

Blue Coat® Systems

ProxySG™

Configuration and Management Guide



Contact Information

Blue Coat Systems Inc.
420 North Mary Ave
Sunnyvale, CA 94085-4121

<http://www.bluecoat.com/support/index.html>

bcs.info@bluecoat.com

support@bluecoat.com

<http://www.bluecoat.com>

For concerns or feedback about the documentation: documentation@bluecoat.com

Copyright© 1999-2006 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. ProxySG™, ProxyAV™, CacheOS™, SGOS™, Spyware Interceptor™, Scope™ are trademarks of Blue Coat Systems, Inc. and CacheFlow®, Blue Coat®, Accelerating The Internet®, WinProxy®, AccessNow®, Ositis®, Powering Internet Management®, and The Ultimate Internet Sharing Solution® 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. DISCLAIMS 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 NONINFRINGEMENT. IN NO EVENT SHALL BLUE COAT SYSTEMS, INC., 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.

Document Number: 231-02679

Document Revision: 3.2.7—02/01/2006

Third Party Copyright Notices

Blue Coat Systems, Inc. utilizes third party software from various sources. Portions of this software are copyrighted by their respective owners as indicated in the copyright notices below.

The following lists the copyright notices for:

BPF

Copyright (c) 1988, 1989, 1990, 1991, 1992, 1993, 1994, 1995, 1996

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that: (1) source code distributions retain the above copyright notice and this paragraph in its entirety, (2) distributions including binary code include the above copyright notice and this paragraph in its entirety in the documentation or other materials provided with the distribution, and (3) all advertising materials mentioning features or use of this software display the following acknowledgement:

This product includes software developed by the University of California, Lawrence Berkeley Laboratory and its contributors.

Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission. THIS SOFTWARE IS PROVIDED ``AS IS'' AND WITHOUT ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, WITHOUT LIMITATION, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE.

DES

Software DES functions written 12 Dec 1986 by Phil Karn, KA9Q; large sections adapted from the 1977 public-domain program by Jim Gillogly.

EXPAT

Copyright (c) 1998, 1999, 2000 Thai Open Source Software Center Ltd.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Finjan Software

Copyright (c) 2003 Finjan Software, Inc. All rights reserved.

Flowerfire

Copyright (c) 1996-2002 Greg Ferrar

ISODE

ISODE 8.0 NOTICE

Acquisition, use, and distribution of this module and related materials are subject to the restrictions of a license agreement. Consult the Preface in the User's Manual for the full terms of this agreement.

4BSD/ISODE SMP NOTICE

Acquisition, use, and distribution of this module and related materials are subject to the restrictions given in the file SMP-READ-ME.

UNIX is a registered trademark in the US and other countries, licensed exclusively through X/Open Company Ltd.

MD5

RSA Data Security, Inc. MD5 Message-Digest Algorithm

Copyright (c) 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.

License to copy and use this software is granted provided that it is identified as the "RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing this software or this function.

License is also granted to make and use derivative works provided that such works are identified as "derived from the RSA Data Security, Inc. MD5 Message-Digest Algorithm" in all material mentioning or referencing the derived work.

RSA Data Security, Inc. makes no representations concerning either the merchantability of this software or the suitability of this software for any particular purpose. It is provided "as is" without express or implied warranty of any kind.

THE BEER-WARE LICENSE" (Revision 42):

<phk@FreeBSD.org<<mailto:phk@FreeBSD.org>>> wrote this file. As long as you retain this notice you can do whatever you want with this stuff. If we meet some day, and you think this stuff is worth it, you can buy me a beer in return. Poul-Henning Kamp

Microsoft Windows Media Streaming

Copyright (c) 2003 Microsoft Corporation. All rights reserved.

OpenLDAP

Copyright (c) 1999-2001 The OpenLDAP Foundation, Redwood City, California, USA. All Rights Reserved. Permission to copy and distribute verbatim copies of this document is granted.

<http://www.openldap.org/software/release/license.html>

The OpenLDAP Public License Version 2.7, 7 September 2001

Redistribution and use of this software and associated documentation ("Software"), with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain copyright statements and notices,
2. Redistributions in binary form must reproduce applicable copyright statements and notices, this list of conditions, and the following disclaimer in the documentation and/or other materials provided with the distribution, and
3. Redistributions must contain a verbatim copy of this document.

The OpenLDAP Foundation may revise this license from time to time. Each revision is distinguished by a version number. You may use this Software under terms of this license revision or under the terms of any subsequent revision of the license.

THIS SOFTWARE IS PROVIDED BY THE OPENLDAP FOUNDATION AND ITS CONTRIBUTORS ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OPENLDAP FOUNDATION, ITS CONTRIBUTORS, OR THE AUTHOR(S) OR OWNER(S) OF THE SOFTWARE BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The names of the authors and copyright holders must not be used in advertising or otherwise to promote the sale, use or other dealing in this Software without specific, written prior permission. Title to copyright in this Software shall at all times remain with copyright holders.

OpenLDAP is a registered trademark of the OpenLDAP Foundation.

OpenSSH

Copyright (c) 1995 Tatu Ylonen <yo@cs.hut.fi>, Espoo, Finland. All rights reserved

This file is part of the OpenSSH software.

The licences which components of this software fall under are as follows. First, we will summarize and say that all components are under a BSD licence, or a licence more free than that.

OpenSSH contains no GPL code.

- 1) As far as I am concerned, the code I have written for this software can be used freely for any purpose. Any derived versions of this software must be clearly marked as such, and if the derived work is incompatible with the protocol description in the RFC file, it must be called by a name other than "ssh" or "Secure Shell".

[Tatu continues]

However, I am not implying to give any licenses to any patents or copyrights held by third parties, and the software includes parts that are not under my direct control. As far as I know, all included source code is used in accordance with the relevant license agreements and can be used freely for any purpose (the GNU license being the most restrictive); see below for details.

[However, none of that term is relevant at this point in time. All of these restrictively licenced software components which he talks about have been removed from OpenSSH, i.e.,

- RSA is no longer included, found in the OpenSSL library
- IDEA is no longer included, its use is deprecated
- DES is now external, in the OpenSSL library
- GMP is no longer used, and instead we call BN code from OpenSSL
- Zlib is now external, in a library
- The make-ssh-known-hosts script is no longer included
- TSS has been removed
- MD5 is now external, in the OpenSSL library
- RC4 support has been replaced with ARC4 support from OpenSSL
- Blowfish is now external, in the OpenSSL library

[The licence continues]

Note that any information and cryptographic algorithms used in this software are publicly available on the Internet and at any major bookstore, scientific library, and patent office worldwide. More information can be found e.g. at "<http://www.cs.hut.fi/crypto>".

The legal status of this program is some combination of all these permissions and restrictions. Use only at your own responsibility. You will be responsible for any legal consequences yourself; I am not making any claims whether possessing or using this is legal or not in your country, and I am not taking any responsibility on your behalf.

NO WARRANTY

BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

2) The 32-bit CRC compensation attack detector in deattack.c was contributed by CORE SDI S.A. under a BSD-style license.

Cryptographic attack detector for ssh - source code

Copyright (c) 1998 CORE SDI S.A., Buenos Aires, Argentina. All rights reserved. Redistribution and use in source and binary forms, with or without modification, are permitted provided that this copyright notice is retained. THIS SOFTWARE IS PROVIDED ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES ARE DISCLAIMED. IN NO EVENT SHALL CORE SDI S.A. BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES RESULTING FROM THE USE OR MISUSE OF THIS SOFTWARE.

Ariel Futoransky <futo@core-sdi.com> <<http://www.core-sdi.com>>

3) ssh-keygen was contributed by David Mazieres under a BSD-style license.

Copyright 1995, 1996 by David Mazieres <dm@lcs.mit.edu>. Modification and redistribution in source and binary forms is permitted provided that due credit is given to the author and the OpenBSD project by leaving this copyright notice intact.

4) The Rijndael implementation by Vincent Rijmen, Antoon Bosselaers and Paulo Barreto is in the public domain and distributed with the following license:

@version 3.0 (December 2000)

Optimised ANSI C code for the Rijndael cipher (now AES)

@author Vincent Rijmen <vincent.rijmen@esat.kuleuven.ac.be>

@author Antoon Bosselaers <antoon.bosselaers@esat.kuleuven.ac.be>

@author Paulo Barreto <paulo.barreto@terra.com.br>

This code is hereby placed in the public domain.

THIS SOFTWARE IS PROVIDED BY THE AUTHORS "AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHORS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

5) One component of the ssh source code is under a 3-clause BSD license, held by the University of California, since we pulled these parts from original Berkeley code.

Copyright (c) 1983, 1990, 1992, 1993, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

6) Remaining components of the software are provided under a standard 2-term BSD licence with the following names as copyright holders:

Markus Friedl

Theo de Raadt

Niels Provos

Dug Song

Aaron Campbell

Damien Miller

Kevin Steves

Daniel Kouril

Wesley Griffin

Per Allansson

Nils Nordman

Simon Wilkinson

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

THIS SOFTWARE IS PROVIDED BY THE AUTHOR ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

OpenSSL

Copyright (c) 1995-1998 Eric Young (eay@cryptsoft.com). All rights reserved.

<http://www.openssl.org/about/>

<http://www.openssl.org/about/>

OpenSSL is based on the excellent SSLeay library developed by [Eric A. Young <mailto:eay@cryptsoft.com>](mailto:eay@cryptsoft.com) and [Tim J. Hudson <mailto:tjh@cryptsoft.com>](mailto:tjh@cryptsoft.com).

The OpenSSL toolkit is licensed under a Apache-style license which basically means that you are free to get and use it for commercial and non-commercial purposes.

This package is an SSL implementation written by Eric Young (eay@cryptsoft.com). The implementation was written so as to conform with Netscapes SSL.

This library is free for commercial and non-commercial use as long as the following conditions are adhered to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed. If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used. This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement: "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)" The word 'cryptographic' can be left out if the routines from the library being used are not cryptographic related :-).
4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement: "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

The license and distribution terms for any publicly available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

Copyright (c) 1998-2002 The OpenSSL Project. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgment:
"This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (<http://www.openssl.org/>)"
4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.
5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.
6. Redistributions of any form whatsoever must retain the following acknowledgment: "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (<http://www.openssl.org/>)"

THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

PCRE

Copyright (c) 1997-2001 University of Cambridge

University of Cambridge Computing Service, Cambridge, England. Phone: +44 1223 334714.

Written by: Philip Hazel <ph10@cam.ac.uk>

Permission is granted to anyone to use this software for any purpose on any computer system, and to redistribute it freely, subject to the following restrictions:

1. This software is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE.
2. Regular expression support is provided by the PCRE library package, which is open source software, written by Philip Hazel, and copyright by the University of Cambridge, England.

<ftp://ftp.csx.cam.ac.uk/pub/software/programming/pcre/>

PHAOSSSLava and SSLavaThin

Copyright (c) 1996-2003 Phaos Technology Corporation. All Rights Reserved.

The software contains commercially valuable proprietary products of Phaos which have been secretly developed by Phaos, the design and development of which have involved expenditure of substantial amounts of money and the use of skilled development experts over substantial periods of time. The software and any portions or copies thereof shall at all times remain the property of Phaos.

PHAOSS MAKES NO WARRANTIES, EXPRESS OR IMPLIED, INCLUDING WITHOUT LIMITATION THE IMPLIED WARRANTY OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE, REGARDING THE SOFTWARE, OR ITS USE AND OPERATION ALONE OR IN COMBINATION WITH ANY OTHER SOFTWARE.

PHAOSS SHALL NOT BE LIABLE TO THE OTHER OR ANY OTHER PERSON CLAIMING DAMAGES AS A RESULT OF THE USE OF ANY PRODUCT OR SOFTWARE FOR ANY DAMAGES WHATSOEVER. IN NO EVENT WILL PHAOSS BE LIABLE FOR SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

RealSystem

The RealNetworks® RealProxy™ Server is included under license from RealNetworks, Inc. Copyright 1996-1999, RealNetworks, Inc. All rights reserved.

SNMP

Copyright (C) 1992-2001 by SNMP Research, Incorporated.

This software is furnished under a license and may be used and copied only in accordance with the terms of such license and with the inclusion of the above copyright notice. This software or any other copies thereof may not be provided or otherwise made available to any other person. No title to and ownership of the software is hereby transferred. The information in this software is subject to change without notice and should not be construed as a commitment by SNMP Research, Incorporated.

Restricted Rights Legend:

Use, duplication, or disclosure by the Government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013; subparagraphs (c)(4) and (d) of the Commercial Computer Software-Restricted Rights Clause, FAR 52.227-19; and in similar clauses in the NASA FAR Supplement and other corresponding governmental regulations.

PROPRIETARY NOTICE

This software is an unpublished work subject to a confidentiality agreement and is protected by copyright and trade secret law. Unauthorized copying, redistribution or other use of this work is prohibited. The above notice of copyright on this source code product does not indicate any actual or intended publication of such source code.

STLport

Copyright (c) 1999, 2000 Boris Fomitchev

This material is provided "as is", with absolutely no warranty expressed or implied. Any use is at your own risk. Permission to use or copy this software for any purpose is hereby granted without fee, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

The code has been modified.

Copyright (c) 1994 Hewlett-Packard Company

Copyright (c) 1996-1999 Silicon Graphics Computer Systems, Inc.

Copyright (c) 1997 Moscow Center for SPARC Technology

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Hewlett-Packard Company makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Silicon Graphics makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

Permission to use, copy, modify, distribute and sell this software and its documentation for any purpose is hereby granted without fee, provided that the above copyright notice appear in all copies and that both that copyright notice and this permission notice appear in supporting documentation. Moscow Center for SPARC Technology makes no representations about the suitability of this software for any purpose. It is provided "as is" without express or implied warranty.

SmartFilter

Copyright (c) 2003 Secure Computing Corporation. All rights reserved.

SurfControl

Copyright (c) 2003 SurfControl, Inc. All rights reserved.

Symantec AntiVirus Scan Engine

Copyright (c) 2003 Symantec Corporation. All rights reserved.

TCPIP

Some of the files in this project were derived from the 4.X BSD (Berkeley Software Distribution) source.

Their copyright header follows:

Copyright (c) 1982, 1986, 1988, 1990, 1993, 1994, 1995

The Regents of the University of California. All rights reserved.

Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.
2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.
3. All advertising materials mentioning features or use of this software must display the following acknowledgement:
This product includes software developed by the University of California, Berkeley and its contributors.
4. Neither the name of the University nor the names of its contributors may be used to endorse or promote products derived from this software without specific prior written permission.

THIS SOFTWARE IS PROVIDED BY THE REGENTS AND CONTRIBUTORS ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE REGENTS OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

Trend Micro

Copyright (c) 1989-2003 Trend Micro, Inc. All rights reserved.

zlib

Copyright (c) 2003 by the [Open Source Initiative](#)

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

ICU License - ICU 1.8.1 and later COPYRIGHT AND PERMISSION NOTICE Copyright (c) 1995-2003 International Business Machines Corporation and others All rights reserved. Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, provided that the above copyright notice(s) and this permission notice appear in all copies of the Software and that both the above copyright notice(s) and this permission notice appear in supporting documentation. THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE COPYRIGHT HOLDER OR HOLDERS INCLUDED IN THIS NOTICE BE LIABLE FOR ANY CLAIM, OR ANY SPECIAL INDIRECT OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER RESULTING FROM LOSS OF USE, DATA OR PROFITS, WHETHER IN AN ACTION OF CONTRACT, NEGLIGENCE OR OTHER TORTIOUS ACTION, ARISING OUT OF OR IN CONNECTION WITH THE USE OR PERFORMANCE OF THIS SOFTWARE. Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder

Contents

Contact Information

Third Party Copyright Notices

Chapter 1: Introducing the ProxySG

Web Security Solution	19
New Features in this Release	22
Protocols Supported.....	26
Supported Browsers.....	27
Upgrading and Upgrade Enhancements	27
About the Document Organization	27
Related Blue Coat Documentation.....	29
Document Conventions.....	29

Chapter 2: Licensing

About Licensing.....	31
Licensable Components.....	31
About the Trial Period	32
About License Expiration.....	32
Installing a System License Key	33
Viewing License Information	36
Updating a License.....	37
Automatically Updating a License	37

Chapter 3: Accessing the ProxySG

Before You Begin: Understanding Modes	39
Accessing the ProxySG	40
Management Console Home Page.....	41
Changing the Login Parameters.....	42
Configuring the SSH Console.....	47

Chapter 4: Configuring the System

Global Configurations	53
Archive Configuration.....	59
Adapters	64
Software and Hardware Bridges.....	68
Gateways	72
Defining Static Routes	74
Using RIP	78
DNS	81
Attack Detection	86
Using a Bypass List	91

Installing WCCP Settings.....	99
Virtual IP Addresses.....	103
Configuring Failover	104
TCP-IP Configuration.....	109

Chapter 5: Managing Port Services

Section A: Managing Multiple Management Consoles

HTTPS Console (Secure Console).....	114
HTTP Console.....	117
SSH Console.....	118
Telnet Console	119

Section B: Creating and Editing Services

About Service Attributes.....	122
DNS-Proxy	122
FTP	125
HTTP	126
HTTPS.....	127
Instant Messaging Protocols.....	129
Streaming Protocols	130
SOCKS	131
TCP Tunneling.....	132
Telnet Shell Proxy Service.....	134

Chapter 6: Configuring Proxies

Section A: About Explicit and Transparent Proxy

Section B: Configuring Explicit Proxies

Creating an Explicit Proxy Server.....	139
Configuring the FTP Proxy.....	140
Configuring FTP Connection Welcome Banners.....	146
Configuring an HTTP Proxy	147
Configuring a SOCKS Proxy	160
Shell Proxies.....	162

Section C: Transparent Proxies

Configuring the Transparent Proxy Hardware	169
IP Forwarding.....	171
Creating a Transparent Proxy Service	171

Chapter 7: Using Secure Services

HTTPS Termination Overview	173
Configuring HTTPS Termination	177
Managing the SSL Client.....	196
Configuring HTTP or HTTPS Origination to the Origin Content Server.....	200
Configuring DNS Resolution to the Origin Content Server	202

Chapter 8: Security and Authentication**Section A: Controlling Access to the ProxySG**

Limiting Access to the ProxySG Appliance	205
About Password Security.....	206
Limiting User Access to the ProxySG—Overview	207
Moderate Security: Restricting Management Console Access Through the Console Access Control List 210	
Maximum Security: Administrative Authentication and Authorization Policy	212

Section B: Controlling Access to the Internet and Intranet

Using Authentication and Proxies.....	217
Using SSL with Authentication and Authorization Services	222
Creating a Proxy Layer to Manage Proxy Operations.....	223

Chapter 9: Using Authentication Services

Understanding Realms.....	233
SSL Between the ProxySG and the Authentication Server	233

Section A: NTLM Realm Authentication and Authorization

How Blue Coat Works with NTLM.....	235
Creating an NTLM Realm	235
NTLM Servers.....	236
Defining NTLM Realm General Properties.....	238
Creating the CPL.....	240
Tips and Boundary Conditions.....	240

Section B: LDAP Realm Authentication and Authorization

Overview	242
Creating an LDAP Realm	243
LDAP Servers	244
Defining LDAP Base Distinguished Names	248
LDAP Search & Groups Tab (Authorization and Group Information)	251
Customizing LDAP Objectclass Attribute Values.....	254
Defining LDAP General Realm Properties.....	255
Creating the CPL.....	257

Section C: RADIUS Realm Authentication and Authorization

Creating a RADIUS Realm.....	258
Defining RADIUS Realm Properties	259
Defining RADIUS Realm General Properties	261
Creating the CPL.....	264

Section D: Local Realm Authentication and Authorization

Creating a Local Realm	265
Changing Local Realm Properties	266
Defining the Local User List.....	268
Creating the CPL.....	275

Section E: Certificate Realm Authentication

How Certificate Realm Works	276
Creating a Certificate Realm.....	276
Defining a Certificate Realm	278
Defining Certificate Realm General Properties	279
Revoking User Certificates	281
Creating the Certificate Authorization Policy	282
Tips.....	282

Section F: Sequence Realm Authentication

Adding Realms to a Sequence Realm"	284
Creating a Sequence Realm	284
Adding Realms to a Sequence Realm.....	285
Defining Sequence Realm General Properties	287

Section G: Netegrity SiteMinder

Understanding SiteMinder Interaction with Blue Coat	290
Participating in a Single Sign-On (SSO) Scheme	292
Creating a SiteMinder Realm	293
SiteMinder Servers.....	297
Defining SiteMinder Server General Properties.....	300
Creating the CPL.....	304

Section H: Forms-Based Authentication

Understanding Authentication Forms	306
Creating and Editing an Authentication Form.....	308
Setting Storage Options.....	313
Using CPL with Forms-Based Authentication.....	314
Tips and Boundary Conditions.....	315

Section I: Managing the Credential Cache**Chapter 10: External Services****Section A: ICAP**

Supported ICAP Servers	322
ICAP v1.0 Features.....	322
About Content Scanning.....	323
Installing the ICAP Server	325
Creating an ICAP Service	325
Deleting an ICAP Service.....	330
Customizing ICAP Patience Text	330
Creating ICAP Policy.....	335
Managing Virus Scanning.....	341
Access Logging.....	342
References.....	343

Section B: Websense

Creating a Websense Service	344
Deleting a Websense Service	346

Section C: Service Groups

Creating a Service Group	348
Deleting a Service Group or Group Entry	350
About Weighted Load Balancing.....	350

Section D: Displaying External Service and Group Information**Chapter 11: Health Checks**

About General Health Checks.....	355
Configuring Service-Specific Health Checks	356
About Global Forwarding and SOCKS Gateway Health Checks	359
Configuring Global Health Checks	359
Pausing or Resuming Global Health Checking	361

Chapter 12: Managing Policy Files

About Policy Files	363
Creating and Editing Policy Files	366
Managing the Central Policy File	371
Viewing Policy Files	373

Chapter 13: The Visual Policy Manager**Section A: About the Visual Policy Manager**

JRE Requirement	379
Launching the Visual Policy Manager	379
About the Visual Policy Manager User Interface	380
About VPM Components.....	383
The Set Object Dialog	386
The Add/Edit Object Dialog	387

Section B: Policy Layer and Rule Object Reference

About the Reference Tables	389
Administration Authentication Policy Layer Reference	389
Administration Access Policy Layer Reference	389
DNS Access Policy Layer Reference.....	389
SOCKS Authentication Policy Layer Reference	390
Web Authentication Policy Layer Reference	391
Web Access Policy Layer Reference	391
Web Content Policy Layer Reference.....	393
Forwarding Policy Layer Reference	393

Section C: Detailed Object Column Reference

Source Column Object Reference.....	396
Destination Column Object Reference	406
Service Column Object Reference.....	411

Time Column Object Reference	416
Action Column Object Reference.....	419
Track Object Column Reference	441
Comment Object Reference	444
Using Combined Objects	444
Creating Categories	446
Restricting DNS Lookups	448
Restricting Reverse DNS Lookups	449
Setting the Group Log Order.....	449
Section D: Managing Policy Layers and Files	
How Policy Layers, Rules, and Files Interact.....	452
Managing Policy Files	455
Installing VPM-Created Policy Files	456
Viewing the Policy/Created CPL.....	459
Section E: Tutorials	
Tutorial—Creating a Web Authentication Policy	461
Tutorial—Creating a Web Access Policy	465
Chapter 14: Advanced Policy	
Blocking Pop-Up Windows	473
Stripping or Replacing Active Content.....	474
About Active Content Types	475
Modifying Headers	476
Defining Exceptions.....	477
About Exception Definitions	480
About the Exceptions Hierarchy.....	481
About the Exceptions Installable List.....	482
Creating or Editing Exceptions	483
Viewing Exceptions	486
Chapter 15: Streaming Media	
Section A: About Streaming Media	
Streaming Media Overview.....	490
Streaming Media Protocols.....	491
Streaming Media Player Support	494
Streaming Media Authentication	494
Streaming Media Caching Behavior.....	496
Section B: Configuring Streaming Media	
Limiting Bandwidth	499
Configuring the Refresh Rate.....	503
Configuring HTTP Handoff	504
Forwarding Client Logs to the Media Server.....	505
Configuring Media Server Authentication Type (Windows Media)	506
About Multicast Streaming.....	506

Managing Multicast Streaming for Windows Media	507
Managing Multicast Streaming for Real Media.....	511
Managing Simulated Live Content (Windows Media)	512
ASX Rewriting (Windows Media).....	514
About Fast Streaming (Windows Media).....	517
Section C: Windows Media Player	
Configuring Windows Media Player	518
Limitations	519
Windows Media Access Log Formats.....	520
Section D: RealPlayer	
Configuring RealPlayer.....	521
Real Media Access Log Formats	523
Limitations and Known Issues.....	523
Section E: QuickTime Player	
Configuring QuickTime Player.....	524
QuickTime Access Log Formats	524
Limitations	524
Access Log Format.....	525
Chapter 16: Instant Messaging	
About Securing Instant Messaging.....	527
Recommended Deployments	527
About the Instant Messaging Protocol Services	527
About HTTP Proxy Support.....	528
About Instant Messaging Reflection	528
IM Reflection Diagrams	528
About Instant Messaging Proxy Authentication.....	532
Securing AOL Encryption Capability	532
Instant Message Proxies	533
Configuring Instant Messenger Clients	536
VPM Examples	539
Statistics	540
Related Material	543
Chapter 17: Content Filtering	
Overview	545
Selecting Category Providers	546
Configuring a Local Database	549
Configuring Blue Coat Web Filter	554
Configuring InterSafe	561
Configuring Proventia Web Filter	566
Configuring SmartFilter.....	571
Configuring SurfControl.....	579
Configuring Websense	583
How to Apply Policy to Categorized URLs	588

Using Content-Filtering Vendors with ProxySG Policies	591
Tips.....	594
Chapter 18: Configuring the Upstream Networking Environment	
Forwarding Configuration	597
SOCKS Gateway Configuration.....	619
Internet Caching Protocol (ICP) Configuration.....	628
Using Policy to Manage Forwarding	636
Chapter 19: Access Logging	
Overview	641
Customizing the Log Procedures	642
Testing Access Log Uploading.....	676
Viewing Access-Log Statistics.....	678
Using Access Logging with Policy Rules	682
Chapter 20: Maintaining the ProxySG	
Restarting the ProxySG	687
Restoring System Defaults.....	689
Purging the DNS Cache	691
Clearing the System Cache	692
Upgrading the ProxySG	692
Managing ProxySG Systems	695
Event Logging and Notification.....	698
Configuring SNMP	705
Disk Reinitialization	708
Deleting Objects from the ProxySG.....	709
Chapter 21: Statistics	
Selecting the Graph Scale.....	711
General Statistics	711
System Usage Statistics	714
HTTP/FTP History Statistics	718
Streaming History Statistics	720
SOCKS History Statistics.....	724
Shell History Statistics	725
Resources Statistics	726
Efficiency Statistics.....	729
Contents Statistics	733
Event Logging.....	734
Failover Statistics.....	735
Advanced Statistics.....	735
Appendix A: Using the Authentication/Authorization Agent	
Installing the BCAAA Service on a Windows or Windows NT System.....	737
NTLM and the BCAAA Service.....	744

SiteMinder and the BCAA Service	744
Troubleshooting Authentication Agent Problems	745
Common BCAA Event Messages	745
 Appendix B: Access Log Formats	
Custom or W3C ELFF Format.....	751
SQUID-Compatible Format.....	754
NCSA Common Access Log Format.....	755
Fields Available for Creating Access Log Formats	756
 Appendix C: Using WCCP	
Overview	785
Quick Start.....	787
Configuring a WCCP Version 2 Service on the Router	788
Creating a ProxySG WCCP Configuration File	795
Examples	802
Troubleshooting: Home Router	806
Tips.....	809
 Appendix D: RIP Commands	
net	811
host	811
RIP Parameters	812
ProxySG-Specific RIP Parameters.....	813
Using Passwords with RIP	814
 Appendix E: Using Regular Expressions	
Regular Expression Syntax	816
Regular Expression Details.....	817
Regular Expression Engine Differences From Perl	828
 Appendix F: Diagnostics	
Service Information.....	832
Packet Capturing (the PCAP Utility)	839
Core Image Restart Options	845
Diagnostic Reporting (Heartbeats).....	846
 Appendix G: Using Blue Coat Director to Manage Multiple Appliances	
How Director Works with ProxySG.....	849
Director Documentation	853
 Index	

Chapter 1: Introducing the ProxySG

The Internet is becoming a primary conduit for Web-based information, applications, and transactions. This growing use of Web applications exposes organizations to new security threats from Web viruses, hostile mobile code, and inappropriate Web content—all of which are capable of using HTTP as an open door into the organization.

While current security infrastructures include firewalls designed to protect enterprises from packet-level threats, they are not designed to handle the sophisticated threats allowed in from content-level applications. This has led organizations to embrace a new security model—one that includes both a firewall for packet-level protection and a Web security solution optimized to provide content-level protection.

Blue Coat™ Systems ProxySG represents the latest in perimeter defense for securing and controlling Web-based content and applications. The Blue Coat ProxySG is designed to integrate protection and control functions for Internet and intranet traffic without sacrificing performance and employee productivity.

Web Security Solution

The Blue Coat ProxySG provides a point of integration, control, and acceleration for enterprise Web security applications, including:

- Layered security approach with content-level protection to combat Web-based threats utilizing port 80.
- Highly scalable, policy-based virus scanning optimized to scan Web-based threats in real-time.
- Flexibility to implement security policies for both uploaded and downloaded Web content.
- Scalable policy-based, URL filtering provides comprehensive control over Web usage and reduces response times for users.
- Integrated caching, content positioning, bandwidth savings and bandwidth management provides superior performance for controlling Web content.
- Optimized design for Web content and security resulting in higher performance and lower management costs.

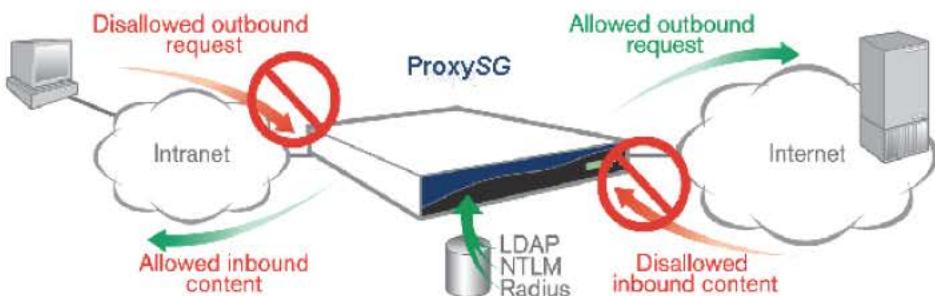


Figure 1-1: The ProxySG Solution

Ease of Deployment

The ProxySG is specifically designed to increase security and reduce costs associated with central, regional, and branch office Web protection. For example, the SG400 platform easily *drops-in* to remote environments where technical support staff is not always available and features simple installation and remote management.

Other platforms also feature a simple-to-manage system that installs in minutes with little ongoing maintenance. In addition, they also provide configuration restoration that allows system configuration to be archived, including all system settings, filtering and policies; removable, hot-swappable disk drives for true fault tolerance, and are field serviceable and upgradeable.

Policy and Management Architecture

Networking environments have become increasingly complex, with a variety of security and access management issues. Enterprises face challenges in configuring products and ensuring the result supports enterprise policies. *Policies* enhance ProxySG features, such as authentication and virus scanning, allowing you to manage Web access specific to the enterprise's needs.

Blue Coat policies provide:

- Fine-grained control over various aspects of ProxySG behavior.
- Multiple policy decisions for each request.
- Multiple actions triggered by a particular condition.
- Bandwidth limits
- Authentication-aware, including user and group configuration.
- Flexibility of user-defined conditions and actions.
- Convenience of predefined common actions and transformations.
- Support for multiple authentication realms.
- Configurable policy event logging.
- Built-in debugging.
- Backward compatibility with older CacheOS filter files. Note that you might receive more warning messages due to more deprecated commands in SGOS 3.x.

The ProxySG uses policies and system configuration together to provide the best-possible security for your network environment.

Blue Coat's unique architecture allows for scalable decision-making. Effectively turning on multiple combinations of granular policy requires a unique level of performance.

Blue Coat's flexible logging features, coupled with integrated authentication and identification capabilities, give organizations the power to monitor Web access for every user in the network at any time, regardless of where they are. Internet access traffic flowing through the ProxySG gives administrators and managers the ability to audit Web traffic as needed.

Content Filtering

As the number of users and the total amount of traffic grows, policy enforcement demands higher performance to provide adequate end-user quality of experience. To satisfy the management level and scalability that enterprise traffic demands, ProxySG Appliances have emerged as a new layer of infrastructure that provide the performance and manageability required for enterprise-wide policy-based content filtering.

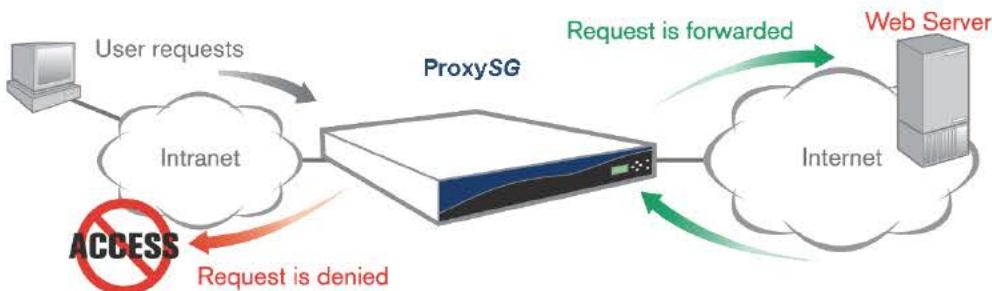


Figure 1-2: Content Filtering

The ProxySG enforces Internet access policies based on:

- **Content categories (gambling, sex, etc.)**—Integrates filtering databases from leading vendors like SmartFilter, SurfControl, and Websense.
- **Content type and protocols (HTTP, FTP, streaming, mime type, etc.)**—Adds the ability to block certain types of content transported on certain types of protocols.
- **Identity (user, group, network)**—Customize policy based on who the users are regardless of location.
- **Network conditions**—Customize based on real-time conditions.

Content Scanning

When integrated with a supported Internet Content Adaptation Protocol (ICAP) server, Blue Coat provides content scanning and filtering, and can repair files affected by an Internet-based malicious code. ICAP is an evolving protocol that allows an enterprise to dynamically scan and change Web content. *Content scanning* includes actions like sending a given request for content to an ICAP server for virus scanning or malicious mobile code detection.

To eliminate threats to the network and to maintain caching performance, the ProxySG sends objects to the integrated ICAP server for checking and saves the scanned objects in its object store. With subsequent content requests, the ProxySG serves the scanned object rather than rescan the same object for each request.

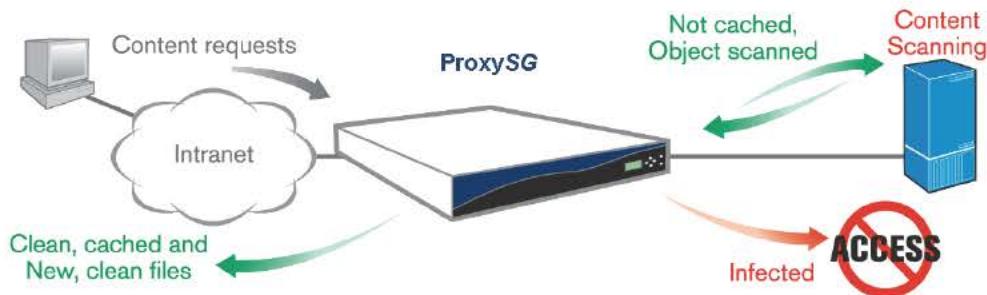


Figure 1-3: Content Scanning

The ProxySG blocks viruses from Web content behind and in front of the firewall. Blue Coat architecture is optimized to handle Web requests and responses that require scanning for potentially malicious mobile code and viruses. The ProxySG uses ICAP to vector responses to supported virus scanning servers to deliver unmatched flexibility and performance in scanning Web content.

Instant Messaging

Instant Message (IM) usage in an enterprise environment creates security concerns because, regardless of how network security is configured, IM connections can be made from any established protocol, such as HTTP or SOCKS, on any open port. Because it is common for coworkers to use IM to communicate, especially in remote offices, classified company information can be exposed outside the network. Viruses and other malicious code can also be introduced to the network from file sharing through IM clients.

The ProxySG serves as an IM proxy, both in transparent and explicit modes. You can control IM actions by allowing or denying IM communications and file sharing based on users (both employee identities and IM handles), groups, file types and names, and other triggers. You can also log and archive all IM chats.

Proxy Gateway

ProxySG Appliances can act as a proxy gateway, an intermediary between a Web client and a Web server that provides authentication for the client. The rules used to authenticate a client are based on the policies you create and manage.

Once configured and with policies in place, the ProxySG can also, through proxying, filter traffic, monitor Internet and intranet resource usage, block specific Internet and intranet resources for individuals or groups, and enhance the quality of Internet or intranet user experiences.

New Features in this Release

ProxySG Appliances combine patent-pending software with robust hardware configurations to deliver performance, manageability, and scalability.

New features in this release include:

- Licensing and registration of SGOS 3.x.
- New Management Console design.
- Enhanced secure access to both the Management Console and the Command Line Interface (CLI).
- Enhanced internal services, such as consoles and proxies.
- Enhanced external services, such as ICAP, off-box Websense, and health checks.
- Improved policy configuration and management.
- Increased access logging capabilities.
- New RTSP proxy.

Registration and Licensing

Once you configure and launch the ProxySG, you must register SGOS 3.x and license the ProxySG features you plan to enable. A 60-day trial period grants unlimited access to all features, although license-expiration warning messages are displayed throughout the trial period. For information about registering SGOS and licensing various SGOS components, see Chapter 2: “Licensing” on page 31.

New Management Console Design

The new Management Console design allows for intuitive feature access. From the Management Console home page, you can launch the Management Console, link to the documentation, or link to Blue Coat technical and customer Web sites.

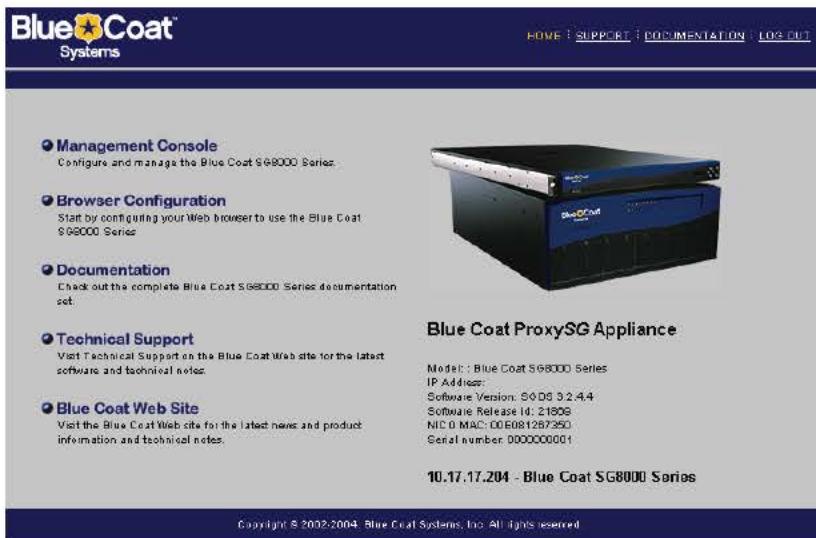


Figure 1-4: ProxySG Home Page

Clicking Management Console displays the ProxySG Management Console.

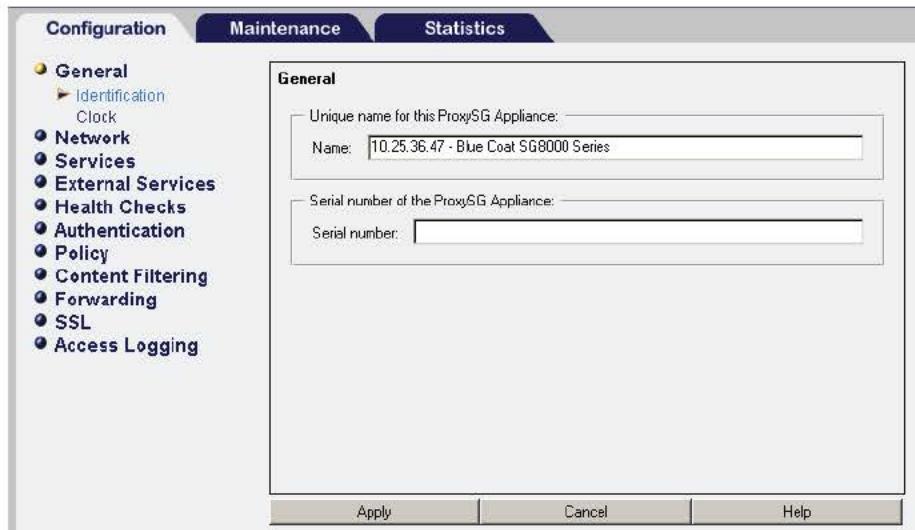


Figure 1-5: Management Console Page

The ProxySG features are categorized under three top-level tabs:

- Configuration—Customize the ProxySG features and create policies that provide the best-possible security for your enterprise.
- Maintenance—Upgrade the system, install and view various licenses, and perform basic troubleshooting.
- Statistics—View ProxySG statistics, as well as content statistics.

Enhanced SGOS Security

New security features for the ProxySG include:

- Default use of SSH and HTTPS
- Configurable sessions before the Management Console logs out

Default Use of HTTPS and SSH

To access the ProxySG through the browser, you must use HTTPS and port 8082. You can still use HTTP (and port 8081), although this protocol is not secure.

Multiple Management Consoles, both HTTP and HTTPS, can be used simultaneously to access a ProxySG Management Console. This might be helpful if you use virtual IP addresses to access the ProxySG.

For the CLI, the default is SSH, which requires an SSH client on your system. You can use a Telnet-Console; for security reasons, Blue Coat does not recommend using this method.

Configurable Management Console Sessions

The ProxySG ships with a default Management Console session timeout of 900 seconds (15 minutes). You can determine whether you want this feature enabled, and the session timeout value can be changed.

At the end of the session, you are prompted to either log out or to log back in. If you do nothing, you are logged out.

To log out before the session is over, click the Log Out link at the top of the page.

HTTPS Termination

The ProxySG ships with a default keyring (name, keypair, certificate, and SSL client) that allows the appliance to authenticate itself to other browsers. You can also configure other keyrings using self-signed certificates or any of the many Certificate-Authority-signed (CA) certificates. Lists of CA-Certificates that can be associated with a particular HTTPS service can be created.

The ProxySG HTTPS termination is implemented as follows:

- Combines hardware-based SSL acceleration with full caching functionality.
- Establishes and services incoming SSL sessions.
- Provides SSL v2.0, v3.0, and TLSv1 protocol support.

Enhanced Services

In SGOS 3.x, configuring and enabling services is more intuitive.

Some services have been renamed to better reflect the fact they control access to the Management Console and CLI. Other services were added for this version of SGOS, including MMS, RTSP, MSN-IM, AOL-IM, and Yahoo-IM.

The streaming services—MMS and RTSP—are part of configuring and enabling streaming proxies. MSN-IM, AOL-IM, and Yahoo-IM are services that can be enabled to use Instant Messaging.

Each of these proxies must be configured through their specific Proxy tab and then configured with a port and enabled through the Service Ports tab.

Increased Policy Configuration and Management

Policies allow you to manage Web access and allow you to control end-user Web access in your existing infrastructure. Policies differ from the ProxySG configuration settings. Configuration sets up a feature; policies determine how the feature is used. Both are essential.

Policy is substantially more robust in SGOS 3.x. Many new conditions, properties, and actions have been added to manage new and improved features, such as Instant Messaging and Access Logging.

The Visual Policy Manager (VPM) contains substantially more functionality than in previous versions. Using just the VPM, you can:

- Generate more complex and granular policy.
- Browse users and groups from Security realms (LDAP, NTLM, and the like) defined on the ProxySG and insert them in policy without typing in complex Distinguished Names (DNs).

- Track specific policy rules.
- Include month and year in the time object.
- Rewrite policy to include server_portal and header rewrite.

Like the Management Console, the VPM has been redesigned.

Increased Logging Capabilities

For SGOS 3.x, Access Logging has been redone, with increased robustness and improved functionality.

Access logging allows you to track the number of visitors, their originating IP address, how many requests for each page at the site, and usage patterns regarding a specific site.

Log takes on additional meaning. In addition to the log, customizable components such as log format, upload schedules, and upload client configurations are also saved with the log and can be reconfigured with new information at any time.

RTSP Proxy Support

SGOS 3.x replaces the former ported Real proxy with new RTSP proxy. Changes include:

- HTTP streaming support through the RTSP proxy
- Ability to use HTTP to the origin content server
- Firewall problems have been eliminated, since RTSP no longer uses ports 3030/7878
- More granular control of RTSP through policy
- Streaming-speed prepopulation
- Line-speed pre-population from a Web server using HTTP download
- Logging user accesses to a single streaming facility, using default ELFF format
- Multicasting to clients.

Protocols Supported

Blue Coat ProxySGs are multi-protocol. Blue Coat supports the following protocols:

- HTTP
- HTTP 1.1—The benefits of HTTP 1.1 include persistent connections that allow multiple requests to be pipelined to the ProxySG and virtual hosting capabilities.

For either HTTP or HTTP 1.1, you must enable the service before using it.

- FTP, Transparent FTP—The ProxySG implementation of transparent FTP is intended for caching *public* FTP objects, which constitute the vast majority of the FTP objects accessed through Web browsers. Public FTP objects are those that are accepted anonymously, using the *anonymous* reserved username of *FTP*.

Transparent FTP is configured and enabled by default.

- HTTPS—This is the default protocol used by the Management Console. It is configured and enabled by default. You can create other HTTPS services.
- Streaming Media—The ProxySG allows streaming of both live and pre-recorded video and audio using unicast one-to-one transmission or multicast (one-to-many) transmission.
MMS and RTSP ports are configured and enabled by default.

Supported Browsers

The ProxySG Management Console supports Microsoft® Internet Explorer 5 and 6, and Netscape® Communicator 4.76 and 6.2.

The Management Console uses the Java Runtime Environment. All browsers come with a default, built-in JRE, and you should use this default JRE rather than an independent JRE version downloaded from Sun® Microsystems.

Upgrading and Upgrade Enhancements

For information on doing upgrades or downgrades, or for restoring default system settings, refer to the *Blue Coat SGOS 3.x Upgrade Guide*.

Where to Go From Here

The following sections describe the top-level tasks you need to carry out to customize the ProxySG to your environment. The tasks are shown in the order of a typical deployment:

Placing the ProxySG in a Network

To install a ProxySG into a network, the network must be set up to present the ProxySG with traffic to control.

- p Explicit Proxy: All the ProxySG needs is IP address connectivity to the network; browsers must be configured to point to the ProxySG through a PAC file.
- p Transparent Proxy: The majority of networks use transparent proxy. Transparent proxying occurs when the ProxySG receives traffic destined for Origin Content Servers (OCS) and terminates the traffic, then initiates the same request to the OCS.
 - Bridging: With this configuration, you do not have to make router or L4 switch configuration changes. The ProxySG is placed inline on a segment of the network where all outgoing traffic flows; one Ethernet interface is connected to the internal network, the other Ethernet interface is connected to the Internet. The ProxySG terminates all traffic on the service ports in which the proxy has been configured and sends the request to the outside OCS. All other traffic is bridged between the two Ethernet interfaces.

