blue Coat Systems, Inc. and its licensors. ProxyAV™, CacheOS™, SGOS™, SG™, Spyware Interceptor™, Scope™, ProxyRA Connector™, ProxyRA Manager™, Remote Access™ and MACH5™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, ProxySG®, WinProxy®, PacketShaper®, PacketShaper Xpress®, PolicyCenter®, PacketWise®, AccessNow®, Ositis®, Powering Internet Management®, The Ultimate Internet Sharing Solution®, Cerberian®, Permeo®, Permeo Technologies, Inc.®, and the Cerberian and Permeo logos are registered trademarks of Blue Coat Systems, Inc. All other trademarks contained in this document and in the Software are the property of their respective owners.

BLUE COAT SYSTEMS, INC. AND BLUE COAT SYSTEMS INTERNATIONAL SARL (COLLECTIVELY “BLUE COAT”) DISCLAIM ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NON-INFRINGEMENT. IN NO EVENT SHALL BLUE COAT, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF BLUE COAT SYSTEMS, INC. HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Americas:

**Blue Coat Systems, Inc.**  
420 N. Mary Ave.  
Sunnyvale, CA 94085

Rest of the World:

**Blue Coat Systems International SARL**  
3a Route des Arsenaux  
1700 Fribourg, Switzerland