Note that this configuration, without using policy controls, can lead to an *open proxy*. An open proxy results when traffic is allowed on the outside (Internet) interface because users are accessing internal Web servers behind the proxy.

- WCCP: If the site has Cisco routers, WCCP can be used to direct certain TCP/IP connections to the ProxySG. TCP/IP ports to forward to the ProxySG are communicated between ProxySG appliances and the Cisco routers. Typically, this is enforced on the outgoing interface on the Cisco router.
- L4 switching: Similar to WCCP, the L4 switch is configured to forward traffic for specific TCP/IP ports to the attached ProxySG.

Initial Setup

The ProxySG must be initially configured before it operates on a network. This can be done through the front panel (if applicable) or the serial console. The initial setup sets not only the IP address, but enable and console passwords. Once completed, the ProxySG can be managed through the serial console, SSH, or HTTPS at port 8082. Information on setting up the ProxySG is in the Quick Start Guide and Installation Guide for your platform.

Simple Policy

The default policy on new ProxySG appliances is to deny everything. To test initial setup, you can create a policy of ALLOW, along with changing access logging to log to the default logs. If the ProxySG is correctly set up, Web browsers can surf the Internet and all transactions are logged. Once the ProxySG setup is verified, the policy should again be set to DENY, unless otherwise required.

If the policy is set to allow everything and a bridged configuration is used, clients can send a connection request for any port, including e-mail, using the proxy to send spam. This is called an *open proxy* and usually results in performance slowdowns (among other things).

To prevent the ProxySG from becoming an open proxy in a bridged configuration if you must use an ALLOW configuration, add the following policy to the end of the local policy:

```
define subnet Trusted_Clients
    10.0.0.0/8
end subnet
define subnet Trusted_Servers
    216.52.23.0/24
end subnet
<Proxy>
    client.address = Trusted_Clients OK ; Policy below applies
    proxy.address = Trusted_Servers OK ; Policy below applies
    FORCE_DENY ; Force a denial for everything else
<Proxy>
    ; Add other allow or deny rules here
    ; Example: Allow all traffic not denied above
    ALLOW
```

Implementing Policies

Once the basic system is set up, you need to decide which controls—policies—to put in place. Typically, the following are configured on the system:

- Proxy caching (HTTP, FTP, Streaming)

- Authentication/single sign-on
- Access control policy
- Content filtering
- Web anti-virus

Implementing policies is a two-step process:

- Configure the feature; for example, choose Blue Coat Web Filter (BCWF) or another content filtering vendor, enable it, and schedule downloads of the database.
- Create policy through the graphical Visual Policy Manager (VPM) or through the Content Policy Language (CPL).

Managing the ProxySG

Once the configuration and policy on the ProxySG are set, you should know how to evaluate the current operating state. This can include reviewing event log messages, utilizing SNMP, or diagnostics such as CPU utilization.

- Archive a configuration file: "Archiving a Configuration" on page 75
- Upgrade the system: "Upgrading the ProxySG" on page 885
- Set up event logging: "Event Logging and Notification" on page 892
- Configure SNMP: "Configuring SNMP" on page 898
- Understand Diagnostics: Appendix E: "Diagnostics" on page 1039

Managing the ProxyAV

The ProxySG with ProxyAV™ integration is a high-performance Web anti-virus (AV) solution. For most enterprises, Web applications and traffic are mission-critical, representing 90% of the total Internet traffic.

By deploying the ProxySG/ProxyAV solution, you gain performance and scalability (up to 250+ Mbps HTTP throughput), along with Web content control.

For information on managing the ProxyAV, refer to the *Blue Coat ProxyAV Configuration and Management Guide*.

Troubleshooting

Use the access logs, event logs, and packet captures to check connections and view traffic passing through the ProxySG. Use policy tracing to troubleshoot policy. Note that policy tracing is global; that is, it records every policy-related event in every layer. Turning on policy tracing of any kind is expensive in terms of system resource usage and slows down the ProxySG's ability to handle traffic.

- Policy tracing: For information on using policy tracing, see "Policy Tracing" on page 516.
- Access Logs: For information on configuring and using access logs, see Chapter 20: "Access Logging" on page 827.

- Event logs: For information on using event logs, see "Event Logging and Notification" on page 892.
- Packet capture: For information on using the PCAP utility, see "Packet Capturing (the PCAP Utility)" on page 1048.

Task Tables

The tables below refer to the sections in the manuals that describe the top-level tasks to customize the ProxySG to your environment. The tables are listed in alphabetical order (for example, *access logging*, *authentication*, *bridging*, *caching*, and so on).

Table 1.1: Access Logging

Task	Reference
Configure access logging with <ul style="list-style-type: none"> • Blue Coat Reporter • SurfControl Reporter 	<ul style="list-style-type: none"> • Blue Coat Reporter: Chapter 3, "Creating the First Profile"; <i>Blue Coat Reporter Configuration and Management Guide</i> • SurfControl Reporter: "Using SurfControl Reporter with SGOS 3.x."

Table 1.2: Anti-Virus

Task	Reference
Block Web viruses using ProxyAV	"Section A: ICAP"; <i>Blue Coat ProxyAV Configuration and Management Guide</i>
Set up anti-virus filtering	<i>Blue Coat ProxyAV Configuration and Management Guide</i>

Table 1.3: Authentication

Task	Reference
Achieve single sign-on with NTLM	"Section A: NTLM Realm Authentication and Authorization"
Select the right authentication mode	"Using Authentication and Proxies"
Install the Blue Coat authentication/authorization agent to work with IWA (formerly NTLM)	Appendix A: "Using the Authentication/Authorization Agent"
Configure authentication to work with an existing authentication service	Chapter 9: "Using Authentication Services"
Set up authentication schemes and use them in policy	Chapter 8: "Security and Authentication"

Table 1.4: Bridging

Task	Reference
Configure bridging (hardware or software)	"Software and Hardware Bridges"
Allow those from outside a bridged deployment to get to internal servers	"Defining Static Routes"

Table 1.5: HTTP

Task	Reference
Redirect HTTP with WCCP	"Standard HTTP Redirection"

Table 1.6: HTTPS

Task	Reference
Create a transparent HTTPS service	"HTTP"

Table 1.7: Management

Task	Reference
Get the Management Console to work	Chapter 3: "Accessing the ProxySG"
Manage the System: <ul style="list-style-type: none"> • License the system • View statistics <ul style="list-style-type: none"> • Resources • Efficiency • SNMP monitoring 	<ul style="list-style-type: none"> • Chapter 2: "Licensing" • Chapter 21: "Statistics" • Chapter 21: "Statistics"

Table 1.8: Policy

Task	Reference
Set up authentication schemes and use them in policy	Chapter 8: "Security and Authentication"
Limit network access and configuring compliance pages	"Section B: Controlling Access to the Internet and Intranet"
Block unwanted content	"How to Apply Policy to Categorized URLs"
Change policy default	"Transaction Settings: Deny and Allow"

Table 1.8: Policy

Write policy using the Visual Policy Manager (VPM)	"Section E: Tutorials"
Write policy using the Content Policy Language (CPL)	<i>Blue Coat Content Policy Language Guide</i>

Table 1.9: Proxies

Task	Reference
Determine the best type of proxy for the environment	Chapter 6: "Configuring Proxies"
Get traffic to the proxy	Chapter 6: "Configuring Proxies"

Table 1.10: Reporter, Blue Coat

Task	Reference
Make Blue Coat Reporter work with access logging	" Customizing the Log: Configuring the Upload Schedule"; Blue Coat Reporter: Chapter 3, "Creating the First Profile," <i>Blue Coat Reporter Configuration and Management Guide</i>
Use Scheduler to set up report generation	Chapter 3, "Using Scheduler," in the <i>Blue Coat Reporter Configuration and Management Guide</i>
Generate specific reports for specific people	<i>Blue Coat Reporter Configuration and Management Guide</i>

Table 1.11: Reporter, SurfControl

Task	Reference
Configure SurfControl Reporter	" Using SurfControl Reporter with SGOS 3.x"

Table 1.12: Services

Task	Reference
Create a port service	"Section B: Creating and Editing Services"

Table 1.13: Streaming

Task	Reference
Control streaming protocols	Chapter 15: "Streaming Media"

Table 1.14: WCCP

Task	Reference
Configure WCCP for multiple ports	"Creating a Configuration File"
Redirect HTTP with WCCP	"Standard HTTP Redirection"
Configure the home-router IP	"Creating a Configuration File"
Configure multiple home-routers	"Creating a Configuration File"
Configure a multicast address as the proxy's home router	"Configuring a WCCP Version 2 Service on the Router"

About the Document Organization

This document is organized for easy reference, and is divided into the following sections and chapters:

Table 1.1: Document Organization

Chapter Title	Description
Chapter 1 – <i>Introducing the ProxySG</i>	This chapter discusses the ProxySG Security Solution and new features and enhancements in SGOS 3.x. It also covers document conventions.
Chapter 2 – <i>Licensing</i>	Several features must be licensed to be used beyond the evaluation trial date. This chapter describes which features require licenses.
Chapter 3 – <i>Accessing the ProxySG</i>	This chapter explains how to log in to the ProxySG command line interface and Web-based Management Console; how to change the administrator username, password, privileged-mode password; and how to make a secure connection using SSH and HTTPS.
Chapter 4 – <i>Configuring the System</i>	Instructions on setting the ProxySG name and system time, configuring the network adapter, load balancing, and FTP port services, and specifying DNS servers. This chapter also covers how to track client IP addresses using server-side transparency or virtual IP addresses.
Chapter 5 – <i>Managing Port Services</i>	This chapter describes port services configurable on the ProxySG, including several kinds of Management Consoles, such as HTTPS, HTTP, SSH, and Telnet Consoles, and application proxies such as Instant Messenger (IM), SOCKS, FTP, MMS, and RTSP, HTTP and HTTPS.
Chapter 6 – <i>Configuring Proxies</i>	Explicit and Transparent proxies are discussed in this chapter, as well as the kinds of proxy you should use.
Chapter 7 – <i>Using Secure Services</i>	HTTPS termination, including SSL, Certificates, keyrings, and keypairs are discussed in this chapter.
Chapter 8 – <i>Security and Authentication</i>	Enabling and maintaining security on the ProxySG is discussed in this chapter.

Table 1.1: Document Organization (Continued)

Chapter Title	Description
<i>Chapter 9 – Using Authentication Services</i>	Blue Coat supports six kinds of authentication, discussed here: LDAP, NTLM, RADIUS, Local (formerly UNIX), Certificate (which allows you to authenticate using certificates), and Sequence (which allows you to authenticate using multiple authentication servers).
<i>Chapter 10 – External Services</i>	ICAP and Websense off-box are described in this chapter.
<i>Chapter 11 – Health Checks</i>	The health of services, such as SOCKS, ICAP, and forwarding services, is discussed in this chapter.
<i>Chapter 12 – Managing Policy Files</i>	Four policy files are used to manage policy: Central, Local, Visual Policy Manager, and Forwarding. This chapter discusses how to manage them.
<i>Chapter 13 – The Visual Policy Manager</i>	This chapter contains a reference guide and several tutorials for using the Visual Policy Manager.
<i>Chapter 14 – Advanced Policy</i>	This chapter discusses using features such as pop-up ad blocking, managing active content, and creating exceptions.
<i>Chapter 15 – Streaming Media</i>	This chapter discusses streaming, including the new RTSP proxy.
<i>Chapter 16 – Instant Messaging</i>	How to configure and use the ProxySG's instant messaging capabilities is discussed in this chapter.
<i>Chapter 17 – Content Filtering</i>	This chapter discusses how to configure and use the ProxySG's content filtering capabilities, as well as configuring and using content filtering vendors to work with the ProxySG.
<i>Chapter 18 – Configuring the Upstream Networking Environment</i>	This chapter discusses how to control upstream interaction with the ProxySG.
<i>Chapter 19 – Access Logging</i>	Log formats, upload clients, upload schedules, and protocols are discussed in this chapter.
<i>Chapter 20 – Maintaining the ProxySG</i>	This chapter discusses upgrading the system and configuring event logs, SMNP, STMP, heartbeats, and core images.
<i>Chapter 21 – Statistics</i>	This chapter discusses viewing various kinds of statistics—system usage, efficiency, resources, and logs of all kinds.
<i>Appendix A – Using the Authentication/Authorization Agent</i>	The ProxySG NTLM agent is discussed in this appendix.
<i>Appendix B – Access Log Formats</i>	ELFF, SQUID, and NCSA/Common logs are discussed in this appendix.
<i>Appendix C – Using WCCP</i>	How to configure and use a WCCP router with the ProxySG is discussed in this appendix.
<i>Appendix D – RIP Commands</i>	Commands supported for the Routing Information Protocol (RIP) configuration text file are discussed in the appendix.
<i>Appendix E – Using Regular Expressions</i>	Regular expressions (regex) are explained in this appendix.
<i>Appendix F – Diagnostics</i>	Determining and resolving ProxySG problems are discussed in this appendix.
<i>Appendix G – Using Blue Coat Director to Manage Multiple ProxySG Appliances</i>	Discusses how Blue Coat Director works with multiple ProxySG Appliances.

Note: The *Blue Coat Configuration and Management Guide* and the *online help* contain the same information but are not identical. For the latest information, refer to the *Blue Coat Configuration and Management Guide*.

Related Blue Coat Documentation

- *Blue Coat 6000 and 7000 Installation Guide*
- *Blue Coat 400 Series Installation Guide*
- *Blue Coat 800 Series Installation Guide*
- *Blue Coat 8000 Series Installation Guide*
- *Blue Coat Content Policy Language Guide*
- *Blue Coat Command Line Interface Reference*

Document Conventions

The following section lists the typographical and Command Line Interface (CLI) syntax conventions used in this manual.

Table 1.2: Typographic Conventions

Conventions	Definition
<i>Italics</i>	The first use of a new or Blue Coat-proprietary term.
Courier font	Command line text that appears on your administrator workstation.
<i>Courier Italics</i>	A command line variable that is to be substituted with a literal name or value pertaining to the appropriate facet of your network system.
Courier Boldface	A ProxySG literal to be entered as shown.
{ }	One of the parameters enclosed within the braces must be supplied
[]	An optional parameter or parameters.
	Either the parameter before or after the pipe character can or must be selected, but not both.

Chapter 2: Licensing

This chapter describes the ProxySG licensing behavior.

About Licensing

SGOS 3.x introduces a global licensing system for the ProxySG. This system improves the correlation between deployed ProxySG appliances and allows for improved communication with Blue Coat Systems Customer Support.

In previous SGOS releases, licenses for features that required them were entered on the feature-specific panel in the Management Console. SGOS 3.x uses one global license key that includes licenses for whichever ProxySG features you have elected to use. Licenses are issued on a per-appliance basis.

Licensable Components

The following table lists the ProxySG licensable components.

Table 2.1: Licensable Components

Component	Description
SGOS 3	The ProxySG operating system, plus base features: HTTP, FTP, TCP-Tunnel, SOCKS, and DNS proxy.
SSL Termination	SSL Termination; includes an SSL termination card to be installed on the appliance.
3rd Party Onbox Content Filtering	Allows use with third-party vendor databases, such as Smartfilter, Websense, and SurfControl.
Websense Offbox Content Filtering	For Websense off-box support only.
ICAP Services	External virus and content scanning with ICAP servers.
AOL Instant Messaging	AIM proxy with policy support for AOL Instant Messenger.
MSN Instant Messaging	MSN proxy with policy support for MSN Instant Messenger.
Yahoo Instant Messaging	Yahoo proxy with policy support for Yahoo Instant Messenger.
Windows Media Streaming	Refer to "Streaming Licenses".
Real Media Streaming	Refer to "Streaming Licenses".
QuickTime Streaming	Refer to "Streaming Licenses".
Netegrity SiteMinder	Allows realm initialization and user authentication to SiteMinder servers.

Streaming Licenses

There are two types of Windows Media and Real Media licenses available, but only one QuickTime license type.

The following table describes each streaming media license type.

Table 2.2: Streaming Licenses Available

License Type	Description
Windows Media Standard	MMS proxy; no caching or splitting; content pass-through. Full policy control over MMS.
Windows Media Premium	MMS proxy; content caching and splitting. Full policy control over MMS. When the maximum concurrent streams is reached, all further streams are denied and the client receives a message.
Real Media Standard	RTSP proxy; no caching or splitting; content pass-through. Full policy control over RTSP.
Real Media Premium	RTSP proxy; content caching and splitting. Full policy control over RTSP. When the maximum concurrent streams is reached, all further streams are denied and the client receives a message.
QuickTime Basic	RTSP proxy; no caching or splitting; content pass-through. Full policy control over RTSP.

About the Trial Period

Blue Coat provides a trial period. For the first 60 days, all licensable components are active and available to use. The initial system boot-up triggers the 60-day trial, which is a grace period you can use to register the ProxySG and SGOS 3.x with Blue Coat.

Note: If you require more time to explore the ProxySG features, a demo license is available; refer to the Blue Coat product registration Web site.

Each time the Management Console home page or Maintenance>Licensing tab is clicked, a pop-up dialog appears warning the user that the trial period expires in so many days (a text message is displayed on a Telnet, SSH, or serial console).

The trial period streaming and IM licenses are no-count licenses—unlimited streams and IM clients are accessible.

Upon installing licenses after or during the trial period, Base SGOS, IM, Windows Media basic, and Real Media premium licenses are also unlimited, but Windows Media premium and IM licenses impose user limits established by each license type.

About License Expiration

At the end of the trial period or when any normally licensed component expires, components that have not been licensed do not process requests. A license expiration notification message is logged in the Event Log, and users are notified of the license expiration.

If a license expires, users might not be informed, depending upon the application they are using:

- HTTP (Web browsers)—An HTML page is displayed stating the ProxySG license has expired.

- Streaming media clients—if the Windows Media Player, RealPlayer, or QuickTime player version supports it, a message is displayed stating the ProxySG license has expired.
- Instant Messaging clients—Users do not receive a message that the ProxySG license has expired. Any IM activity is denied, and to the user it appears that the login connection has failed.
- FTP clients—if the FTP clients supports it, a message is displayed stating the ProxySG license has expired.

You can still perform ProxySG configuration tasks through the Management Console, CLI, SSH console, serial console, or Telnet connection. Although the component becomes disabled, feature configurations are *not* altered. Also, policy restrictions remain independent of component availability.

Installing a System License Key

This section describes how to register the ProxySG with Blue Coat and install the system license key.

System Serial Number Prerequisite

As each ProxySG serial number is the appliance identifier used to assign a license key, the serial number must be recognized before a license can be installed. If the ProxySG contains an EEPROM with the serial number encoded, the serial number is recognized upon system boot-up. If not, the serial number must be entered manually before a license can be installed.

To verify a serial number is defined:

- In the Management Console, navigate to Configuration>General>Identification. If a serial number exists in the Serial Number field, the ProxySG is ready to be registered and licensed.
- In the Management Console, navigate to Maintenance>Licensing>Install. If Request is active, a serial number has been entered or detected and the ProxySG is ready to be registered and licensed. If Request is greyed-out, a serial number must be entered.
- In the Management Console, navigate to Maintenance>Licensing>View. If a serial number has been entered or detected, it appears in the Hardware Serial Number line. If the line is blank, a serial number must be entered.

To enter a serial number, see "Configuring the Serial Number" on page 54.

Registering with Blue Coat

When your ProxySG was shipped from Blue Coat, a corresponding license key was created that licenses the system with the set of base and value-added software components. Before you can obtain this license, you must register the ProxySG and obtain a Blue Coat WebPower user account.

To Register with Blue Coat through the Management Console:

1. Select Maintenance>Licensing>Install.

In the License Administration field, click Register/Manage. A new window opens to the Blue Coat ProxySG Registration page.

2. Follow the instructions on this page to create a Blue Coat WebPower account user ID and password. Each created license is linked to the ProxySG by the serial number, and you are prompted to enter the serial number of each ProxySG you are registering.

This page allows you to manage all of your ProxySG licenses.

To Register with Blue Coat through the CLI:

Note: To request a license through the CLI, you must already have a WebPower user ID and password.

At the enable prompt, enter the following command:

```
SGOS# licensing request-key user_ID password
```

Downloading the License

After registering the ProxySG, you can download the license key. This is accomplished by using the automatic installation feature or by receiving the key through e-mail and manually installing it from a Web server or a local file.

Automatic License Installation

If the ProxySG has Internet access, you can use the automatic license installation feature to retrieve and install the license from Blue Coat.

To Automatically Obtain and Install the License:

1. Select Maintenance>Licensing>Install.
2. In the License Key Automatic Installation field, click Retrieve.

The Request License Key dialog appears.



Figure 2-1: Requesting a License

3. Enter your Blue Coat WebPower user ID and password. If you do not yet have a WebPower User ID, or have forgotten the password to your current account, click the appropriate link to take you to the relevant Blue Coat Systems Web page.
4. Click **Send Request**.
The ProxySG fetches the license associated with the serial number that is displayed.
5. The Installation Status field displays relevant information. When installation is complete, click **Results**; examine the results and click **OK**; click **Close**. The ProxySG is now licensed.

Manual License Installation

If the ProxySG does not have Internet access, Blue Coat can send you the license in an E-mail. The file can then be installed from a Web server or a local directory.

To Manually Obtain and Install the License:

1. Select **Maintenance>Licensing>Install**.
2. Click **Register/Manage**. A new window opens to the Blue Coat ProxySG Registration page. This Web page provides instructions for requesting that the license (associated to the ProxySG by the serial number) be sent through E-mail.
3. When the E-mail arrives, save the attached license file on a Web server or to a local file.
4. In the **License Key Manual Installation** field, select one of the following from the drop-list:
 - Remote URL**—If the file resides on a Web server.

The Install License Key dialog displays.



Figure 2-2: Installing a License from a Web Server

Enter the URL path and click **Install**. The **Installation Status** field displays relevant information. When installation is complete, click **Results**; examine the results and click **OK**; click **Close**.

- Local File**—If the file resides in a local directory.

The Upload and Install File window opens.

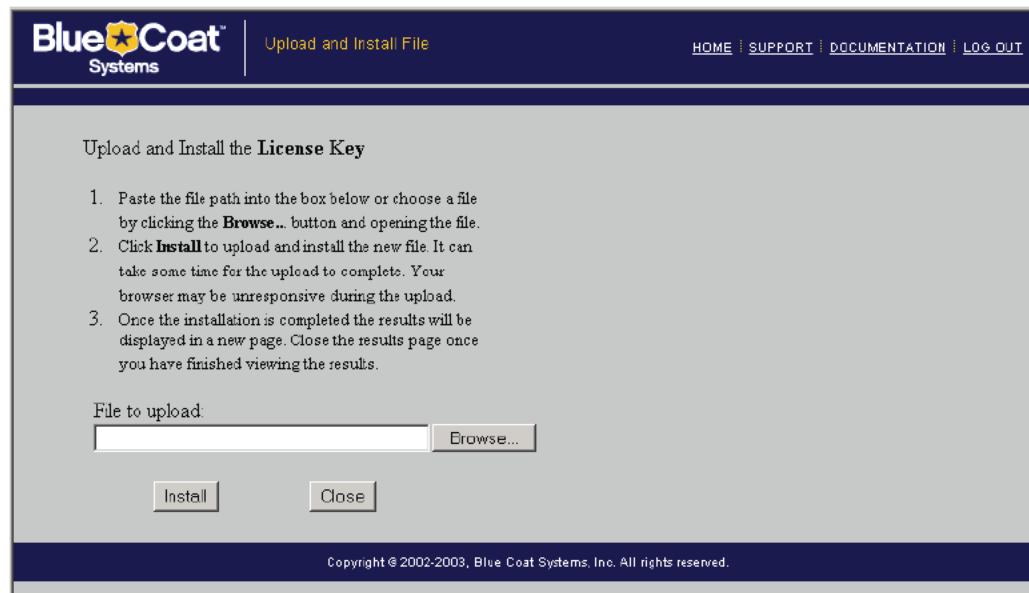


Figure 2-3: Uploading a License from a Local File

Enter a path to the license file or click Browse and navigate to the file. Click Install. A results window opens. Examine the license installation results; close the window. Click Close. Click Apply.

The ProxySG license is now installed. All features that you subscribed to are fully operational.

Viewing License Information

You can review the validity and expiration date of any licensed feature.

To View the License Information through the Management Console:

Select Maintenance>Licensing>View.

 A screenshot of a software interface titled 'View' under the 'Install' tab. The main area is titled 'Licensed Components' and contains a table with columns 'Component', 'Valid', and 'Expiration Date'. The table lists several components with their status and expiration dates. Below the table are buttons for 'View Details' and 'Refresh Data'. Another section titled 'General License Information' shows the 'Hardware serial number: 12345 (configured)' and 'Trial expiration date: 2004-05-01'. At the bottom of the screen are buttons for 'Apply', 'Cancel', and 'Help'.

Component	Valid	Expiration Date
SGOS 3	yes	2004-05-01
SSL Termination	yes	2004-05-01
3rd Party Onbox Content Filtering	yes	2004-05-01
WebSense Onbox Content Filtering	yes	2004-05-01
ICAP Services	yes	2004-05-01
AOL Instant Messaging	yes	2004-05-01

Figure 2-4: Viewing License Information

Each licensable component is listed, along with its validity state and its expiration date.

Note: To view the most current information, click Refresh Data.

You can also highlight a license component and click View Details. A dialog appears displaying more detailed information about that component. For example, a streaming component displays maximum number of streams allowed.

Updating a License

After the initial license installation, you might decide to use another feature that requires a license. For example, you currently support Windows Media, but want to add Real Media support. The license must be updated to allow this support.

To Update a License through the Management Console:

1. Select Maintenance>Licensing>Install.
2. Click Register/Manage.
3. Follow the instructions on the Blue Coat Registration page.
4. If using the automatic license installation feature, click Update; otherwise, manually install the license as described in "Manual License Installation" on page 35.

To Update a License through the CLI:

At the enable prompt, enter the following command:

```
SGOS# licensing update-key
```

Automatically Updating a License

The license automatic update feature allows the ProxySG to contact the Blue Coat licensing Web page 31 days before the license is to expire. If a new license has been purchased and authorized, the license is automatically downloaded. The ProxySG continues to contact the Web site up to 30 days after the license is set to expire. Outside the above license expiration window, the ProxySG performs this connection once every 30 days to check for new license authorizations. This feature is enabled by default.

To Configure the License Auto-Update Feature through the Management Console:

1. Select Maintenance>Licensing>Install.
2. Select or deselect Use Auto-Update.
3. Click Apply.

To Configure the License Auto-Update Feature through the CLI:

At the (config) prompt, enter the following command:

```
SGOS# (config) license-key path url
SGOS# (config) license-key auto-update {enable | disable}
```

Note: If the automatic license update fails and you receive a Load from Blue Coat error, you must login to your License Management account:
https://services.bluecoat.com/eservice_enu/licensing/mgr.cgi. Click Update License Key.

Chapter 3: Accessing the ProxySG

The Blue Coat Systems ProxySG uses the Secure Shell (SSH) and HTTPS protocols to securely access the ProxySG CLI and Management Console. Both SSHv1 and SSHv2 are enabled by default, and host keys have already been created on the ProxySG.

All data transmitted between the client and the ProxySG using SSH/HTTPS is encrypted.

During initial configuration, you assigned the ProxySG a username and password and a privilege mode (enable/configuration) password. These passwords are always stored and displayed hashed.

This chapter discusses:

- "Before You Begin: Understanding Modes"
- "Accessing the ProxySG"
- "Management Console Home Page"
- "Changing the Login Parameters"
- "Configuring the SSH Console"

Important: This chapter assumes that you have completed the first-time setup of the ProxySG using either the front panel or serial console, and that the appliance is running on the network. These steps must be completed before accessing the appliance.

You can manage the ProxySG by logging into and using one of the following:

- An SSH session to access the CLI.
- The Management Console graphical interface.

You can also use a serial console to access the CLI.

Note: To use a Telnet session, you must use a serial console connection until you have configured Telnet for use. (For security reasons Blue Coat does not recommend using Telnet).

Before You Begin: Understanding Modes

SGOS 3.x supports different levels of command security:

- Standard, or unprivileged, mode is read-only. You can see but not change system settings and configurations. This is the level entered when you first access the CLI.
- Enabled, or privileged, mode is read-write. You can make immediate but not permanent changes to the ProxySG, such as restarting the box. This is the level entered when you first access the Management Console.
- Configuration is a mode within the enabled mode. From this level, you perform permanent changes to the ProxySG configuration.

If you use the Management Console, you are in configuration mode when you are completely logged into the system.

If you use the CLI, you must enter each level separately:

```
Username: admin
Password:
SGOS> enable
Enable Password:
SGOS# configure terminal
Enter configuration commands, one per line. End with CTRL-Z.
SGOS# (config)
```

For detailed information about the CLI and the CLI commands, refer to the *Blue Coat Command Line Interface Reference*.

Note: Although most administrator tasks can be performed using either the Management Console or the CLI, there is the occasional task that can only be done using one of the two: these are specified in the manual.

Accessing the ProxySG

You can access the ProxySG through either the CLI or the Management Console. By default, SSHv2 (CLI) and HTTPS (Management Console) are used to connect to the appliance.

The SSH and HTTPS ports are configured and enabled. For SSH, you can use either version 1 or version 2 (with password or RSA client key authentication).

Accessing the CLI

If you use the CLI, you can use SSHv2 to access the ProxySG, but you cannot use SSHv1 or Telnet without additional configuration.

Note: Enabling the Telnet-Console introduces a security risk, so it is not recommended.

To use SSHv1, you must first create a SSHv1 host key. For more information on creating SSH host keys, see "Configuring the SSH Console" on page 47.

To login to the CLI, you must have:

- the account name that has been established on the ProxySG
- the IP address of the ProxySG
- the port number (8082 is the default port number)

You must login from your SSH client.

Accessing the Management Console

The Management Console is a graphical Web interface that allows you to manage, configure, monitor, and upgrade the ProxySG from any location.

In the Web browser, enter HTTPS, the ProxySG IP address, and port 8082 (the default management port). For example, if the IP address configured during first-time installation is 10.25.36.47, enter the URL <https://10.25.36.47:8082> in the Web browser.

The Management Console consists of a set of Web pages and Java applets stored on the ProxySG. The appliance acts as a Web server on the management port to serve these pages and applets. From the ProxySG home page on the appliance, you can access the management applets, statistics applets, and documentation. The Management Console is supported with a complete online help facility to assist you in defining the various configuration options.

Management Console Home Page

When you access the Management Console home page (see "Accessing the Management Console" on page 40), you are prompted to log into the box.

Logging In

Each time you access the Management Console, you must log in.



Figure 3-1: Login Dialog

- The **Site** is the IP address of the ProxySG you are logging into.
- The **Realm** is a configurable name that can be anything you choose. The ProxySG IP address is the default. For more information on configuring the realm name, see "Changing the ProxySG Realm Name" on page 45.
- The **User Name** is the name of the account you are using on this ProxySG. The name must already exist. It cannot be created here.
- The **Password** is the password for the account you are using. It cannot be changed here.

You can change the username and password for the console through the Management Console or the CLI. See "Changing the Login Parameters" on page 42.

Note: All successful and failed login attempts are logged to the ProxySG event log.

Logging Out

Once you have logged in, you do not have to log in again unless you exit the current session or if the session times out. The session timeout period, with a default of 900 seconds (15 minutes), is configurable.

Thirty seconds before the session times out, a warning dialog displays. Click the **Keep Working** button or the X in the upper-right-corner of the dialog box to keep the session alive.

Note: The **Keep Working** button saves your changes to the current applet. You cannot work in other applets without logging back into the ProxySG.

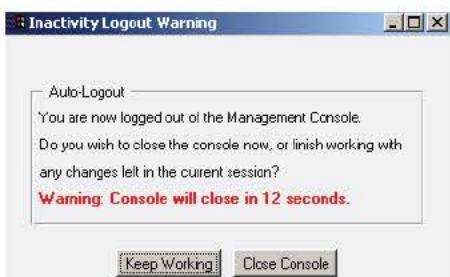


Figure 3-2: Automatic Logout Warning

If you do not click **Keep Working** or the X in the upper-right-hand corner within the thirty-second period, you are logged out. You must log back in to access the Management Console.

You have logged out. Please close the browser window.

[You need to log in again to use the console](#)

Figure 3-3: Logout Dialog

Click the hyperlink to log back into the ProxySG.

Note: If no applet is running when the session times out (you are on the Management Console home page), you are logged out without seeing the logout warning dialog. You might not be aware that you are logged out until you try to access an applet. You must enter the login information again.

Changing the Login Parameters

You can change the console username and password, the console realm name (which displays when you log into the ProxySG), and the auto-logout timeout (in seconds; the default is 900 seconds.)

The Management Console requires a valid administrator username and password to have full read-write access; you do not need to enter a privileged-mode password as you do when using the CLI. A privileged-mode password, however, must already be set.

Note: To prevent unauthorized access to the ProxySG, only give the console username and password to those who administer the ProxySG.

Changing the Username and Password through the Management Console

You can change either the username or the password without changing both.

Changing the Username through the Management Console

The console account username was assigned during initial setup of the system. You can change the username at any time.

To Change the Username through the Management Console:

1. Select Configuration>Authentication>Console Access>Console Account.

The Console Account tab displays.

Figure 3-4: Console Account Tab

Note: Changing the Console Account username or password change causes the Management Console to refresh and log back in using the new information. Note that each parameter must be changed and a refresh done individually. You cannot change both parameters at the same time.

2. Enter the username of the administrator or administrator group who is authorized to view and revise console properties.

Only one console account exists on the ProxySG. If you change the console account username, that username overwrites the existing console account username.

The console account username can be changed to anything that is not null and contains no more than 64 characters.

3. Click Apply.

After clicking Apply, an Unable to Update configuration error is displayed. The username change was successfully applied, but the configuration could not be fetched from the ProxySG, as the username offered in the fetch request is still the old username.

4. Refresh the screen. You are then challenged for the new username.

To Change the Password through the Management Console:

The console password and privileged mode password were defined during initial configuration of the system. The console password can be changed at any time through the Management Console. The privileged mode, or enable mode, password can only be changed through the CLI or the serial console.

1. Select Configuration>Authentication>Console Access>Console Account.

The Console Account tab displays.

2. Click Change Password.



Figure 3-5: Setting or Changing a Password

3. Enter and re-enter the console password that is used to view and edit configuration information. The password must be from 1 to 64 characters long. As you enter the new password, it is obscured with asterisks. Click OK.

Note: This does not change the enable password. You can only change the enable password through the CLI.

4. Refresh the screen, which forces the ProxySG to re-evaluate current settings. When challenged, enter the new password.
5. (Optional) Restrict access by creating an access control list or by creating a policy file containing <Admin> layer rules. For more information, see "Moderate Security: Restricting Management Console Access Through the Console Access Control List" on page 210.

Changing the Username and Password through the CLI

To Change the Console Account Username or Password, Privileged-Mode Password, and the Front-Panel PIN through the CLI:

1. Open a terminal session with the ProxySG and enter the current username and password as prompted.

2. At the command prompt, enter the following command:

```
SGOS>enable
```

3. Enter the privileged mode password when prompted.

4. At the command prompt, enter the following commands (note that usernames and passwords can each be from 1 to 64 characters in length):

```
SGOS#configure terminal  
SGOS#(config) security username username
```

This command specifies the administrator username.

```
SGOS#(config) security password password  
-or-  
SGOS#(config) security hashed-password hashed_password
```

These commands specify the administrator console password.

```
SGOS#(config) security enable-password password  
-or-  
SGOS#(config) security hashed-enable-password hashed_password
```

Specifies the administrator privileged mode password. The ProxySG hashes the password if you enter it in clear text.

5. (Optional, for maximum security. Note that these commands are not available if the ProxySG does not have a front panel.) At the command prompt, change the ProxySG front panel PIN:

```
SGOS#(config) security front-panel-pin pin  
-or-  
SGOS#(config) security hashed-front-panel-pin hashed-pin
```

6. (Optional) Restrict access by creating an access control list or by creating a policy file containing <Admin> layer rules. For more information, see "Section A: Controlling Access to the ProxySG".

Changing the ProxySG Realm Name

The realm name displays when you log in to the ProxySG Management Console. The default realm name is the connection used to access the ProxySG, usually the IP address of the system.

To Change the Realm Name through the Management Console:

1. Select Configuration>Authentication>Console Access>Console Account.

The Console Account tab displays.

2. Enter a new realm name.

The new realm name displays the next time you log into the ProxySG Management Console.

3. Click Apply.

To Change the Realm Name through the CLI:

1. At the (config) prompt, enter the following command to change the name from the default.

```
SGOS#(config) security management display-realm name
```

The new realm name displays the next time you log into the ProxySG Management Console.

2. (Optional) View the results. As the `show security` command displays lengthy output, only the relevant section is displayed in the following example:

```
SGOS#(config) show security
Account:
  Username:           "admin"
  Hashed Password:   $1$aWMpN$/dsvVrZK6R68KH8r2SQxt/
  Hashed Enable Password: $1$P4lpm$ZqFXg4J4A/T.ORgUbr0B/1
  Hashed Front Panel PIN: "$1$GGsf2$1EhLm9oITgny9PDF2kVfp."
  Management console display realm name: ""
  Management console auto-logout timeout: Never
```

You can negate the `security management display-realm` values by entering `no` before the command; for example, `security management no display-realm`.

Changing the ProxySG Timeout

The timeout is the length of time a session persists before you are logged out. The default timeout is 900 seconds (15 minutes).

To Change the Timeout through the Management Console:

1. Select Configuration>Authentication>Console Access>Console Account.

The Console Account tab displays.

2. Either deselect Enforce auto-logout (which eliminates auto-logout entirely) or change the auto-logout timeout from its default of 900 seconds (15 minutes) to another time (in seconds). This is the allowable time on the ProxySG before the current session times out. Acceptable values are between 300 and 86400 seconds (5 minutes to 24 hours).

If you change the timeout value, the change takes effect on the next refresh of any applet on the Management Console.

3. Click **Apply**.

To Change the Timeout through the CLI:

1. To change the timeout from its default of 900 seconds (15 minutes), enter:

```
SGOS#(config) security management auto-logout-timeout seconds
```

The change takes effect on the next refresh of any applet in the Management Console. Acceptable values are between 300 and 86400 seconds (5 minutes to 24 hours).

2. (Optional) View the results. As the `show security` command displays lengthy output, only the relevant section is displayed in the following example:

```
SGOS# (config) show security
Account:
  Username:           "admin"
  Hashed Password:   $1$a2zT1EE$1b88R3SXUTXS.zO7lh8db0
  Hashed Enable Password: $1$xQnqGerX$LU65b20trsIAF6yJox26L.
  Hashed Front Panel PIN: "$1$ThSEiB1v$seyBhSxtTXEtUGDZ5NOB1/"
  Management console display realm name: "Aurora"
  Management console auto-logout timeout: Never
```

You can negate the security management auto-logout-timeout values by entering `no` before the command; for example, `security management no auto-logout-timeout`.

Configuring the SSH Console

By default, the ProxySG uses Secure Shell (SSH) and password authentication so administrators can access the ProxySG CLI or Management Console securely. SSH is a protocol for secure remote login over an insecure network. No action is required unless you want to change the existing SSH host key, disable a version of SSH, or import RSA host keys. Only one SSH service is allowed on the ProxySG.

To disable the SSH port, see "Managing the SSH Host Connection" below.

Managing the SSH Host Connection

You can manage the SSH host connection through either the Management Console or the CLI.

To Manage the SSH Connection through the Management Console:

Note: Only one SSH Console can be enabled at a time. By default, both SSHv1 and SSHv2 are enabled and assigned to port 22. You do not need to create a new host key unless you want to change the existing configuration.

1. Select Configuration>Services>SSH Console>SSH Host.

The SSH Host tab displays.

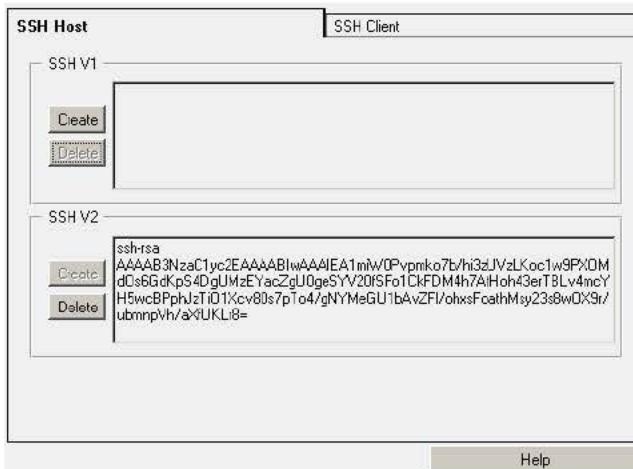


Figure 3-6: SSH Host Tab

2. To delete either SSHv1 or SSHv2 support on the ProxySG, click the appropriate Delete button. The change is made on the ProxySG instantly.

Important: Do not delete both versions. This disables the SSH Console. Even if you add SSH v1 or SSH v2 client keys back, you will have to enable the service through Configuration>Services>Service Ports.

The SSH host tab redisplays with the appropriate host key deleted.

3. To add SSH v1 or v2 support, select the Create checkbox for the version you want. Remember that if both versions are deleted, you must re-enable the SSH service on port 22.
4. The SSH host key displays in the appropriate pane.

To Manage SSH Host Keys through the CLI:

Note: Only one SSH Console can be enabled at a time. By default, both SSHv1 and SSHv2 are enabled and set up on port 22. You do not need to create a new host key unless you want to change the existing configuration. In fact, you cannot create a new host key unless you delete one of the existing client keys.

You must set up RSA client keys to connect to the ProxySG using RSA. To set up RSA client keys, see "Managing the SSH Client" below.

1. From the (config) prompt of the ProxySG, enter the following commands to create a host key.

```
SGOS# (config) services
SGOS# (config services) ssh-console
SGOS# (config services ssh-console) create host-keypair {[sshv1] | [sshv2]}
```

The client key, either SSHv1 or SSHv2 or both, is created, depending on which client key was previously deleted.

2. (Optional) View the results.

```
SGOS# (config services ssh-console) view host-public-key { [sshv1] | [sshv2] }
1024 35
190118975106704546356706163851813093052627858203406609264841510464285480824
068799445880489701889675368436600545643174140823440610328520806007156774811
989754027101280816905716431491183274963949027032871437205903863441301419664
1366408168414061584835486361481236628643756053169543839452802141370496747163
3977037

ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEA2rSeDb3vrh78AFmd7TbdtsiYfUQybaDxdMBbSLuyJVgwVbq+
tIVs4L6kDsTuFYGVR8Cg74Xqsj2k06iwo71YGwdUnDXEzIFBwl0nvS4LkV2UINUwbuP0R0hD4Dt
jVTKsURr0HbTxckFipplDwFPDiCKOIQLm4ypcaC/Pj+Juq0=
```

3. To disable SSH, enter:

```
SGOS# (config services ssh-console) delete host-keypair { [sshv1] | [sshv2] }
```

Deleting both of the client keys disables the SSH service on port 22, which then must be re-enabled before you can use SSH Console services again, even if you re-create the host keys.

Managing the SSH Client

You can have multiple RSA client keys on the ProxySG to allow for actions such as logging into the ProxySG from different locations. You cannot create an RSA client key through the appliance, only through an SSH client. Many SSH clients are commercially available for UNIX and Windows.

Once you have created an RSA client key following the instructions of your SSH client, you can import the key onto the ProxySG using either the Management Console or the CLI.

Understanding Open SSH.pub format

Blue Coat supports the OpenSSH.pub format. Keys created in other formats will not work.

An OpenSSH.pub public key is similar to the following:

```
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAwFI78MKyvL8DrFgcVxpNRHMFKJrBMeBn2PKcv5oAJ2qz+uZ7
hiv7Zn43A6hXwY+DekhtNLOk3HCWmgsrDBE/NOOEnDpLQjBC6t/T3cSQKZjh3NmBbpE4U49rPdu
iiufvWkuoEiHUb5ylzRGdXRSNJHxxmg5LiGEiKaoELJfsDMc= user@machine
```

One of the public key format examples (this one created by the SSH client) is similar to the following:

```
---- BEGIN SSH2 PUBLIC KEY ----
Comment: "[1024-bit rsa, user.name@machine, Wed Feb 19 2003 19:2\8:09]"
AAAAB3NzaC1yc2EAAAADAQABAAAQgQCw52JeWr6Fv4kLkzbPZePvapCpaTadPYQwqsGnCIYdf1We7/8336EmzV918G1jb/VT1SI1tM1Ku1BTal7uWAi+aUBGKL1YuyhCTo03IZFMnsQC7QYzY1y3ju
fUP3H0be52fg7n7p7gNZR11yzWhVeilvIKiyVKpjqiq6hxCbMb2Q==
---- END SSH2 PUBLIC KEY ----
```

The OpenSSH.pub format appends a <space> and a user ID to the end of the client key.

The user ID for the key must be unique. Because the ProxySG manages the keys through the user, no two can be the same.

Other caveats:

- 1024 bits is the maximum supported key size.
- An "ssh-rsa" prefix must be present.
- Trailing newline characters must be removed from the key before it is imported.

To Import RSA Client Keys through the Management Console:

1. From your SSH client, create a client key and copy it to the clipboard.

Note: The above step must be done with your SSH client. The ProxySG cannot create client keys.

2. Select Configuration>Services>SSH Console>SSH Client.

The SSH Client tab displays.

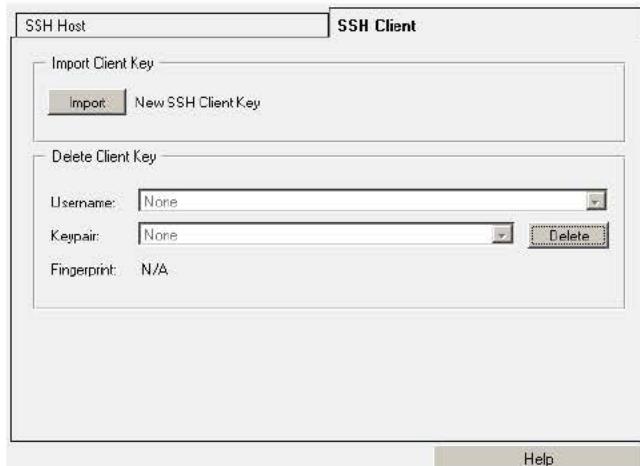


Figure 3-7: SSH Client Tab

3. Click Import to import a new host key.

The Import Client Key dialog displays.

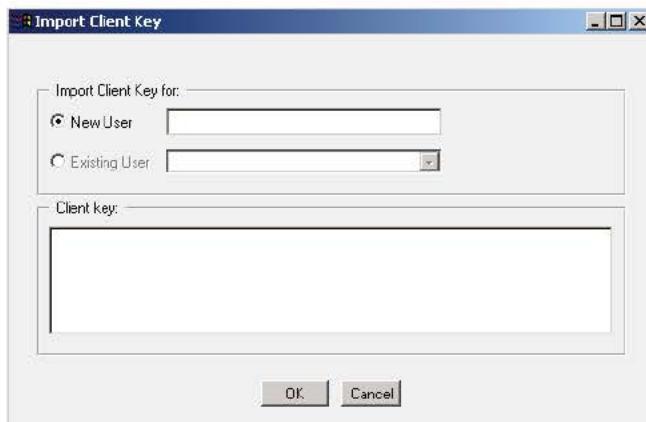


Figure 3-8: Import Client Key Dialog

4. Specify whether the client key is associated with an existing user or a new user, and enter the name.
5. Paste the RSA key that you previously created with an SSH client into the Client key field. Ensure that a key ID is included at the end. Otherwise, the import fails.
6. Click OK.

The SSH Client tab reappears, with the fingerprint of the imported key displayed.

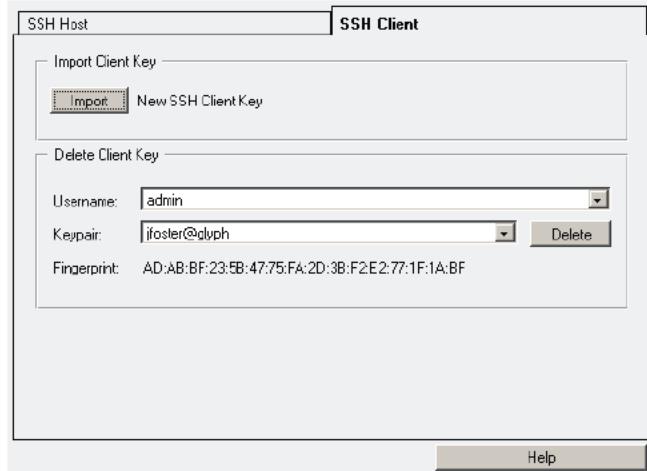


Figure 3-9: SSH Client with Imported Client Key

To Import a Client Key through the CLI:

1. From your SSH client, create a client key and copy it to the clipboard.
2. From the (config) prompt, enter the following commands to import a client key.

```
SGOS#(config) services
SGOS#(config services) ssh-console
SGOS#(config ssh-console) import client-key user_name
Paste client key here, end with "..." (three periods)
ssh-rsaAAAAB3NzaC1yc2EAAAABIwAAAIEAtAy+axsx0iwroFN7B9qSJYjfVbsxPfyC0aoZpSMBd
g97/oiFozDXPhrRmPI3c42EiVdJtVo65r0Aerpu4ybCYVeq6MjRwdsszaezY+VdqtfyYVptC6V1
7Pmj2erw4+A9AggKHTp56BBCm3mEPQDdVW7J6QBrJ+U1C1FS/sMcBV8= laptop@GLYPH
...
ok
```

3. (Optional) View the results.

```
SGOS#(config services ssh-console) view client-key username
user_ID@PC 45:5C:3F:5F:EA:65:6E:CF:EE:4A:05:58:9A:C5:FB:4F
user_ID@LAPTOP 61:ED:79:23:F5:2A:1A:6D:84:81:A0:5B:25:36:C7:5F
```


Chapter 4: Configuring the System

This chapter describes how to configure various ProxySG system configurations, such as setting the time, configuring adapters, and creating software bridges.

This chapter contains the following topics:

- "Global Configurations"
- "Archive Configuration"
- "Adapters"
- "Software and Hardware Bridges"
- "Gateways"
- "Defining Static Routes"
- "Using RIP"
- "DNS"
- "Attack Detection"
- "Installing WCCP Settings"
- "Virtual IP Addresses"
- "Configuring Failover"
- "TCP-IP Configuration"

During initial configuration, Interface 0 was configured by default. The NTP server was defined to keep the system time correct. You also optionally configured a bridge, a gateway, and a DNS server.

These configurations require no further modification. These procedures are provided if you need to configure other adapters in the system or if the need to change a configuration occurs.

Global Configurations

The ProxySG global configurations include: defining the ProxySG name and serial number, setting the time, and configuring NTP for your environment.

Configuring the ProxySG Name

You can assign any name to a ProxySG. A descriptive name helps identify the system.

To Set the ProxySG Name through the Management Console:

1. Select Configuration>General>Identification.

The General tab displays.

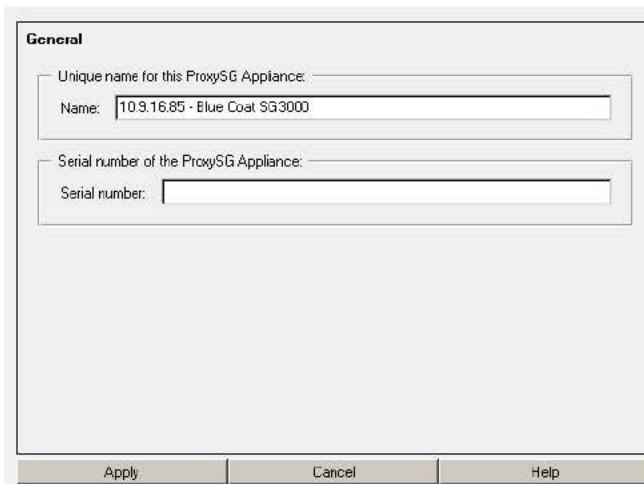


Figure 4-1: General Identification Tab

2. In the Unique name for this ProxySG Appliance field, enter a ProxySG name.
3. Click Apply.

To Set the ProxySG Name through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) hostname name
```

Configuring the Serial Number

The ProxySG serial number assists Blue Coat Systems Customer Support when analyzing configuration information, including heartbeat reports. This number is found on the ProxySG. Once the serial number is entered, the ProxySG does not verify the validity of the number, only that it is numeric.

Note: If the EPROM contains the ProxySG serial number, you cannot manually enter a serial number.

To Enter the Serial Number through the Management Console:

1. Select Configuration>General>Identification.
2. The General tab displays.
3. In the Serial Number field, enter the serial number.
4. Click Apply.

To Enter the Serial Number through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) serial-number serial_number
```

Displayed Information

The serial number is visible on the Management Console home page, and is displayed using the `show serial-number` command. If the serial number was entered through the Management Console or the CLI, it is appended with `(configured)` to indicate a manual entry.

Configuring the System Time

To manage objects, the ProxySG must know the current Universal Time Coordinates (UTC) time, which is the international time standard and is based on a 24-hour clock.

By default, the ProxySG attempts to connect to an NTP server to acquire the UTC time. The Appliance ships with a list of NTP servers available on the Internet, and attempts to connect to them in the order they appear in the NTP server list on the NTP tab. If the Appliance cannot access any of the listed NTP servers, you must manually set the UTC time.

To Set UTC Time through the Management Console:

1. Select Configuration>General>Clock>Clock.

The Clock tab displays.

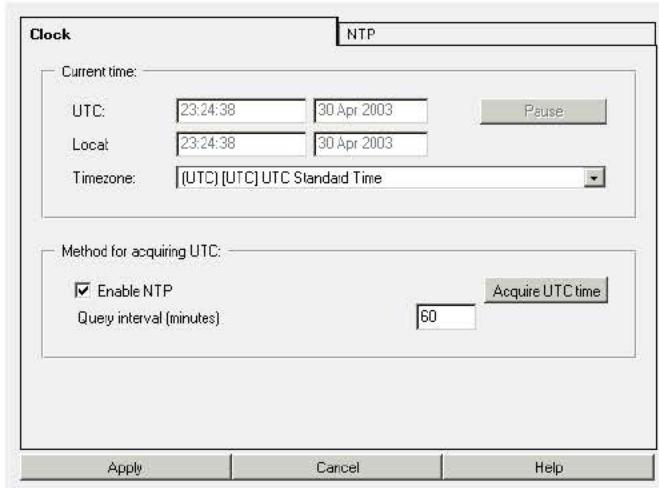


Figure 4-2: General Clock Tab

2. Verify that **Enable NTP** is selected.
3. To set your local time, select a time zone from the **Timezone** drop-down list.

Once the local time zone is selected, event logs record the local time instead of GMT.

4. Click **Acquire UTC time**.
5. Click **Apply**.

To Set UTC Time through the CLI:

At the enable prompt, enter the following command:

```
SGOS# acquire-utc
```

If NTP is disabled, an error is displayed.

To Manually Set UTC Time through the Management Console:

1. Select Configuration>General>Clock>Clock.

The Clock tab displays.

2. De-select Enable NTP.

The UTC time and date fields become editable when NTP is disabled.

3. To set your local time, select a time zone from the Timezone drop-down list.

Once the local time zone is selected, event and access logs record the local time instead of GMT.

4. Click Pause in the upper-right-hand corner to stop the system clock.

5. Enter the current UTC time and date in the UTC time and date fields.

6. Click Resume to start the system clock.

7. Click Apply.

To Manually Set UTC Time through the CLI:

1. At the (config) command prompt, enter the following commands

```
SGOS# (config) clock day 1-31
SGOS# (config) clock hour 0-23
SGOS# (config) clock minute 0-59
SGOS# (config) clock month 1-12
SGOS# (config) clock second 0-59
SGOS# (config) clock year year
```

2. (Optional) View the results.

```
SGOS# (config) show clock
2003-08-28 22:50:56+00:00UTC
2003-08-28 22:50:56+00:00UTC
```

Network Time Protocol

The Network Time Protocol (NTP) is used to synchronize the time of a computer client or server to another server or reference time source, such as a radio or satellite receiver or modem. There are more than 230 primary time servers, synchronized by radio, satellite and modem.

The ProxySG ships a list of NTP servers available on the Internet, and attempts to connect to them in the order they appear in the NTP server list on the NTP tab. You can add others, delete NTP servers, and reorder the NTP server list to give a specific NTP server priority over others.

The ProxySG uses NTP and the Universal Time Coordinates (UTC) to keep the system time accurate.

You can add and reorder the list of NTP servers the ProxySG uses for acquiring the time through the Management Console. The reorder feature is not available through the CLI.

To Add an NTP Server through the Management Console:

1. Select Configuration>General>Clock>NTP.

The NTP tab displays.



Figure 4-3: General Clock NTP Tab

2. Click New to add a new server to the list.
3. Enter either the domain name or IP address of the NTP server and click OK.
4. Click Apply.

To Add an NTP Server through the CLI:

1. At the (config) command prompt, enter:

```
SGOS#(config) ntp server domain_name
SGOS#(config) ntp interval minutes
SGOS#(config) ntp enable
```

2. (Optional) View the results.

```
SGOS#(config) show ntp
NTP is enabled
NTP servers:
  ntp.bluecoat.com
  ntp2.bluecoat.com
Query NTP server every 60 minutes
```

3. To remove a server from the NTP server list:

```
SGOS#(config) ntp no server domain_name
```

To Change the Access Order through the Management Console:

NTP servers are accessed in the order displayed. You can organize the list of servers so the preferred server appears at the top of the list. This feature is not available through the CLI.

1. Select Configuration>General>Clock>NTP.

The NTP tab displays.

2. Select an NTP server to promote or demote.
3. Click Promote entry or Demote entry as appropriate.
4. Click Apply.

Configuring HTTP Timeout

You can configure various network receive timeout settings for HTTP transactions. You can also configure the maximum time that the HTTP proxy will wait before reusing a client-side or server-side persistent connection. You must use the CLI to configure these settings.

To Configure the HTTP Receive Timeout Setting through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) http receive-timeout {client | refresh | server} #_seconds
```

where:

client	#_seconds	Sets the receive timeout for client to #_seconds. The default is 120 seconds.
refresh	#_seconds	Sets receive timeout for refresh to #_seconds. The default is 90 seconds.
server	#_seconds	Sets receive timeout for server to #_seconds. The default is 180 seconds.

To Configure the HTTP Persistent Timeout Setting through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) http persistent-timeout {client | server} #_seconds
```

where:

client	#_seconds	The maximum amount of time the HTTP proxy waits before closing the persistent client connection if another request is not made. The default is 360 seconds.
server	#_seconds	The maximum amount of time the HTTP proxy waits before closing the persistent server connection if that connection is not re-used for any subsequent request from the proxy. The default is 900 seconds.

Archive Configuration

Blue Coat allows you to both use an existing configuration (modified to include only general parameters, not system-specific settings) to quickly set up a newly-manufactured ProxySG and to save the running configuration off-box for archival purposes.

To share configurations among systems, continue with the next section; to archive a configuration for later use, skip to "Archiving a Configuration" on page 62.

Sharing Configurations

You can share configuration between two ProxySG Appliances. You can take a *post-setup* configuration file (one that does not include those configuration elements that are established in the setup console) from an already-configured ProxySG and push it to a newly-manufactured system.

Note: Blue Coat Director allows you to push configuration from one ProxySG to multiple ProxySG Appliances at the same time. For more information on using Director, see Appendix G: "Using Blue Coat Director to Manage Multiple Appliances" on page 849.

The new configuration is applied to the existing configuration, changing any existing values. This means, for instance, that if the new configuration creates a realm called *RealmA* and the existing configuration has a realm called *RealmB*, the combined configuration includes two realms, *RealmA* and *RealmB*.

You can use either the Management Console or the CLI to create a post-setup configuration file on one ProxySG and push it to another.

Note: You cannot push configuration settings to a newly manufactured system until you have completed initial setup of the system.

To Create and Push a Configuration to a Newly-Manufactured ProxySG through the Management Console:

From the already configured ProxySG:

1. Select Configuration>General>Archive.

The Archive Configuration tab displays.

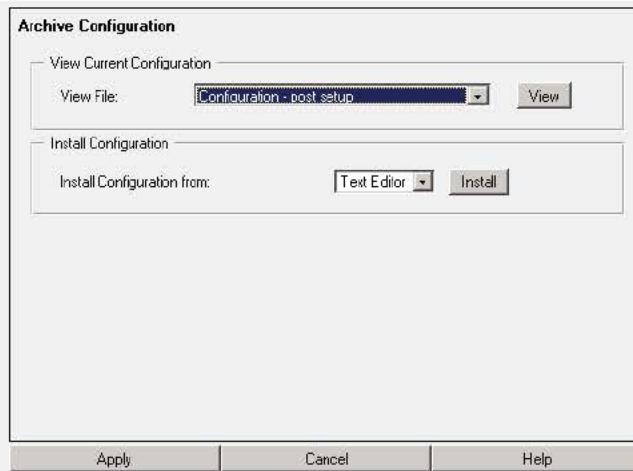


Figure 4-4: Archive Configuration Tab

2. In the View Current Configuration panel, select the configuration from the drop-down list that you want to use for the newly-manufactured machine:
 - Configuration - post setup: This displays the configuration on the current system, minus any configurations created through the setup console, such as the hostname and IP address. It also includes the installable lists.
 - Configuration - brief: This displays the configuration on the current system, but does not include the installable lists.
 - Configuration - expanded: This is the most complete snapshot of the system configuration, but it contains system-specific settings that should not be pushed to a new system.
 - Results of Configuration Load: This displays the results of the last configuration pushed to the system.
3. View the configuration you selected by clicking View. You can also view the file by selecting Text Editor in the Install Configuration panel and clicking Install.
4. Save the configuration. You can save the file two ways:
 - Save it as a text file on your local system. This is advised if you want to re-use the file.
 - Copy the contents of the configuration. (You will paste the file into the Text Editor on the newly manufactured system.)

From the newly manufactured ProxySG:

1. Launch the Management Console in a new browser window.

2. Select Configuration>General>Archive.
3. The Archive Configuration tab displays.
4. In the Install Configuration panel, select either Local File or Text Editor from the drop-down list (depending on whether you saved the file to your system or just copied it to the clipboard) and click Install.
 - If you saved the file to your system, browse to the location of the Local File, highlight the file, and click Install. The configuration is installed, and the results screen displays.
 - If you copied the contents of the file, paste it into the Text Editor and click Install. The configuration is installed, and the results screen displays.
5. Click Close.

To Create and Push a Configuration to a Newly-Manufactured ProxySG through the CLI:

From the already configured ProxySG:

1. From the enable prompt (#), determine which configuration you want to use for the new system:

```
SGOS# show configuration {post-setup | brief | expanded}
```

where:

post-setup	This displays the configuration on the current system, minus any configurations created through the setup console, such as the hostname and IP address. It also includes the installable lists.
brief	This displays the configuration on the current system, but does not include the installable lists.
expanded	This is the most complete snapshot of the system configuration, but it contains system-specific settings that should not be pushed to a new system.

The selected configuration displays on the screen.

2. Save the configuration. You can save the file two ways:

- Copy the contents of the configuration to the clipboard. (You will paste the file into the terminal on the newly-manufactured system.)
- Save it as a text file on a download FTP server accessible to the ProxySG. This is advised if you want to re-use the file.

From the newly manufactured ProxySG, do one of the following:

- If you saved the configuration to the clipboard, go to the (config) prompt and paste the configuration into the terminal.
- If you saved the configuration on the FTP server:

At the enable command prompt, enter the following command:

```
SGOS# configure network "url"
```

where *url* must be in quotes and is fully-qualified (including the protocol, server name or IP address, path, and filename of the configuration file). The configuration file is downloaded from the server, and the ProxySG settings are updated.

Note: If you rename the archived configuration file so that it does not contain any spaces, the quotes surrounding the URL are unnecessary.

The username and password used to connect to the FTP server can be embedded into the URL. The format of the URL is:

`ftp://username:password@ftp-server`

where *ftp-server* is either the IP address or the DNS resolvable hostname of the FTP server.

If you do not specify a username and password, the ProxySG assumes that an anonymous FTP is desired and thus sends the following as the credentials to connect to the FTP server:

`username: anonymous
password: proxy@`

Archiving a Configuration

In the rare case of a complete system failure, restoring a ProxySG to its previous state is simplified by loading an archived system configuration from an FTP or TFTP server. The archive, taken from the running configuration, contains all system settings differing from system defaults, along with any installable lists configured on the ProxySG.

Archive and restore operations must be done through the CLI.

Note: You can archive a system configuration to an FTP or TFTP server that allows either anonymous login or requires a specific username and password. Likewise, to restore a system configuration, the server storing the archive can be configured either to allow anonymous login or to require a username and password.

Preparing to Archive a System Configuration

1. Obtain write permission to a directory on an FTP server. This is where the archive will be stored.

The system configuration must be stored using FTP.

2. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) archive-configuration protocol {ftp | tftp}  
SGOS#(config) archive-configuration host host_name
```

where *host_name* is the IP address of the server.

Note: TFTP does not require a password, path, or username.

```
SGOS# (config) archive-configuration password password
-or-
SGOS# (config) archive-configuration encrypted-password encrypted-password
where password is the password (or encrypted password) used to access the server.

SGOS# (config) archive-configuration path path
where path is the directory on the server where the archive is to be stored, relative to the
preset FTP directory.

SGOS# (config) archive-configuration filename-prefix filename
where filename can contain % strings that represent the information in the upload filename.
If you do not use the filename command, the ProxySG creates a name with a timestamp and
the filename SG_last-ip-octet_timestamp. For % string substitutions, see "Fields
Available for Creating Access Log Formats" on page 756.

SGOS# (config) archive-configuration username user_name
where user_name is the username used to access the server.
```

Example Session

```
SGOS# (config) archive-configuration host 10.25.36.47
ok
SGOS# (config) archive-configuration password access
ok
SGOS# (config) archive-configuration username admin1
ok
SGOS# (config) archive-configuration path ftp://archive.server/stored
ok
SGOS# (config) archive-configuration protocol ftp
ok
```

Note: To clear the host, password, or path, type the above commands using empty double-quotes instead of the variable. For example, to clear the path, enter archive-configuration path "".

To Archive a System Configuration through the CLI:

At the enable command prompt, enter the following command:

```
SGOS# upload configuration
```

To Restore a System Configuration through the CLI:

At the enable command prompt, enter the following command:

```
SGOS# configure network "url"
```

where *url* must be in quotes and is fully-qualified (including the protocol, server name or IP address, path, and filename of the configuration file). The configuration file is downloaded from the server, and the ProxySG settings are updated.

Note: If you rename the archived configuration file so that it does not contain any spaces, the quotes surrounding the URL are unnecessary.

The username and password used to connect to the FTP server can be embedded into the URL. The format of the URL is:

`ftp://username:password@ftp-server`

where *ftp-server* is either the IP address or the DNS resolvable hostname of the FTP server.

If you do not specify a username and password, the ProxySG assumes that an anonymous FTP is desired and thus sends the following as the credentials to connect to the FTP server:

`username: anonymous
password: proxy@`

Adapters

This section describes ProxySG network adapters and interfaces.

About Adapters

ProxySG Appliances ship with one or more network adapters. You can change interface parameters or configure additional adapters in the appliance. You can also accept or reject inbound connections, change link settings in the event the system did not correctly determine them, and configure the browser for proxy settings.

Network Interface States

As you select adapters from the picklist, the Adapter panel (Configuration>Network>Adapters) displays the state of the configured adapters and interfaces. When you initially set up the ProxySG, you optionally configured Interface 0. If your system has only one adapter, you can skip this section. If your system shipped with other adapters, you can configure them through these procedures.

Configuring an Adapter

The following procedure describes how to configure an adapter. Repeat the process if the system has additional adapters.

To Configure a Network Adapter through the Management Console:

1. Select Configuration>Network>Adapters>Adapters.

The Adapters tab displays.

Note: Different ProxySG models have different adapter configurations, and the appearance of the Adapters tab varies accordingly.

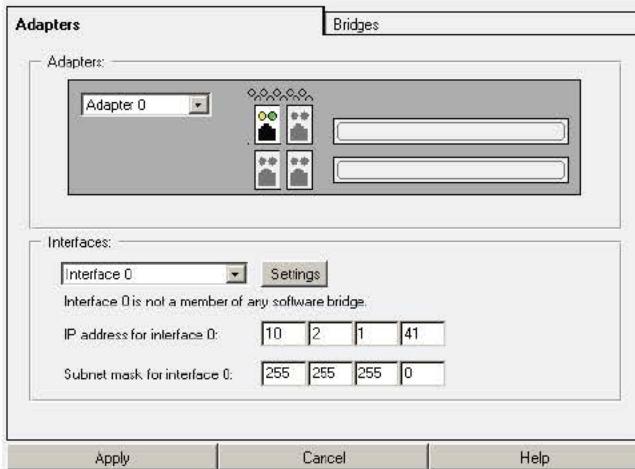


Figure 4-5: Network Adapters Tab

2. Select an adapter from the Adapter drop-down list.

Notice that in the Interfaces field, a message displays stating whether the interface belongs to a bridge. For more information about network bridging, see "Software and Hardware Bridges" on page 68.

3. (Optional) If you have a dual port adapter, select an interface from the drop-down list.
4. Enter the IP address and subnet mask for the adapter into the IP address for interface x and Subnet mask for interface x fields (where interface x refers to the interface selected in the Interfaces drop-down list.)
5. (Optional) To configure link settings, restrict inbound connections, or set up browser proxy behavior for the adapter, select the adapter (under Interfaces) and click Settings. Enter any changes and click OK to close the Settings dialog.

Note: The default is to permit all inbound connections. Link settings are automatically determined and should not need to be modified. The browser default is to use the proxy's default PAC file. (See "About the Settings Button" below for more information on link settings and inbound connections.)

6. Click Apply.

To Configure a Network Adapter through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) interface fast-ethernet interface_number
```

where *interface_number* is 0, 1, or *n*, up to one number less than the number of interface cards in the system.

```
SGOS#(config interface interface_#) ip-address ip_address
SGOS#(config interface interface_#) subnet-mask subnet
SGOS#(config interface interface_#) exit
```

About the Settings Button

The **Settings** button in the **Interfaces** field allows you to restrict inbound connections on the selected adapter, and to choose manual or automatic configuration of the adapter link settings.

The default for Inbound connections is to permit all incoming connections. The link settings are automatically determined and should not normally require modification.

Note: Rejecting inbound connections improperly, or manually configuring link settings improperly, can cause the ProxySG to malfunction. Make sure that you know the correct settings before attempting either of these. If the ProxySG fails to operate properly after changing these settings, contact Blue Coat Support.

Rejecting Inbound Connections

The default setting allows inbound connections on all network adapters.

To Reject Inbound Connections through the Management Console:

1. Select Configuration>Network>Adapters>Adapters.
The Adapters tab displays.
2. Select an adapter from the Adapter drop-down list.

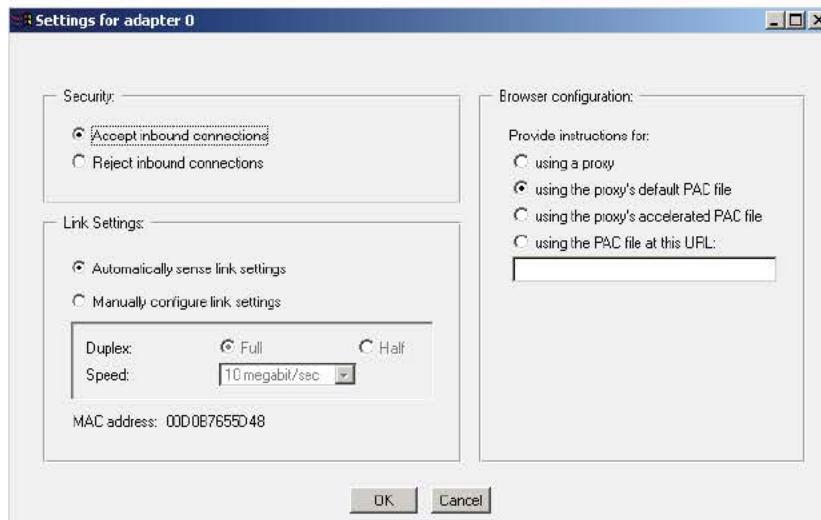


Figure 4-6: Settings for Individual Network Adapters

3. Click Settings.
4. To allow inbound connections, select the Accept inbound connections radio button. To reject inbound connections, select the Reject inbound connections radio button.
5. Click OK to close the Settings dialog.
6. Click Apply.

To Reject Inbound connections through the CLI:

At the (config) command prompt, switch to the interface submode to enter the following commands:

```
SGOS#(config) interface interface_#
SGOS#(config interface interface_#) no accept inbound
SGOS#(config interface interface_#) exit
```

Manually Configuring Link Settings

By default, the ProxySG automatically determines the link settings for all network adapters. If the device incorrectly identifies the network adapter, you can manually configure the link settings.

To manually configure link settings through the Management Console:

1. Select Configuration>Network>Adapters>Adapters.
- The Adapters tab displays.
2. Select an adapter from the Adapters drop-down list.
3. Click Settings.
4. Select Manually configure link settings.
5. Select Half or Full duplex.
6. Select the correct network speed.
7. Click OK to close the Advanced Settings dialog.
8. Click Apply.

To Manually Configure Link Settings through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) interface fast-ethernet interface_#
SGOS#(config interface interface_#) full-duplex | half-duplex
SGOS#(config interface interface_#) speed 10 | 100 | 1gb
SGOS#(config interface interface_#) exit
```

Setting Up Proxies

To set up proxies, see "Configuring Proxies" on page 137.

Detecting Network Adapter Faults

The ProxySG can detect whether the network adapters in an Appliance are functioning properly. If the Appliance finds that an adapter is faulty, it stops using it. When the fault is remedied, the ProxySG detects the functioning adapter and uses it normally.

To determine whether an adapter is functioning properly:

1. Check whether the link is active (that is, a cable is connected and both sides are up).
2. Check the ratio of error packets to good packets: both sent and received.
3. Check if packets have been sent without any packets received.

If an adapter fault is detected, and the adapter has an IP address assigned to it, the ProxySG logs a severe event. When an adapter does not have an IP address, the Appliance does not log an entry.

Software and Hardware Bridges

This section describes the ProxySG hardware and software bridging capabilities.

About Bridging

Network bridging through the ProxySG provides transparent proxy pass-through and failover support. This functionality allows ProxySG Appliances to be deployed in environments where L4 switches and WCCP-capable routers are not feasible options.

The ProxySG provides bridging functionality by two methods:

- Software—A software, or *dynamic*, bridge is constructed using a set of installed interfaces. Within each logical bridge, interfaces can be assigned or removed.
- Hardware—A hardware, or *pass-through*, bridge uses a 10/100 dual interface Ethernet card. This type of bridge provides pass-through support.

About the Pass-Through Card

A pass-through card is a 10/100 dual port Ethernet adapter designed by Blue Coat to provide an efficient fault-tolerant bridging solution. If this card is installed on a ProxySG, SGOS detects the card upon system bootup and automatically creates a bridge—the two Ethernet ports serve as the bridge ports. If the ProxySG is powered down or loses power for any reason, the bridge fails open; that is, Web traffic passes from one Ethernet port to the other. Therefore, Web traffic is uninterrupted, but does not route through the appliance.

Important: This scenario creates a security vulnerability.

Once power is restored to the ProxySG, the bridge opens and Web traffic is routed to the appliance and thus is subject to that appliance's configured features, defined policies, and content scanning redirection instructions.

Note: Bridging supports only failover; it does not support load balancing.

The following figure provides an example of how the ProxySG indicates that an installed adapter is a pass-through card.

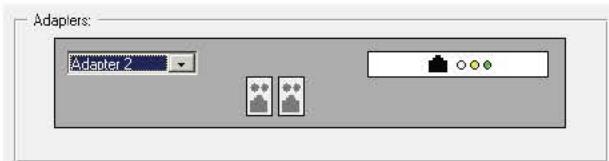


Figure 4-7: Pass-through Card

Note: The adapter state is displayed on Configuration>Network>Adapters>Adapters.

ProxySG Prerequisites

Before configuring a software bridge, the following conditions must be satisfied:

- Adapters—The adapters must of the same type. Although the software does not restrict you from configuring bridges with adapters of different types (10/100 or GIGE), the resultant behavior is unpredictable.
- IP addresses—if any of the interface ports to be added to the bridge already have IP addresses assigned to them, those IP addresses must be removed.

Configuring a Software Bridge

This section describes how to use the Management Console or the CLI to link interfaces and ports to create a network bridge.

To Configure a Software Bridge through the Management Console:

1. Select Configuration>Network>Adapters>Bridges.
The Bridges tab displays.
2. In the Software Bridges area, click Create.
3. In the New Bridge Name field of the dialog that appears, enter a name for the bridge, up to 16 characters; click OK.
4. In the Bridge IP Address field, enter the IP address of the interface.
5. In the Bridge Subnet Mask field, enter the subnet mask of the interface.
6. To add a port to the bridge:
 - a. In the Ports field, click New; the *Create a port for bridge name* dialog appears.
 - b. From the drop-down lists, select a port number and interface.
 - c. By default, link settings are automatically sensed. To change the Duplex and Speed options, click Link Settings, select Manually configure link settings, and change as required.
 - d. Click OK.

7. Further customize the bridge:
 - a. In the Software Bridges field, click **Settings**; the *Settings for bridge name* dialog appears.
 - b. In the Security field, the default is to accept inbound connections on this interface. To disallow inbound connections, select **Reject**.
 - c. In the Browser Configuration field, the default browser instruction is to use the browser's default PAC file. To use a proxy or other PAC file type, select from the list.
8. Click **Apply**.

The Bridge Settings options allow you to clear bridge forwarding table and clear bridge statistics.

To Configure a Software Bridge through the CLI:

1. At the `(config)` command prompt, enter the following commands:

```
SGOS# (config) bridge  
SGOS# (config bridge) edit bridge_name
```

where `name` designates the bridge name. The limit is 16 characters.

```
SGOS# (config bridge bridge_name) ip-address ip_address
```

where `ip_address` designates the IP address of the interface.

```
SGOS# (config bridge bridge_name) subnet-mask subnet_mask
```

where `subnet_mask` designates the subnet mask of the interface.

2. To configure a port on a bridge, enter the following commands at the `(config)` command prompt (repeat to add more ports):

```
SGOS# (config bridge bridge_name) port port_number  
SGOS# (config bridge bridge_name port port_number)
```

where `port_number` identifies a port on the interface.

- By default, link settings are automatically sensed. To perform an auto-sense, enter the following command:


```
SGOS# (config bridge bridge_name port port_number) port port_number
```
- To attach a port to an interface or change the Duplex and Speed options, enter the following commands:

```
SGOS# (config bridge bridge_name port port_number) attach-interface  
interface_number  
SGOS# (config bridge bridge_name port port_number) full-duplex  
SGOS# (config bridge bridge_name port port_number) half-duplex  
SGOS# (config bridge bridge_name port port_number) speed {10 | 100 | 1gb}
```

where:

attach-interface	<i>interface_number</i>	Attaches an interface for this port.
full-duplex		Configures this port for full duplex.
half-duplex		Configures this port for half duplex.
speed	10 100 1gb	Configures speed for this port.

```
SGOS#(config bridge bridge_name port port_number) exit
SGOS#(config bridge bridge_name)
```

- To specify the maximum transmission unit (MTU), enter the following command:

```
SGOS#(config bridge bridge_name) mtu-size size
```

- The default is to accept inbound connections on this interface. To disallow inbound connections, enter the following command:

```
SGOS#(config bridge bridge_name) no accept-inbound
```

- The default browser instruction is to use the browser's default PAC file. To instruct to use a proxy or other PAC file type, enter the following command:

```
SGOS#(config bridge bridge_name) instructions {proxy | default-pac | central-pac url | accelerated-pac}
```

where:

proxy	Use a proxy.
default-pac	Use the Blue Coat default PAC file.
central-pac	Use the PAC file specified at the given URL.
accelerated-pac	Use the proxy's accelerated PAC file.

Configuring Failover

You can configure failover for software bridges, not hardware bridges. Failover is accomplished by creating virtual IPs on each proxy, creating a failover group, and attaching the bridge configuration. One of the proxies *must* be designated with a higher priority (a master proxy).

Example

The following example creates a bridging configuration with one bridge on standby.

Note: This deployment requires a hub on both sides of the bridge or a switch capable of port mirroring.

- ProxySG A—software bridge IP address: 10.0.0.2. Create a virtual IP address and a failover group, and designate this group the *master*.

```
ProxySG_A#(config) virtual-ip address 10.0.0.4
ProxySG_A#(config) failover
ProxySG_A#(config failover) create 10.0.0.4
ProxySG_A#(config failover) edit 10.0.0.4
ProxySG_A#(config failover 10.0.0.4) master
ProxySG_A#(config failover 10.0.0.4) priority 100
ProxySG_A#(config failover 10.0.0.4) interval 1
```

- ProxySG B—software bridge IP address: 10.0.0.3. Create a virtual IP address and a failover group.

```
ProxySG_B#(config) virtual-ip address 10.0.0.4
ProxySG_B#(config) failover
ProxySG_B#(config failover) create 10.0.0.4
ProxySG_B#(config failover) edit 10.0.0.4
ProxySG_B#(config failover 10.0.0.4) priority 100
ProxySG_B#(config failover 10.0.0.4) interval 1
```

- In the bridge configuration on each ProxySG, attach the bridge configuration to the failover group:

```
ProxySG_A#(config bridge bridge_name) failover 10.0.0.4
ProxySG_B#(config bridge bridge_name) failover 10.0.0.4
```

Static Forwarding Tables

Certain firewall configurations require the use of static forwarding tables. Failover configurations use virtual IP (VIP) addresses and virtual MAC (VMAC) addresses. When a client sends an ARP request to the firewall VIP, the firewall replies with a VMAC (which can be an Ethernet multicast address); however, when the firewall sends a packet, it uses a physical MAC address, not the VMAC.

The solution is to create a static forwarding table that defines the next hop gateway that is on the correct side of the bridge.

Note: A port must have an interface attached to allow creation of the static forwarding table, and you can only create one forwarding table per bridge.

To Create a Static Forwarding Table through the CLI:

1. At the (config) prompt, enter the following commands:

```
SGOS# (config) bridge
SGOS# (config bridge) bridge_name
SGOS# (config bridge bridge_name) port port_number
SGOS# (config bridge_name port_number) static-fwtable-entry mac_address
```

2. Add up to 256 entries per bridge.

To Clear a Static Forwarding Table through the CLI:

At the (config) prompt, enter the following commands:

```
SGOS# (config) bridge
SGOS# (config bridge) bridge_name
SGOS# (config bridge bridge_name) clear-fwtable
```

Gateways

A key feature of the ProxySG is the ability to distribute traffic originating at the Appliance through multiple gateways. You can also fine tune how the traffic is distributed to different gateways. This feature works with any routing protocol (such as static routes or RIP).

Note: Load balancing through multiple gateways is independent from the per-interface load balancing the ProxySG automatically does when more than one network interface is installed.

About Gateways

During the initial setup of the ProxySG, you optionally defined a gateway (a device that serves as entrance and exit into a communications network) for the ProxySG.

By using multiple gateways, an administrator can assign a number of available gateways into a preference group and configure the load distribution to the gateways within the group. Multiple preference groups are supported.

The gateway specified applies to all network adapters in the system.

ProxySG Specifics

Which gateway the ProxySG chooses to use at a given time is determined by how the administrator configures the assignment of preference groups to default gateways. You can define multiple gateways within the same preference group. A ProxySG can have from 1 to 10 preference groups. If you have only one gateway, it automatically has a weight of 100.

Initially, all gateways in the lowest preference group are considered as the active gateways. If a gateway becomes unreachable, it is dropped from the active gateway list, but the remaining gateways within the group continue to be used until they all become unreachable, or until an unreachable gateway in a lower preference group becomes reachable again. If all gateways in the lowest preference group become unreachable, the gateways in the next lowest preference group become the active gateways.

In addition to a preference group, each gateway within a group can be assigned a relative weight value from 1 to 100. The weight value determines how much bandwidth a gateway is given relative to the other gateways in the same group. For example, in a group with two gateways, assigning both gateways the same weight value, whether 1 or 100, results in the same traffic distribution pattern. In a group with two gateways, assigning one gateway a value of 10 and the other gateway a value of 20 results in the ProxySG sending approximately twice the traffic to the gateway with a weight value of 20.

Switching to a Secondary Gateway

When a gateway goes down, the ProxySG takes from 120 to 180 seconds to determine that the gateway is unreachable. At that point, the ProxySG switches to a secondary gateway if one is configured.

The ProxySG continues to check failed gateways once a minute using Address Resolution Protocol (ARP). The gateways are declared unreachable after three attempts. When a preferred gateway comes back on line, however, it might take up to 180 seconds for the ProxySG to confirm the preferred gateway is reachable and to switch back to that gateway.

These times are not user-configurable.

To Configure Multiple Gateway Load Balancing through the Management Console:

1. Select Configuration>Network>Routing>Gateways.

The Gateways tab displays.

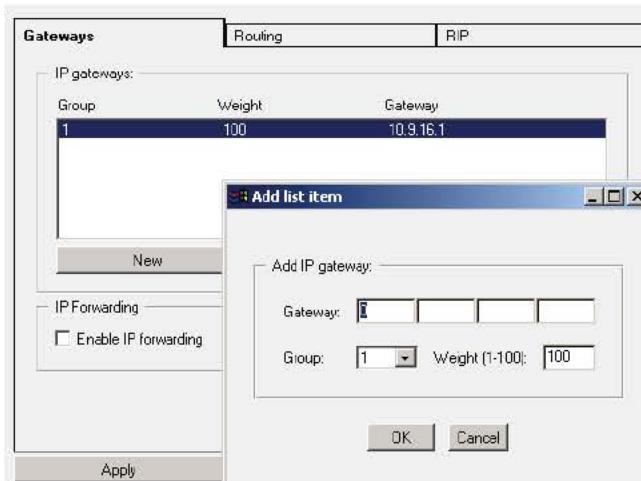


Figure 4-8: Network Routing Gateways Tab

2. Click New.
3. Enter the IP address, group, and weight for the gateway into the Add list item dialog that appears.
4. Click OK.
5. Repeat steps 2 to 4 until IP addresses, groups, and weights have been defined for all of your gateways.
6. Click Apply.

To Configure Multiple Gateway Load Balancing through the CLI:

1. At the `(config)` command prompt, enter the following command:

```
SGOS#(config) ip-default-gateway ip_address preference_group weight
```

The first value is the IP address of the gateway, the second value is the preference group, and the third value is the relative weighting for this gateway. For example, to use the gateway 10.25.36.1, the preference group 1, and the relative weighting 100, enter:

```
ip-default-gateway 10.25.36.1 1 100
```

2. Repeat until all IP addresses, groups, and weights of your IP gateways have been defined.
3. (Optional) View the results.

```
SGOS#(config) show ip-default-gateway
Default IP gateways
Gateway          Weight  Group
10.25.36.1      100     1
```

Defining Static Routes

The ProxySG can be configured to use *static routes*, a manually-configured route that specifies the transmission path a packet must follow, based on the packet's destination address. A static route specifies a transmission path to another network.

Note: You are limited to 10,000 entries in the static routes table.

You can install the routing table several ways.

- Using the ProxySG Text Editor, which allows you to enter settings (or copy and paste the contents of an already-created file) directly onto the appliance.
- Creating a local file on your local system; the ProxySG can browse to the file and install it.
- Using a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the ProxySG.
- Using the CLI `inline static-route-table` command, which allows you to paste a static route table into the ProxySG.
- Using the CLI `static-routes` command, which requires that you place an already-created file on an FTP or HTTP server and enter the URL into the ProxySG.

The routing table is a text file containing a list of IP addresses, subnet masks, and gateways. The following is a sample router table:

```
10.25.36.0  255.255.255.0  10.25.46.57
10.25.37.0  255.255.255.0  10.25.46.58
10.25.38.0  255.255.255.0  10.25.46.59
```

When a routing table is loaded, all requested URLs are compared to the list, and routed based on the best match.

To install a routing table through the Management Console:

1. Select Configuration>Network>Routing>Routing.

The Routing tab displays.

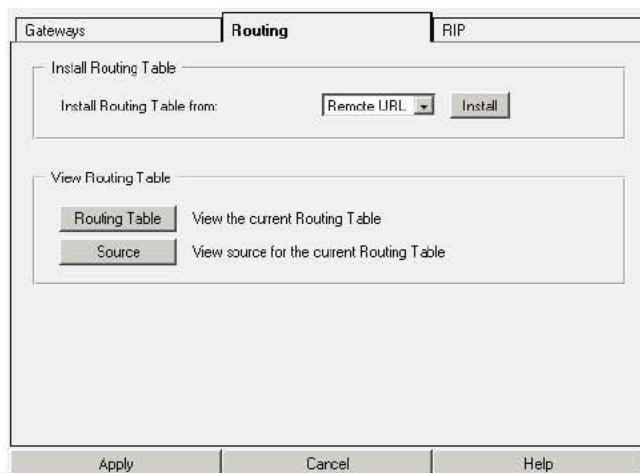


Figure 4-9: Network Routing Tab

2. From the drop-down list, select the method used to install the routing table; click **Install**.
- Remote URL:

Enter the fully-qualified URL, including the filename, where the routing table is located. To view the file before installing it, click **View**. Click **Install**. View the installation status and click **OK**.

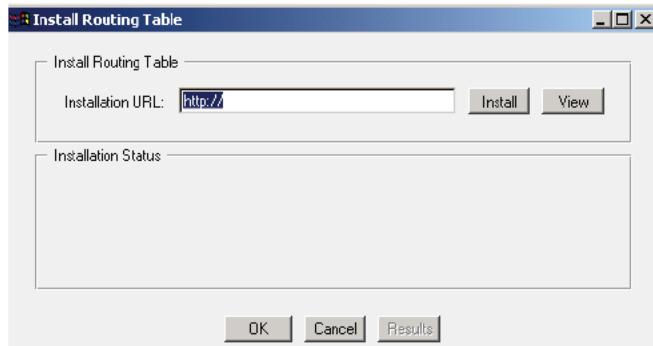


Figure 4-10: Specifying the Remote Location of a Routing Table

Local File:

Click **Browse** to bring up the Local File Browse window. Browse for the file on the local system. Open it and click **Install**. When the installation is complete, a results window opens. View the results, close this window, and click **Close**.

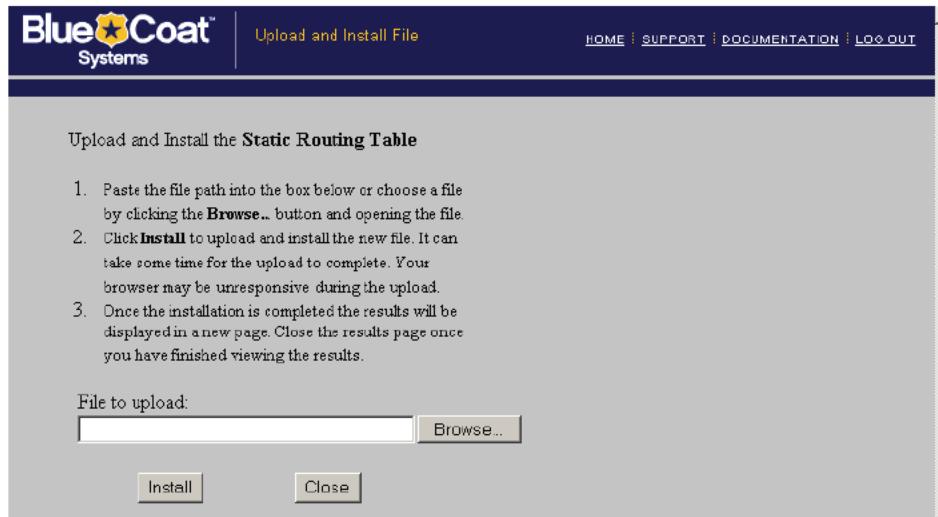


Figure 4-11: Specifying the Local Location of a Routing Table

Text Editor:

The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click **Install**. When the installation is complete, a results window opens. View the results, close this window, and click **Close**.

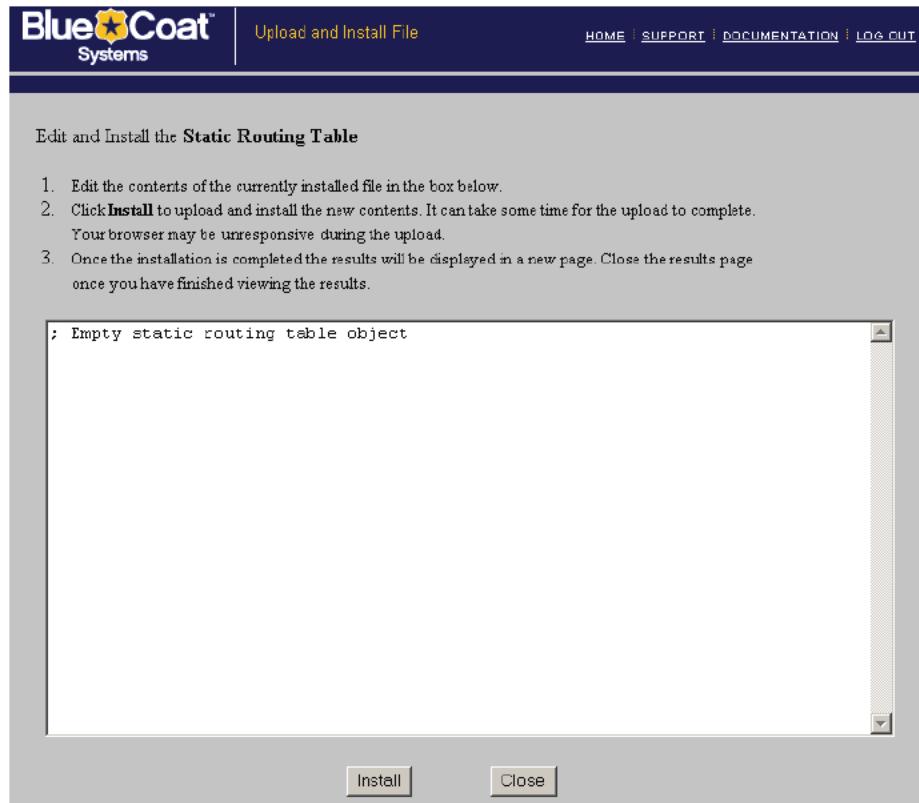


Figure 4-12: Creating a Static Routing Table on the ProxySG

3. Click **Apply**.

Installing a Routing Table Through the CLI

To install a routing table through the CLI, you can use the `inline` command to install the table directly, or enter a path to a remote URL that has an already-created text file ready to download.

When entering input for the `inline` command, you can correct mistakes on the current line using the `<Backspace>` key. If you detect a mistake in a line that has already been terminated using the `<Enter>` key, you can abort the `inline` command by typing `<Ctrl>c`. If the mistake is detected after you terminate input to the `inline` command, type the same `inline` command again, but with the correct configuration information. The corrected information replaces the information from the last `inline` command.

The end-of-input marker is an arbitrary string chosen by the you to mark the end of input for the current `inline` command. The string can be composed of standard characters and numbers, but cannot contain any spaces, punctuation marks, or other symbols.

Take care to choose a unique end-of-input string that does not match any string of characters in the configuration information.

To Install a Routing Table through the CLI:

Do one of the following:

- To paste a static route table directly into the CLI, enter the following command at the `(config)` command prompt, then paste the table on the line after the first *end-of-file* marker:

```
SGOS#(config) inline static-route-table end-of-file_marker  
paste static routing table  
eof  
ok
```

- To enter the static route table manually, enter the following command, then enter each IP address/subnet on the second line, following the first *end-of-file* marker:

```
SGOS#(config) inline static-route-table end-of-file_marker  
10.25.36.0 255.255.255.0 10.25.46.57  
10.25.37.0 255.255.255.0 10.25.46.58  
10.25.38.0 255.255.255.0 10.25.46.59  
eof  
ok
```

- To enter a path to a remote URL where you have placed an already-created static route table, enter the following commands at the `(config)` command prompt:

```
SGOS#(config) static-routes path url  
SGOS#(config) load static-route-table
```

Using RIP

The Routing Information Protocol (RIP) is designed to select the fastest route to a destination. RIP support is built into the ProxySG, and is configured by creating and installing an RIP configuration text file onto the ProxySG. (No RIP configuration file is shipped with the appliance.) For commands that can be entered into the RIP configuration file, see Appendix D: "RIP Commands" on page 811.

Once you have created an RIP configuration file, you can install it several ways:

- Using the ProxySG Text Editor, which allows you to enter settings (or copy and paste the contents of an already-created file) directly onto the appliance.
- Creating a local file on your local system; the ProxySG can browse to the file and install it.
- Using a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the ProxySG.
- Using the CLI `inline rip-settings` command, which allows you to paste the RIP settings into the CLI.
- Using the CLI `rip` commands, which require that you place an already-created file on an FTP or HTTP server and enter the URL into the CLI. You can also enable or disable RIP with these commands.

To Install an RIP Configuration File through the Management Console:

Note: When entering RIP settings that will change current settings (for instance, when switching from ripv1 to ripv2), disable RIP before you change the settings; re-enable RIP when you have finished.

1. Select Configuration>Network>Routing>RIP.

The RIP tab displays.

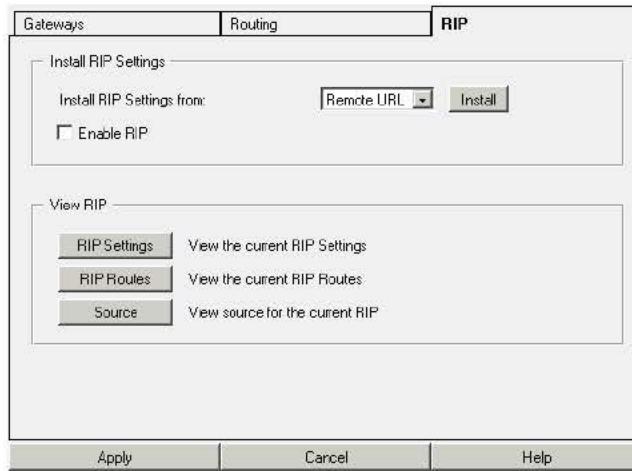


Figure 4-13: Network Routing RIP Tab

2. To display the configuration file before installing it, click View RIP.
3. In the Install RIP Setting from the drop-down list, select the method used to install the routing table; click Install.

Remote URL:

Enter the fully-qualified URL, including the filename, where the routing table is located. To view the file before installing it, click View. Click Install. Viewing the installation status that displays; click OK.

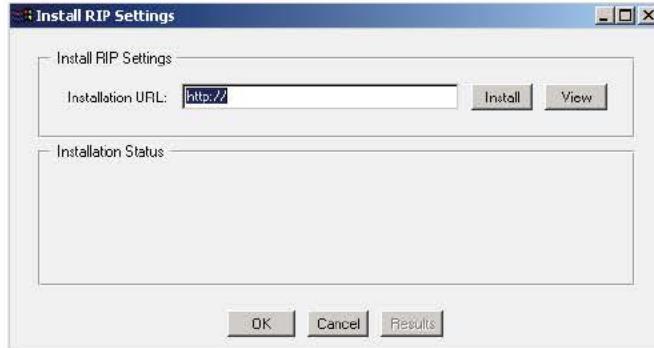


Figure 4-14: Specifying the Remote Location of a RIP Configuration File

Local File:

Click **Browse** to display the Local File Browse window. Browse for the file on the local system. Open it and click **Install**. When the installation is complete, a results window opens. View the results, close the window, and click **OK**.

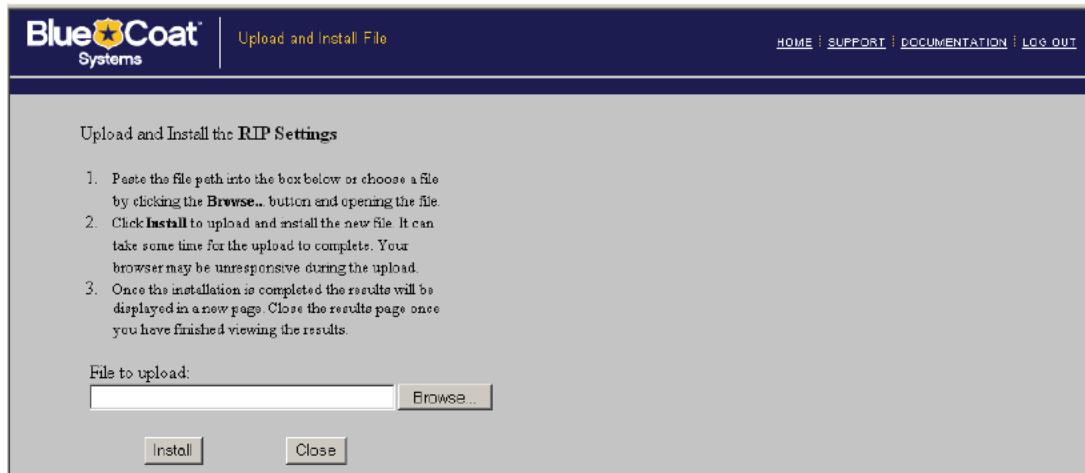


Figure 4-15: Specifying the Local Location of a RIP File

Text Editor:

The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click **Install**. When the installation is complete, a results window opens. View the results, close the window, and click **OK**.

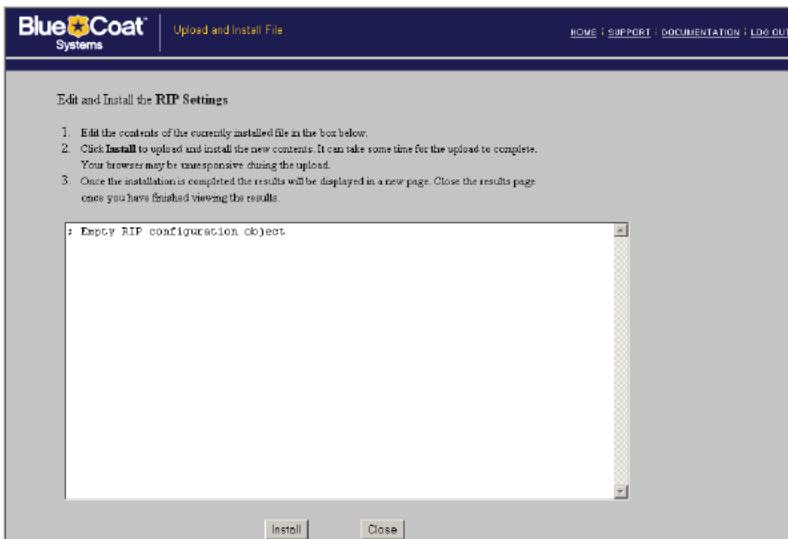


Figure 4-16: Creating an RIP file on the ProxySG

4. Click Apply.
5. Select Enable RIP.
6. Click Apply.

Configuring RIP through the CLI

Note: When entering RIP settings that will change current settings (for instance, when switching from ripv1 to ripv2), disable RIP before you change the settings; re-enable RIP when you have finished.

To Disable/Enable RIP through the CLI:

Enter the following command at the `(config)` command prompt:

```
SGOS#(config) rip {disable | enable}
```

To Install an RIP Configuration through the CLI:

Do one of the following:

- To enter a path to a remote URL where you have placed an already-created RIP configuration file, enter the following commands at the `(config)` command prompt:

```
SGOS#(config) rip path url
SGOS#(config) load rip-settings
```

- To paste an RIP configuration directly into the CLI, enter the following command at the `(config)` command prompt:

```
SGOS#(config) inline rip-settings eofm
```

At this point you can paste RIP settings into the `inline` command, or you can enter values for specific settings. When you finish, enter your `end-of-file_marker` command.

Example

```
SGOS#(config) inline rip-settings eofm
ripv2
ripv1_out
no_rdisc eofm
ok
```

DNS

During first-time installation of the ProxySG, you configured the IP address of a single primary DNS server. Using the Configuration>Network>DNS tab, you can change this primary DNS server at any time, and you can also define additional primary DNS servers and one or more alternate DNS servers.

ProxySG Specifics

If you have defined more than one Domain Name Service (DNS) server, the ProxySG uses the following logic to determine which servers will be used to resolve a DNS host name and when to return an error to the client:

- The ProxySG first sends requests to DNS servers in the primary DNS server list.
- Servers are always contacted in the order in which they appear in a list.
- The next server in a list is only contacted if the ProxySG does not receive a response from the current server.
- If none of the servers in a list returns a response, ProxySG returns an error to the client.
- ProxySG only sends requests to servers in the alternate DNS server list if a server in the primary list indicates that a DNS host name cannot be resolved.

If a DNS server returns any other error (other than an indication that a DNS host name could not be resolved), ProxySG returns the error to the client.

If a server in both the primary and alternate DNS server lists are unable to resolve a DNS host name, an error is returned to the client.

The ProxySG always attempt to contact the first server in the primary DNS server. If a response is received from this server, no attempts are made to contact any other DNS servers in the primary list.

If the response from the first primary DNS server indicates the host name cannot be translated to an IP address, the ProxySG sends a DNS request to the first alternate DNS server, if one is defined. If no alternate DNS servers have been defined, an error is returned to the client indicating that the host name could not be resolved. If the first alternate DNS server is unable to resolve the host name, an error is returned to the client, and no attempt is made to contact any other DNS servers in either the primary or alternate DNS server lists.

If a response is not received from any DNS server in a particular DNS server list, the ProxySG sends a DNS request to the next server in the list. The ProxySG returns an error to the client if none of the servers in a DNS server list responds to the DNS request. The ProxySG only sends requests to servers in the alternate DNS server list if a server in the primary list returns a response indicating that the host name could not be translated to an IP address.

If the ProxySG receives a negative DNS response (a response with an error code set to Name Error), it caches that negative response. You can configure the ProxySGs negative response time-to-live value. (A value of zero disables negative caching.) If the ProxySG is not configured (the default), the ProxySG caches the negative response and uses the TTL value from the response to determine how long it should be cached.

Configuring Split DNS Support

Customers with split DNS server configuration (for example, environments that maintain private internal DNS servers and external DNS servers) might choose to populate an Alternate DNS server list as well as the Primary DNS server list. In the ProxySG, the internal DNS servers are placed in the Primary list, while external DNS servers (with the Internet information) populate the Alternate list.

Complete the following steps to configure Primary and Alternate DNS servers:

To Add a Primary DNS Server through the Management Console:

1. Select Configuration>Network>DNS>DNS.

The DNS tab displays.

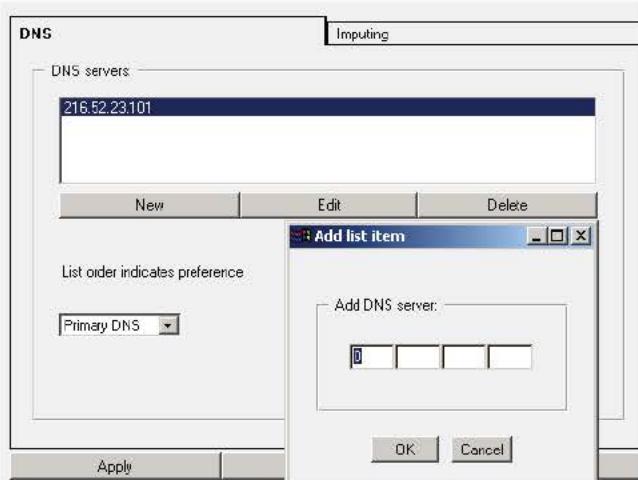


Figure 4-17: Network DNS Tab

2. Click New.
3. Enter the IP address of the DNS server and click OK.
4. Click Apply.

To Add a Primary DNS Server through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) dns server ip_address
```

To Add an Alternate DNS Server through the Management Console:

1. Select Configuration>Network>DNS>DNS.
- The DNS tab displays.
2. Select Alternate DNS in the drop-down list.
3. Click New.
4. Enter the IP address of the DNS server and click OK.
5. Click Apply.

To add an Alternate DNS Server through the CLI:

1. At the (config) command prompt, enter the following command:

```
SGOS#(config) dns alternate ip_address
```

2. Repeat until alternate DNS servers have been defined.

Changing the Order of DNS Servers

The ProxySG uses DNS servers in the order displayed. You can organize the list of servers so that the preferred servers appear at the top of the list. This functionality is not available through the CLI.

To Change the Order of DNS Servers through the Management Console:

1. Select Configuration>Network>DNS>Imputing.

The Imputing tab displays.

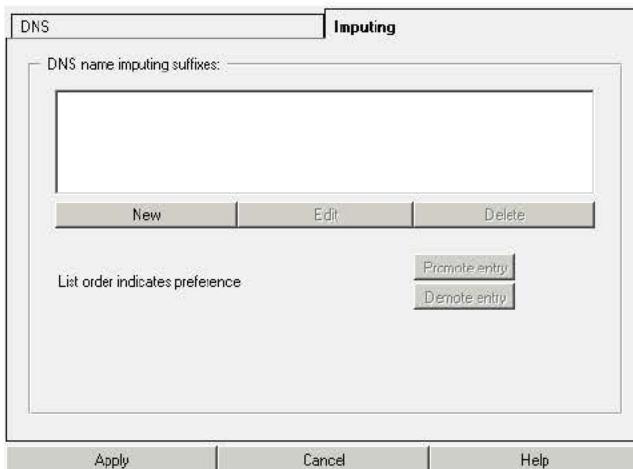


Figure 4-18: Network DNS Imputing Tab

2. Select the DNS server to promote or demote.
3. Click Promote or Demote as appropriate.
4. Click Apply.

Unresolved Host Names (Name Imputing)

Name imputing allows the ProxySG to resolve host names based on a partial name specification. When the ProxySG submits a host name to the DNS server, the DNS server resolves the name to an IP address. The ProxySG queries the original host name before checking imputing entries unless there is no period in the host name, in which case imputing is applied first. The ProxySG tries each entry in the name-imputing list until the name is resolved, or it comes to the end of the list. If by the end of the list the name is not resolved, the ProxySG returns a DNS failure.

For example, if the name-imputing list contains the entries `company.com` and `.com`, and a user submits the URL `http://www.eeddept`, the ProxySG resolves the host names in the following order.

```
http://www.eeddept
http://www.eeddept.company.com
http://www.eeddept.com
```

To Add Names to the Imputing List through the Management Console:

1. Select Configuration>Network>DNS>Imputing.

The Imputing tab displays.

2. Click New to add a new name to the imputing list.
3. Enter the name and click OK.
4. Click Apply.

To Add Names to the Imputing List through the CLI:

1. At the `(config)` command prompt, enter the following command:

```
SGOS# (config) dns imputing suffix
```

For example, to use `company.com` as the imputing suffix, enter `dns-imputing company.com`.

2. Repeat until all imputing suffixes have been entered.

Changing the Order of DNS Name Imputing Suffixes

The ProxySG uses imputing suffixes in the order displayed. You can organize the list of suffixes so the preferred suffix appears at the top of the list. This functionality is only available through the Management Console. You cannot configure DNS name inputing through the CLI.

To Change the Order through the Management Console:

1. Select Configuration>Network>DNS>Imputing.
The Imputing tab displays.
2. Select the imputing suffix to promote or demote.
3. Click Promote entry or Demote entry as appropriate.
4. Click Apply.

Caching Negative Responses

By default, the ProxySG caches negative DNS responses sent by a DNS server. You can configure the ProxySG to set the time-to-live (TTL) value for a negative DNS response to be cached. You can also disable negative DNS response caching.

Note: The ProxySG generates more DNS requests when negative caching is disabled.

Both type A and type PTR DNS responses are affected by negative caching.

This functionality is only available through the CLI. You cannot configure DNS negative caching through the Management Console.

To Configure Negative Caching TTL Values:

From the `(config)` prompt:

```
SGOS# (config) dns negative-cache-ttl-override seconds
```

where `seconds` is any integer between 0 and 600.

Setting the TTL value to 0 seconds disables negative DNS caching; setting the TTL setting to a non-zero value overrides the TTL value from the DNS response.

To Restore Negative Caching Defaults:

From the (config) prompt:

```
SGOS#(config) dns no negative-cache-ttl-override
```

Attack Detection

The ProxySG can reduce the effects of distributed denial of service (DDoS) attacks and port scanning, two of the most common virus infections.

A DDoS attack occurs when a pool of machines that have been infected with a DDoS-type of virus attack a specific website. As the attack progresses, the target host shows decreased responsiveness and often stops responding. Legitimate HTTP traffic will be unable to proceed because the ProxySG is still waiting for a response from the target host.

Port scanning involves viruses trying to self-propagate to other machines by arbitrarily trying to connect to other hosts on the Internet. If the randomly selected host is unavailable or behind a firewall or does not exist, the ProxySG continues to wait for a response, thus denying legitimate HTTP traffic.

The ProxySG prevents attacks by limiting the number of simultaneous TCP connections from each client IP address and either will not respond to connection attempts from a client already at this limit or will reset the connection. It also limits connections to servers known to be overloaded.

You can configure attack detection for both clients and servers or server groups, such as `http://www.bluecoat.com`. The *client* attack-detection configuration is used to control the behavior of virus-infected machines behind the ProxySG. The *server* attack-detection configuration is used when an administrator knows ahead of time that a virus is set to attack a specific host.

This feature is only available through the CLI. You cannot use the Management Console to enable attack detection.

For information on configuring a client, continue with the next section. To configure a server for attack detection, continue with "Configuring Attack-Detection Mode for a Server or Server Group" on page 91.

Configuring Attack-Detection Mode for the Client

To Enter Attack Detection Mode for the Client:

From the (config) prompt, enter the following commands:

```
SGOS#(config) attack-detection  
SGOS#(config attack-detection) client
```

The prompt changes to:

```
SGOS#(config client)
```

To Change Global Settings

The following defaults are global settings, used if a client does not have specific limits set. They do not need to be changed for each IP address/subnet if they already suit your environment:

- client limits enabled: true
- client interval: 20 minutes

- block-action: drop (for each client)
- connection-limit: 100 (for each client)
- failure-limit: 50 (for each client)
- unblock-time: unlimited
- warning-limit: 10 (for each client)

To Change the Global Defaults

Remember that enable/disable limits and interval affect all clients. The values cannot be changed for individual clients. Other limits can be modified on a per-client basis.

Note: If you edit an existing client's limits to a smaller value, the new value only applies to new connections to that client. For example, if the old value was 10 simultaneous connections and the new value is 5, existing connections above 5 will not be dropped.

```
SGOS#(config client) enable-limits | disable-limits
SGOS#(config client) interval minutes
SGOS#(config client) block ip_address [minutes] | unblock ip_address
SGOS#(config client) default block-action {drop | send-tcp-rst}
SGOS#(config client) default connection-limit integer_between_1_and_65535
SGOS#(config client) default failure-limit integer_between_1_and_500
SGOS#(config client) default unblock-time minutes_between_10_and_1440
SGOS#(config client) default warning-limit integer_between_1_and_100
```

where:

enable-limits disable-limits		Toggles between enabled and disabled. The default is disabled. Note that this is a global setting and cannot be modified for individual clients.
interval	integer	Indicates the amount of time, in multiples of 10 minutes, that client activity is monitored. The default is 20. Note that this is a global setting and cannot be modified for individual clients.
block unblock	<i>ip_address [minutes]</i>	Blocks a specific IP address for the number of minutes listed. If the optional <i>minutes</i> argument is omitted, the client is blocked until explicitly unblocked. Unblock releases a specific IP address.
default block-action	drop send-tcp-rst	Indicates the behavior when clients are at the maximum number of connections: drop the connections that are over the limit or send TCP RST for connections over the limit. The default is drop. This limit can be modified on a per-client basis.
default connection-limit	integer	Indicates the number of simultaneous connections between 1 and 65535. The default is 100. This limit can be modified on a per-client basis.
default failure-limit	integer	Indicates the maximum number of failed requests a client is allowed before the proxy starts issuing warnings. Default is 50. This limit can be modified on a per-client basis.
default unblock-time	minutes	Indicates the amount of time a client is blocked at the network level when the client-warning-limit is exceeded. Time must be a multiple of 10 minutes, up to a maximum of 1440. The default is unlimited. This limit can be modified on a per-client basis.
default warning-limit	integer	Indicates the number of warnings sent to the client before the client is blocked at the network level and the administrator is notified. The default is 10; the maximum is 100. This limit can be modified on a per-client basis.

To Create and Edit a Client IP Address:

1. Make sure you are in the attack-detection client submode.

```
SGOS# (config) attack-detection
SGOS# (config attack-detection) client
SGOS# (config client)
```

2. Create a client.

```
SGOS# (config client) create client ip_address or ip_and_length
```

3. Move to edit mode.

```
SGOS# (config client) edit client_ip_address
```

The prompt changes to:

```
SGOS# (config client ip_address)
```

4. Change the client limits as necessary.

```
SGOS#(config client ip_address) block-action drop | send-tcp-rst
SGOS#(config client ip_address) connection-limit integer_between_1_and_65535
SGOS#(config client ip_address) failure-limit integer_between_1_and_65535
SGOS#(config client ip_address) unblock-time minutes
SGOS#(config client ip_address) warning-limit integer_between_1_and_65535
```

where:

block-action	<i>drop</i> <i>send-tcp-rst</i>	Indicates the behavior when the client is at the maximum number of connections: drop the connections that are over the limit or send TCP RST for the connection over the limit. The default is drop.
connection-limit	<i>integer</i>	Indicates the number of simultaneous connections between 1 and 65535. The default is 100.
failure-limit	<i>integer</i>	Indicates the behavior when the specified client is at the maximum number of connections: drop the connections that are over the limit or send TCP RST for the connection over the limit. The default is 50.
unblock-time	<i>minutes</i>	Indicates the amount of time a client is locked out at the network level when the client-warning-limit is exceeded. Time must be a multiple of 10 minutes, up to a maximum of 1440. The default is unlimited.
warning-limit	<i>integer</i>	Indicates the number of warnings sent to the client before the client is locked out at the network level and the administrator is notified. The default is 10; the maximum is 100.

To View the Specified Client Configuration, Enter:

```
SGOS#(config client ip_address) view
Client limits for 10.25.36.47:
Client connection limit:      700
Client failure limit:         50
Client warning limit:         10
Blocked client action:        Drop
Client connection unblock time:   unlimited
```

To View the Configuration for all Clients:

1. Exit from the edit client submode:

```
SGOS#(config client ip_address) exit
```

2. Use the following syntax to view the client configuration:

```
view <cr> | blocked | connections | statistics
```

To View All Settings:

```
SGOS#(config client) view
Client limits enabled:          true
Client interval:                20 minutes
```

```
Default client limits:  
  Client connection limit:      100  
  Client failure limit:        50  
  Client warning limit:        10  
  Blocked client action:       Drop  
  Client connection unblock time:  unlimited  
  
Client limits for 10.25.36.47:  
  Client connection limit:      700  
  Client failure limit:        50  
  Client warning limit:        10  
  Blocked client action:       Drop  
  Client connection unblock time:  unlimited
```

To View the Number of Simultaneous Connections to the ProxySG

```
SGOS#(config client) view connections  
Client IP      Connection Count  
127.0.0.1      1  
10.9.16.112    1  
10.2.11.133    1
```

To View the Number of Blocked Clients:

```
SGOS#(config client) view blocked  
Client           Unblock time  
10.11.12.13     2004-07-09 22:03:06+00:00UTC  
10.9.44.73      Never
```

To View Client Statistics:

```
SGOS#(config client) view statistics  
Client IP          Failure Count      Warning Count  
10.9.44.72         1                  0
```

To Disable Attack-Detection Mode for all Clients:

```
SGOS#(config client) disable-limits
```

Configuring Attack-Detection Mode for a Server or Server Group

You can create, edit, or delete a server. A server must be created before it can be edited. You can treat the server as an individual host or you can add other servers, creating a server group. All servers in the group have the same attack-detection parameters, meaning that if any server in the group gets the maximum number of simultaneous requests, all servers in the group are blocked.

To Create a Server or Server Group:

1. At the (config) prompt, enter the following commands:

```
SGOS#(config) attack-detection  
SGOS#(config attack-detection) server
```

The prompt changes to:

```
SGOS#(config server)
```

2. Create the first host in a server group, using the fully qualified domain name:

```
SGOS#(config server) create hostname
```

To Edit a Server or Server Group:

1. At the `(config server)` prompt, enter the following commands:

```
SGOS#(config server) edit hostname
```

The prompt changes to `(config server hostname)`.

```
SGOS#(config server hostname) add | remove hostname
SGOS#(config server hostname) request-limit integer_from_1_to_65535
```

where:

<i>hostname</i>	The name of a previously created server or server group. When adding a hostname to the group, the hostname does not have to be created.
-----------------	---

The host that was added when creating the group cannot be removed.

<i>add remove</i>	Adds or removes a server from this server group.
---------------------	--

<i>request-limit integer</i>	Indicates the number of simultaneous requests allowed from this server or server group. The default is 1000.
------------------------------	--

View the Server or Server Group Configuration:

```
SGOS#(config server hostname) view
Server limits for hostname:
Request limit: 1500
```

Using a Bypass List

A bypass list prevents the ProxySG from transparently accelerating requests to servers that perform IP authentication with clients. The bypass list contains IP addresses, subnet masks, and gateways. When a request matches an IP address and subnet mask specification in the bypass list, the request is sent to the designated gateway. A bypass list is only used for transparent caching.

There are three types of bypass lists: local list, central list, and policy-based list. Each of these bypass lists are discussed below.

The first two lists are not the same as the Local Policy file and the Central Policy file. The policy-based bypass list is a list maintained in the Forward Policy file or Local Policy file.

The local and central bypass lists can be managed two ways: either through the Management Console or through the CLI. For installation procedures for the two lists, see "Creating and Installing Local or Central Bypass Lists" on page 97.

Using the Local Bypass List

The local bypass list is one you create and maintain on your network. You can use a local bypass list alone, or in conjunction with a central list. You can also use a dynamic local bypass list to increase ProxySG efficiency. For more information on dynamic bypass lists, see "Using Dynamic Bypass" on page 93.

The gateways specified in the bypass list must be on the same subnet as the ProxySG. Note also that you are limited to 10,000 entries in the local bypass list.

The local bypass list contains a list of IP addresses, subnet masks, and gateways. It can also define the default bypass gateway to be used by both the local bypass list and central bypass list. The gateways specified in the bypass list must be on the same subnet as the ProxySG. When you download a bypass list, the list is stored in the appliance until it is replaced by downloading a new list.

The following is a sample of a local bypass list:

```
;define the default gateway for the local and central bypass list
BYPASS_GATEWAY 10.25.46.57
;define addresses to bypass
;IP address    subnet                  gateway (or use default gateway)
10.25.36.47    255.255.255.255
10.25.36.48    255.255.255.255
10.25.0.0      255.255.255.0        10.25.46.58
```

Note: The `BYPASS_GATEWAY` and default gateway must be on a different subnet from the IP addresses.

If you do not specify the `BYPASS_GATEWAY`, and you do not designate the gateway in the address specification, the ProxySG forwards the request to the default gateway defined in the network configuration.

For installation procedures for the local bypass list, see "Creating and Installing Local or Central Bypass Lists" on page 97.

Using Dynamic Bypass

Dynamic bypass provides a maintenance-free method for improving performance of the ProxySG by automatically compiling a list of requested URLs that return various kinds of errors.

With dynamic bypass, the ProxySG adds dynamic bypass entries containing the server IP address of sites that have returned an error to the appliance's local bypass list. For a configured period of time, further requests for the error-causing URLs are sent immediately to the origin server, saving the ProxySG processing time. The amount of time a dynamic bypass entry stays in the list and the types of errors that cause the ProxySG to add a site to the list, as well as several other settings, are configurable from the CLI.

Once the dynamic bypass timeout for a URL has ended, the ProxySG removes the URL from the bypass list. On the next client request for the URL, the ProxySG attempts to contact the origin server. If the origin server still returns an error, the URL is once again added to the local bypass list for the configured dynamic bypass timeout. If the URL does not return an error, the request is handled in the normal manner.

Dynamic bypass increases ProxySG efficiency because redundant attempts to contact the origin server are minimized.

Limitations

- Dynamic bypass applies to transparent proxy connections only.

- Dynamic bypass entries are lost when the ProxySG is restarted or the static bypass file is reinstalled.
- No filtering checks are performed on client requests that match entries in the dynamic bypass list.
- Requests to sites that are put into the dynamic bypass list will bypass future policy evaluation. Therefore, if a site that requires forwarding policy to reach its destination is populated into the dynamic bypass list, the site might be inaccessible.

Sites requiring that client accesses always be subjected to ProxySG filtering considerations must either use the appliance in explicit proxy mode or leave dynamic bypass functionality disabled.

Configuring Dynamic Bypass

Dynamic bypass is disabled by default. Enabling and fine-tuning dynamic bypass is a two-step process:

- Edit or create a local bypass list, adding the desired dynamic bypass timeout and threshold parameters.
- Use the CLI to enable dynamic bypass and set the types of errors that will cause dynamic bypass to add an entry to the bypass list.

Adding Dynamic Bypass Parameters to the Local Bypass List

The first step in configuring dynamic bypass is to edit the local bypass list to set the SERVER_BYPASS_THRESHOLD, MAX_DYNAMIC_BYPASS_ENTRY, and/or DYNAMIC_TIMEOUT values. This step is optional, as the ProxySG uses default configurations if you do not specify them in the local bypass list. Use the default values unless you have specific reasons for changing them. Contact Blue Coat technical support for detailed advice on customizing these settings.

The SERVER_BYPASS_THRESHOLD value defines the maximum number of entries in the dynamically generated portion of the local bypass list before the ProxySG consolidates client-server pair entries into a single server entry. The range is 1 to 256. The default is 16. When a consolidation occurs, the lifetime of the consolidated entry is set to the value of DYNAMIC_TIMEOUT.

The MAX_DYNAMIC_BYPASS_ENTRY defines the maximum number of total dynamic bypass entries. The range is 1 to 50,000. The default value is 16,000. When the number of entries exceeds the MAX_DYNAMIC_BYPASS_ENTRY value, the oldest entries will be removed to make way for new entries.

The DYNAMIC_TIMEOUT value defines the number of minutes a dynamic bypass entry can remain unreferenced before it is deleted from the bypass list. The range is 1 to 6000. The default value is 60.

Enabling Dynamic Bypass and Specifying Triggers

Enabling dynamic bypass and specifying the types of errors that will cause a URL to be added to the local bypass list are done with the CLI.

To Enable Dynamic Bypass and Trigger Events through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) dynamic-bypass enable  
SGOS#(config) dynamic-bypass trigger trigger_event
```

where *trigger_event* can be any item in listed in Table 4.1 on page 95.

Enabling dynamic bypass causes the following warning to appear:

WARNING:

Requests to sites that are put into the dynamic bypass list will bypass future policy evaluation. This could result in subversion of on-box policy. The use of dynamic bypass is cautioned.

Table 4.1: Values for the Dynamic-Bypass Trigger Event

Event	Description
all	Enables all dynamic bypass triggers.
non-http	Enables dynamic bypass for non-HTTP responses.
connect-error	Enables dynamic bypass for any connection failure to the origin server, including timeouts.
receive-error	Enables dynamic bypass for when a TCP connection to an origin server succeeds, but the cache does not receive an HTTP response.
400	Enables dynamic bypass for HTTP 400 responses.
401	Enables dynamic bypass for HTTP 401 responses.
403	Enables dynamic bypass for HTTP 403 responses.
405	Enables dynamic bypass for HTTP 405 responses.
406	Enables dynamic bypass for HTTP 406 responses.
500	Enables dynamic bypass for HTTP 500 responses.
502	Enables dynamic bypass for HTTP 502 responses.
503	Enables dynamic bypass for HTTP 503 responses.
504	Enables dynamic bypass for HTTP 504 responses.

Example

For instance, the following command will enable connection error events:

```
SGOS# (config) dynamic-bypass trigger connect-error
```

Bypassing Connection and Receiving Errors

In addition to HTTP code triggers, you can configure the ProxySG to trigger dynamic bypass for connection and receiving errors.

If `connect-error` is enabled, any connection failure to the origin server, including timeouts, inserts the origin server destination IP address into the dynamic bypass list. From this instance, the ProxySG bypasses any connection attempts from the client to this IP address. By default, the timeout duration is 20 seconds, and the retry count is 3. These parameters are not configurable. Both the timeout duration and the retry attempt, whichever occurs first, triggers `connect-error`.

If `receive-error` is enabled, when the cache does not receive an HTTP response on a successful TCP connection to the origin server, the origin server destination IP address is inserted into the dynamic bypass list. From this instance, the appliance bypasses any attempts from the client to this IP address. Server timeouts can also trigger `receive-error`. The default timeout value is 180 seconds, which can be changed (see "Configuring HTTP Timeout" on page 58).

Disabling Dynamic Bypass Triggers

Disabling one or more specific dynamic bypass triggers is an easy way to customize which errors cause a dynamic bypass entry to be created. For example, if you want all error events except 401 responses to create a dynamic bypass entry, you can enable all triggers and then disable only the 401-event trigger.

To Disable One or More Dynamic Bypass Triggers through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) dynamic-bypass no trigger event
```

where *event* can be any item listed above in Table 4.1.

To Clear the Dynamic Bypass List through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) dynamic-bypass clear
```

To Disable Dynamic Bypass through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) dynamic-bypass disable
```

Viewing the Dynamic Bypass List

You can view the dynamic bypass list several ways:

To Display the Dynamic Bypass List through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) show bypass-list
```

To Display the Dynamic Bypass List through the Management Console:

In a Web browser, enter the following URL:

```
https://ip_address_of_ProxySG:8082/TCP/IP-bypass
```

To view the Current Dynamic Bypass Configuration through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) show dynamic-bypass
```

To Disable Dynamic Bypass through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) dynamic-bypass disable
```

Using the Central Bypass List

The central bypass list is a shared list of addresses that is used by multiple ProxySG Appliances. The central list contains addresses to bypass, but does not specify gateways (because the ProxySG Appliances are located on different subnets, using different gateways). The gateway used for matches in the central bypass list is defined using the `BYPASS_GATEWAY` command in the local bypass list. If there is no `BYPASS_GATEWAY` option, the ProxySG uses the default gateway defined by the network configuration.

You can create your own central bypass list to manage multiple ProxySG Appliances, or you can use the central bypass list maintained by Blue Coat Technical Support at:

<https://download.bluecoat.com/release/SG3/files/CentralBypassList.txt>

Note: The central bypass list is limited to 10,000 entries.

The central bypass list maintained by Blue Coat contains addresses Blue Coat has identified as using client authentication. You can determine whether to download the list automatically when it changes or to just be sent an e-mail notifying you of the update. By default, neither is enabled.

For installation procedures for the central bypass list, continue with the next section.

Creating and Installing Local or Central Bypass Lists

You can install the local and central bypass lists several ways:

- Use the ProxySG Text Editor, which allows you to enter the lists (or copy and paste the contents of an already-created file) directly onto the ProxySG through the Management Console (see the instructions below).
- Create a local file on your local system; use the Management Console to browse to the file and install it (see the instructions below).
- Use a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the ProxySG. This can be done through either the Management Console or the CLI (see the instructions below).
- Use the CLI `inline bypass-list central | local` command, which allows you to paste the configurations onto the ProxySG (see the instructions below). For more information on using the CLI `inline` command, see "Using the Local Bypass List" on page 92 or "Using the Central Bypass List" on page 97.

To Install Bypass Lists through the Management Console:

1. Select Configuration>Network>Advanced>Bypass List.

The Bypass List tab displays.

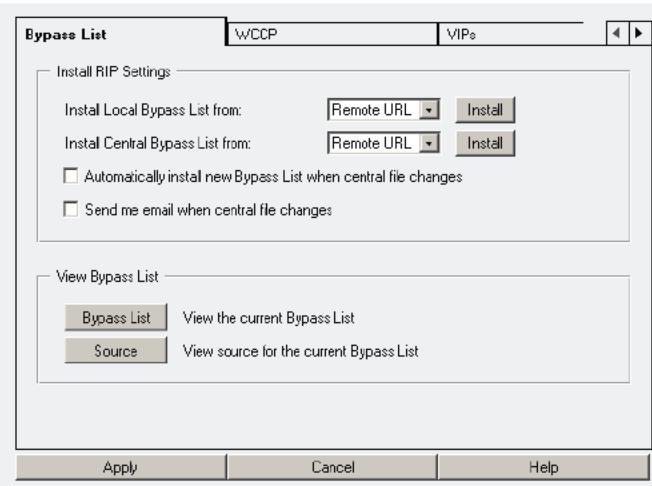


Figure 4-19: Bypass List Tab

2. To view the current bypass list or the source for the current bypass list before installing it, click **Bypass List** or **Source**.
3. (Optional) If installing the central bypass list, you can select whether to download the list automatically when it changes, or be sent an e-mail notifying you of the update. By default, neither is enabled.
4. Select a method to install the file for either the local or central bypass list; click **Install**.
 - Remote URL:**
Enter the fully-qualified URL, including the filename, where the routing table is located. To view the file before installing it, click **View**. Click **Install**. View the installation status that displays; click **OK**.

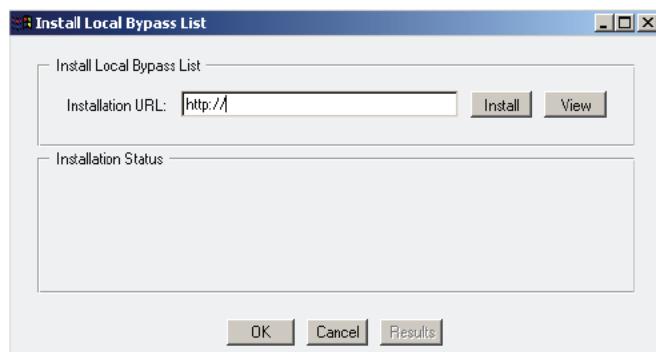


Figure 4-20: Specifying the Remote Location of a Local Bypass List Configuration File

Local File:

Click **Browse** to bring up the Local File Browse window. Browse for the file on your local system. Open it and click **Install**. When the installation is complete, a results window opens. View the results, close the window, and click **Close**.

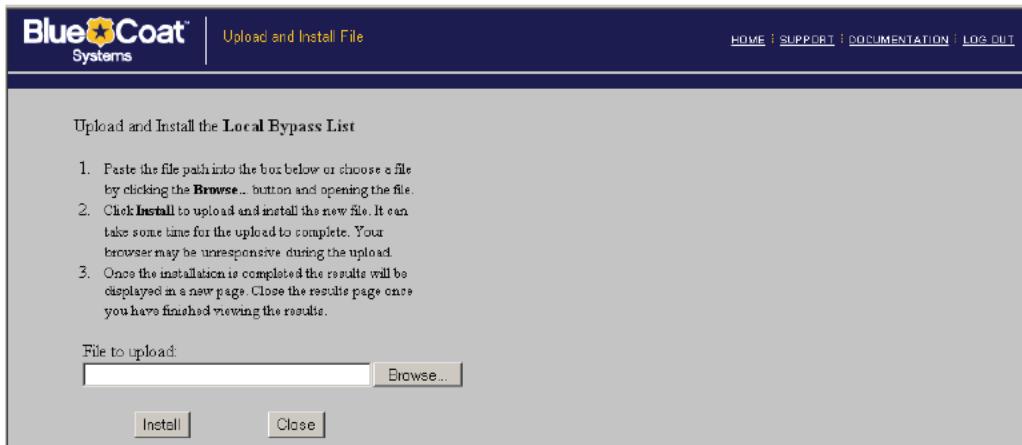


Figure 4-21: Specifying the Local Location of a Local Bypass List

Text Editor:

The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click **Install**. When the installation is complete, a results window opens. View the results, close the window, and click **Close**.

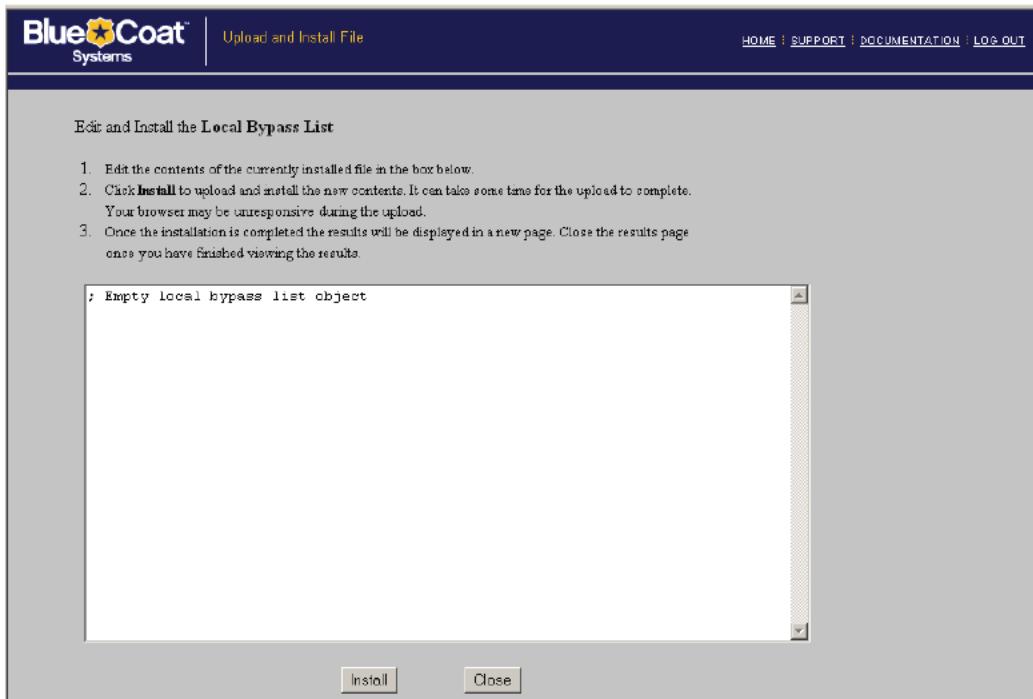


Figure 4-22: Creating a Local Bypass List on the ProxySG

5. Click **Apply**.

To Install an Already Existing Bypass List through the CLI:

At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) bypass-list {local-path | central-path} url
SGOS#(config) load bypass-list {local | central}
```

To Install a Bypass List through the CLI inline Command:

At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) inline bypass-list {local | central} end-of-file_marker
```

At this point you can paste in local or central configuration files, or you can enter values for specific settings, such as `server_bypass_threshold`, `max_dynamic_bypass_entry` or `dynamic_timeout`. When you finish, enter your `end-of-file` string.

Example

```
SGOS#(config) inline bypass-list local eof
max_dynamic_bypass_entry 20000
server_bypass_threshold 30
dynamic_timeout 100 eof
ok
```

Policy-Based Bypass Lists

ProxySG policies support the ability to define bypass lists. This section describes a property used to define a policy-based bypass list that can go into the Local Policy or Forward Policy file. For more information on defining policies, refer to the *Blue Coat Content Policy Language Guide*.

While static and dynamic bypass lists allow traffic to bypass the ProxySG based on a destination IP address, the `bypass_cache` property is intended to allow a bypass based on the properties of the client. This property uses the following syntax:

```
bypass_cache (yes | no)
```

If set to `yes`, the ProxySG is not queried and the response is not stored. Set to `no` to specify the default behavior, which is to follow standard caching behavior. This property is available only in the `<proxy>` layer.

This property has no effect on streaming objects, but does affect the following types of transactions: HTTP, HTTPS, FTP over HTTP, and transparent FTP.

Example

```
; Bypass the cache for requests from this client IP.
client_address=10.25.198.0 bypass_cache(yes)
```

Installing WCCP Settings

The ProxySG can be configured to participate in a WCCP (Web Cache Control Protocol) scheme, where a WCCP-capable router collaborates with a set of WCCP-configured ProxySG Appliances to service requests.

Before you can install the WCCP configurations, you must create a WCCP configuration file for the ProxySG. The ProxySG does not ship with a default WCCP configuration file.

You can install the WCCP settings several ways:

- Using the ProxySG Text Editor, which allows you to enter settings (or copy and paste the contents of an already-created file) directly onto the appliance.
- Creating a local file on your local system; the ProxySG can browse to the file and install it.
- Using a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the ProxySG.
- Using the CLI `inline wccp-settings` command, which allows you to paste the WCCP settings into the CLI.
- Using the CLI `wccp` command, which requires that you place an already-created file on an FTP or HTTP server and enter the URL into the CLI.

For more information about WCCP, see Appendix C: "Using WCCP" on page 785.

To Install WCCP Settings through the Management Console:

1. Select Configuration>Network>Advanced>WCCP.

The WCCP tab displays.

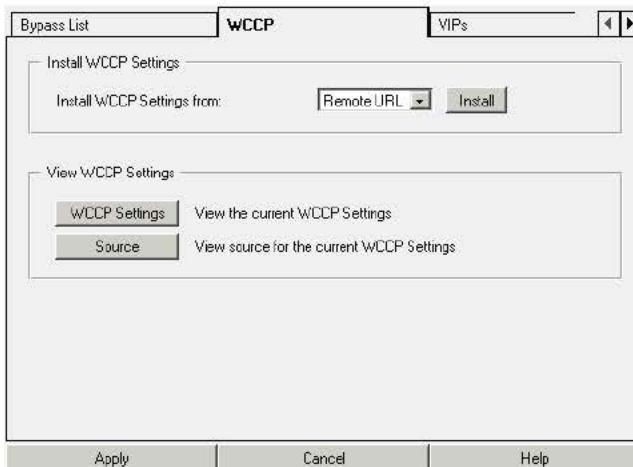


Figure 4-23: Network Advanced WCCP Tab

2. From the drop-down list, select the method used to install the WCCP settings; click **Install**.
 - Remote URL:

Enter the fully-qualified URL, including the filename, where the WCCP file is located. To view the file before installing it, click View. Click Install. Viewing the installation status that displays; click OK.

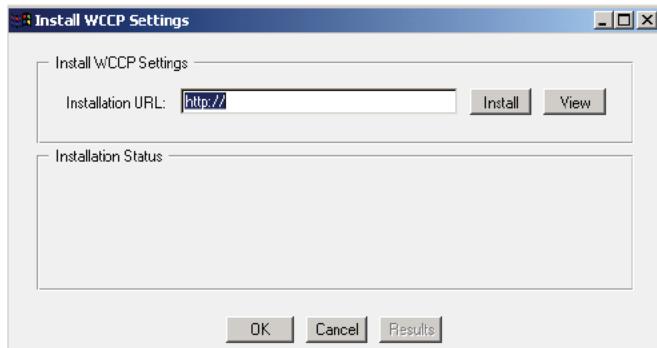


Figure 4-24: Specifying the Remote Location of a WCCP Settings File

Local File:

Click Browse to display the Local File Browse window. Browse for the file on the local system. Open it and click Install. When the installation is complete, a results window opens. View the results, close the window, and click Close.

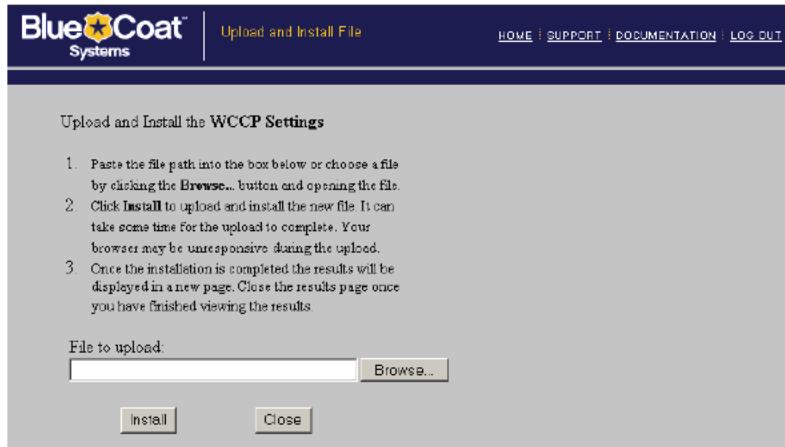


Figure 4-25: Specifying the Local Location of a WCCP Settings File

Text Editor:

The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click **Install**. When the installation is complete, a results window opens. View the results, close the window, and click **Close**.

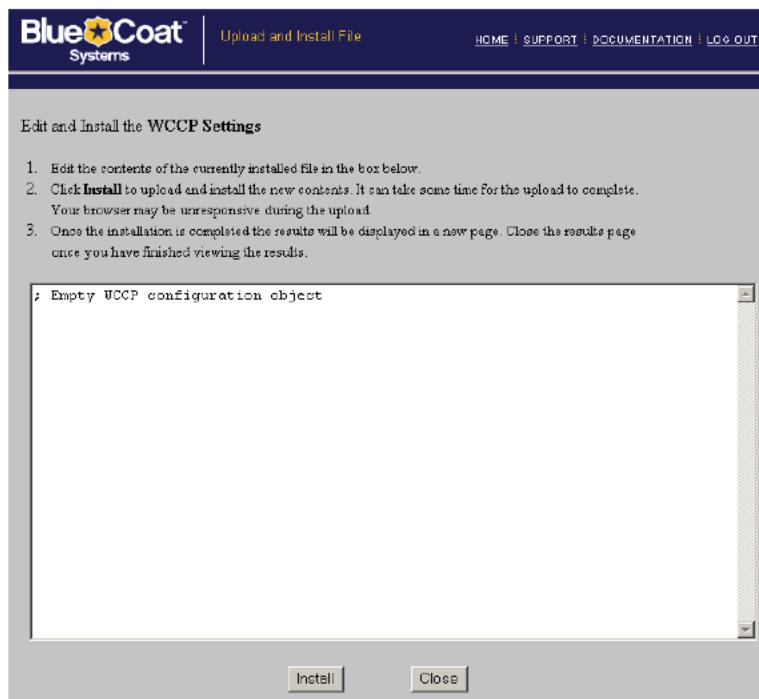


Figure 4-26: Creating a WCCP Settings File on the ProxySG

3. Click **Apply**.

To Install WCCP Settings through the CLI:

Do one of the following:

- To enter WCCP settings directly onto the ProxySG, enter the following commands at the (config) command prompt:

```
SGOS#(config) inline wccp-settings end-of-file_marker
wccp enable
wccp version 2
service-group 9
priority 1
protocol 6
service-flags destination-ip-hash
service-flags ports-defined
ports 80 21 1755 554 80 80 80 80
interface 6
home-router 10.16.18.2
forwarding 12
eof
```

Note: For detailed instructions on configuring an WCCP file, see Appendix C: "Using WCCP" on page 785.

- To enter a path to a remote URL where you have placed an already-created static route table, enter the following commands at the (config) command prompt:

```
SGOS# (config) wccp path url
```

where *url* is a fully qualified URL, including the filename, where the configuration file is located.

```
SGOS# (config) load wccp-settings
SGOS# (config) wccp enable
```

Virtual IP Addresses

Virtual IP (VIP) addresses are addresses assigned to a system that are recognized by other systems on the network. Up to 255 VIPs can be configured on each ProxySG. They have several uses:

- Assign multiple identities to a system on the same or different network, partitioning the box in to separate logical entities for resource sharing or load sharing.
- Create an HTTPS Console to allow multiple, simultaneous, secure connections to the system.
- Direct authentication challenges to different realms.
- Set up failover among multiple ProxySG s on the same subnet.

For information on creating an HTTPS Console, see "Creating and Editing Services" on page 121; for information on using VIPs with authentication realms, see Chapter 9: "Using Authentication Services" on page 233; to use VIPs with failover, see "Configuring Failover" on page 105.

To Create a VIP through the Management Console:

- Select Configuration>Network>Advanced>VIPs.

The VIPs tab displays.

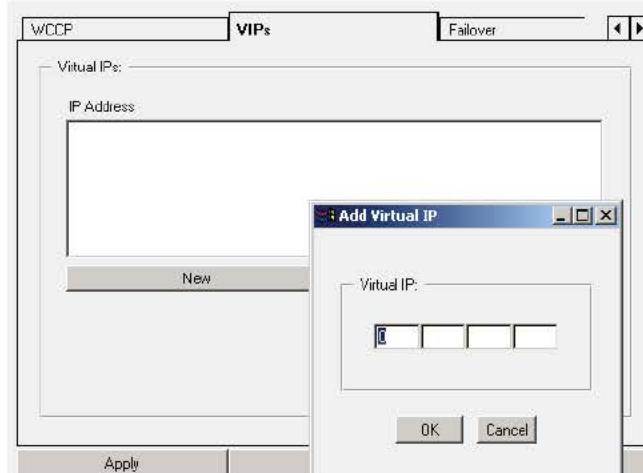


Figure 4-27: Network Advanced VIPs Tab

2. Click New.

The Add VIP dialog displays.

3. Enter the virtual IP address you want to use. It can be any IP address, except a multicast address. (A multicast address is a group address, not an individual IP address.)

Note: You cannot create a VIP address that is the IP address used by the origin server. You must assign a different address on the ProxySG, and use DNS and forwarding to point to the origin server's real IP address.

4. Click OK; click Apply.

The VIP address can now be used.

To Create a VIP through the CLI:

At the (config) command prompt, run the `virtual ip-address` command:

```
SGOS#(config) virtual address ip_address
      ok
```

To Delete a VIP through the CLI:

Note that VIP addresses are deleted silently. If you are using a VIP for a service, the service will no longer work once the VIP is deleted.

```
SGOS#(config) virtual no address ip_address
      ok
```

To Clear all VIP Addresses in the System:

```
SGOS#(config) virtual clear
      ok
```

To View all the VIPs in the System:

```
SGOS#(config) show virtual
Virtual IP addresses:
SGOS#(config) accelerated-pac path 10.25.36.47
  10.9.36.47
  10.25.36.48
  10.25.36.47
```

Configuring Failover

Using IP address failover, you can create a redundant network for any explicit proxy configuration. If you require transparent proxy configuration, you can create software bridges to use failover. For information on creating software bridges, see "About Bridging" on page 68.

Note: If you use the Pass-Through card for transparent proxy, you must create a software bridge rather than configuring failover. For information on using the Pass-Through card, see "About the Pass-Through Card" on page 68.

Using a pool of IP addresses to provide redundancy and load balancing, Blue Coat migrates these IP addresses among a group of machines.

About Failover

Failover allows a second machine to take over if a first machine fails, providing redundancy to the network through a master/slave relationship. In normal operations, the master (the machine whose IP address matches the group name) owns the address. The master sends keepalive messages (*advertisements*) to the slaves. If the slaves do not receive advertisements at the specified interval, the slave with the highest configured priority takes over for the master. When the master comes back online, the master takes over from the slave again.

The Blue Coat failover implementation resembles the Virtual Router Redundancy Protocol (VRRP) with the following exceptions:

- A configurable IP multicast address is the destination of the advertisements.
- The advertisements' interval is included in protocol messages and is learned by the slaves.
- A virtual router identifier (VRID) is not used.
- Virtual MAC addresses are not used.
- MD5 is used for authentication at the application level.

Masters are elected, based on the following factors:

- If the failover mechanism is configured for a physical IP address, the machine owning the physical address will have the highest priority. This is not configurable.
- If a machine is configured as a master using a virtual IP address, the master has a priority that is higher than the slaves.

Configuring Failover

Before you begin, be aware that software bridges must already exist before you can use them to configure failover. For information on configuring bridges, see "Adapters" on page 64.

You also need to decide which machine will be the master and which machines will be the slaves, and whether you want to configure explicit proxy or transparent proxy network.

When configuring the group, the master and all the systems in the group must have exactly the same failover configuration except for priority, which is used to determine the rank of the slave machines. If no priority is set, a default priority of 100 is used. If two ProxySG appliances have equal priority, the one with the highest physical address ranks higher.

To Configure Failover through the Management Console:

1. Go to Configuration>Network>Advanced>Failover.

The Failover tab displays.

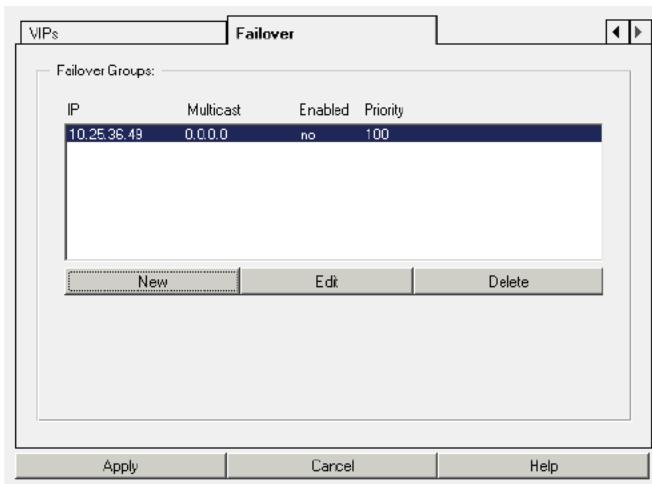


Figure 4-28: Network Advanced Failover Tab

2. Click New.

The Add Failover Group dialog displays.

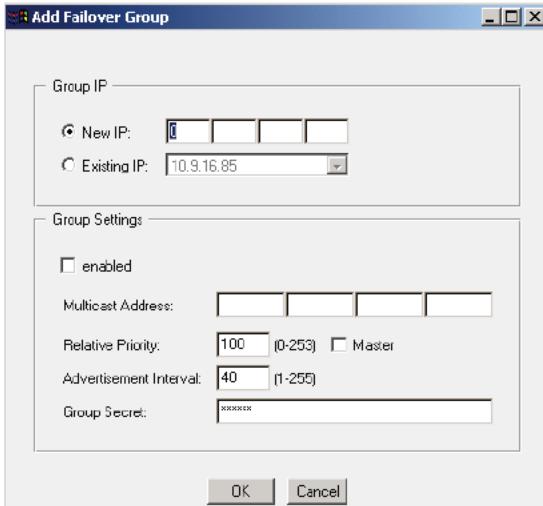


Figure 4-29: Add Failover Group Dialog

3. In the Add Failover Group dialog that appears, fill in the fields as appropriate:

- Create a group using either a new IP address or an existing IP address. If the group has already been created, you cannot change the new IP address without deleting the group and starting over.
- The **enabled** option specifies whether this group is active or inactive. Select **enabled** to enable the failover group.
- Multicast address refers to a Class D IP address that is used for multicast. It is not a virtual IP address.

Note: Class D IP addresses are reserved for multicast. A Class D IP address has a first bit value of 1, second bit value of 1, third bit value of 1, and fourth bit value of 0. The other 28 bits identify the group of computers that receive the multicast message.

- ❑ Relative Priority refers to a range from 1-255 that is assigned to systems in the group. 255 is reserved for the system whose failover group ID equals the real IP address.
 - ❑ (Optional) Master identifies the system with the highest priority.
 - ❑ (Optional) Advertisement Interval refers to the length of time between advertisements sent by the group master. The default is 40 seconds. Once the group master has failed, the slave with the highest priority takes over (after approximately three times the interval value). The failover time of the group can be controlled by setting this value.
 - ❑ (Optional, but recommended) Group Secret refers to a password shared only with the group.
4. Click OK; click Apply.

To Configure Failover through the CLI:

1. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) failover
SGOS#(config failover) create group_address
```

The IP address does not have to exist.

```
SGOS#(config failover) edit group_address
SGOS#(config failover group_address) multicast-address multicast_address
SGOS#(config failover group_address) master
SGOS#(config failover group_address) priority number
SGOS#(config failover group_address) interval seconds
SGOS#(config failover group_address) secret secret
-or-
SGOS#(config failover group_address) encrypted-secret encrypted_secret
SGOS#(config failover group_address) enable
```

where:

<i>group_address</i>	Refers to the IP address or VIP address that will be monitored by this group. Once the group has been named, you cannot change the name. To change the name, you must delete the group and start over.
<i>multicast-address</i> <i>multicast_address</i>	Refers to a multicast address where the master sends the keepalives (advertisements) to the slave systems.
<i>master</i>	(Optional) Identifies the system to be used as the master.
<i>no</i>	Negates these settings: multicast-address, priority, interval, secret, and master.
<i>priority number</i>	(Optional) Refers to the rank of slave systems. The range is from 1 to 254. (The master system, the one whose IP address matches the group address, gets 255.) Note that output of show config and show failover might differ when the master system is also the holder of the physical IP address.
<i>interval seconds</i>	(Optional) Refers to the time between advertisements from the master to the multicast address. The default is 40 seconds. Entering <i>no interval</i> resets the interval to the default time of 40 seconds.
<i>secret secret</i> -or- <i>encrypted-secret</i> <i>encrypted_secret</i>	(Optional but recommended) Refers to a password shared only with the group. You can create a secret, which will then be hashed, or you can provide an encrypted secret.
<i>enable disable</i>	Enables or disables failover on the ProxySG.

2. (Optional) View the results.

```
SGOS#(config) show failover configuration group_address
Failover Config
Group Address: 10.25.36.47
Multicast Address      : 224.1.2.3
Local Address          : 10.9.17.159
Secret                 : none
Advertisement Interval: 40
Priority               : 100
Current State          : DISABLED
Flags                  : V M
```

Three flags exist, set as you configure the group.

V—Specifies the group name is a virtual IP address.

R—Specifies the group name is a physical IP address

M—Specifies this machine can be configured to be the master if it is available

3. (Optional) You can view Failover Group Statistics

These are all integers/counters that count various events.

```
SGOS#(config) show failover statistics
Failover Statistics
Advertisements Received   : 0
Advertisements Sent       : 194
States Changes           : 2
Bad Version              : 0
```

Bad Packet	:	0
Bad Checksum	:	0
Packet Too Short	:	0
Bad Packet Header	:	0
Invalid Group	:	0

Viewing Statistics

At any time, you can view statistics for any failover group you have configured on your system.

Complete the following steps to view failover statistics.

1. Select Configuration>Statistics>Failover.

The Status tab displays.

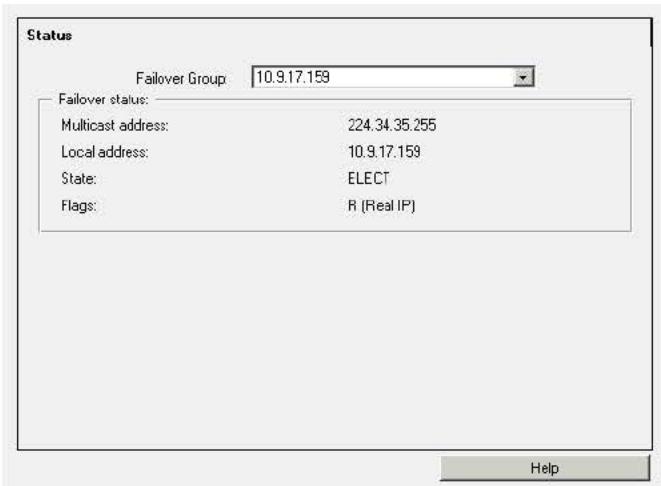


Figure 4-30: Statistics Failover Tab

2. From the drop-down list, select the group whose statistics you want to view.

The information displayed includes the multicast address, the local address, the state, and any flags, where V specifies the group name is a virtual IP address, R specifies the group name is a physical IP address, and M specifies this machine can be configured to be the master if it is available.

TCP-IP Configuration

Use the TCP-IP configuration options to enhance the performance and security of the ProxySG. Except for IP Forwarding (see "IP Forwarding" on page 171), these commands are only available through the CLI.

- RFC-1323: Enabling RFC-1323 support enhances the high-bandwidth and long-delay operation of the ProxySG over very high-speed paths, ideal for satellite environments.
- TCP NewReno: Enabling TCP NewReno support improves the fast recovery of the ProxySG.
- ICMP Broadcast Echo: Disabling the response to these messages can limit security risks and prevent an attacker from creating a distributed denial of service (DDoS) to legitimate traffic.

- ICMP Timestamp Echo: Disabling the response to these messages can prevent an attacker from being able to reverse engineer some details of your network infrastructure.
- PMTU Discovery: Enabling PMTU Discovery prevents packets from being unable to reach their destination because they are too large.

To view the TCP-IP configuration, see "Viewing the TCP-IP Configuration" on page 113.

RFC-1323

The RFC-1323 TCP-IP option enables the ProxySG to use a set of extensions to TCP designed to provide efficient operation over large bandwidth-delay-product paths and reliable operation over very high-speed paths, including satellite environments. RFC-1323 support can only be configured through the CLI, and is enabled by default.

To Enable or Disable RFC-1323 Support through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) tcp-ip rfc-1323 {enable | disable}
```

TCP NewReno

NewReno is a modification of the Reno algorithm. TCP NewReno improves TCP performance during fast retransmit and fast recovery when multiple packets are dropped from a single window of data. TCP NewReno support is disabled by default.

To Enable or Disable TCP NewReno Support through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) tcp-ip tcp-newreno {enable | disable}
```

ICMP Broadcast Echo Support

Disabling the ICMP broadcast echo command can prevent the ProxySG from participating in a Smurf Attack. A Smurf attack is a type of Denial-of-Service (DoS) attack, where the attacker sends an ICMP echo request packet to an IP broadcast address. This is the same type of packet sent in the ping command, but the destination IP is broadcast instead of unicast. If all the hosts on the network send echo reply packets to the ICMP echo request packets that were sent to the broadcast address, the network will be jammed with ICMP echo reply packets, making the network unusable. By disabling ICMP broadcast echo response, the ProxySG will not participate in the Smurf Attack.

This setting is disabled by default.

To Enable or Disable ICMP Broadcast Echo Support through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) tcp-ip icmp-bcast-echo {enable | disable}
```

For more information on preventing DDoS attacks, see "Attack Detection" on page 87.

ICMP Timestamp Echo Support

By disabling the ICMP timestamp echo commands, you can prevent an attacker from being able to reverse engineer some details of your network infrastructure.

For example, by disabling the ICMP timestamp echo commands, you can prevent an attack that occurs when the ProxySG responds to an ICMP timestamp request by accurately determining the target's clock state, allowing an attacker to more effectively attack certain time-based pseudo-random number generators (PRNGs) and the authentication systems on which they rely.

This setting is disabled by default.

To Enable or Disable ICMP Timestamp Echo Support through the CLI:

At the `(config)` command prompt, enter the following command:

```
SGOS#(config) tcp-ip icmp-timestamp-echo {enable | disable}
```

PMTU Discovery

PMTU (Path Maximum Transmission Unit) is a mechanism designed to discover the largest packet size that can be sent that will not be fragmented anywhere along the path between two communicating ProxySG Appliances that are not directly attached to the same link. A ProxySG doing PMTU sets the `Do-Not-Fragment` bit in the IP header when transmitting packets. If fragmentation becomes necessary before the packets arrive at the second ProxySG, a router along the path discards the packets and returns an `ICMP Host Unreachable` error message, with the error condition of `Needs-Fragmentation`, to the original ProxySG. The first ProxySG then reduces the PMTU size and re-transmits the transmissions.

The discovery period temporarily ends when the ProxySG's estimate of the PMTU is low enough that its packets can be delivered without fragmentation or when the ProxySG stops setting the `Do-Not-Fragment` bit. Five minutes later (this value is configurable), rediscovery is used to see if the transmittable packet size has changed.

Following discovery and rediscovery, the size of the packets that are transferred between the two communicating nodes dynamically adjust to a size allowable by the path, which might contain multiple segments of various types of physical networks.

PMTU is disabled by default.

A ProxySG that is not running PMTU might send packets larger than that allowed by the path, resulting in packet fragmentation at intermediate routers. Packet fragmentation affects performance and can cause packet discards in routers that are temporarily overtaxed.

Configuring PMTU Discovery through the CLI

Note: PMTU discovery can only be configured through the CLI. It is not available through the Management Console.

At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) tcp-ip pmtu-discovery enable | disable
SGOS#(config) tcp-ip pmtu-discovery expire-period seconds
SGOS#(config) tcp-ip pmtu-discovery probe-interval seconds
```

where

tcp-ip	enable disable	Allows you to enable PMTU discovery. The default is disabled.
pmtu-discovery	expire-period <i>seconds</i>	Determines the time, in seconds, when PMTU rediscovery takes place after receiving the ICMP Host Unreachable - Needs Fragmentation error message. The default is 600 seconds.
	probe-interval <i>seconds</i>	Determines the time, in seconds, when the next PMTU rediscovery takes place following a previous consecutive successful expansion of the PMTU value. The default is 120 seconds.

Viewing the TCP-IP Configuration

To view the TCP-IP configuration:

```
SGOS#(config) show tcp-ip
RFC-1323 support:           enabled
TCP Newreno support:         disabled
IP forwarding:               disabled
ICMP bcast echo response:   disabled
ICMP timestamp echo response: disabled
Path MTU Discovery:          enabled
PMTU expiration period:     600 seconds
PMTU probe interval:         120 seconds
TCP window size:              65535 bytes
```


Chapter 5: Managing Port Services

This chapter describes port services that are configurable on the ProxySG. These services run on the ProxySG, and include Management Consoles such as HTTPS, HTTP, SSH, and Telnet Consoles, and application proxies such as Instant Messenger (IM), SOCKS, FTP, MMS, and RTSP, HTTP and HTTPS.

Other proxy services, like ICAP and Websense, are remote to the ProxySG and are discussed in Chapter 10: "External Services" on page 321.

This chapter discusses

- "Managing Multiple Management Consoles"
- "Creating and Editing Services"

This chapter does not discuss configuration of some of the port services that are enabled here. The following are discussed in Chapter 6: "Configuring Proxies" on page 137:

- FTP Proxy
- HTTP Proxy
- SOCKS Proxy
- Shell Proxies (Telnet)

Section A: Managing Multiple Management Consoles

Section A: Managing Multiple Management Consoles

The ProxySG ships with number of already existing consoles designed to manage the system and communication with the system:

- HTTP and HTTPS Consoles: These consoles are designed to allow you access to the ProxySG. The HTTPS Console is created and enabled; the HTTP Console is created by default but not enabled because it is less secure than HTTPS.
- SSH Console: This console is created and enabled by default, allowing you to gain access to the ProxySG through the CLI with your SSH service.
- Telnet Console: This console is created but is disabled by default because of security concerns. You must enable the service before you can access the ProxySG through a Telnet client (not recommended).

HTTPS Console (Secure Console)

The HTTPS Console provides secure access to the Management Console through the HTTPS protocol.

You can create multiple management HTTPS consoles, allowing you to simultaneously access the Management Console using any IP address belonging to the box as well as any of the ProxySG's virtual IP (VIP) addresses. The default is HTTPS over port 8082.

The ProxySG ships with an HTTPS Console already created and enabled. You do not need to create other HTTPS Consoles unless you need them for other purposes.

An HTTPS Console and an HTTPS service are not the same. The HTTPS Console is meant only for accessing the ProxySG. An HTTPS service is meant to allow secure access to other systems.

Creating a new HTTPS Console port requires three steps, discussed more fully in the following sections:

- Selecting a keyring (a keypair and a certificate that is stored together)
- Selecting an IP address and port on the system that the service will use, including virtual IP addresses
- Putting the keyring and service together into an HTTPS Console

Selecting a Keyring

The ProxySG ships with a default keyring that can be reused with each HTTPS service that you create. You can also create your own keyrings for other purposes.

To use the default keyring, simply accept the default keyring through the Management Console, or, if you're using the CLI, enter `default` for the keyring ID when using the `services https-console create` command.

Note: When using certificates for the HTTPS Console or for HTTPS termination services that are issued by Certificate Signing Authorities that are not well-known, see "Troubleshooting Certificate Problems" on page 195.

Section A: Managing Multiple Management Consoles

For information on creating a keypair and a certificate to make a keyring, see "Configuring HTTPS Termination" on page 176.

Selecting an IP Address

You can use any IP address on the ProxySG for the HTTPS Console service, including virtual IP addresses. To create a virtual IP address, see "Virtual IP Addresses" on page 104.

Enabling the HTTPS Console Service

The final step in editing or creating an HTTPS Console service is to select a port and enable the service.

To Create or Edit an HTTPS Console Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.

The Service Ports tab displays.

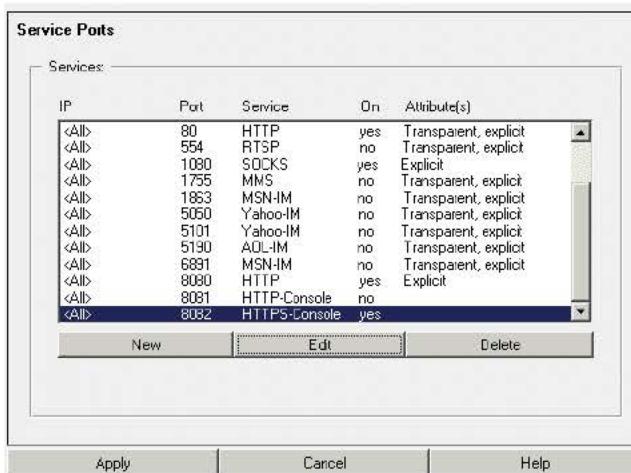


Figure 5-1: Service Ports Tab

2. Do one of the following:

- To create a new HTTPS Console port service, click New; the Add Service dialog appears. Select HTTPS-Console from the Protocol drop-down list.
- To edit an existing HTTP Console port service, highlight the HTTPS Console and click Edit; the Edit Service dialog appears.

Continue with the next step.

Section A: Managing Multiple Management Consoles



Figure 5-2: HTTPS-Console Add Service Dialog

3. The default IP address value is <All>. To limit the service to a specific IP address, select the IP address from the drop-down list. It must already exist.
4. Identify the port you want to use for this service.
5. In the Keyring drop-down list, select any already created keyring that is on the system. The system ships with a default keyring that can be reused for each HTTPS service.

Note: The configuration-passwords-key keyring that shipped with the ProxySG does not contain a certificate and cannot be used for HTTPS Consoles.

6. (Optional) In the SSL Versions drop-down list, select the version that you want to use for this service. The default is SSL v2/v3 and TLS v1.
7. Click OK; click Apply.

Note: For information on creating keyrings and client certification lists, see "Configuring HTTPS Termination" on page 176.

To Create Another HTTPS Console Port Service through the CLI:

1. At the **(config)** command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) https-console
SGOS#(config services https-console) create [ip_address:]port [keyring id]
```

If you do not specify a keyring, the default is used.

```
SGOS#(config services https-console) attribute cipher-suite ip_address:port
```

2. (Optional) View the results:

Section A: Managing Multiple Management Consoles

```
SGOS#(config services https-console) view
Port: 8082 IP: 0.0.0.0 Type: https-console
Keyring: default
Properties: explicit, enabled
Cipher suite:
RC4-MD5:RC4-SHA:DES-CBC3-SHA:DES-CBC3-MD5:RC2-CBC-MD5:RC4-64-MD5:DES-CBC-SHA:DE
S-CBC-MD5:EXP1024-RC4-MD5:EXP1024-RC4-SHA:EXP1024-RC2-CBC-MD5:EXP1024-DES-CBC-S
HA:EXP-RC4-MD5:EXP-RC2-CBC-MD5:EXP-DES-CBC-SHA:
+SSLv2:+SSLv3+LOW:+SSLv2+LOW:+EXP0HTTP
```

Note: To create client-certification lists and keyrings, see "Configuring HTTPS Termination" on page 176. To set the cipher-suite to the ciphers you want to use, see "Changing the Cipher Suites of the SSL Client" on page 199.

HTTP Console

The HTTP Console is meant to allow you to access the ProxySG if you require a less secure environment. The default HTTP Console is already configured; you must enable it before it can be used.

You can create and use more than one HTTP Console as long the IP address and the port do not match the existing HTTP Console settings.

To Create or Edit an HTTP Console Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.

The Service Ports tab displays.

2. Do one of the following:

- To create a new HTTP-Console port service, click New; the Add Service dialog appears. Select HTTP-Console from the Protocol drop-down list.
- To edit an existing HTTP-Console port service, highlight the HTTP-Console and click Edit; the Edit Service dialog appears.



Figure 5-3: HTTP-Console Add Service Dialog

In either case, continue with the next step.

Section A: Managing Multiple Management Consoles

3. The default IP address value is <All>. To limit the service to a specific IP address, select the IP address from the drop-down list. It must already exist.
4. Identify the port you want to use for this service.
5. Click OK; click Apply.

To Create or Edit an HTTP Console Port Service and Enable It through the CLI:

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) http-console
SGOS#(config services http-console) create [ip_address:]port
```

2. (Optional) View the results:

```
SGOS#(config services http-console) view
Port: 8085 IP: 0.0.0.0 Type: http-console
Properties: enabled
```

SSH Console

The SSH Console is created and enabled by default. Only one SSH Console can exist on the ProxySG. If you inadvertently deleted the SSHv1 and SSHv2 host keys from the system at the same time, you automatically disabled the SSH Console and will have to enable the SSH Console after you create a host key.

For information on managing SSH, see "Configuring the SSH Console" on page 47.

To Edit an SSH Console Service through the Management Console:

1. Select Configuration>Services>Service Ports.
The Service Ports tab displays.
2. To edit the existing SSH-Console port service, highlight the SSH-Console and click Edit.
The Edit Service dialog appears.



Figure 5-4: SSH-Console Add Service Dialog

3. The default IP address value is all. To limit the service to a specific IP address, select the IP address from the drop-down list.

Section A: Managing Multiple Management Consoles

4. In the Port field, specify a port number; select Enable.
5. Click OK; click Apply.

To Create an SSH Port Service through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) services
SGOS# (config services) ssh-console
SGOS# (config services ssh-console) create [ip_address:]port
SGOS# (config services ssh-console) enable [ip_address:]port
```

Telnet Console

The Telnet Console allows you to connect to and manage the ProxySG using the Telnet protocol. Remember that Telnet is an insecure protocol that should not be used in insecure conditions. By default, only SSH is created and enabled.

Blue Coat Systems recommends against using Telnet because of the security hole it creates.

Note: If you do enable the Telnet Console, be aware that you cannot use Telnet everywhere in the CLI. Some modules, such as SSL, respond with the error message:

Telnet sessions are not allowed access to ssl commands.

To Create or Edit a Telnet Console Port Service through the Management Console:

Before you begin, make sure that no Telnet service exists on the default telnet port (23). If it does exist, delete it and apply the changes before continuing. If you also want a Telnet service, you can re-create it later, being sure to use a different port. For information on the Telnet service, see "Telnet Shell Proxy Service" on page 134.

1. Select Configuration>Services>Service Ports.

The Service Ports tab displays.

2. Do one of the following:

- To create a new Telnet-Console port service, click New; the Add Service dialog appears. Select Telnet-Console from the Protocol drop-down list.
- To edit an existing Telnet-Console port service, highlight the Telnet-Console and click Edit; the Edit Service dialog appears.

In either case, continue with the next step.

Section A: Managing Multiple Management Consoles



Figure 5-5: Telnet Console Edit Service Dialog

3. Select Telnet protocol from the drop-down list.
4. The default IP address value is all. To limit the service to a specific IP address, select the IP address from the drop-down list.
5. In the Port field, specify a port number; 23 is the default.

Note: If you want to use the Telnet shell proxy and retain the Telnet Console as well, you must change the port number on one of them. Only one service is permitted on a port. For more information on the Telnet shell proxy, see "Telnet Shell Proxies" on page 164.

6. Select Enabled.
7. Click OK; click Apply.

To Create or Edit a Telnet Port Service through the CLI:

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) telnet-console
SGOS#(config services telnet-console) create [ip_address:]port
```

2. (Optional) View the results.

```
SGOS#(config services telnet-console) view
Port: 23          IP: 0.0.0.0          Type: telnet-console
Properties: enabled
```

Section B: Creating and Editing Services

Section B: Creating and Editing Services

Port services define attributes for ports on which the ProxySG listens for Web requests. Each service applies to all IP addresses, or can be limited to a specific address.

You can create as many services as you require, keeping in mind that every newly created service uses up resources.

Note: When multiple non-wildcard services are created on a port, all of them must be of the same service type. So you can have HTTP listening on a given port on some subset of interfaces (or VIPs), but you can't have HTTP on one interface and HTTPS on a different interface with both using the same port.

Also note that wildcard services and non-wildcard services cannot both exist at the same time on a given port.

The following table lists the available ProxySG services, including their attributes and default status. The defaults are for a new ProxySG. If you have an upgraded appliance, the settings do not change.

Table 5.1: Proxy Port Services

Proxy Service	Default Port	Default	Configuration Discussed
DNS	53 (both transparent and explicit)	Disabled	"DNS-Proxy"
FTP	21 (transparent and explicit)	Disabled	"FTP"
HTTP	80 (transparent and explicit)	Enabled	"HTTP"
HTTP	8080 (explicit only)	Enabled	"HTTP"
HTTP-Console	8081	Disabled	"HTTP Console"
HTTPS		Disabled	"HTTPS"
HTTPS-Console	8082	Enabled	"HTTPS Console (Secure Console)"
MSN-IM	1863 (transparent and explicit) and 6891 (transparent and explicit)	Disabled	"Instant Messaging Protocols"
Yahoo-IM	5050 (transparent and explicit) and 5101 (transparent and explicit)	Disabled	"Instant Messaging Protocols"
AOL-IM	5190 (transparent and explicit)	Disabled	"Instant Messaging Protocols"
MMS	1755 (transparent and explicit)	Disabled	"Streaming Protocols"
RTSP	554 (transparent and explicit)	Disabled	"Streaming Protocols"
SOCKS	1080	Disabled	"SOCKS"
SSH-Console	22	Enabled	"SSH Console"
TCP-Tunnel		Disabled	"TCP Tunneling"
Telnet-Console	23	Disabled	"Telnet Console"
Telnet shell proxy	23	Disabled	"Telnet Shell Proxy Service"

Section B: Creating and Editing Services

Note: If HTTP is configured to be explicit, Internet Explorer version 5.5 and 6.0 users accessing FTP sites over HTTP must disable the browser setting Enable folder view for FTP sites. To access this attribute in Internet Explorer, select Tools>Internet Options, click the Advanced tab, deselect Enable folder view for FTP sites, and click OK.

About Service Attributes

The service attributes define the parameters the ProxySG uses for a particular service. In addition to configuring the default port services, you can create additional ports and define their attributes.

Note: For all service types except HTTPS, a specific listener cannot be posted on a port if the same port has a wildcard listener of any service type already present.

The following table describes the attributes; however, depending on the protocol, not all attributes are available.

Table 5.2: Attributes

Attribute	Description
Explicit	Enables or disables explicit attribute for port. (Explicit allows connections to a ProxySG IP address.)
Transparent	Enables or disables transparent-proxy attribute for port. (This allows connections to any IP address other than those belonging to the ProxySG.)
Authenticate-401	All transparent and explicit requests received on the port always use transparent authentication (cookie or IP, depending on the configuration). This is especially useful to force transparent proxy authentication in some proxy-chaining scenarios.
Send client IP	Enables or disables sending of client's IP address instead of the ProxySG's IP address. For more information, see the section on tracking client IP addresses using server-side transparency.

Note: If you use the CLI to create a service, specify 0.0.0.0 to define that the service listens on all IP addresses; specify the individual IP address to limit the service to one IP address.

DNS-Proxy

When a DNS-Proxy service is enabled, it listens on port 53 for both explicit and transparent DNS domain query requests. By default, the service is created but not enabled.

The DNS-Proxy does a lookup of the DNS cache to determine if requests can be answered. If yes, the ProxySG responds. If not, the DNS-Proxy forwards the request to the DNS server list configured on the ProxySG. (To configure the DNS server list, see Configuration>Network>DNS.)

Note: The ProxySG is not a DNS server. It does not perform zone transfers, and recursive queries are forwarded to other name servers.

Section B: Creating and Editing Services

Through policy, you can configure the list of resolved domain names (the *resolving name list*) the DNS-Proxy uses. The domain name in each query received by the ProxySG is compared against the resolving name list. Upon a match, the ProxySG checks the resolving list. If a domain name match is found but no IP address was configured for the domain, the ProxySG sends a DNS query response containing its own IP address. If a domain name match is found with a corresponding IP address, that IP address is returned in a DNS query response. All unmatched queries are sent to the name servers configured on the ProxySG.

To Create or Edit a DNS-Proxy Service through the Management Console:

1. Select Configuration>Services>Service Ports.

The Service Ports tab displays.

2. Click New or Edit; the Add (or Edit) Service dialog appears.
3. Select DNS-Proxy from the Protocol drop-down list.

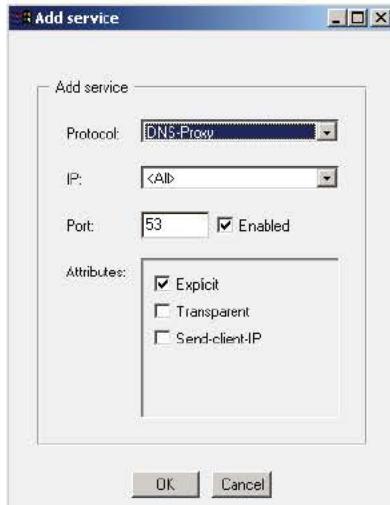


Figure 5-6: DNS-Proxy Add Service Dialog

4. The default IP address value is All. To limit the service to a specific IP address, select the IP address from the drop-down list.
5. In the Port field, 53 displays; you can change it to any unused port.
6. Select Enabled.
7. In the Attributes field, select Transparent, Explicit, Send-client-IP (spoofing), or all three. Explicit is the default.
8. Click OK; click Apply.

To Create or Edit a DNS-Proxy Service through the CLI:

1. At the (config) command prompt, enter the following commands to set the value returned to the client before configuring the DNS service.:

Section B: Creating and Editing Services

```
SGOS#(config) services
SGOS#(config services) dns
SGOS#(config services dns) create ip_address:port
```

2. If you do not need to change the defaults, you have completed the procedure. To change the attributes, enter the following command:

```
SGOS#(config services dns) attribute {explicit | transparent | send-client-ip}
{enable | disable} [ip_address:] port
```

where:

attribute explicit transparent send-client-ip enable [ip_address:]port	Give the DNS proxy explicit and transparent attributes, and create IP spoofing (where the ProxySG pretends to be a client so the OCS can see the client's IP address).
enable [ip_address:]port	Enable the new Telnet shell proxy.

3. (Optional) View the results:

```
SGOS#(config services dns) view
Port: 53           IP: 0.0.0.0          Type: dns
Properties: transparent, explicit, enabled
Port: 54           IP: 0.0.0.0          Type: dns
Properties: transparent, enabled
```

Creating a Resolving Name List:

You can create the resolving name list that the DNS proxy uses to resolve domain names. This procedure can only be done through policy. (For a discussion on using the <DNS-Proxy> layer, refer to the *Blue Coat Content Policy Language Guide*.)

Each name resolving list entry contains a domain-name matching pattern. The matching rules are:

- `test.com` matches only `test.com` and nothing else.
- `.test.com` matches `test.com`, `www.test.com` and so on.
- `."` matches all domain names.

An optional IP address can be added, which allows the DNS proxy to return any IP address if the DNS request's name matches the domain name suffix string (`domain.name`).

To create a resolving name list, create a policy, using the <DNS-Proxy> layer, that contains text similar to the following:

```
<DNS-Proxy>
  dns.request.name=www.example.com dns.respond.a(vip)
-or-
<DNS-Proxy>
  dns.request.name=.example.com dns.respond.a(vip)
-or-
<DNS-Proxy>
  dns.request.name=www.example.com dns.respond.a(10.1.2.3)
```

Section B: Creating and Editing Services

Note: You can also create a resolving name list using VPM. For more information on using the DNS-Proxy layer in VPM, see "Web Content Policy Layer Reference" on page 393.

FTP

To configure the native FTP proxy, see "Configuring the FTP Proxy" on page 140.

To Create or Edit an FTP Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.
The Service Ports tab displays.
2. Click New or Edit; the Add (or Edit) Service dialog appears.
3. Select FTP from the Protocol drop-down list.

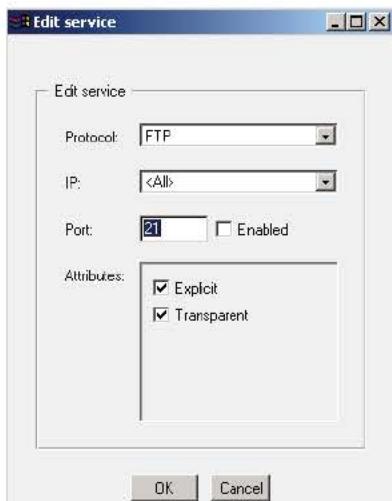


Figure 5-7: FTP Edit Service Dialog

4. The default IP address value is all. To limit the service to a specific IP address, select the IP address from the drop-down list.
5. In the Port field, specify a port number; select the Enabled checkbox.
6. In the Attributes field, both Explicit and Transparent are selected. You can de-select one of them if necessary
7. Click OK; click Apply.

To Create an FTP Service through the CLI:

1. At the (config) command prompt, enter the following commands:

Section B: Creating and Editing Services

```
SGOS# (config) services
SGOS# (config services) ftp
SGOS# (config services ftp) create [ip_address:]port
SGOS# (config services ftp) attribute passive-mode {enable | disable}
-or-
SGOS# (config services ftp) attribute {explicit | transparent} {enable | disable}
[ip_address:]port
```

2. (Optional) View the results.

```
10.9.17.159 - Blue Coat SG3000#(config services ftp) view
Port: 21 IP: 0.0.0.0 Type: ftp
Properties: transparent, enabled, passive-allowed
```

HTTP

Two HTTP services exist by default and are enabled, one with explicit and transparent attributes on port 80 and one with explicit attributes on port 8080. You can change the attributes or create other HTTP ports if needed.

To Create or Edit an HTTP Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.

The Service Ports tab displays.

2. Click New or highlight the service and click Edit; the Add (or Edit) Service dialog appears.
3. Make sure HTTP is selected from the Protocol drop-down list.

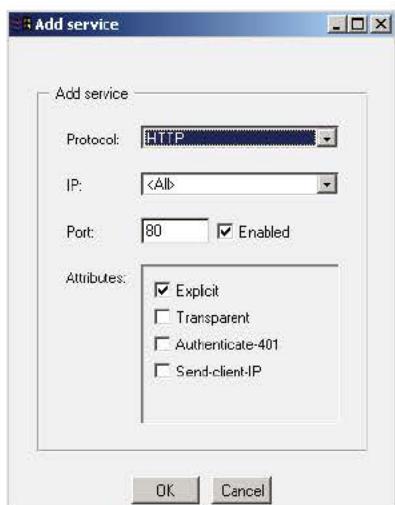


Figure 5-8: HTTP Edit Service Dialog

4. The default IP address value is all. To limit the service to a specific IP address, select the IP address from the drop-down list.
5. In the Port field, specify a port number; be sure Enabled is selected.

Section B: Creating and Editing Services

6. In the Attributes field, select all that apply: Explicit, Transparent, Authenticate-401, or Send-client-IP.
7. Click OK; click Apply.

To Create an HTTP Service through the CLI:

Two HTTP services exist and are enabled on the ProxySG. If you need to create another at a different port in addition to the services already existing on the system, complete the following steps:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) http
SGOS#(config services http) create [ip_address:]port
SGOS#(config services http) attribute {authenticate-401 | explicit |
send-client-ip | transparent} {enable | disable} [ip_address:]port
-or-
SGOS#(config services http) attribute {connect | head} {enable | disable {drop |
error}} [ip_address:]port
```

To view the results:

```
SGOS#(config services http) view
Port: 8080 IP: 0.0.0.0 Type: http
Properties: explicit, enabled
Port: 80 IP: 0.0.0.0 Type: http
Properties: transparent, explicit, enabled
```

HTTPS

The HTTPS service is not configured or enabled by default when the ProxySG ships. You can configure and use multiple HTTPS services.

To Create an HTTPS Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.
The Service Ports tab displays.
2. Click New; the Add Service dialog appears.
3. Select HTTPS from the Protocol drop-down list.

Section B: Creating and Editing Services

Figure 5-9: HTTPS Add Service Dialog

4. To select or add an IP address, do one of the following:
 - To select a local address, specify a real IP address from the IP drop-down list. All is not a selection option.
 - To add a non-local IP address, first select the Transparent attribute, then enter a non-local IP address that is not bound to the ProxySG.
5. In the Port field, specify a port number; select Enable.
6. In the Attributes field, select all that apply: Explicit, Transparent, Send-client-IP, Verify-client, or Forward-client-cert.
7. In the Keyring drop-down list, select any already-created keyring that is on the system. The system ships with a default keyring that can be reused for each HTTPS service. Keep in mind that the default certificate associated with the default keyring is self-signed and might not be trusted by all clients.

Note: The configuration-passwords-key keyring that shipped with the ProxySG does not contain a certificate and cannot be used for HTTPS services.

8. In the SSL Versions drop-down list, select the version that you want to use for this service. The default is SSL v2/v3 and TLS v1.
9. In the CA-Cert Lists drop-down list, select the list (already created) for the HTTPS service to use.
10. Click OK; click Apply.

Section B: Creating and Editing Services

Note: To create client-certification lists and keyrings, see "Configuring HTTPS Termination" on page 176.

To Create an HTTPS Service through the CLI:

- At the `(config)` command prompt, enter the following commands:

```
SGOS# (config) services
SGOS# (config services) https
SGOS# (config services https) create ip_address:port keyring
SGOS# (config services https) attribute ccl list_name ip_address:port
-or-
SGOS# (config services https) attribute cipher-suite ip_address:port
-or-
SGOS# (config services https) attribute {forward-client-cert | send-client-ip | verify-client} {enable | disable} ip_address:port
-or-
SGOS# (config services https) attribute ssl-protocol-version {sslv2 | sslv3 | tlsv1 | sslv2v3| sslv2tlsv1 | sslv3tlsv1 | sslv2v3tlsv1} ip_address:port
```

- (Optional) View the results:

```
SGOS# (config services https) view
Port: 1000 IP: 10.9.17.159 Type: https
Keyring: default
Properties: explicit, enabled
SSL Protocol version: SSLv2v3TLSv1
CA Certificate List: not configured
Cipher suite:
RC4-MD5:RC4-SHA:DES-CBC3-SHA:DES-CBC3-MD5:RC2-CBC-MD5:RC4-64-MD5:DES-CBC-SHA:DES-CBC-MD5:EXP1024-RC4-MD5:EXP1024-RC4-SHA:EXP1024-RC2-CBC-MD5:EXP1024-DES-CBC-SHA:EXP-RC4-MD5:EXP-RC2-CBC-MD5:EXP-DES-CBC-SHA:+SSLv2:+SSLv3+LOW:+SSLv2+LOW:+EXPO
```

Instant Messaging Protocols

Supported instant messaging (IM) services are present by default with the transparent and explicit attributes selected and listening on all IP addresses; none of them are enabled. Note that the explicit attribute is not user-configurable.

To Create or Enable an AOL, Yahoo, or MSN Port Service through the Management Console:

- Select Configuration>Services>Service Ports.
The Service Ports tab displays.
- Click New or highlight the service you want and select Edit; the Add (or Edit) Service dialog appears.
- Select the IM service you want to create or edit from the Protocol drop-down list.
- The default port is determined by the protocol:
 - AOL— Port 5190

Section B: Creating and Editing Services

- Yahoo—Ports 5050 and 5101
 - MSN—1863 and 6891
5. Click OK; click Apply.

To Manage an Instant Messaging Service through the CLI:

1. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) aol-im | msn-im | yahoo-im
SGOS#(config services protocol) create port
SGOS#(config services protocol) attribute send-client-ip {enable | disable} port
```

2. (Optional) View the results:

```
SGOS#(config services aol-im) view
Port:      5190 IP: 0.0.0.0          Type: aol-im
Properties: transparent, explicit, enabled
SGOS#(config services aol-im) exit
SGOS#(config services) yahoo-im
SGOS#(config services yahoo-im) view
Port:      5050 IP: 0.0.0.0          Type: yahoo-im
Properties: transparent, explicit, enabled
```

Streaming Protocols

MMS and RTSP services are configured on the system, but are disabled by default. To enable the default MMS and RTSP service, follow the steps below.

To Enable an MMS or RTSP Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.

The Service Ports tab displays.

2. Click New to create a new MMS or RTSP port service or highlight the existing service and click Edit.

The Add (or Edit) Service dialog appears.

3. Select MMS or RTSP from the Protocol drop-down list.

4. The default IP address value is All. To limit the service to a specific IP address, select the IP address from the drop-down list.

5. In the Port field, specify a port number; select Enabled.

6. In the Attributes field, select the attributes you want the service to have.

7. Click OK; click Apply.

To Enable an MMS or RTSP Service through the CLI:

1. At the `(config)` command prompt, enter the following commands:

Section B: Creating and Editing Services

```
SGOS#(config) services
SGOS#(config services) {mms | rtsp}
SGOS#(config services protocol) create [ip_address:]port
SGOS#(config services protocol) attribute {explicit | send-client-ip |
transparent} {enable | disable} [ip_address:]port
```

2. (Optional) View the results:

```
SGOS#(config services mms) view
Port: 1755 IP: 0.0.0.0 Type: mms
Properties: transparent, explicit, enabled
SGOS#(config services mms) exit
SGOS#(config services rtsp)
SGOS#(config services rtsp) view
Port: 554 IP: 0.0.0.0 Type: rtsp
Properties: transparent, explicit, enabled
```

SOCKS

By default, a SOCKS service is configured with explicit attribute on port 1080, but not enabled. You can create additional SOCKS services.

To enable a SOCKS port service, complete the steps below. To configure SOCKS gateway forwarding, see "SOCKS Gateway Configuration" on page 619.

Note: The version of SOCKS used is controlled through policy. For example, to use only SOCKSv5:

```
<proxy> client.protocol=socks
    ALLOW socks.version=4 deny
    DENY
```

To Create or Edit a SOCKS Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.
The Service Ports tab displays.
2. Click New to create a new SOCKS service or select Edit to enable the existing service; the Add (or Edit) Service dialog appears.
3. Select SOCKS from the Protocol drop-down list.

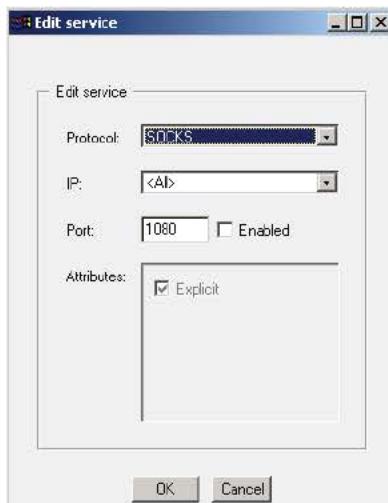
Section B: Creating and Editing Services

Figure 5-10: SOCKS Edit Service Dialog

4. The default IP address value is All. To limit the service to a specific IP address, select the IP address from the drop-down list.
5. In the Port field, specify a port number; select Enable.
6. Click OK; click Apply.

To Create a SOCKS Port Service through the CLI:

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) socks
SGOS#(config services socks) create [ip_address:]port
SGOS#(config services socks) enable [ip_address:]port
```

2. (Optional) View the results:

```
SGOS#(config services socks) view
Port: 1080      IP: 10.25.36.48 Type: socks
Properties: explicit, enabled
```

TCP Tunneling

Tunneling, or port forwarding, is a way to forward TCP traffic. Any application protocol running over TCP can be tunneled using this service. Client-server applications carry out any authentication procedures just as they do when TCP tunneling is not involved.

SGOS uses a `tcp://` scheme for tcp-tunnel transactions instead of HTTPS because SGOS does not actually know that it is HTTPS that is being tunneled.

Both explicit and transparent TCP tunneling are supported. Which one you use depends on your needs.

Section B: Creating and Editing Services

Explicit TCP tunneling allows connections to one of the ProxySG's IP addresses.

Transparent TCP tunneling allows connections to any IP address other than those belonging to the ProxySG. TCP tunneling in transparent mode supports categorization as well as blocking of destination IP address, port, host, and domain.

Note: The TCP-Tunnel service does not support content filtering with Websense offbox or ICAP.

If you want to create a transparent TCP tunneling protocol, you can do so from either the CLI or the Management Console. When a TCP-Tunnel service is created, it is by default created as an explicit service and is also enabled automatically.

To Create a Transparent or Explicit TCP-Tunnel Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.
The Service Ports tab displays.
2. Click New; the Add Service dialog appears.
3. Select TCP-Tunnel from the Protocol drop-down list.
The Add Service dialog displays.

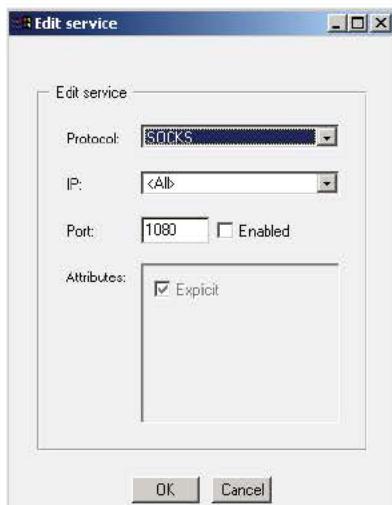


Figure 5-11: TCP-Tunnel Add Service Dialog

4. The default IP address value is All. To limit the service to a specific IP address, select the IP address from the drop-down list.
5. In the Port field, specify a port number; select Enabled.
6. If you are configuring a transparent TCP-Tunnel service, make sure Transparent is selected in the Attributes field; if you are configuring an explicit TCP-Tunnel service, make sure Explicit is selected.
7. Click OK; click Apply.

Section B: Creating and Editing Services

To Create a TCP-Tunnel Transparent or Explicit Port Service through the CLI:

1. At the `(config)` prompt, enter the following commands to create a transparent or explicit service:

```
SGOS# (config) services
SGOS# (config services) tcp-tunnel
SGOS# (config services tcp-tunnel) create [ip_address:]port
```

where `ip_address` is the IP address of the ProxySG (use 0.0.0.0 to indicate all available IP addresses), and `port` is the number of the port where you want the ProxySG to listen. You must choose a port that is not configured for any other service.

2. Enable the service to be transparent or explicit. By default, the port service is explicit.

```
SGOS# (config services tcp-tunnel) attribute {explicit | transparent} {enable | disable} [ip_address:]port
```

3. (Optional) View the results.

```
SGOS# (config services tcp-tunnel) view
Port: 7080      IP: 0.0.0.0          Type: tcp-tunnel
Properties: transparent, explicit, enabled
```

If you created a transparent TCP-Tunnel service, you have completed the procedure. If you created an explicit TCP-Tunnel service, you must configure a forwarding destination port.

Configuring a Forwarding Destination Port through the CLI:

1. Create a forwarding destination port, where the ProxySG directs traffic.

```
SGOS# (config services tcp-tunnel) exit
SGOS# (config services) exit
SGOS# (config) forwarding
SGOS# (config forwarding) create host_alias ip_address tcp=port
```

2. (Optional) View the results:

```
SGOS# (config forwarding) view
Forwarding Groups: (*) = host unresolved
No forwarding groups defined.
Individual Hosts: (*) = host unresolved
Host_Alias 10.25.36.47 tcp=port_number
```

Telnet Shell Proxy Service

On a new system, Telnet proxy service is configured and disabled on port 23. On an upgrade, Telnet proxy service is not created.

To Enable or Create a Telnet Proxy Service through the Management Console

Important: If you want to use Telnet to manage the ProxySG, create a Telnet-Console rather than a Telnet service. The Telnet service allows you to use Telnet for outbound connections, and the ProxySG functions as Shell proxy in that situation. For more information on the Telnet-Console, see "Telnet Console" on page 119.

Section B: Creating and Editing Services

1. Select Configuration>Services>Service Ports.
 2. Click New if you are creating a new Telnet service; highlight the Telnet service and click Edit if you are enabling an existing Telnet service;
- The Add or Edit Service dialog appears.

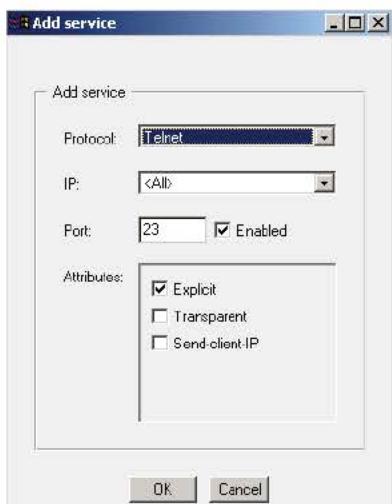


Figure 5-12: Creating a Telnet Service

3. In the Protocol drop-down list, select Telnet.
4. The default IP address value is all. To limit the service to a specific IP address, select the IP address from the drop-down list.
5. In the Port field, specify a port number; select Enable. Port 23 is the default.

Important: You can have only one service on a port, so you must choose a port number for the Telnet service that is different from the port chosen for the Telnet Console.

6. In the Attributes field, select Transparent, Explicit, Send-client-IP (spoofing), or all three. Explicit is the default.
7. Click OK; Click Apply.

To Enable or Create a Telnet Proxy Service through the CLI

Note: The explicit attribute is enabled by default and the transparent and send-client-ip attributes are disabled by default. Note also that only one service can use a port, so if you have Telnet-Console enabled on Port 23, you must choose a different port number for the Telnet shell proxy.

From the (config) prompt, enter the following commands:

Section B: Creating and Editing Services

```
SGOS# (config) services
SGOS# (config services) telnet
SGOS# (config services telnet) create [ip_address:]port
SGOS# (config services telnet) attribute {explicit | transparent |
send-client-ip} enable [ip_address:]port
SGOS# (config services telnet) enable [ip_address:]port
```

where:

create	[ip_address:]port	Create a Telnet shell proxy service at the (optional) address and port number.
attribute	explicit transparent send-client-ip enable [ip_address:]port	Give the Telnet shell proxy explicit and transparent attributes, and create IP spoofing (where the ProxySG pretends to be a client so the OCS can see the client's IP address).
enable	[ip_address:]port	Enable the new Telnet shell proxy.

To view the results:

```
SGOS# (config services telnet) view
Port: 23 IP: 0.0.0.0 Type: telnet
Properties: transparent, explicit, disabled
Port: 24 IP: 10.25.36.47 Type: telnet
Properties: explicit, enabled
```

Chapter 6: Configuring Proxies

A *proxy* filters traffic, monitors Internet and intranet resource usage, blocks specific Internet and intranet resources for individuals or groups, and enhances the quality of Internet or intranet user experiences.

A proxy also serves as an intermediary between a Web client and a Web server and can require authentication to allow identity-based policy and logging for the client. The rules used to authenticate a client are based on the policies created and implemented through your existing security framework, such as LDAP, RADIUS, and NTLM, and are further discussed in "Using Authentication Services" on page 233.

Explicit/Transparent proxy specifies the mode the client requests get to the proxy.

- Explicit—The default, requiring software configuration for both browser and service.
- Transparent—Requires a Layer-4 switch or a WCCP-compliant router. You can also transparently redirect requests through a ProxySG by setting the workstation's gateway to the ProxySG IP address. You can also use the ProxySG software bridge to transparently proxy requests.

Some software configuration on the ProxySG is also required to allow the appliance to know what traffic to intercept.

You might also configure both proxy types, depending on the services you require.

This chapter contains the following topics:

- "Section A: About Explicit and Transparent Proxy"
- "Section B: Configuring Explicit Proxies"
- "Section C: Transparent Proxies"

Section A: About Explicit and Transparent Proxy

Whether you select explicit or transparent proxy deployment is determined by factors such as network configuration, number of desktops, desired user experience, and desired authentication approach.

Note: While you must configure proxying to do authentication, verify the proxy is configured correctly and is functioning before adding authentication to the mix. Many network or other configuration problems can appear similar to authentication errors.

Explicit Proxy

In an explicit proxy configuration, the client (browser) is explicitly configured to use a proxy server. The browser is given the IP address and port number of the proxy service (the ProxySG). It is also possible to configure the browser to download the proxy settings from a Web server. This is called a Proxy Auto-Configuration (PAC) file. When a user makes a request, the browser connects to the proxy service and sends the request. Since the browser knows it is talking to a proxy, the browser provides the proxy server with the destination server.

The proxy service accepts the explicit connection to it, and fetches the request from the browser. The request identifies the desired origin server and the resource on that server. The proxy service uses this information to contact the origin server if necessary.

The disadvantage to explicit proxy is that each desktop must be properly configured to use the proxy, which might not be feasible in a large organization.

Transparent Proxy

When transparent proxy is enabled, the client (browser) does not know the traffic is being processed by a machine other than the origin server. The browser believes it is talking to the origin server, so the request is formatted for the origin server, and the proxy determines for itself the destination server based on information in the request, such as the destination IP address in the packet, or the `Host:` header in the request.

To enable the ProxySG to intercept traffic sent to it, you must create a service and define it as transparent. The service is configured to intercept traffic for a specified port, or for all IP addresses on that port. A transparent HTTP proxy, for example, typically intercepts all traffic on port 80 (all IP addresses).

To make sure that the appropriate traffic is directed to the ProxySG, deploy hardware such as a Layer-4 switch or a WCCP router, or the ProxySG appliance's software bridge that can redirect selected traffic to the appliance. Traffic redirection is managed through policies you create on the redirection device.

For detailed information on explicit proxies, continue with the next section; for detailed information on transparent proxies, continue with "Transparent Proxies" on page 169.

Section B: Configuring Explicit Proxies

You can configure several different explicit proxy servers and services:

- Native FTP—See "Configuring the FTP Proxy" on page 140.
- HTTP Proxy—See "Configuring an HTTP Proxy" on page 147.
- SOCKS—See "Configuring a SOCKS Proxy" on page 160.
- Shell Proxies—See "Customizing Policy Settings for Shell Proxies" on page 163

For information on creating an explicit proxy server, regardless of type, continue with "Creating an Explicit Proxy Server".

Creating an Explicit Proxy Server

If your network does not use transparent proxy, clients on the network must configure their browsers to use either an explicit proxy server or a Proxy Auto-Configuration (PAC) file. The ProxySG generates client instructions that describe how to configure Microsoft Internet Explorer, Netscape Communicator, and other browsers based on instructions selected by the ProxySG administrator. You can configure client instructions for each network adapter in the ProxySG with the Configuration>Network>Adapters>Interface>Settings button.

After selecting client instructions, the ProxySG administrator directs clients to go to the ProxySG home page and follow the instructions in the Browser Configuration section. The ProxySG detects the browser installed on the client and displays the appropriate instructions.

Using the ProxySG as an Explicit Proxy

To use the ProxySG as an explicit proxy and use services such as SOCKS or FTP, you must provide custom instructions to clients instructing them how to configure their browsers to use the ProxySG as a proxy server.

This is a two-step process, requiring that you add the proxy IP address to the browser and also instruct the ProxySG which interface uses the proxy IP address.

Before the proxy can be used, you must:

- Configure the proxy server.
- Enable the explicit proxy (whether a service or a server).

The browsers described here are Internet Explorer 6.0 and Netscape 6.2. If you have different browsers or different versions of Internet Explorer or Netscape, refer to the vendor documentation for information on configuring proxies.

From Internet Explorer:

1. Select Tools>Internet Options>Connections>LAN Settings.
2. Select Use a proxy server.

Section B: Configuring Explicit Proxies

3. Enter the IP address and port number for the proxy, or click Advanced to set proxy server IP addresses and port numbers for services such as HTTP, FTP, and SOCKS. (Configure HTTPS through the Secure field.)
4. Click OK to exit the Advanced Settings tab, then continue to click OK until you exit the Tools menu.

From Netscape 6.2:

1. Select Edit>Preferences>Advanced>Proxies.
2. Select Manual proxy configuration.
3. Enter proxy server IP addresses and port numbers for services such as HTTP, FTP, SOCKS and SSL.
4. Click OK.

Note: Explicit proxy allows a redundant configuration using IP address failover among a cluster of machines. For information on creating a redundant configuration for failover, see "Configuring Failover" on page 105.

Interface Proxy Settings

Once the explicit proxy is configured on the browser, decide which interface cards listen for which service. Each interface card can listen for only one IP address; you can configure multiple proxies on one ProxySG using the same IP address.

To Provide Configuration Instructions through the Management Console:

1. Select Configuration>Network>Adapters.
2. Select an interface and click Settings.
3. Select Using a proxy.
4. Click OK to close the Settings dialog.
5. Click Apply.

To Provide Configuration Instructions through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) interface fast-ethernet interface_#
SGOS#(config interface interface_#) instructions proxy
```

Configuring the FTP Proxy

In previous SGOS releases, connections to FTP origin servers were only accomplished over HTTP. SGOS 3.x supports Native FTP proxy.

Note: As in previous releases, FTP requests sent through the HTTP proxy are still valid.

Section B: Configuring Explicit Proxies

Configuring an FTP proxy requires ProxySG configuration and specific configuration of the FTP client. The service must be enabled on the ProxySG before it can be used.

Data connections initiated by an FTP client to an FTP server are known as passive mode data connections. This type of connection is useful in situations where an FTP server is unable to make a connection to an FTP client because the client is located behind a firewall or other similar device where outbound connections from the client are allowed, but inbound connections to the client are blocked.

This functionality allows administrators to select how the ProxySG responds to a request from an FTP client for a passive mode data connection (PASV command). This functionality does not affect HTTP requests for FTP objects (for example, those originating from browsers that are explicitly proxied to a ProxySG).

If the FTP server responds that it supports PASV, but the ProxySG is unable to connect because of a firewall blocking the port, the ProxySG only attempts a PORT command. Some FTP clients do not open a passive mode data connection to an IP address that is different from the IP address used for the control connection.

Disabling passive mode data connections on the ProxySG servicing requests from this type of FTP client might provide a more acceptable response to the end user.

When passive mode data connections are disabled, the ProxySG returns a response to the FTP client indicating that the server does not support passive mode. The FTP client software controls any messages displayed to the end user as a result of this response from the ProxySG.

Limitations

- Internet Explorer does not support proxy authentication for Native FTP.
- The ProxySG FTP proxy does not support exceptions.

FTP Spoofing

Using policy, you can spoof the IP addresses for FTP data connections in both transparent and explicit deployments, for both active and passive modes; certain deployments are subject to limitations. The client and server-side policies are:

- `ftp.match_client_data_ip(yes)`—Matches the source IP address of the ACTIVE data connection with the destination IP address of the control connection (client side).
- `ftp.match_server_data_ip(yes)`—Matches the source IP address of the PASV data connection with the source IP address of the ProxySG control connection (server side).

Note: To always use the ProxySG physical IP address (no spoofing), define policy as
`ftp.match_[client | server]_data_ip(no).`

The following points describe the various data flow scenarios:

- Outbound client data connection (ProxySG to client)—When the client issues a PORT command, the ProxySG opens a data connection to the FTP client with the source IP address of whatever destination IP address the client used when opening the control connection.

Section B: Configuring Explicit Proxies

- Inbound client data connection (client to ProxySG)—When the client issues a PASV command, the ProxySG returns the IP address and port to which client makes a data connection.
 - Explicit—The ProxySG returns the destination IP address of the control connection; this can be a physical or virtual ProxySG IP address.
 - Transparent—The ProxySG returns the IP address of the physical interface on which the control connection arrived.
- Outbound server data connection (ProxySG to FTP server)—When the ProxySG issues a PASV command upstream, the server returns an IP address and port to connect to. The ProxySG then opens a data connection to the server with the same source IP address it used to open the control connection. This address is defined by the `reflect_ip` property.
- Inbound server data connection (FTP server to ProxySG)—When the ProxySG issues a PORT command, the ProxySG provides the IP address and port number to which the server makes a data connection.
 - The ProxySG sends the control connection's source IP address if that IP is a local ProxySG (virtual or physical) IP address; or
 - The ProxySG sends the IP address of the physical interface that was used to make the outgoing control connection.

FTP Server Limitations

Consider the following limitations when defining FTP spoofing policy:

- IIS and WS_FTP servers do not support PASV data connections with a source IP address that is different from the source IP address of the control connection.
- IIS and WS_FTP servers do not support ACTIVE data connections with a destination IP address that differs from the source IP address of the control connection.

Configuring the ProxySG

This section describes how to configure the ProxySG through the Management Console and the CLI.

To Configure Native FTP Proxy through the Management Console:

1. Select Configuration>Services>FTP Proxy.

The FTP Proxy tab displays.

Section B: Configuring Explicit Proxies

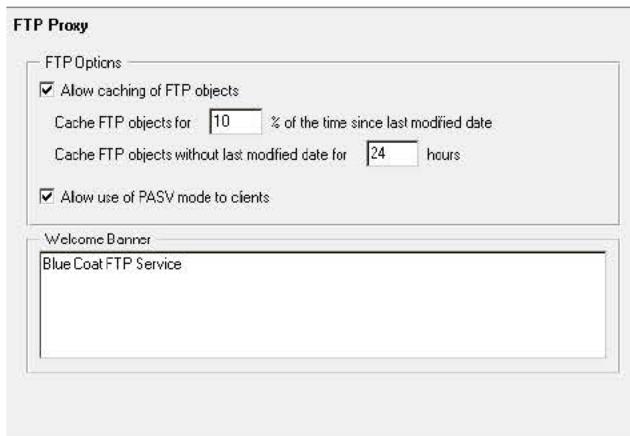


Figure 6-1: FTP Proxy Tab

2. Select the checkbox to Allow caching of FTP objects. The default is enabled.
3. Determine the amount of time in percentage of how long since the object was last modified. The default is 10%.
4. Enter an amount, in hours, that the object remains in the cache before becoming eligible for deletion. The default is 24 hours.
5. Select the checkbox to Allow use of PASV mode to clients. The default is enabled.

To Configure Native FTP Proxy through the CLI:

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) caching
SGOS#(config caching) max-cache-size 18
SGOS#(config caching) ftp
SGOS#(config caching ftp) enable
SGOS#(config caching ftp) type-m-percent 20
SGOS#(config caching ftp) type-n-initial 12
```

where:

max-cache-size	megabytes	The maximum size, in megabytes, of the largest object that can stored on the ProxySG. Note that max-cache-size sets the maximum object size for both HTTP <i>and</i> FTP.
enable disable		Enables or disables the caching of FTP objects.
type-m-percent	percent	Time to live for objects with a last-modified time.
type-n-initial	hours	Time to live for objects without a last-modified time.

2. (Optional) View the result.

```
SGOS#(config caching ftp) view
Caching FTP objects is enabled
FTP objects with last modified date, cached for 20% of last modified time
FTP objects without last modified date, initially cached for 12 hours
```

Section B: Configuring Explicit Proxies

3. (Optional) Change the default login syntax. The default syntax is Raptor. The ProxySG also supports the Checkpoint authentication syntax. The supported Checkpoint formats are:
 - `remoteuser@proxyuser@host` (in `USER` command) for explicit FTP.
 - `remotepass@proxypass` (in `PASS` command) for explicit FTP.
 - `remoteuser@proxyuser` (in `USER` command) for transparent FTP.
 - `remotepass@proxypass` (in `PASS` command) for transparent FTP.

Enter the following command to change the login syntax:

```
SGOS# (config) ftp login-syntax {raptor | checkpoint}
```

Note: Neither proxy authentication for transparent FTP nor proxy chaining are supported with the Checkpoint syntax.

Enabling the FTP Service

By default, an FTP service is already created with explicit and transparent attributes, but it is disabled. You must enable the FTP port before it can be used.

To Create and Enable a Native FTP Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.
The Service Ports tab displays.
2. Click New; the Add Service dialog appears.

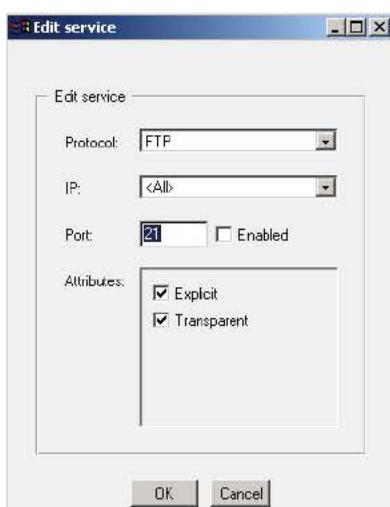


Figure 6-2: FTP Add Service Dialog

3. In the Protocol drop-down list, select FTP.
4. The default IP address value is All. To limit the service to a specific IP address, select the IP address from the drop-down list.

Section B: Configuring Explicit Proxies

5. In the Port field, specify a port number; select Enabled.
6. Choose the attributes you want the FTP proxy to have: Explicit, Transparent, or both.
7. Click OK; Click Apply.

To Create a Native FTP Port Service through the CLI:

1. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) ftp
SGOS#(config services ftp) create [ip_address:]port
SGOS#(config services ftp) attribute passive-mode {enable | disable}
SGOS#(config services ftp) attribute explicit enable [ip_address:]port
SGOS#(config services ftp) attribute transparent enable [ip_address:]port
```

2. (Optional) View the results.

```
SGOS#(config services ftp) view
Port: 25 IP: 0.0.0.0 Type: ftp
Properties: transparent, explicit, enabled, passive-allowed
```

Configuring FTP Clients

FTP clients must be configured as follows:

- Enable firewall.
- Select **USER** with no logon.
- For proxy authentication, select **USER remoteID@remoteHost fireID** and specify a proxy username and password.

Example

The following graphic demonstrates configuring a WSFtp client.

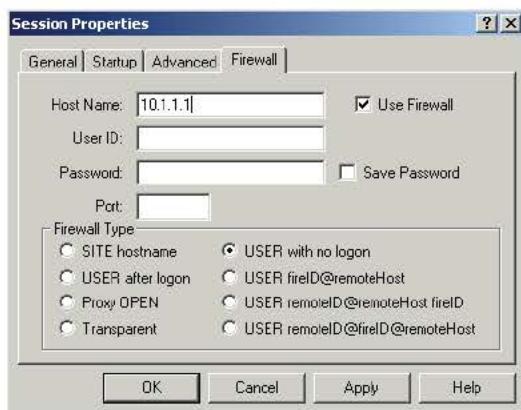


Figure 6-3: Configuring the WSFtp Client for Native FTP

Section B: Configuring Explicit Proxies

Configuring FTP Connection Welcome Banners

You can customize banners that usually describe the policies and content of the FTP server displayed to FTP clients. Without modification, the ProxySG sends a default banner to newly-connected FTP clients: Welcome to Blue Coat FTP. However, you might not want users to know that a Blue Coat ProxySG exists on the network. A default banner can be defined in the Management Console or the CLI, but other banners defined for specific groups can be created in policy layers.

Note: Configurable banners are only displayable when FTP is explicit through the ProxySG. In transparent deployments, the banner is sent to the client when proxy authentication is required; otherwise, the banner is forwarded from the FTP server.

To Define the Default FTP Banner through the Management Console:

1. Select Configuration>Services>FTP Proxy.
2. In the Welcome Banner field, enter a line of text that is displayed on FTP clients upon connection. If the message length spans multiple lines, the ProxySG automatically formats the string for multiline capability.
3. Click Apply.

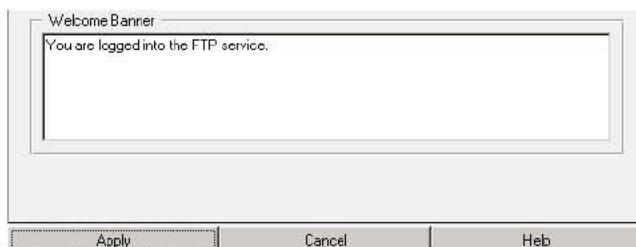


Figure 6-4: Configuring an FTP Connection Welcome Banner

To Define the Default FTP Banner through the CLI:

At the (config) prompt, enter the following command:

```
#SGOS#(config) ftp  
#SGOS#(config) ftp welcome-banner "message"
```

To Create Policy that Overrides the Default Banner:

Add the following property to a policy:

```
<Proxy>  
  ftp.welcome_banner "message"
```

If entering text that spans more than one line, use \$(crlf) for line breaks.

Section B: Configuring Explicit Proxies

Configuring an HTTP Proxy

By default, an HTTP proxy service, with both explicit and transparent attributes set, is enabled on port 80. To change the attributes of the proxy service or create new HTTP proxy services, see "HTTP" on page 126.

The HTTP proxy is the first line of defense for the ProxySG, controlling all traffic that arrives on port 80 to the ProxySG. You can also configure the HTTP proxy as a server accelerator to improve response times.

You can set a limit to the maximum bandwidth the ProxySG is allowed to use for refreshing objects in the background. In most situations, however, the default settings produces optimal performance.

Terms:

- Caching Policy—The HTTP Proxy policy determines the maximum size of objects to cache and the number of minutes the ProxySG remembers that an object is not stored, as well as whether to verify the freshness of an object (an option that can affect performance) and whether to verify server certificates for secure connections.
- Freshness—Guarantees that all objects served from the ProxySG are current. An object is *fresh* if its age does not exceed its freshness lifetime.
- HITs—Objects that are in the ProxySG and can be retrieved when an end user requests the information.
- Maximum Object Size—The maximum object size stored in the ProxySG. All objects retrieved that are greater than the maximum size are delivered to the client but are not stored in the ProxySG.
- MISSes—Objects that can be stored but have never been requested before are called MISSes; they were not in the ProxySG to start, so they must be brought in and stored there as a side effect of processing the end-user's request. If the object is cacheable, it is stored and served the next time it is requested.
- Negative Responses—if the ProxySG receives an origin server error response code indicating, for example, that the requested page or image does not exist, it caches that negative response. If the ProxySG is configured to cache such negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes. If it is not configured, which is the default, the ProxySG attempts to retrieve the page or image every time it is requested.
- Refresh Bandwidth—if set to zero, the ProxySG does not do active refresh.
- Server Acceleration Profile—Normal (the default), Portal, or Bandwidth Gain, to cause the ProxySG to behave as a server accelerator and help improve object response time.

For more information on controlling HTTP proxy traffic, continue with the next section. For more information on using the HTTP proxy as a server accelerator, see "Controlling the HTTP Proxy Profile" on page 153.

Section B: Configuring Explicit Proxies

Controlling HTTP Proxy Traffic

With the HTTP proxy, you can control which objects are stored in the ProxySG, how long they are stored, how often the objects are verified that the content has not changed. You can also change the profile for the HTTP proxy, allowing you to configure the proxy for accelerated performance, or leave it at a normal setting.

To control HTTP proxy traffic, you can configure the following settings:

- "Refresh Bandwidth" on page 148
- "Setting Proxy Policies" on page 150: This includes setting maximum object size, meta tag headers, strict HTTP parsing.
- "Controlling the HTTP Proxy Profile" on page 153: You have three profiles to choose among: normal, bandwidth, or portal.

Refresh Bandwidth

The ProxySG uses as much bandwidth as necessary for refreshing to achieve the desired access freshness.

The amount of bandwidth used varies depending on client demands. If you determine that the ProxySG is using too much bandwidth (by reviewing the logged statistics and examine current bandwidth used shown in the Refresh bandwidth field), you can specify a limit to the amount of bandwidth the ProxySG uses to try to achieve the desired freshness. Be aware, however, that if you limit the amount of bandwidth the ProxySG can use, you might prohibit the ProxySG from achieving the desired freshness. If the refresh bandwidth configuration remains at the recommended default (Let the ProxySG manage refresh bandwidth), then the ProxySG uses whatever bandwidth is available in its efforts to maintain 99.9% estimated freshness of the next access.

To Set Refresh Bandwidth through the Management Console:

1. Select Configuration>Services>HTTP Proxy>Freshness.

The Freshness tab displays.

Section B: Configuring Explicit Proxies

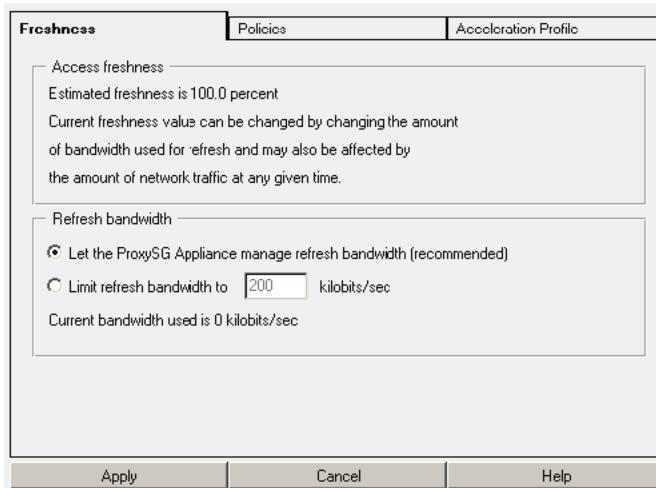


Figure 6-5: Freshness Tab

The Refresh bandwidth field displays the refresh bandwidth options.

Important: Blue Coat strongly recommends that you not change the setting from the default.

2. Do one of the following:
 - To turn off automatic bandwidth refresh, select Limit refresh bandwidth to (not recommended). Enter a new value into the kilobits/sec field, if necessary.
 - To return the ProxySG to automatic bandwidth refresh, select Let the ProxySG manage refresh bandwidth (recommended).
3. Click Apply.

To Set Refresh Bandwidth through the CLI:

1. To disable automatic bandwidth refresh (not recommended), enter the following commands at the (config) command prompt:


```
SGOS#(config) caching
SGOS#(config caching) refresh no automatic
```
2. (Optional) To adjust the kilobit/sec refresh bandwidth value, enter the following commands:

Note: Adjusting the refresh bandwidth value automatically turns off the automatic refresh bandwidth option.

```
SGOS#(config) caching
SGOS#(config caching) refresh bandwidth Kbps
```

3. To return the ProxySG to automatic bandwidth refresh (recommended), enter the following commands:

Section B: Configuring Explicit Proxies

```
SGOS# (config) caching
SGOS# (config caching) refresh automatic
```

4. (Optional) View the (truncated) results:

```
SGOS# (config caching) view
Refresh:
Estimated access freshness is 100.0%
Let the ProxySG Appliance manage refresh bandwidth
Current bandwidth used is 0 kilobits/sec
```

To view all HTTP settings, see "Viewing the HTTP Settings through the CLI" on page 159.

Setting Proxy Policies

Through policies, you can configure the length of time an object is cached, the length of time that the ProxySG remembers that an object is not cached, whether the ProxySG revalidates each object before serving it, whether the server certificate is verified by default, and how headers are parsed.

Note: Tolerant HTTP request parsing can only be done through the CLI; it is not available through the Management Console.

To Set Proxy Policies through the Management Console:

1. Select Configuration>Services>HTTP Proxy>Policies.

The Policies tab displays.

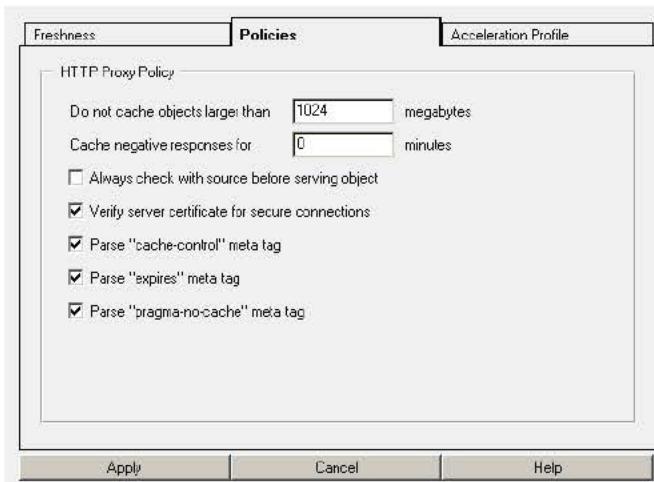


Figure 6-6: Policies Tab

2. Fill in the fields as appropriate:

- In the Do not cache objects larger than field, enter the maximum object size to cache. The default is 1024 MB. This configuration determines the maximum object size to store in the ProxySG. All objects retrieved that are greater than the maximum size are delivered to the client but are not stored in the ProxySG.

Section B: Configuring Explicit Proxies

- In the Cache negative responses for field, enter the number of minutes the ProxySG remembers that the object is not stored. The default is 0, meaning that the ProxySG will not remember and will always attempt to retrieve the object.

When the ProxySG receives an origin server error response code indicating, for example, that the requested page or image does not exist, it caches that negative response. If the ProxySG is configured to cache such negative responses, it returns that response in subsequent requests for that page or image for the specified number of minutes. If it is not configured, which is the default, the ProxySG attempts to retrieve the page or image every time it is requested.

- To always verify that each object is fresh, select the Always check with source before serving object checkbox. Remember that this affects performance.
- If you communicate with the origin server through HTTPS and want the origin server's certificate to be verified by the ProxySG, make sure that the Verify server certificate for secure connection checkbox is checked.

Note: If the ProxySG HTTPs service is configured to require a client certificate, information from the client certificate is extracted and put into a header that is included in the request when it is forwarded to the OCS.

The name of the header is `Client-Cert`. The header contains the certificate serial number, subject, validity dates and issuer (all as `name=value`) pairs.

The actual certificate itself is not forwarded.

- The default is to parse HTTP meta tag headers in HTML documents if the MIME type of the object is text/HTML. The function of all meta tags is same as the corresponding HTTP headers.

To disable meta-tag parsing, remove the check from the checkbox for:

- Parse “cache-control” meta tag
- Parse “expires” meta tag
- Parse “pragma-no-cache” meta tag

The following sub-headers are parsed when this checkbox is selected: private, no-store, no-cache, max-age, s-maxage, must-revalidate, proxy-revalidate.

3. Click Apply.

Setting Proxy Policies through the CLI:

1. At the `(config)` command prompt, enter the following commands:

```
SGOS# (config) caching
SGOS# (config caching) max-cache-size megabytes
SGOS# (config caching) negative-response minutes
SGOS# (config caching) no always-verify-source
```

Section B: Configuring Explicit Proxies

where:

max-cache-size	<i>megabytes</i>	The maximum size, in megabytes, of the largest object that can be stored on the ProxySG. Note that max-cache-size sets the maximum object size for both HTTP and FTP.
negative-response	<i>minutes</i>	The amount of time, in minutes, that the ProxySG remembers that an object is not stored.
always-verify-source		Ensures that every object is always fresh. This severely impacts performance.
no	always-verify-source	The default is no always-verify-source. This tells the ProxySG never to check objects on the source before serving them to the client.

2. (Optional) If you use HTTPS, you might want to change the verify-server certificate from the default of enabled to suppress verification of the origin server certificate:

```
SGOS# (config caching) exit
SGOS# (config) services
SGOS# (config services) https
SGOS# (config services) https attribute verify-client disable
```

Note: If the ProxySG HTTPs service is configured to require a client certificate, information from the client certificate is extracted and put into a header that is included in the request when it is forwarded to the OCS.

The name of the header is Client-Cert. The header contains the certificate serial number, subject, validity dates and issuer (all as name=value) pairs.

The actual certificate itself is not forwarded.

3. (Optional) To disable meta-tag parsing (parsing is enabled by default), enter the following command:

```
SGOS# (config services) exit
SGOS# (config) http no parse meta-tag {cache-control | expires | pragma-no-cache}
```

To view all HTTP settings, see "Viewing the HTTP Settings through the CLI" on page 159.

Tips on Parsing Meta Tags

- If ICAP response modification is occurring, the response body modified by ICAP server is not parsed.
- Relevant HTTP meta tags must appear within the first 1000 bytes of HTTP object body. If the meta tag does not appear within the first 1000 bytes, it is ignored.

Tips on Using Meta Tags With Policy

- The following meta tags can be used in the <Cache> layer for HTTP proxy, HTTP refresh, and HTTP pipeline transactions:

Section B: Configuring Explicit Proxies

```
http.response.parse_meta_tag.Pragma.no-cache(yes|no)
http.response.parse_meta_tag.Cache-Control(yes|no)
http.response.parse_meta_tag.Expires(yes|no)
```

- VPM support for this feature is not available.

Tolerant HTTP Request Parsing

The tolerant HTTP request parsing flag prevents certain syntax errors in an HTTP request from generating a *400 Invalid Request* error.

By default, a header line not beginning with a <tab> or space character must consist of a header name (which contains no <tab> or space characters), followed by a colon, followed by an optional value, or an error is reported. With tolerant request parsing enabled, a request header name is allowed to contain <tab> or space characters, and if the request header line does not contain a colon, then the entire line is taken as the header name.

A header containing one or more <tab> or space characters, and nothing else, is considered ambiguous. Blue Coat doesn't know if this is a blank continuation line or if it is the blank line that signals the end of the header section. By default, an ambiguous blank line is illegal, and an error is reported. With tolerant request parsing enabled, an ambiguous blank line is treated as the blank line that signals the end of the header section.

To Enable the HTTP Tolerant Request Parsing Flag through the CLI:

Note: This feature is only available through the CLI. It cannot be set through the Management Console.

From the `(config)` prompt, enter the following command to enable tolerant HTTP request parsing (the default is disabled):

```
SGOS# (config) http tolerant-request-parsing
```

To disable HTTP tolerant request parsing, enter the following command:

```
SGOS# (config) http no tolerant-request-parsing
```

To view all HTTP settings, including `http tolerant-request-parsing` if it is enabled, see "Viewing the HTTP Settings through the CLI" on page 159.

Controlling the HTTP Proxy Profile

When configured as a server accelerator, the ProxySG improves object response time to client requests, scalability of the origin server site, and overall Web performance at the origin server. A server accelerator services requests meant for an origin server as if it is the origin server itself.

Because an origin server can actually consist of many servers—a single Web server or an entire server farm—origin servers are identified by domain name or IP address. To the ProxySG, the domain name or IP address is treated as the origin server, regardless of how many back-end Web servers might be installed.

When a ProxySG is first manufactured, it is set to a *Normal* profile. You can also use a Bandwidth Gain profile or the Portal profile. You can also combine needed elements of all three profiles.

Section B: Configuring Explicit Proxies

Table 6.3: Differences Among Normal, Bandwidth Gain, and Portal Profiles

Configuration	Normal	Bandwidth Gain	Portal
Pipeline embedded objects in client requests	Enabled	Disabled	Disabled
Pipeline embedded objects in prefetch requests	Enabled	Disabled	Disabled
Pipeline redirects for client requests	Enabled	Disabled	Disabled
Pipeline redirects for prefetch requests	Enabled	Disabled	Disabled
Cache expired objects	Enabled	Enabled	Disabled
Enable Bandwidth Gain Mode	Disabled	Enabled	Disabled
Substitute GET for IMS ("if modified since")	Disabled	Enabled	Enabled
Substitute GET for PNC (Pragma no cache)	Disabled	-	Enabled
Substitute GET for HTTP 1.1 conditionals	Disabled	Enabled	Enabled
Substitute GET for IE (Internet Explorer) reload	Disabled	-	Enabled
Never refresh before expiration	Disabled	Enabled	Enabled
Never serve after expiration	Disabled	-	Enabled

Note: A “-” (dash) in Table 6.3 indicates that the corresponding configuration does not change when the profile changes.

To Configure the Acceleration Profile through the Management Console:

1. Select Configuration>Services>HTTP Proxy>Acceleration Profile.

The Acceleration Profile tab displays with the Normal Profile.

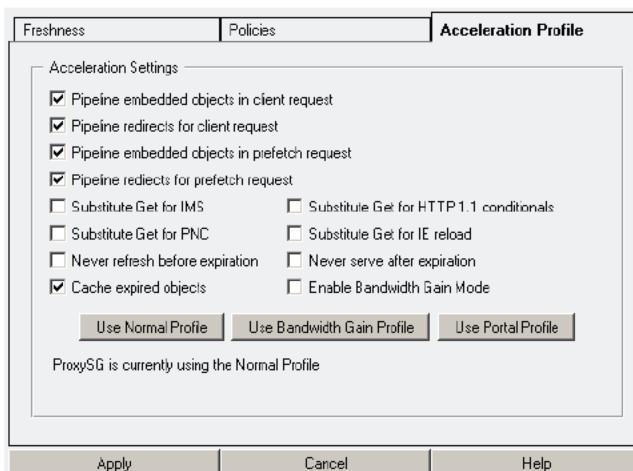


Figure 6-7: Acceleration Profile Tab

Important: The existing configuration is *not* preserved.

Once the ProxySG is set to a specific profile, the profile is maintained in the event the ProxySG is upgraded.

Section B: Configuring Explicit Proxies

Note: You can customize the settings, no matter which button you select.

2. Click Use Bandwidth Gain Profile or Use Portal Profile.
The default settings change to reflect the new profile.
3. Click Apply.

To Switch Profiles through the CLI:

1. At the `(config)` command prompt, enter the profile you want:

```
SGOS#(config) profile {normal | portal | bwgain}
```

Note: You cannot mix and match profiles through the CLI. Customizing the profile is only available through the Management Console.

2. (Optional) View the settings. (This example assumes you have selected the Portal profile.)

```
SGOS#(config) show profile
SG is currently using the Portal Profile

Pipeline client requests:           Disabled
Pipeline client redirects:          Disabled
Pipeline prefetch requests:         Disabled
Pipeline prefetch redirects:        Disabled
Substitute Get "if-modified-since": Enabled
Substitute Get "pragma: no-cache":  Enabled
Substitute HTTP 1.1 Conditional Get: Enabled
Substitute Internet Explorer reload: Enabled
Never refresh before expiration:   Enabled
Never serve after expiration:      Enabled
Cache expired objects:             Disabled
Bandwidth gain mode:               Disabled
```

You can view all HTTP settings. See "Viewing the HTTP Settings through the CLI" on page 159 for more information.

Using Explicit HTTP Proxy with Internet Explorer

Internet Explorer does not allow origin content server (OCS) NTLM authentication through a ProxySG when explicitly proxied. To correct this, Blue Coat has added a "Proxy-Support: Session-based-authentication" header that is sent by default when the ProxySG receives a 401 authentication challenge from upstream when the client connection is an explicit proxy connection.

For older browsers or if both the ProxySG and the OCS do NTLM authentication, the Proxy-Support header might not work. In this case, you can disable the header and instead enable NTLM-force, which converts the 401-type server authentication challenge to a 407-type proxy authentication challenge, supported by Internet Explorer. The ProxySG also converts the resulting Proxy-Authentication headers in client requests to standard server authorization headers, which allows an origin server NTLM authentication challenge to pass through when Internet Explorer is explicitly proxied through the ProxySG.

Section B: Configuring Explicit Proxies

Disabling the Proxy-Support Header

You can control the header using header modification policy. Suppression or modification of the Proxy-Support custom header keeps the ProxySG from sending this default header. Use either the Visual Policy Manager (VPM) or CPL to disable the header through policy. For complete information on using VPM, see Chapter 13: "The Visual Policy Manager" on page 377.

Note: If you want to suppress the Proxy-Support header globally, you can use the `http force-ntlm` command to change the option. To suppress the header only in certain situations, continue with the procedures below.

VPM

To suppress the header using VPM, create a new Web Access Layer. Then:

1. Right click in the Action field to see the drop-down list; select Set.
The Existing Action Object dialog displays.
2. Click New to see the drop-down list; select Control Response Header.
The Add Control Response Header Object dialog displays.

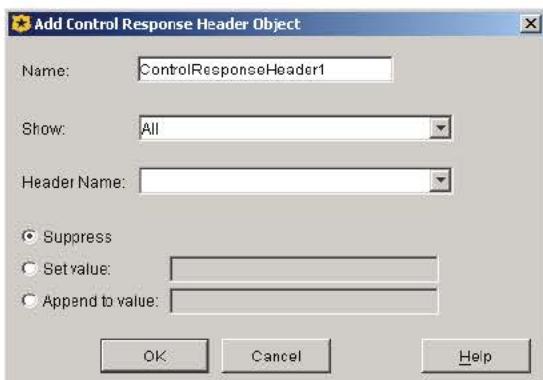


Figure 6-8: Add Control Response Header Object

3. Fill in the fields as follows:
 - Name:** Enter a meaningful name. This name will display in the Existing Action Objects dialog.
 - Show:** Select Custom from the drop-down list.
 - Header Name:** Enter Proxy-Support.
 - Make sure the Suppress radio button is selected.
4. Click OK.
5. Scroll to the bottom of the Add Control Response Header Object dialog to see the Proxy-Support header.
6. Click OK.

Section B: Configuring Explicit Proxies

CPL

Use CPL to define the Proxy-Support custom header object and to specify what action you want to take. The example below uses Proxy-Support as the action name, but you can choose any name meaningful to you. The result of this action is to suppress the Proxy-Support header

```
<proxy>
    action.Proxy-Support(yes)
    define action Proxy-Support
        delete(response.x_header.Proxy-Support)
    end action Proxy-Support
```

Enabling or Disabling NTLM Authentication for Internet Explorer Clients

The following procedure forces Internet Explorer clients explicitly-proxied through a ProxySG to participate in NTLM authentication. Note that this CLI setting is global, affecting all clients. You can also use VPM or CPL to provide granular control for NTLM authentication. (See "VPM" on page 157 and "CPL" on page 157.) These commands should only be used if the Proxy-support header is not suitable for the situation.

Note: These procedures can only be done through the CLI. The Management Console is not available.

Do one of the following (note that the default is `http no force-ntlm`):

- To force NTLM authentication for Internet Explorer clients, enter the following command at the (config) command prompt:
`SGOS#(config) http force-ntlm`
- To disable NTLM authentication for Internet Explorer clients, enter the following command at the (config) command prompt:
`SGOS#(config) http no force-ntlm`

To view all HTTP settings, see "Viewing the HTTP Settings through the CLI" on page 159.

VPM

To use VPM to force NTLM authentication, create a new Web Access Layer. Then:

1. Right click in the Action field to see the drop-down list; select Set.
The Existing Action Object dialog displays.
2. Scroll to the Force NTLM for Server Auth static object; select it.
3. Click OK.

CPL

Global configuration of NTLM authentication behavior is set through the CLI command `http force-ntlm` (the default is `http no force-ntlm`). The `http.force_ntlm_for_server_auth()` CPL property can be used to override the global settings for a particular subset.

Section B: Configuring Explicit Proxies

To create a rule to force NTLM authentication for explicitly proxied Internet Explorer clients, first define the action, then define the rule.

This example implements the following policies:

- All clients from the “ForceNTLM_subnet” have force-ntlm turned on. These clients do not use the Proxy-Support header.
- Requests for all other hosts have force-ntlm turned off. These hosts use the Proxy-Support header.

```
define subnet ForceNTLM_subnet
    10.10.0.0/16
end

<Proxy>
    client.address=ForceNTLM_subnet http.force_ntlm_for_server_auth(yes)
    http.force_ntlm_for_server_auth(no)
end
```

Byte Range Support

HTTP byte range support on the ProxySG can be enabled or disabled through the CLI. If byte range support is disabled, then HTTP will treat all byte range requests as non-cacheable. This means that HTTP will never even check to see whether the object is in the cache, but will forward the request to the Origin Content Server (OCS) and not cache the result. Thus, a byte range request has no affect on the cache when byte range support is disabled.

If byte range support is enabled (the default setting), the ProxySG will try to serve the byte range request from the cache. With byte range support enabled, if the object is already cached and the ProxySG does not need to reload the object from the OCS, the ProxySG will serve the byte range request from the cache only. But if the object is not in the cache or if it requires a reload of the object from the OCS, the ProxySG may treat the byte range request as if the byte range support is disabled.

Most download managers make byte range requests with a PNC (pragma-no-cache) header. In order to serve such requests from the cache, you should also configure the PNC settings as described below. For more information, see "Controlling the HTTP Proxy Profile" on page 153.

Configuring Byte Range Support

Byte range support can be enabled or disabled through the CLI. You cannot configure this setting through the Management Console.

To Enable Byte Range Support through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) http byte-ranges
```

To Disable Byte Range Support through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) http no byte-ranges
```

Section B: Configuring Explicit Proxies

To Configure the PNC Setting through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) http revalidate-pragma-no-cache
-or-
SGOS# (config) http no revalidate-pragma-no-cache
```

To view all HTTP settings, see "Viewing the HTTP Settings through the CLI".

Viewing the HTTP Settings through the CLI

You can view the existing HTTP settings by entering the following command:

Note: The tolerant-request-parsing option displays only if it is enabled.

```
SGOS# (config) show http
Supported protocol version: HTTP 1.1
Caching options:
  Cache authenticated data: enabled
  Cache expired objects: enabled
  Cache personal pages: disabled
  Reverse DNS lookup on IP: disabled
  Strip From Headers: disabled
  Byte range support: enabled
  Force NTLM on proxy IE: disabled
  Rewrite redirects for XP: disabled
  Revalidate "pragma: no-cache": disabled
  WWW redirect if host not found: enabled
Force explicit expirations:
  Never refresh before: disabled
  Never serve after: disabled
Add headers:
  "Front-end-https": disabled
  "Via": disabled
  "X-forwarded-for": disabled
  "Client-ip": disabled
Parsing options:
  HTML meta tag "Cache-Control": enabled
  HTML meta tag "Expires": enabled
  HTML meta tag "Pragma: no-cache": enabled
Persistent connections:
  Client connections: enabled
  Server connections: enabled
Pipeline:
  Client requests: enabled
  Client redirects: enabled
  Prefetch requests: enabled
  Prefetch redirects: enabled
Substitute simple Get for:
  Get "if-modified-since": disabled
  Get "pragma: no-cache": disabled
HTTP 1.1 Conditional get: disabled
```

Section B: Configuring Explicit Proxies

```
Internet Explorer reload: disabled
Proprietary header extensions:
    Blue Coat extensions:      disabled
FTP proxy:
    Url path is:           absolute from root
    Configuration/access log uploads: will use PASV
Persistent connection timeouts:
    Server:                 900
    Client:                 360
Receive timeouts:
    Server:                 180
    Client:                 120
    Refresh:                90
Https:
    ssl-verify-server:      enabled
    tolerant-request-parsing: enabled
```

Configuring a SOCKS Proxy

While SOCKS servers are generally used to provide firewall protection to an enterprise, they also can be used to provide a generic way to proxy any TCP or UDP protocols. The ProxySG supports both SOCKS v4/4a and SOCKS v5; however, because of increased username and password authentication capabilities, Blue Coat recommends that you use SOCKS v5.

Note: For Blue Coat compatibility with SOCKS clients, check with customer support.

Configuring a SOCKS proxy requires two steps:

- Creating and configuring the service
- Creating and enabling the port service

Creating and Configuring the Service

Complete the following steps to create a SOCKS proxy and to configure SOCKS-proxy connection and timeout values.

Note: Policy allows you to control the version of SOCKS is accepted. For example, to use only SOCKS v5, enter the following in the Local Policy file:

```
<proxy>
    client.protocol=socks
    ALLOW socks.version=5
DENY
```

To Create a SOCKS Proxy Server through the Management Console:

1. Select Configuration>Services>SOCKS Proxy.

The SOCKS Proxy tab displays.

Section B: Configuring Explicit Proxies

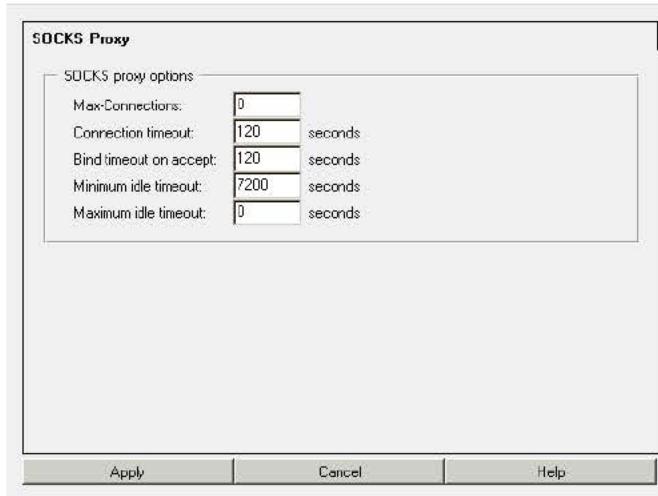


Figure 6-9: SOCKS Proxy Tab

- Fill in the option fields (described below) as needed. The defaults are displayed and should be sufficient for most purposes.

Max-Connections	connections	Set maximum allowed SOCKS client connections. The default of 0 indicates an infinite number of connections are allowed.
Connection timeout	seconds	Set maximum time to wait on an outbound CONNECT.
Bind timeout on accept	seconds	Set maximum time to wait on an inbound BIND.
Minimum idle timeout	seconds	Set minimum SOCKS client idle time threshold.
Maximum idle timeout	seconds	Set maximum SOCKS client idle time threshold.

To Configure the SOCKS Proxy through the CLI:

- At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) socks-proxy accept-timeout seconds | connect-timeout seconds |  
max-connections number | max-idle-timeout seconds | min-idle-timeout seconds
```

- (Optional) View the results.

```
SGOS#(config) show socks-proxy  
max-connections: 0  
accept-timeout: 120  
connect-timeout: 120  
min-idle-timeout: 7200  
max-idle-timeout: 0
```

Enabling the SOCKS Proxy

Note that a SOCKS port is already configured on port 1080 and enabled.

Section B: Configuring Explicit Proxies

To Edit an Existing SOCKS Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.
2. Highlight the SOCKS server.
3. Click Edit; the Edit Service dialog appears.

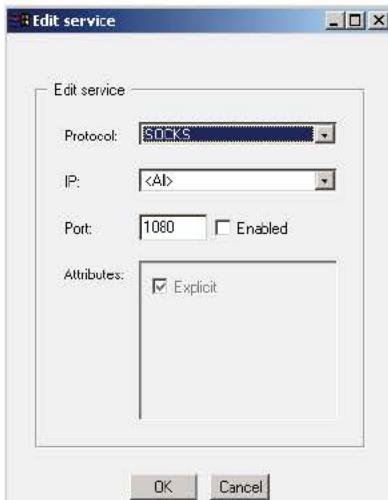


Figure 6-10: SOCKS Add Service Dialog

4. In the Protocol drop-down list, select SOCKS.
5. The default IP address value is all. To limit the service to a specific IP address, select it from the drop-down list.
6. In the Port field, specify a port number; select Enable.
7. Click OK; Click Apply.

To Edit an Existing SOCKS Port Service through the CLI:

1. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) socks
SGOS#(config services socks) enable [ip_address:]port
```

2. (Optional) View the results:

```
SGOS#(config services socks) view
Port: 1080 IP: 10.9.87.85 Type: socks
Properties: explicit, enabled
```

Shell Proxies

Shell proxies are those that provide a shell allowing a client to connect to the ProxySG. In this version, only a Telnet shell proxy is supported.

Section B: Configuring Explicit Proxies

Using a shell proxy, you can:

- terminate a Telnet protocol connection either transparently or explicitly.
- authenticate users either transparently or explicitly.
- view the access log.
- enforce policies specified by CPL.
- communicate through an upstream SOCKS gateway and HTTP proxy using the CONNECT method.

Within the shell, you can configure the prompt and various banners using CPL \$substitutions. You can also use hard-coded text instead of CPL substitutions (available substitutions are listed in the table below). The syntax for a CPL substitution is:

`$ (CPL_property)`

Table 6.4: Substitutions Available at New Connection Time

<code>proxy.name</code> or <code>appliance.name</code>	Configured name of the ProxySG.
<code>proxy.address</code>	IP address of the appliance on which this connection is accepted.
<code>proxy.card</code>	Interface number of the appliance on which this connection is accepted.
<code>client.protocol</code>	This is "telnet".
<code>client.address</code>	IP address of the client.
<code>proxy.primary_address</code> -or- <code>appliance.primary_address</code>	Primary address of the proxy, not where the user is connected.
<code>release.id</code>	SGOS version.

Customizing Policy Settings for Shell Proxies

To manage a shell proxy through policy, you can use the conditions, properties, and actions list below. For information on using CPL to manage shell proxies, refer to the *Blue Coat Content Policy Language Guide*.

Conditions:

All time and date related triggers	<code>proxy.address=</code>
All exception related triggers	<code>proxy.card=</code>
All server_url triggers	<code>proxy.port=</code>
All url triggers	<code>client.protocol=</code>
All authentication related triggers	<code>user-defined conditions</code>
<code>category=</code>	<code>client.protocol=telnet</code>
<code>client.address=</code>	<code>url.scheme=telnet</code>

Section B: Configuring Explicit Proxies

Properties:

allow, deny, force_deny	force_exception(exception_id[, details])
action.action_name{yes no}	forward(alias_list no)
All trace() properties	forward.fail_open(yes no)
All access_log() properties	reflect_ip(auto no client vip ip-address)
All log.xxx() properties	socks_gateway(alias_list no)
access_server(yes no)	socks_gateway.fail_open(yes no)
authenticate.force(yes no)	telnet.prompt(no string)
authenticate(realm)	telnet.realm_banner(no string)
exception(exception_id[, details])	telnet.welcome_banner(no string)

The banner strings support \$-sign substitutions.

Actions:

rewrite(url.host, host_regex_pattern, log_message() replacement_pattern)	
rewrite(url, url_regex_pattern, replacement_pattern)	notify_email(subject, body)
set(url_port, port_number)	notify_snmp(message)

Boundary Conditions for Shell Proxies

- A hardcoded timeout of five minutes is enforced from the acceptance of a new connection until destination information is provided using the Telnet command.
- If proxy authentication is enabled, users have three chances to provide correct credentials.
- Users will not be authenticated until destination information is provided.
- Users can only enter up to an accumulated 2048 characters while providing the destination information. (Previous attempts count against the total number of characters.)
- Connection to an upstream HTTP proxy is not encouraged.
- If connections from untrustworthy IP address or subnet are not desired, then a client IP/subnet-based *deny* policy must be written.

Telnet Shell Proxies

The Telnet shell proxy allows you to manage a Telnet protocol connection to the ProxySG. Using the Telnet shell proxy, you can do:

- Explicit termination without proxy authentication, where you explicitly connect, through Telnet, to the ProxySG hostname or IP address. In this case, the ProxySG provides a shell.
- Explicit termination with proxy authentication, where after obtaining the destination host and port information from user, the ProxySG challenges for proxy credentials. Once the correct proxy credentials are provided and authenticated, the ProxySG makes an upstream connection and goes into tunnel mode. In this case, the ProxySG provides a shell.

Section B: Configuring Explicit Proxies

- Transparent termination without proxy authentication, where the ProxySG intercepts Telnet traffic through an L4 switch, software bridge, or any other transparent redirection mechanism. From the destination address of TCP socket, the ProxySG obtains origin server contact information and makes the appropriate upstream connection, either directly or through any configured proxy. For more information on configuring a transparent proxy, see "Transparent Proxies" on page 169.
- Transparent termination with proxy authentication, where, after intercepting the transparent connection, the ProxySG challenges for proxy credentials. Once the correct proxy credentials are provided and authenticated, the ProxySG makes an upstream connection and goes into tunnel mode. For more information on configuring a transparent proxy, see "Transparent Proxies" on page 169.

Once in the shell, the following commands are available:

- help: Displays available commands and their effects.
- telnet <server[:port]>: Makes an outgoing telnet connection to specified server. The colon (:) between server and port can be replaced with a space, if preferred.
- exit: Terminates the shell session.

Creating a Telnet Shell Proxy Service

On a new system, Telnet proxy service is configured but disabled on port 23. On an upgrade, a Telnet proxy service is not created.

To enable or create a Telnet proxy service, use Services>Service Ports on the Management Console, or config>services>telnet from the CLI. For more information, see "Telnet Shell Proxy Service" on page 134.

Customizing Welcome and Realm Banners and Prompt Settings

You can configure banners for the Telnet shell and the realm and set the prompt that users see when entering the shell.

To Customize Telnet Shell Proxy Settings through the Management Console:

1. Select Configuration>Services>Shell Proxies>Telnet Proxy Settings.

The Telnet Proxy Settings Tab displays.

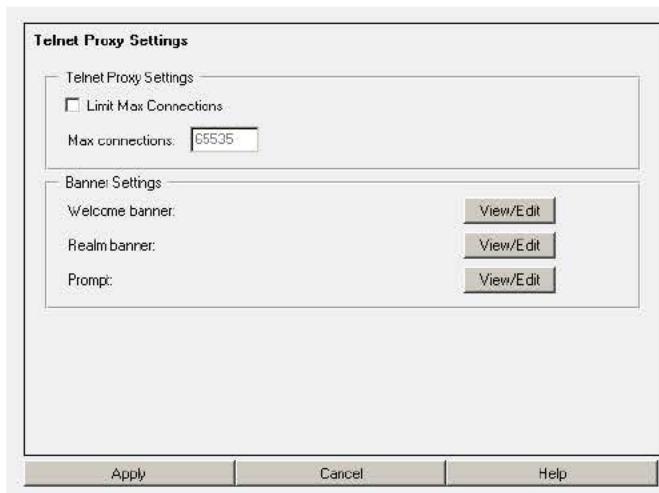
Section B: Configuring Explicit Proxies

Figure 6-11: Telnet Proxy Settings

2. If you want to set the maximum concurrent connections, check the Limit Max Connections checkbox. Then enter the number of maximum concurrent connections allowed for this service. Allowed values are between 1 and 65535.
3. Set the banner settings:
 - a. To set the Welcome banner message (users see this when they enter the shell), click View/Edit next to the Welcome Banner. The Edit Welcome Banner dialog displays. (If you do not want this banner displayed, remove the text.)

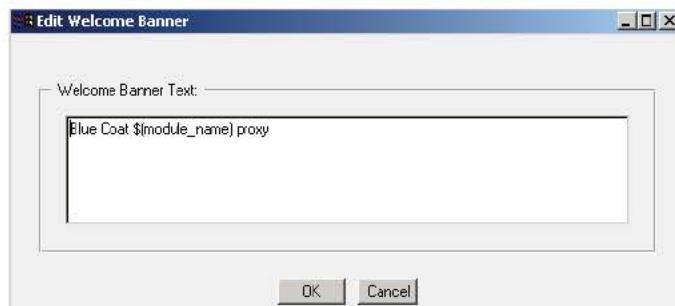


Figure 6-12: Editing Welcome Banner Properties.

Change the banner as necessary. The `$(client.protocol)` text is a CPL variable indicating that Telnet is the protocol. You do not have to use a variable. (For a list of available \$substitutions, see "Substitutions Available at New Connection Time" on page 163.) When finished, click OK. Click Apply.

- b. To set the realms banner message (users see this help message just before they see the Username prompt for proxy authentication), click View/Edit next to the Realms Banner. The Edit Realms Banner dialog displays. (If you do not want this banner displayed, remove the text.)

Section B: Configuring Explicit Proxies

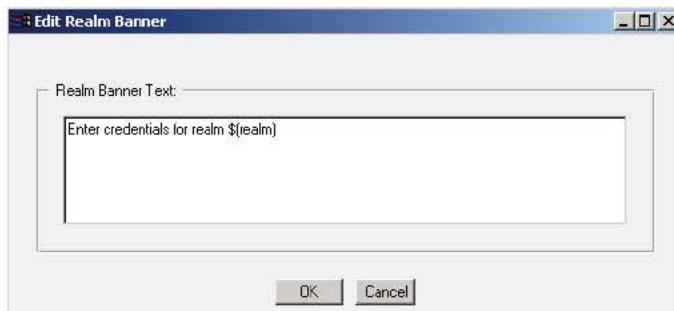


Figure 6-13: Editing Realm Banner Properties

Change the banner as necessary. The `$(realm)` text is a CPL variable indicating the name of the realm. You do not have to use a variable. (For a list of available substitutions, see "Substitutions Available at New Connection Time" on page 163.) When finished, click OK. Click Apply.

- c. To set the prompt, click View/Edit next to the Prompt line. The Prompt dialog displays.

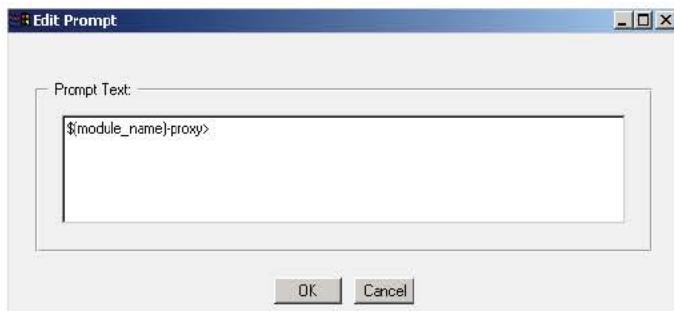


Figure 6-14: Editing the Prompt

Change the banner as necessary. The default is `$(client-protocol)>`, where `$(client-protocol)` is Telnet. You do not have to use a variable. (For a list of available substitutions, see "Substitutions Available at New Connection Time" on page 163.) When finished, click OK. Click Apply.

To Customize Telnet Shell Proxy Settings through the CLI:

You can use CPL substitutions when creating welcome and realm banners and Telnet prompts. For a list of available CPL substitutions, see "Substitutions Available at New Connection Time" on page 163.

1. From the (config) prompt, enter the following commands:

```
SGOS#(config) shell max-connections number
SGOS#(config) shell welcome-banner welcome-banner-string (Enclose string in quotes if string includes spaces)
SGOS#(config) shell realm-banner realm-banner-string (Enclose string in quotes if string includes spaces)
SGOS#(config) shell prompt prompt-string (Enclose string in quotes if string includes spaces)
```

Section B: Configuring Explicit Proxies

where:

max-connections	number	Allowed values are between 1 and 65535.
welcome-banner	string	The text a user sees when the shell is entered. You can hide this banner by using <code>shell no welcome-banner</code> .
realm-banner	string	The text a user sees when the realm is entered. You can hide this banner by using <code>shell no welcome-banner</code> .
prompt	string	The prompt a user sees when the shell is entered. You can hide the prompt by using <code>shell no prompt</code> .

2. (Optional) To view the shell's settings:

```
SGOS#(config) show shell
max-connections: Unlimited
prompt: Telnet #
realm-banner: Enter credentials for realm Test
welcome-banner: Welcome to Blue Coat Telnet shell proxy
```

To hide the shell's settings:

```
SGOS#(config) shell no welcome-banner
SGOS#(config) shell no realm-banner
SGOS#(config) shell no prompt
SGOS#(config) shell no max-connections
```

Boundary Conditions for Telnet Shell Proxies

- Telnet credential exchange is in clear text.
- A Telnet proxy cannot be used to communicate with non-Telnet servers (such as Web servers on port 80) because Telnet proxies negotiate Telnet options with the client before a server connection can be established.

Section C: Transparent Proxies

Section C: Transparent Proxies

To use transparent proxy, you must:

- Configure the network to redirect client requests.
- Create a transparent proxy service

Configuring the Transparent Proxy Hardware

For transparent proxy to work, you must use one of the following:

- ProxySG Pass-Through card
- ProxySG software bridge
- Layer-4 switch
- WCCP

Configuring the Pass-Through Card for Hardware Bridging

The Blue Coat Pass-Through card is a device that enables a bridge, using its two interface cards, so that packets can be forwarded across it. However, if the system crashes, the Pass-Through card becomes a network: the two Ethernet cables are connected so that traffic can continue to pass through without restriction.

Configure a transparent service on the bridge's IP address just like for any other IP address, and it intercepts traffic as usual.

The differences are:

- Forwards traffic: it does not intercept without enabling global IP packet forwarding.
- Proxies for requests on either interface card, so if you have connected one side of the bridge to your Internet connection, you must be careful.

Configuring the ProxySG for Software Bridging

Blue Coat supports a software or *dynamic* bridge that is constructed using a set of installed interface cards. Keep in mind the following about software bridges:

- The adapters must of the same type. Although the software does not restrict you from configuring bridges with adapters of different types (10/100 or GIGE), the resultant behavior is unpredictable.
- IP addresses—if any of the interface ports to be added to the bridge already have IP addresses assigned to them, those IP addresses must be removed.

To set up a software bridge, see "Configuring a Software Bridge" on page 69.

Section C: Transparent Proxies

Configuring a Layer-4 Switch for Transparent Proxy

In Transparent Proxy Acceleration, as traffic is sent to the origin server, any traffic sent on TCP port 80 is redirected to the ProxySG Appliances by the Layer 4 switch. The benefits to using a Layer 4 switch include:

- Built-in failover protection. In a multi-ProxySG setup, if one ProxySG fails, the Layer 4 switch can route to the next ProxySG.
- Request partitioning based on IP address instead of on HTTP transparent proxying. (This feature is not available on all Layer 4 switches.)
- ProxySG bypass prevention. You can configure a Layer 4 device to always go through the Blue Coat ProxySG machine even for requests to a specific IP address.
- ProxySG bypass enabling. You can configure a Layer 4 device to never go through the ProxySG.

The following are very generic directions for configuring transparent proxy using a Layer 4 switch and ProxySG Appliances. The steps to perform depend on the brand of Layer 4 switch. Refer to the Layer 4 switch manufacturer's documentation for details.

To Set up Transparent Proxy Using a Layer-4 Switch and the ProxySG:

From the Layer 4 switch:

1. Configure the Layer 4 switch according to the manufacturer's instructions.
2. Configure for global transparent cache switching (TCS). With global TCS, incoming traffic from all devices attached to all ports of the Layer-4 switch is redirected to the ProxySG. Assign an IP address, default gateway, and subnet mask to the Layer-4 switch.
3. Configure TCS using a global policy, enabling redirection for all ports.
4. Identify one or more ProxySG Appliances.
5. Create a device server group.
6. Apply the ProxySG name to the device group.
7. Configure Ethernet interface 2.
8. Disable the redirection policy for the port to which the ProxySG is connected.
9. Configure Ethernet interface 4.
10. Disable the redirection policy for the port to which the router is connected.
11. (Optional) Configure the Layer-4 switch for server load balancing.
12. Save the Layer-4 switch configuration.

From the ProxySG, all you need to do is:

- Define the appropriate IP configurations per the instructions in the *Installation Guide* that accompanied the ProxySG.
- Test the new network configuration.

Section C: Transparent Proxies

Configuring WCCP for Transparent Proxy

WCCP is a Cisco®-developed protocol that allows you to establish redirection of the traffic that flows through routers.

The main benefits of using WCCP are:

- Scalability—With no reconfiguration overhead, redirected traffic can be automatically distributed to up to 32 ProxySG Appliances.
- Redirection safeguards—if no ProxySG Appliances are available, redirection stops and the router forwards traffic to the original destination address.

For information on using WCCP with a Blue Coat ProxySG, see Appendix C: “Using WCCP” on page 785.

IP Forwarding

IP Forwarding is a special type of transparent proxy. The ProxySG is configured to act as a gateway. The gateway is configured so that if a packet is addressed to the gateway’s interface card, but not to its IP address, the packet is forwarded toward the final destination. (If IP forwarding is turned off, the packet is rejected as being mis-addressed).

By default, IP forwarding is set to off (disabled) to maintain a secure network.

To Enable IP Forwarding through the Management Console:

1. Select Configuration>Network>Routing>Gateways.
2. Select the Enable IP forwarding checkbox.
3. Click Apply.

To Enable IP Forwarding through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) tcp-ip ip-forwarding enable
```

When upgrading to SGOS 2.x from CacheOS 4.x, the ProxySG retains the setting.

Important: When IP forwarding is enabled, be aware that all ProxySG ports are open and all the traffic coming through them is not subjected to policy, with the exception of the ports explicitly defined (Configuration> Services>Service Ports).

Creating a Transparent Proxy Service

As noted earlier, Blue Coat recommends that you ignore authentication until the proxy service is configured and running.

The below example uses HTTP. Note that two HTTP services are already configured and enabled on SGOS 3.x.

Section C: Transparent Proxies

To Create a Transparent HTTP Port Service through the Management Console:

1. Select Configuration>Services>Service Ports.
2. Click New; the Add Service dialog appears.

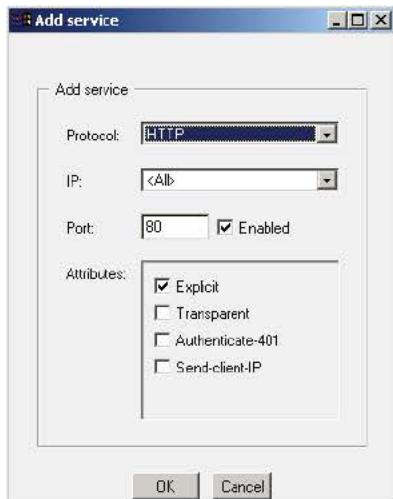


Figure 6-15: HTTP Add Service Dialog

3. In the Protocol drop-down list, select HTTP.
4. The default IP address value is all. To limit the service to a specific IP, select the IP from the drop-down list.
5. In the Port field, specify a port number; select Enable.
6. In the Attributes field, select Transparent.
7. Click OK; Click Apply.

To Create a Transparent HTTP Port Service through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) services
SGOS#(config services) http
SGOS#(config services http) create [ip_address:]port
SGOS#(config services http) attribute transparent enable [ip_address:]port
SGOS#(config services http) enable [ip_address:]port
```

To view the results:

```
SGOS#(config services http) view
Port: 8080      IP: 0.0.0.0          Type: http
Properties: explicit, enabled
Port: 80        IP: 0.0.0.0          Type: http
Properties: transparent, explicit, enabled
```

Chapter 7: Using Secure Services

Secure services allow you to provide the maximum security level for your enterprise. Maximum security is provided by using:

- SSH (with RSA authentication) instead of Telnet for basic communication between machines.
- HTTPS instead of HTTP for secure communication over insecure channels.
- A method of authenticating (identifying your users) and authorizing (limiting what a user can do).

Configuring secure services requires creating and using keypairs and certificates to verify trusted hosts.

This chapter discusses:

- "HTTPS Termination Overview"
- "Configuring HTTPS Termination"
- "Managing the SSL Client"
- "Enabling an HTTPS Service"
- "Configuring HTTP or HTTPS Origination to the Origin Content Server"
- "Configuring DNS Resolution to the Origin Content Server"

HTTPS Termination Overview

Offloading SSL processing from the origin server (referred to as *HTTPS termination*), allows more requests to be processed more quickly from the ProxySG.

The HTTPS termination implementation:

- Combines hardware-based SSL acceleration with full caching functionality.
- Establishes and services incoming SSL sessions.
- Provides SSL v2.0, v3.0, and TLSv1 protocol support.

A common scenario in using HTTPS termination is in conjunction with HTTPS origination. HTTPS termination is used to connect the client to the ProxySG; HTTPS origination is used to connect from the ProxySG to the Origin Content Server (OCS).

Before discussing the specifics of how a ProxySG accelerates HTTPS requests, it is important to understand securing data using HTTPS. There are several RFCs and books on the public key cryptographic system (PKCS). This discussion of the elements of PKCS is relevant to their implementation in SGOS.

The key concepts to understand are:

- Public keys and private keys

- Certificates
- Keyrings
- Cipher Suites
- SSL client

There are many network infrastructure variables that must be considered in your key and certificate management plan. A good publication that addresses such issues is *Understanding Public-Key Infrastructure; Concepts, Standards, and Deployment Considerations* by Carlisle Adams and Steve Lloyd - ISBN 1-57870-166-X.

Public Keys and Private Keys

The intended recipient of encrypted data generates a private/public keypair, and publishes the public key, keeping the private key secret. The sender encrypts the data with the recipient's public key, and sends the encrypted data to the recipient. The recipient uses the corresponding private key to decrypt the data.

For two-way encrypted communication, the endpoints can exchange public keys, or one endpoint can choose a symmetric encryption key, encrypt it with the other endpoint's public key, and send it.

A keyring contains a public/private keypair. It can also contain a certificate signing request or a signed certificate.

Certificates

Certificates are used to authenticate the identity of a server by associating a public key with a particular server. A certificate is electronic confirmation of the owner of a public key, and contains other information, such as its expiration date. Several kinds of certificates are used.

Self-Signed Certificates

A self-signed certificate is a certificate that you create and authorize yourself that has no official guarantees or authority in the real world. It is mainly used for intranet security.

CA Certificates

This association is performed by a certificate signing authority (CA), who verifies the identity of a server and then signs the server's public key. The resulting certificate can then be offered by the server to clients who can recognize the CA's signature and trust that the server is who it claims to be. Such use of certificates issued by CAs has become the primary infrastructure for authentication of communications over the Internet.

ProxySG appliances come with many popular CA certificates already installed. You can review these certificates using the `ssl view summary ca-certificate` command.

Additionally, CA certificates installed on the ProxySG are used to verify client certificates (when browsers are configured to offer them during negotiation) and are also required to verify secure servers in communication with the ProxySG.

External Certificates

An external certificate is an X.509 certificate created outside the ProxySG for the purpose of encrypting access logs. When you import an external certificate to the ProxySG, you can use it to encrypt your access logs so that only those with the appropriate security credential can decrypt them. See "Customizing the Log: Configuring the Upload Client" on page 655 for information about encrypting access logs.

Wildcard Certificates

Wildcard certificates are certificates that contain wildcard characters in the common name field of an X.509 certificate. Wildcards certificates are typically used in order to share a single certificate among multiple hosts belonging to the same DNS domain.

Wildcard certificates during SSL termination are supported. Keep in mind that Microsoft's implementation of wildcard certificates is as described in RFC 2595, allowing an * (asterisk) in the leftmost-element of the server's common name only. For information on wildcards supported by Internet Explorer, refer to the Microsoft knowledge base, article: 258858.

Cipher Suites Supported by SGOS

A cipher suite is an object that specifies the algorithms used to secure an SSL connection. When a client makes an SSL connection to a server, it sends a list of the cipher suites that it supports. The server compares this list with its own supported cipher suites and chooses the first cipher suite proposed by the client that they both support. Both the client and server then use this cipher suite to secure the connection.

All cipher suites supported by the ProxySG use the RSA key exchange algorithm, which uses the public key encoded in the server's certificate to encrypt a piece of secret data for transfer from the client to server. This secret is then used at both endpoints to compute encryption keys.

By default, the ProxySG is configured to allow SSLv2 v3 as well as TLSv1 traffic. The cipher suites available to use differ depending on whether you configure SSL for version 2, version 3, TLS, or a combination of these.

Table 7.1: SGOS Cipher Suites Shipped with the ProxySG

SGOS Cipher #	Cipher Name	Strength	Exportable	Description
1	RC4-MD5	Medium	No	128-bit key size.
2	RC4-SHA	Medium	No	128-bit key size.
3	DES-CBC3-SHA	High	No	168-bit key size.
4	DES-CBC3-MD5	High	No	168-bit key size.
5	RC2-CBC-MD5	Medium	No	128-bit key size.
6	RC4-64-MD5	Low	No	64-bit key size.
7	DES-CBC-SHA	Low	No	56-bit key size.
8	DES-CBC-MD5	Low	No	56-bit key size.
9	EXP1024-RC4-MD5	Export	Yes	56-bit key size.
10	EXP1024-RC4-SHA	Export	Yes	56-bit key size.
11	EXP1024-RC2-CBC-MD5	Export	Yes	56-bit key size.

Table 7.1: SGOS Cipher Suites Shipped with the ProxySG

SGOS Cipher #	Cipher Name	Strength	Exportable	Description
12	EXP1024-DES-CBC-SHA	Export	Yes	56-bit key size.
13	EXP-RC4-MD5	Export	Yes	40-bit key size.
14	EXP-RC2-CBC-MD5	Export	Yes	40-bit key size.
15	EXP-DES-CBC-SHA	Export	Yes	40-bit key size.

Server Gated Cryptography and International Step-Up

Due to US export restrictions, international access to a secure site requires the site negotiate export-only ciphers. These are relatively weak ciphers ranging from 40-bit to 56-bit key lengths, and are vulnerable to attack.

Server Gated Cryptography (SGC) is a Microsoft extension to the certificate that allows the client receiving the certificate to first negotiate export strength ciphers, followed by a re-negotiation with strong ciphers. Netscape has a similar extension called International Step-up.

The ProxySG supports both SGC and International Step-up in its SSL implementation. There are, however, known anomalies in Internet Explorer's implementation that can cause SSL negotiation to fail. Refer to the following two documents for more detail and check for recent updates on the Microsoft support site.

<http://support.microsoft.com/support/kb/articles/Q249/8/63.ASP>
<http://support.microsoft.com/support/kb/articles/Q244/3/02.ASP>

To take advantage of this technology, the ProxySG supports VeriSign's Global ID Certificate product. The Global ID certificate contains the extra information necessary to implement SGC and International Step-up.

Note: When requesting a Global ID certificate, be sure to specify bluecoat as the server.

SSL Client

The SSL client is used to determine the protocol of outgoing HTTPS connections. The protocol must be specified when a ProxySG obtains content from the origin server using an encrypted connection.

Although only one SSL client exists on a ProxySG, the SSL client:

- Determines which certificates can be presented to origin servers by associating a keyring with the SSL client.
- Identifies the protocol version the ProxySG uses in negotiations with origin servers.
- Identifies the cipher suites used.

Configuring HTTPS Termination

To configure HTTPS termination, you must complete the following tasks:

- Create a keyring. A default keyring is shipped with the system. You can create others.

- (Optional) Create Certificate Signing Requests (CSRs) that can be sent to Certificate Signing Authorities (CAs).
- Create or import certificates and associate them with the keyring.
- Associate the keyring with the SSL client, if necessary.
- Enable the HTTPS Service.

Do these steps in order.

Note: These steps must be done with a serial console or SSH connection; you cannot use Telnet.

Before you begin, you should be familiar with the following terms:

CA Certificates	This is a certificate that has been signed by a CA. You only need this certificate if the ProxySG will be obtaining data through an encrypted source. CA certificates are also used to verify the client certificates that browsers can be configured to present.
CA-Cert Lists	CA-Cert lists allow you to associate a specific CA certificate (or a list of CA certificates) with the HTTPS service you create.
Certificates	A certificate can be created (self-signed), imported from another machine, or sent by Certificate Signing Authorities (CA Certificates). Certificates and CA Certificates are imported differently on the ProxySG.
Certificate Signing Authority (CA)	CAs receive Certificate Signing Requests and create signed certificates from the information and the keypair provided. The signed certificate is then returned to the originator, who can import it into the ProxySG.
Certificate Signing Request (CSR)	CSRs are used to send a keypair and critical information to a Certificate Signing Authority. You can use Blue Coat to create a CSR or you can create a CA Certificate off-line. Once the certificate is sent from the CA, you can import into the ProxySG. (For information on importing CA certificates, see "Importing a CA-Certificate" on page 190.)
SSL Client	Only one SSL client can be used on the ProxySG, and only one keyring can be associated with it. If a keyring is associated with the SSL client and you change the association, the old association is overwritten by the new. When the ProxySG is acting as SSL client (SSL origination), SSL sessions are re-used until the server forces a fresh handshake or until the same session ID has been used 255 times.
SSL Server	When the ProxySG is acting as an SSL server (SSL termination), SSL sessions are cached for one hour. This timeout value is not configurable.
HTTPS Service	Once the keyrings are configured properly, you can create an HTTPS service and associate any keyring that has certificates with the HTTPS service.
Keyring	A keyring holds a keypair and a certificate, and can be used when configuring secure connections on the ProxySG. When a keyring is created, it only contains a keypair. You can associate a certificate with this keyring. If you have multiple certificates, you can configure multiple keyrings and associate the certificates and the keyrings.

Creating a Keyring

The ProxySG ships with two keyrings already created:

- The default
- configuration-passwords-key

The default keyring contains a certificate and an automatically-generated keypair. Because the default keyring is self-signed, you might want to create other keyrings signed by a well-known Certificate Signing Authority.

You must associate a keyring with the SSL client if the ProxySG will be obtaining content from an origin server using HTTPS. For information on associating a keyring with the SSL client, see "Managing the SSL Client" on page 196.

The configuration-passwords-key keyring contains a keypair but does not contain a certificate. It is a keyring created for encrypting passwords in the `show config` command and should not be used for other purposes.

To Create a Keyring through the Management Console:

1. Select Configuration>SSL>Keyrings>SSL Keyrings.

The SSL Keyrings tab displays.



Figure 7-1: SSL Keyring Tab

2. Click **Create**; the Create Keyring dialog appears.



Figure 7-2: Create Keyring Dialog

3. If you want to be able to show the keypair in the future, select Show-private-key.

The Show-private-key option allows the keys to be viewed and exported in the future, while the default is to never allow the keys to be viewed or exported from this ProxySG. If you think that the keypair-certificate combination will be needed in the future (for example to put onto an origin server or onto another ProxySG), then select the Show-private-key option. The default of not allowing keys to be viewed or exported is provided as additional security for environments where the keys will never be used outside of the particular ProxySG.

4. Select either the Create a new or Import keyring radio button.

If you select Create new, enter a Keyring value into the field and press OK. The keyring, containing a keypair, is created with the name you chose. It does not have a certificate associated with it yet. To associate a certificate, see "Managing SSL Certificates" on page 180.

If you select Import keyring, the grayed-out Keyring field is enabled, allowing you to paste in the already existing keypair. The certificate associated with this keypair must be imported separately. For information on importing a certificate, see "Importing an Existing Keyring and Certificate" on page 184.

If the keypair that is being imported has been encrypted with a password, select Keyring Password and enter the password into the field.

5. Click OK.

To Create an SSL Keyring through the CLI:

At the (config) command prompt, enter the following commands to create an SSL keyring:

```
SGOS#(config) ssl
SGOS#(config ssl) create keyring {show | no-show} keyring_id [key_length]
```

where:

<code>show no-show</code>	The show option allows the keys to be viewed and exported in the future, while the no-show option will never allow the keys to be viewed or exported from this ProxySG. If you think that the keypair-certificate combination will be needed in the future (for example to put onto an origin server or onto another ProxySG), then the show option should be selected. The no-show option is provided as additional security for environments where the keys will never be used outside of the particular ProxySG.
<code>keyring_id key_length</code>	<p>The name, meaningful to you, of the keyring.</p> <p>Longer keypairs provide better security, but with a slight performance expense on the ProxySG Appliance. The default keylength used in SGOS and most U.S.-based servers is 1024, which is the maximum keylength. Be aware that the maximum keylength allowed for international export might be different than the default. For deployments reaching outside of the U.S., determine the maximum keylength allowed for export.</p>

To Import a Keyring through the CLI:

Note: This procedure can only be done if the keyring containing the keypair was created using the `show` parameter.

1. Copy the certificate to the clipboard.
2. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) ssl  
SGOS#(config ssl) import keyring {show | no-show} keyring_id  
Paste keypair here, end with "..." (three periods) on a new line
```

To View the Results of a New or Imported Keyring through the CLI:

Note: This example shows the default keyring.

```
SGOS#(config ssl) view keyring [keyring_id]  
KeyringID: default  
Is private key showable? yes  
Have CSR? no  
Have certificate? yes  
Is certificate valid? yes  
CA: Blue Coat SG110  
Expiration Date: Dec 16 22:37:30 2013 GMT  
Fingerprint: AA:E2:34:DB:5D:06:A7:FF:D8:69:BE:0D:12:FC:34:D5  
KeyringID: configuration-passwords-key  
Is private key showable? yes  
Have CSR? no  
Have certificate? no
```

Managing SSL Certificates

The ProxySG ships with a certificate associated with a default keyring. The certificate, self-signed and associated with the default keyring, can be reused in other keyrings meant for internal use.

You can add three kinds of SSL certificates:

- A self-signed certificate
- A certificate signed by a CA
- An external certificate

Note: You can create a Certificate Signing Request either on the ProxySG or off-box to send to a Certificate Signing Authority.

To create a self-signed certificate, continue with the next section. To import an existing certificate, continue with "Importing an Existing Keyring and Certificate"; to import an external certificate, see "Importing an External Certificate" on page 186; to import a CA certificate, see "Importing a CA-Certificate" on page 190.

Adding a Self-Signed Certificate

Self-signed certificates are generally meant for intranet use, not extranet.

To Create a Self-Signed Certificate through the Management Console:

Note: A keyring must already exist.

1. Select Configuration>SSL>Keyrings>SSL Certificates.

The SSL Certificates tab displays.

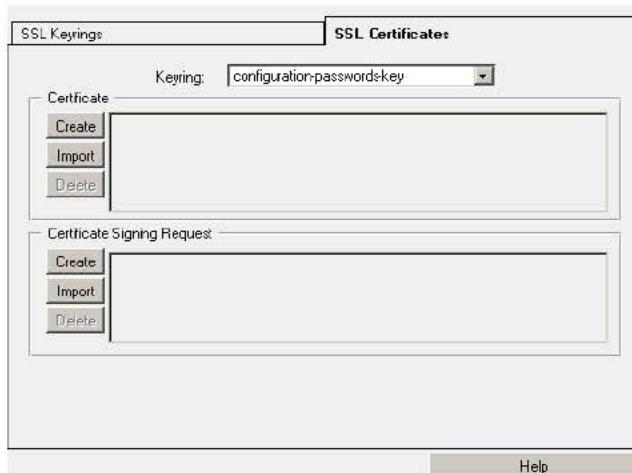


Figure 7-3: SSL Certificates Tab

2. Select the keyring for which you want to add a certificate in the keyring drop-down list.
3. Click Create in the Certificate tab.

The Create Certificate dialog displays.

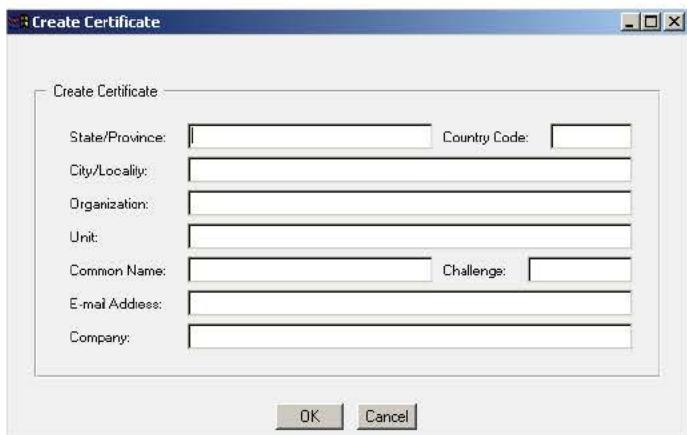


Figure 7-4: Create Certificate Dialog

4. Fill in the fields as appropriate:
 - State/Province—Enter the state or province where the machine is located.
 - Country Code—Enter the two-character ISO code of the country.
 - City/Locality—Enter the city.
 - Organization—Enter the name of the company.
 - Unit—Enter the name of the group that will be managing the machine.
 - Common Name—A common name should be the one that contains the URL with which the client access that particular origin server.
 - Challenge—Enter a 4-16 character alphanumeric challenge.
 - E-mail Address—The e-mail address you enter must be 40 characters or less. A longer e-mail address will generate an error.
 - Company—Enter the name of the company.
5. The Create tab displays the message: Creating.....

To Create a Self-Signed Certificate through the CLI:

Note: The associated keyring must already exist.

1. At the (config) command prompt, enter the following commands to create a self-signed certificate

```
SGOS#(config ssl) create certificate keyring_id
Country code []: US
State or province []: CA
Locality or city []: SV
Organization name []: Blue Coat
Organization unit []: Docs
```

```
Common name []: www.bluecoat.com
Email address []: test@bluecoat.com
Challenge []: test
Company name []: Blue Coat
ok
```

where:

Country code	At the Country code prompt, enter the two-character ISO code of the country.
State or province	Name of the state or province where the machine is located.
Locality or city	Name of the town where the machine is located.
Organization name	Name of the company.
Organization unit	Name of the group within the company.
Common name	Verify the Common name is the same as the domain name of the Web site being terminated. If the Common name and site domain name do not match, a client browser generates a warning whenever the ProxySG terminates an HTTPS request for that site. The use of wildcards is supported in the Common name.
Email address	The e-mail address you enter must be 40 characters or less. A longer e-mail address will generate an error
Challenge	At the Challenge prompt, enter a 4-16 character alphanumeric secret.
Company name	Name of the company.

2. View the certificate.

```
SGOS# (config ssl) view certificate keyring_id
-----BEGIN CERTIFICATE-----
MIIB3zCCAZmgAwIBAgIBADANBgkqhkiG9w0BAQQFADCBhzELMAkGA1UEBhMCVVMxCzAJBgNVBAgT
AkNBMQswCQYDVQQHEwJTVjESMBAGA1UEChMJQmx1ZSBDb2F0MQ0wCwYDVQQLEwREb2NzMRkwFwY
DVQQDExb3d3cuYmx1ZWNvYXQuY29tMSAwHgYJKoZIhvcNAQkBFhF0ZXN0QGJsdbWVjb2F0LmNvbT
AeFw0wMzAzMDQyMTA2NTThaFw0wMzA0MDMyMTA2NTThaMIGHMQswCQYDVQQGEwJVUzELMAkGA1UEC
BMCQ0ExCzAJBgNVBAcTA1NWMRIwEAYDVQQKEw1CbHV1IENvYXQxDTALBgNVBAAsTBERvY3MxGTAX
BgNVBAMTEHd3dy5ibHV1Y29hdC5jb20xIDAeBgkqhkiG9w0BCQEWEZR1c3RAYmx1ZWNvYXQuY29
tMEwwDQYJKoZIhvcNAQEBBQADowAwOAIxAK+AGYRMbnjyGr7U0oZUYds106y8uQnxq2PV6qCr4Q
BpN1Vqyr1Fi7ZEaw0lyMs5FwIDAQABMA0GCSqGSIb3DQEBAUAAzEAe8zoYW0igTcGRGG7sBpc
U95J907ZVm8qSU/PQfx1IrDzKdRSQPO9Gs1I8MqXi0D
-----END CERTIFICATE-----
```

About Certificate Chains

A certificate chain is one that requires that the certificates form a chain where the next certificate in the chain validates the previous certificate, going up the chain to the root, which is signed by a well-known root certificate provider. However, expiration is done at the single certificate level and is checked independently of the chain verification. Each certificate in the chain must not have expired for the entire chain to be valid. You can import a certificate chain containing multiple certificates in a single operation.

The valid certificate chain can be presented to a browser. To get the ProxySG to present a valid certificate chain, the keyring for the HTTPS service must be updated.

The ProxySG Appliance's CA-certificate list must also be updated if the ProxySG uses HTTPS to communicate with the origin server and if the ProxySG is configured, through the `ssl-verify-server` option, to verify the certificate (chain) presented by HTTPS server. If the ProxySG uses HTTP to communicate with the origin server, updating the CA-certificate list has no effect.

Importing an Existing Keyring and Certificate

If you have an unused certificate, or a keyring and certificate from another system, you can import it for use on a different system. You can import a certificate chain containing multiple certificates in a single operation. Use the `import certificate` command to import multiple certificates through the CLI.

If you are importing a keyring and one or more certificates onto a ProxySG, first import the keyring, followed by the related certificates. Note that the certificates contain the public key from the keyring, and the keyring and certificates are related.

To Import a Keyring through the Management Console:

1. Copy the already-created certificate onto the clipboard.
2. Select Configuration>SSL>Keyrings>SSL Keyrings.
3. Click Create.

The Create Keyring dialog appears.

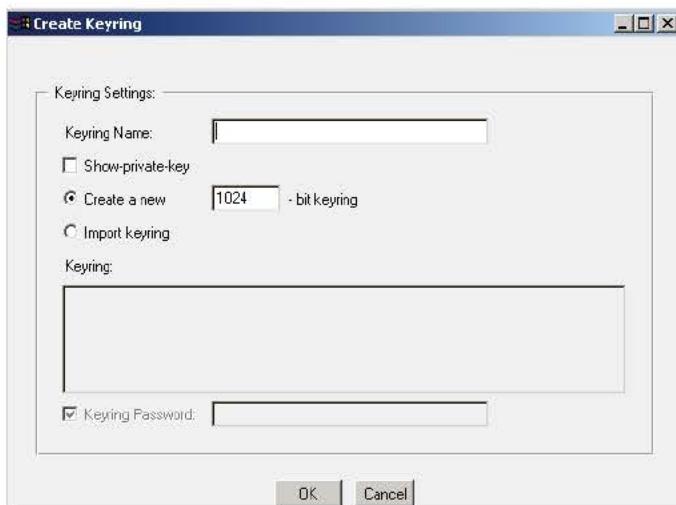


Figure 7-5: Import a Keyring

4. In the Keyring Name field, enter the name of the keyring you are importing.
5. Select Show private-key if you might want the keyring to be reused in the future.
6. Click the Import keyring radio button.
7. Paste the keyring into the Keyring field.
8. (Optional) Select Keyring Password and fill in the field, if needed.
9. Click OK; Click Apply.

To Import a Certificate and Associate it with a Keyring through the Management Console:

1. Copy the certificate onto the clipboard.
2. Select Configuration>SSL>Keyrings>SSL Certificates and select the keyring that you just imported from the Keyring drop-down list.
3. Click Import in the Certificate field.
4. Paste the certificate into the Import Certificate dialog that appears. Be sure to include the ----BEGIN CERTIFICATE---- and ----END CERTIFICATE---- statements.
5. Click OK.

To Import a Keyring through the CLI:

This procedure can only be performed if the keyring containing the keypair and certificate was created using the `show` parameter.

1. Copy the certificate to the clipboard.
2. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) ssl
SGOS#(config ssl) import keyring {show | no-show} keyring_id
Paste certificate here, end with "..." (three periods) on a new line
```

To Import a Certificate and Associate it with a Keyring through the CLI:

Note: The keyring you want to associate with the certificate must already be on this ProxySG. The key and certificate must be imported onto the ProxySG in PEM (base64 encoded text) format.

1. Copy the certificate or certificate chain to the clipboard. Be sure to include the ----BEGIN CERTIFICATE---- and ----END CERTIFICATE---- statements.
2. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) ssl
SGOS#(config ssl) import certificate keyring-id
Paste certificate here, end with "..." (three periods) on a new line
-----BEGIN CERTIFICATE-----
MIIB7TCCAaegAwIBAgIBADANBgkqhkiG9w0BAQQFADCBj jELMAkGA1UEBhMCVVMx
CzAJBgNVBAgTAkNBMRlIwEAYDVQQHEwlTdW5ueXZhbGUxEjAQBgNVBAoTCUJsdWUg
Q29hdDENMASGA1UECxMERG9jczEZMBcGA1UEAxMQd3d3LmJsdWVjb2F0LmNvbTEg
MB4GCSqGSIb3DQEJARYRdGVzdEBibHV1Y29hdC5jb20wHhcNMDMwMjA1MjM1OTM1
WhcNMDMwMzA3MjM1OTM1WjCBj jELMAkGA1UEBhMCVVMxCzAJBgNVBAgTAkNBMRlIw
EAYDVQQHEwlTdW5ueXZhbGUxEjAQBgNVBAoTCUJsdWUgQ29hdDENMASGA1UECxME
RG9jczEZMBcGA1UEAxMQd3d3LmJsdWVjb2F0LmNvbTEgMB4GCSqGSIb3DQEJARYR
dGVzdEBibHV1Y29hdC5jb20wTDANBgkqhkiG9w0BAQEFAAM7ADA4AjEAvs3U2zu2
WQ25ewgb/AyiGTHMAEgyC/vpQ2TN4+IOriIUGItjvtnytYbhi6nwmbKPAgMBAAEw
DQYJKoZIhvcNAQEEBQADMQBc1s6HS0XewGG390Vh4B7wwXloXWEz4SDoGuspP211
gu7UjWYUd+h/dZxbERv8gzQ=
-----END CERTIFICATE-----
...
ok
```

Deleting an Existing Keyring and Certificate

To Delete a Keyring and the Associated Certificate through the Management Console:

1. Select Configuration>SSL>Keyrings>SSL Keyrings.
2. Highlight the name of the keyring that you want to delete.
3. Click Delete.

The Confirm delete dialog appears.

4. Click OK in the Confirm delete dialog that appears.

To Delete a Keyring and the Associated Certificate through the CLI:

From the `(config)` prompt, enter the following commands:

```
SGOS# (config) ssl
SGOS# (config ssl) delete certificate keyring_id
```

Importing an External Certificate

You can import an X.509 certificate into ProxySG to use for encrypting the access log files (see "Customizing the Log: Configuring the Upload Client" on page 655).

To Import an External Certificate through the Management Console:

1. Copy the certificate onto the clipboard.
2. Select Configuration>SSL>External Certificates.

The External Certificates tab displays.

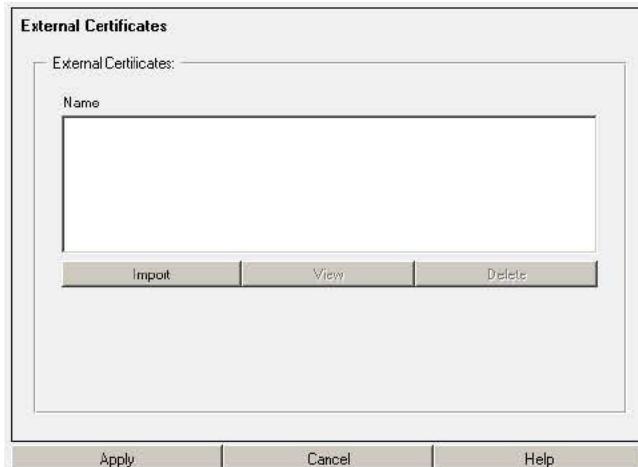


Figure 7-6: External Certificates Tab

3. Click Import.

The Import External Certificate dialog displays.



Figure 7-7: Import External Certificate Dialog

4. Enter the name of the external certificate into the External Cert Name field and paste the certificate into the External Certificate field. Be sure to include the **-----BEGIN CERTIFICATE-----** and **-----END CERTIFICATE-----** statements.
5. Click OK.
6. Click Apply.

To Import an External Certificate through the CLI:

1. From the (config) prompt, enter the following commands:

```
SGOS#(config) ssl
SGOS#(config ssl) import external-certificate name
  Paste certificate here, end with "..." (three periods) on a new line
-----BEGIN CERTIFICATE-----
MIICitCCAfKgAwIBAgIEN4dnrDANBgkqhkiG9w0BAQUFADB1MQswCQYDVQQGEwJi
ZTERMA8GA1UEChMIQmVsZ2Fjb20xDDAKBgNVBAsTA01UTTEkMCIGA1UEAxMbQmVs
Z2Fjb20gRS1UcnVzdCBQcmlyXJ5IENBMR8wHQYKCZImiZPyLGQBAAxQPaW5mb0B1
LXRydXN0LmJ1MB4XDTk4MTEwNDEzMDQzOVoXDTEwMDEyMTEzMDQzOVowdTELMAkG
A1UEBhMCYmUxETAPBgNVBAoTCEJ1bGdhY29tMQwwCgYDVQQLEwNNVE0xJDAiBgNV
BAMTG0J1bGdhY29tIEUTVHJ1c3QgUHJpbWFyeSBDQTEfMB0GCgmSJomT8ixkAQMU
D21uZm9AZS10cnVzdC5iZTCBnzANBgkqhkiG9w0BAQEFAAOBjQAwgYkCgYEaqtm5
s9VPak3FQdB7BGFqi3GBB9pk41huJ1XCrc4XsPz6ko0I8Bxy/7LDMf7gaoeXTMxD
V6coeTqlg12kHWrxasU+FCIdWQzv8KYxd9ywSTjmywwP/qpyNIjaKDohWu50Kxuk
21sTFrVzX8OujNLAPj2wy/Dsi4YLwsFEGFpjqNUCAwEAAaMmMCQwDwYDVR0TBAgw
BgEB/wIBATARBg1ghkgBvhvCAQEEBAMCAcwbDQYJKoZIhvNAQEFBQADgYEaerKx
pbF9M+nC4Rv0050MfwH9Gx1amq6rB1Ev7Ymr3VBCux//SrWknLFhKQpM6oNZSY2v
hmnxgaxHqqRxblnvynxqb1SK2qiSyfVms3lf1IsBniFjRjWTpcJfImIDcB1jI+hr
SB0jECFy9t9HorrsFBKbMRwpnrkdCJ/9oRiMn7=
-----END CERTIFICATE-----
...
ok
```

Deleting an External Certificate

To Delete an External Certificate through the Management Console:

1. Select Configuration>SSL>External Certificates.

The External Certificates tab displays.

2. Highlight the name of the external certificate that you want to delete.
3. Click Delete.

The Confirm delete dialog appears.

4. Click OK in the Confirm delete dialog that appears; click Apply.

To Delete an External Certificate through the CLI:

From the `(config)` prompt, enter the following commands:

```
SGOS# (config) ssl
SGOS# (config ssl) delete external-certificate name
```

Managing CA-Certificates

If you plan to use certificates issued by well-known Certificate Authorities, you can use the ProxySG to create certificate signing requests (CSRs). These can be sent to the Certificate Authority for signing.

Obtain the keypair and CSR to send to the CA in two ways:

- Use the Blue Coat Signing Request
- Obtain the keypair and CSR off-box

Once the signed request is returned to you from the CA, you can import the certificate into the ProxySG.

Note: If you have a CA certificate that is not on the ProxySG default CA certificate list, you might receive the following message when you attempt to connect to a Web site:

```
Network Error (ssl_failed)
A secure SSL session could not be established with the Web Site:
```

You must import the CA-Certificate before the ProxySG can trust the site.

To import a CA-Certificate, go to "Importing a CA-Certificate" on page 190; to create a CSR to be sent to a CA, continue with the next section.

Creating a CSR through the Management Console:

1. Select Configuration>SSL>SSL Keyrings>SSL Certificates.

The SSL Certificates tab displays.

2. Select, from the drop-down list, the keyring for which you need a signed certificate.
3. From the Certificate Signing Request tab, click the Create button.

The Create Certificate-signing-request dialog displays.

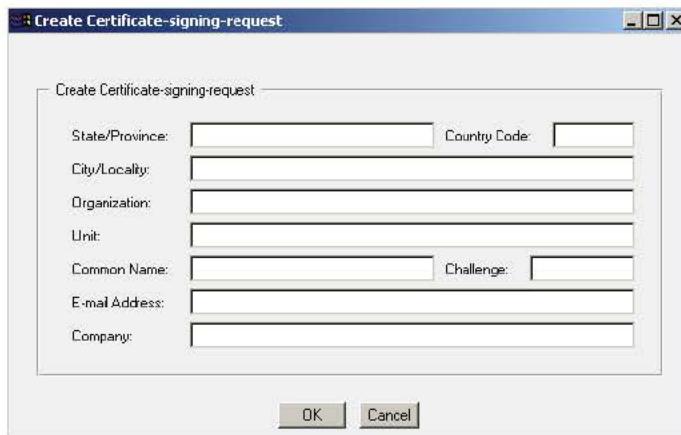


Figure 7-8: Create Certificate-Signing-Request Dialog

4. Fill in the fields as appropriate:
 - State/Province—Enter the state or province where the machine is located.
 - Country Code—Enter the two-character ISO code of the country.
 - City/Locality—Enter the city.
 - Organization—Enter the name of the company.
 - Unit—Enter the name of the group that will be managing the machine.
 - Common Name—Enter the URL of the company.
 - Challenge—Enter a 4-16 character alphanumeric challenge.
 - E-mail Address—The e-mail address you enter must be 40 characters or less. A longer e-mail address will generate an error.
 - Company—Enter the name of the company.
5. The Create tab displays the message: Creating....
6. Click OK.

Creating a CSR through the CLI:

Note: The keyring must already exist.

1. At the `(config)` command prompt, enter the following commands to create an SSL CSR:

```
SGOS#(config) ssl
SGOS#(config ssl) create signing-request keyring_id
Country code []: US
State or province []: CA
Locality or city []: SV
Organization name []: Blue Coat
Organization unit []: Docs
```

```
Common name []: www.bluecoat.com
Email address []: test@bluecoat.com
Challenge []: test
Company name []: Blue Coat
ok
```

where:

Country code	At the country code prompt, enter the two-character ISO code of the country.
State or province	Name of the state or province where the machine is located.
Locality or city	Name of the town where the machine is located.
Organization name	Name of the company.
Organization unit	Name of the group within the company.
Common name	Verify the Common name is the same as the domain name of the Web site being terminated. If the Common name and site domain name do not match, a client browser generates a warning whenever the ProxySG terminates an HTTPS request for that site. The use of wildcards is supported in the Common name.
Email address	The e-mail address you enter must be 40 characters or less. A longer e-mail address will generate an error
Challenge	At the challenge prompt, enter a 4-16 character alphanumeric secret.
Company name	Name of the company.

2. View the results.

```
SGOS# (config ssl) view signing-request keyring_id
-----BEGIN CERTIFICATE REQUEST-----
MIIBVDCCAQ4CAQAwgYcxCzAJBgNVBAYTA1VTMQswCQYDVQQIEwJDQTELMAkGA1UEBxMCU1YxEjAQ
BqNVBAoTCUJsdWUgQ29hdDENMAsGA1UECxMERG9jczEZMBCGA1UEAxMqd3d3LmJsdWVjb2F0LmN
vbTEgMB4GCSqGSIB3DQEJARYRdGVzdEBibHV1Y29hdC5jb20wTDANBgkqhkiG9w0BAQEFAAM7AD
A4AjEAobHjK0AsnKV0TcsntWCdfTaNyCgwNDXffxT5FwM0xkzQi0pCSku27CJXn7TahrKRAgMBA
AGgMTAUBgkqhkiG9w0BCQcxBxMFdGVzdAAwGQYJKoZIhvCNQkCMQwWCKJsdWUgQ29hdAAwDQYJ
KoZIhvCNQEEBQADMQBooZfEnzZT2WMMi3oT9EP3CdtddOTtdB1mWUXPdHJGfm1vEJ7HI0ce0W
71JP6pUY=
-----END CERTIFICATE REQUEST-----
```

Importing a CA-Certificate

A CA-Certificate is a certificate that verifies the identity of a Certificate Authority. The certificate is used by the ProxySG to verify server certificates and client certificates.

To Import an Approved CA-Certificate through the Management Console:

1. Copy the certificate to the clipboard.
2. Select Configuration>SSL>Keyrings>SSL Certificates.

The SSL Certificates tab displays.

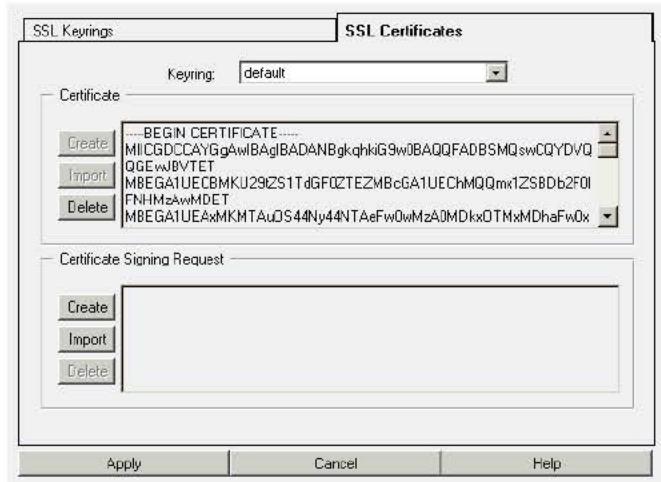


Figure 7-9: SSL Certificates

3. From the drop-down list, select the keyring for which you want to import a certificate. Note that the keyring must already exist.
4. Click Import in the Certificate panel.

The Import Certificate dialog displays.



Figure 7-10: Import Certificate Dialog

5. Paste the signed CA-Certificate into the Import Certificate field.
6. Click OK.
7. When the certificate displays in the Certificate tab, click Apply.

To View a CA-Certificate through the Management Console:

1. Select Configuration>SSL>CA Certificates>CA Certificates.

The CA Certificates tab displays.

2. Select the certificate you want to view.
3. Click View.

The certificate displays.



Figure 7-11: View CA Certificate

4. Examine the contents and click Close.

To Delete a CA-Certificate through the Management Console:

1. Select Configuration>SSL>CA Certificates>CA Certificates.
2. Select the certificate to delete.
3. Click Delete.
4. Click OK.
5. Click Apply.

To Import a CA-Certificate through the CLI:

1. Copy the certificate to the clipboard.
2. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) ssl
SGOS#(config ssl) import ca-certificate ca_cert_name
Paste certificate here, end with "..." (three periods) on a new line
```

3. (Optional) You can view the certificate you just imported, a summary of the just-imported certificate, or a summary of all CA-Certificates.
 - a. To view the certificate you just imported:

```
SGOS#(config ssl) view ca-certificate keyring_id
-----BEGIN CERTIFICATE-----
MIIEJzCCA5CgAwIBAgIEN35hxjANBgkqhkiG9w0BAQQFADCBgzELMAkGA1UEBhMC
VVMxLTArBgNVBAoTJEZpcnN0IERhdGEgRGlnaXRhbCBDZXJ0aWZpY2F0ZXmgSW5j
LjFFMEMGA1UEAxM8Rmlyc3QgRGF0YSBEawdpdGFsiENlcnRpZmljYXRLcyBJbmMu
IENlcnRpZmljYXRpb24gQXV0aG9yaXR5MB4XDTk5MDcwMzE4NDczNFoXDTE5MDcw
MzE5MTczNFowgYMXcAJBgNVBAYTA1VTMS0wKwYDVQQKEYRGaXJzdcBEYXRhIERp
Z2l0YWwgQ2VydGlmaWNhdGVzIEluYy4xRTBDBqNVBAMTPEZpcnN0IERhdGEgRGln
aXRhbCBDZXJ0aWZpY2F0ZXmgSW5jLiBDZXJ0aWZpY2F0aW9uIEF1dGhvcm10eTCB
nTANBgkqhkiG9w0BAQEFAAOBiAwgYcCgYEAs3xwUHgm5v6RAciCZebaEIvTXhZLF
BCToBy4C5BeVBTeVdj38seUPhw5iuSwlybhCxVnAKYV3uiNy5XsAlhSwEdlM0xW
nwofBMA3UIFXut/68mtn68vQgA/ZV5UQZXsGRVjrrrRe45MVK5m8tikv+0KfRysu
Tos0KDKZDu//b6ECAQOjggGmMIIBojARBglghkgBvhvCAQEEBAMCAcwgawGA1Ud
HwSBpDCBoTCBnqCBm6CBmKSBlTCBkjELMAkGA1UEBhMCVVMxLTArBgNVBAoTJEZp
```

```

cnN0IERhdGEgRGlnaXRhbCBDZXJ0aWzpY2F0ZXMgSW5jLjFFMEMGA1UEAxM8Rmly
c3QgRGF0YSBEaWdpdGFsIENlcnRpZmljYXR1cyBJbmMuIENlcnRpZmljYXRpb24g
QXV0aG9yaXR5MQ0wCwYDVQQDEwRDukwxMCsGA1UdEAQkMCKADzE5OTkwNzAzMTg0
NzM0WoEPmjAxOTA3MDMxODQ3MzRaMAsGA1UdDwQEAWIBBjAfBgNVHSMEGDAwgbSm
uCDJFkuPT1wMw8PumA0+fu5WVTAdBqNVHQ4EFgQUprgggRZLj09cDMPD7pgNPn7u
VlUwDAYDVR0TBAUwAwEB/zA7BgNVHSUENDayBgrBgfEFBQcDAQYIKwYBBQUHAWIG
CCsGAQUFbwMDBggrBgfEFBQcDBAYIKwYBBQUHawgwGQYJKoZIhvZ9B0EABAwwChsE
VjQuMAMCBJAwdQYJKoZIhvCNAQEEBQADgYEAEObEaCOpbLeXSbFzNp3+v3KiDhLC
K1EGH2mT1DARNYVOqHkG43FVPBxWYx5Ee2qBwjB1bN7z8gzDTsp/ycbAX1/vxAZi
qk/6EN4yzOAu/2rixcdFKXU5+YzC8ZrmQSYWsy6v7F4ApGqtoeAO1cUWzz8zAPK
hqGZqDpta2V+Ubg=
-----END CERTIFICATE-----

```

- b. To view a summary of the certificate you just imported.

```

SGOS#(config ssl) view summary ca-certificate ca_cert_name
CA Certificate ID: ca_cert_name
Is certificate valid? yes
CA: First Data Digital Certificates Inc.
Expiration Date: Jul 03 19:17:34 2019 GMT
Fingerprint: 70:B5:7C:48:81:95:3E:80:DC:28:9B:BA:EF:1E:E4:85

```

- c. To view summaries of all CA-Certificates on the ProxySG:

```
SGOS#(config ssl) view summary ca-certificate
```

A long list of certificates are displayed, each with the summary information displayed above.

To Delete a CA-Certificate through the CLI:

At the (config) command prompt, enter the following commands:

```

SGOS#(config) ssl
SGOS#(config ssl) delete ca-certificate ca_cert_name

```

Creating CA-Certificate Lists

You can select from among the CA-Certificates on the ProxySG, including those you added from a CA, by using CA-Certificate lists. These lists can include as many or as few CA-Certificates as you need. These lists can be used by the specific HTTPS service you enable for HTTPS termination.

The default is that no list is configured, so all certificates are used in authentication.

To Create a CA-Certificate List through the Management Console:

1. Select Configuration>SSL>CA Certificates>CA Certificate Lists.

The CA Certificate Lists tab displays.



Figure 7-12: SSL CA-Certificates Lists Dialog

The current CA-Certificate lists display in the pane.

2. Click New to create a new list.

The Create CA Certificate List dialog displays.

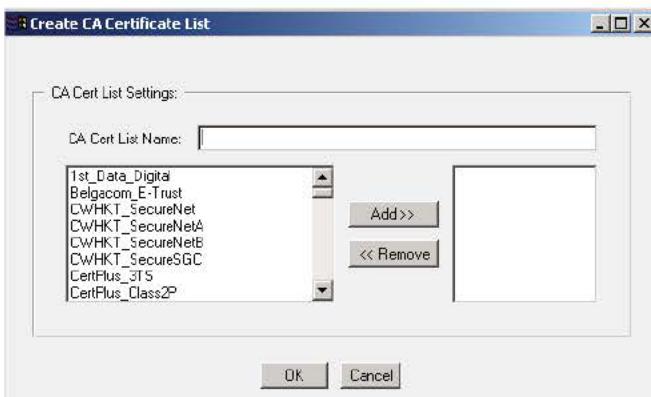


Figure 7-13: Create CA Certificate List Dialog

3. Enter a name meaningful to you for the list in the CA-Certificate List Name.
4. To add CA-Certificates to the list, highlight the certificate and click the Add button. You cannot add a certificate to a certificate list if it is not already present.
5. To remove CA-Certificates from the list, highlight the certificate in the Add list and click the Remove button.
6. Click OK when you finish; click Apply.

To Create CA-Certificate Lists through the CLI:

1. At the (config) command prompt, view the CA certificates already existing on the system. You cannot add a certificate to a certificate list if it is not already present.

```
SGOS# (config) ssl
SGOS# (config ssl) view summary ca-certificate
```

All the CA-Certificates on the system display.

2. Enter the followings commands to create a list and add existing certificates to it, using the list you just generated.

```
SGOS# (config ssl) create ccl list_name
SGOS# (config ssl) edit ccl list_name
```

The prompt changes, putting you in **ccl** submode.

```
SGOS# (config ssl ccl list_name) add ca_cert_name
```

3. Repeat the above command until you have entered all the needed certificates. You can have more than one CA-Certificate list. Each list can have an unlimited number of certificates.

4. (Optional) View the list.

```
SGOS# (config ssl ccl list_name) view
CA Certificate ID: VRSN_Secure_Server_CA
Is certificate valid? yes
CA: RSA Data Security, Inc.
Expiration Date: Jan 07 23:59:59 2010 GMT
Fingerprint: 74:7B:82:03:43:F0:00:9E:6B:B3:EC:47:BF:85:A5:93

CA Certificate ID: DeutscheTelekom
Is certificate valid? yes
CA: Deutsche Telekom AG
Expiration Date: Jul 09 23:59:00 2019 GMT
Fingerprint: 9B:34:0D:1A:31:5B:97:46:26:98:BC:A6:13:6A:71:96

CA Certificate ID: CWHKT_SecureNetA
Is certificate valid? yes
CA: C&W HKT SecureNet CA Class A
Expiration Date: Oct 15 23:59:00 2009
Fingerprint: E2:D5:20:23:EC:EE:B8:72:E1:2B:5D:29:6F:FA:43:DA
```

Troubleshooting Certificate Problems

If the client does not trust the Certificate Signing Authority that has signed the ProxySG Appliance's certificate, you will see an error message in the event log similar to the following:

```
2004-02-13 07:29:28-05:00EST "CFSSL:SSL_accept error:14094416:SSL
routines:SSL3_READ_BYTES:sslv3 alert certificate unknown" 0 310000:1
..../cf_ssl.cpp:1398
```

This commonly occurs when you use the HTTPS-Console service on port 8082, which uses a self-signed certificate by default. When you access the Management Console over HTTPS, the browser shows a pop-up that says that the security certificate is not trusted and asks if you want to proceed. If you select *No* instead of proceeding, the browser sends an *unknown CA alert* to the ProxySG.

You can eliminate the error message one of two ways:

- If this was caused by Blue Coat' self-signed certificate (the certificate associated with the default keyring), import the certificate as from a trusted Certificate Signing Authority in Internet Explorer.
- Import a certificate on the ProxySG that is signed by a well-known Certificate Signing Authority and use that for HTTPS Console access and HTTPS termination.

Managing the SSL Client

Although only one SSL client exists on a ProxySG, the SSL client:

- Determines which certificates can be presented to origin servers if the secure server requires the ProxySG to present a certificate.
- Identifies the protocol the ProxySG uses in negotiations with origin servers.
- Identifies the cipher suites to be used with the certificate.

You can change the protocol and the cipher suites used.

Creating an SSL Client

Only one SSL client can be created on a ProxySG. Creation of the SSL client means that for every HTTPS connection to the destination server, the ProxySG picks the parameters needed for negotiating the SSL connection from the SSL-client configuration. Thus, multiple SSL connections to different HTTPS destination servers can be supported with a single SSL-client configuration. This is similar to a browser where one configuration is used to negotiate multiple connections with different hosts.

If you just need to change the protocol, the cipher suites, or the keyring associated with the SSL client, you do not need to recreate the client. Continue with "Associating a Keyring and Protocol with the SSL Client" on page 197 or "Changing the Cipher Suites of the SSL Client" on page 199.

To Create the SSL Client through the CLI:

```
SGOS# (config ssl) create ssl-client default
defaulting protocol to SSLv2v3TLSv1
defaulting associated keyring-id to default
ok
```

To Delete the SSL Client through the CLI:

```
SGOS# (config ssl) delete ssl-client default
ok
```

Associating a Keyring and Protocol with the SSL Client

The SSL client already exists on the ProxySG. Keyrings that are not used to authenticate encrypted connections do not need to be associated with the SSL client.

Important: Only one keyring can be associated with the SSL client at a time.

To Associate a Keyring with the SSL Client and Change the Protocol Version through the Management Console:

1. Select Configuration>SSL>SSL Client.

The SSL Client tab displays.

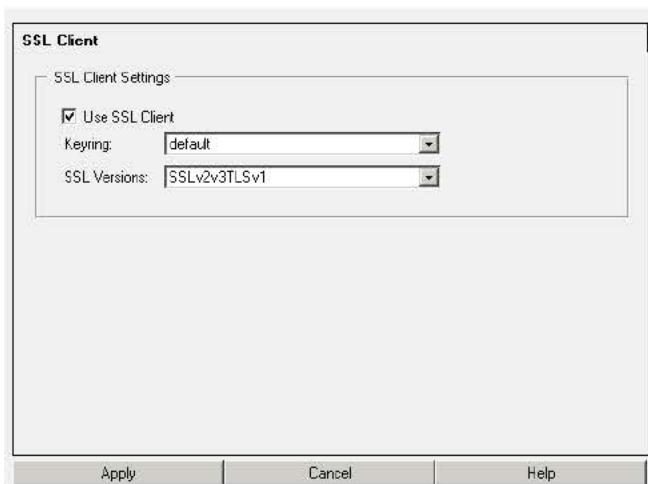


Figure 7-14: SSL Client

2. To use the SSL client, verify Use SSL Client is selected.
3. Only keyrings with certificates can be associated with the SSL client, displayed in the Keyring drop-down list. Select the keyring you want to use to negotiate with origin content servers through an encrypted connection.
4. You can change the SSL Versions default from SSLv2v3TLSv1 to any other protocol listed in the drop-down list.
5. Click Apply.

To Associate a Keyring and Protocol with the SSL Client and to Verify the Validity of Server Certificates through the CLI:

1. To associate a keyring with the SSL client, enter the following commands at the (config) command prompt:

```
SGOS#(config) ssl
SGOS#(config ssl) edit ssl-client default
SGOS#(config ssl ssl-client default) keyring-id keyring_id
SGOS#(config ssl ssl-client default) protocol {sslv2 | ssiv3 | tlsv1 | ssiv2v3 |
ssiv2tlsv1 | ssiv3tlsv1 | ssiv2v3tlsv1}
```

Note: To configure the ProxySG to accept only SSL version 3 traffic, for example, use the **ssiv3** parameter. To configure the ProxySG to accept SSL version 2 and version 3 traffic, use the **ssiv2v3** parameter.

2. View the results. The results also show the current value of the cipher suites, which is discussed in "Changing the Cipher Suites of the SSL Client" on page 199.

```
SGOS#(config ssl ssl-client default) view
```

SSL-Client Name	Keyring Name	Protocol
default	default	SSLv2v3TLSv1

Changing the Cipher Suites of the SSL Client

The cipher suite sets the encryption method used by the ProxySG. As the encryption key strength is determined by the signed certificate, configuring a higher cipher suite than defined by the certificate will have no affect. Conversely, the cipher suite configuration must be high enough to accommodate certification encryption values.

This can only be done through the CLI.

To Change the Cipher Suite of the SSL Client through the CLI:

1. Note that the Use Column in the set cipher-suite output below indicates that the default is to use all ciphers.

```
SGOS#(config ssl ssl-client default) ciphersuite
      SSL-Client          Name          Keyring Name      Protocol
-----  -----  -----
      default            default        SSLv2v3TLSv1

      Cipher#   Use    Description          Strength
-----  ---  -----
      1         yes    RC4-MD5           Medium
      2         no     RC4-SHA           Medium
      3         no     DES-CBC3-SHA       High
      4         no     DES-CBC3-MD5      High
      5         no     RC2-CBC-MD5      Medium
      6         no     RC4-64-MD5        Low
      7         no     DES-CBC-SHA       Low
      8         no     DES-CBC-MD5      Low
      9         no     EXP1024-RC4-MD5   Export
     10        no     EXP1024-RC4-SHA   Export
     11        no     EXP1024-RC2-CBC-MD5 Export
     12        no     EXP1024-DES-CBC-SHA Export
     13        no     EXP-RC4-MD5      Export
     14        no     EXP-RC2-CBC-MD5   Export
     15        no     EXP-DES-CBC-SHA  Export

Select cipher numbers to use, separated by commas: 1,3,4
      ok
```

2. (Optional) View the results. Note the change in the Use column.

```
SGOS#(config ssl ssl-client default) view
      SSL-Client          Name          Keyring Name      Protocol
-----  -----  -----
      default            default        SSLv2v3TLSv1

      Cipher#   Use    Description          Strength
-----  ---  -----
      1         yes    RC4-MD5           Medium
      2         no     RC4-SHA           Medium
      3         yes    DES-CBC3-SHA       High
      4         yes    DES-CBC3-MD5      High
      5         no     RC2-CBC-MD5      Medium
```

6	no	RC4-64-MD5	Low
7	no	DES-CBC-SHA	Low
8	no	DES-CBC-MD5	Low
9	no	EXP1024-RC4-MD5	Export
10	no	EXP1024-RC4-SHA	Export
11	no	EXP1024-RC2-CBC-MD5	Export
12	no	EXP1024-DES-CBC-SHA	Export
13	no	EXP-RC4-MD5	Export
14	no	EXP-RC2-CBC-MD5	Export
15	no	EXP-DES-CBC-SHA	Export

Troubleshooting Server Certificate Verification

Server certificate verification can be disabled for all upstream hosts or specific upstream hosts. The ProxySG, by default, verifies the SSL certificate presented by the upstream HTTPS server. However, it fails to negotiate the SSL connection if SSL certificate verification fails. The most common reason for server certificate verification failure is the absence of a suitable CA certificate on the ProxySG. Ensure that the SG is configured with the relevant CA certificates to avoid unwanted verification failures. The default behavior can be changed by using the `http ssl-verify-server` option.

If a forwarding host of type HTTPS server is being used, you can override the default behavior by changing the `ssl-verify-server` option on a per-host basis.

Enabling an HTTPS Service

The final step in creating HTTPS termination is to select a port and enable the HTTPS service on that port. For general information on enabling services, see Chapter 5: "Managing Port Services" on page 113. For more information on enabling the HTTPS Service, see "HTTPS" on page 127.

Configuring HTTP or HTTPS Origination to the Origin Content Server

In previous procedures, you configured HTTPS termination to the ProxySG. In two common termination scenarios, you must also configure HTTPS origination to the Origin Content Server (OCS).

The first two scenarios are used to provide a secure connection between the proxy and server, if, for example, the proxy is in a branch office and is not co-located with the server.

Table 7.2: Scenario 1: HTTPS Termination with HTTPS Origination

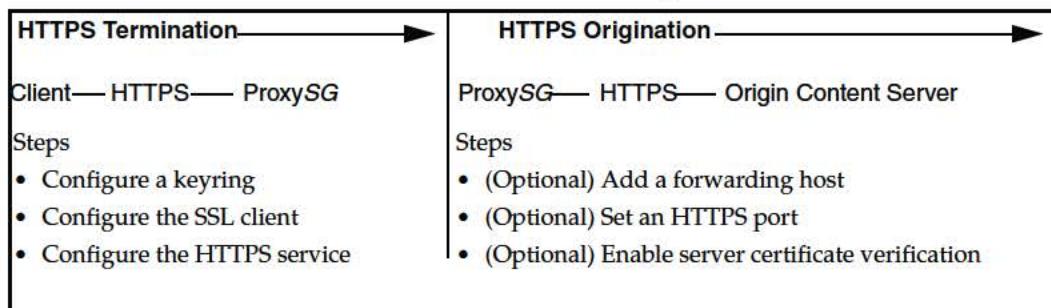


Table 7.3: Scenario 2: HTTP Termination with HTTPS Origination

HTTP Termination →	HTTPS Origination →
<p>Client—HTTP—ProxySG</p> <p>Steps:</p> <ul style="list-style-type: none"> • Client is explicitly proxied 	<p>ProxySG—HTTPS—Origin Content Server</p> <p>Steps</p> <ul style="list-style-type: none"> • Server URL rewrite -or- • Add a forwarding host (only for SGOS 3.1 or higher) • Set an HTTP port • Enable server certificate verification

You can only configure HTTPS origination through the CLI. You cannot use the Management Console.

To Configure HTTPS Origination:

At the (config) command prompt, enter the following commands:

```
SGOS#(config forwarding) create host_alias host_name https=port_number
ssl-verify-server=yes server
```

where:

<i>host_alias</i>	<i>ip_address</i>	Specifies the IP address of the OCS.
<i>host_name</i>	<i>url</i>	Specifies the URL of the OCS, such as www.bluecoat.com.
<i>https=</i>	[no] <i>port_number</i>	Specifies the port number on the OCS in which HTTPS is listening.
<i>ssl-verify-</i> <i>server=</i>	{yes no} <i>server</i>	Specifies whether the upstream server certificate should be verified. You can only use this command if the upstream host is a server, not a proxy, and you must specify <i>server</i> at the end of the command.

The next scenario is useful when the ProxySG is deployed as a reverse proxy. This scenario is used when it's not necessary for a secure connection between the proxy and server. For information on using the ProxySG as a reverse proxy, see "Controlling HTTP Proxy Traffic" on page 148.

Table 7.4: Scenario 3: HTTPS Termination with HTTP Origination

HTTPS Termination →	HTTP Origination →
<p>Client—HTTPS—ProxySG</p> <p>Steps</p> <ul style="list-style-type: none"> • Configure a keyring • Configure the SSL client • Configure the HTTPS service 	<p>ProxySG—HTTP—Origin Content Server</p> <p>Steps</p> <ul style="list-style-type: none"> • Server URL rewrite -or- • Add a forwarding host (only for SGOS 3.1 or higher) • Set an HTTP port

For information on rewriting the server URL, refer to the *Blue Coat Content Policy Language Guide*. For information on adding a forwarding host, see "Forwarding Configuration" on page 597.

Configuring DNS Resolution to the Origin Content Server

In different server accelerator scenarios, you might be required to use DNS resolution to the OCS instead of HTTPS origination.

As long as the DNS that the ProxySG points to correctly resolves the domain name that the client seeks to access, no addition configuration is required. Verify that the ProxySG has the certificate of the Certificate Authority that signs the certificate on the OCS.

Chapter 8: Security and Authentication

Enterprise-wide security begins with security on the ProxySG itself, and continues with controlling user access to the intranet and Internet.

Terms:

Access Control Lists (ACLs)	A list maintained by the ProxySG that restricts access to the ProxySG to certain IP addresses.
proxy	Caches content, filters traffic, monitors Internet and intranet resource usage, blocks specific Internet and intranet resources for individuals or groups, and enhances the quality of Internet or intranet user experiences. A proxy can also serve as an intermediary between a Web client and a Web server and can require authentication to allow identity based policy and logging for the client.
	The rules used to authenticate a client are based on the policies you create on the ProxySG, which can reference an existing security infrastructure—LDAP, RADIUS, NTLM, and the like, discussed in more detail in Chapter 9: “Using Authentication Services” on page 233.
explicit proxy	A configuration in which the browser is explicitly configured to communicate with the proxy server for access to content. This is the default for the ProxySG, and requires configuration for both browser and the interface card.
transparent proxy	A configuration in which traffic is redirected to the ProxySG without the knowledge of the client browser. No configuration is required on the browser, but network configuration, such as an L4 switch or a WCCP-compliant router, is required.
forward proxy	A proxy server deployed close to the clients and used to access many servers. A forward proxy can be explicit or transparent.
reverse proxy	A proxy that acts as a front-end to a small number of pre-defined servers, typically to improve performance. Many clients can use it to access the small number of predefined servers.
SSL	A standard protocol for secure communication over the network. Blue Coat recommends using this protocol to protect sensitive information.
authentication	The process of identifying a specific user.
authorization	The permissions given to a specific user.
realms	A realm is a named collection of information about users and groups. The name is referenced in policy to control authentication and authorization of users for access to Blue Coat Systems ProxySG services. Note that multiple authentication realms can be used on a single ProxySG. Realm services include NTLM, LDAP, Local, and RADIUS. For detailed information on realms, see Chapter 9: “Using Authentication Services” on page 233.

serial console	A device that allows you to connect directly to the serial port for the ProxySG when it is otherwise unreachable, without using the network. It can be used to administer the ProxySG through the CLI. You must use the CLI to use the serial console.
setup console	This allows you to create initial network and configuration settings, including password creation, and helps you recover from Management Console problems. The setup console can only be reached through the serial port.
serial port	The serial port provides a direct connection to the ProxySG. Through the serial port, you can go to either the serial console and use the CLI just as if you were using the CLI through SSH, or you can go to the setup console. If you put a password on the serial port, you can only access the setup console after successfully responding to the password challenge.

SSH and HTTPS are the recommended (and default) methods for managing access to the ProxySG. SSL is the recommended protocol for communication between the ProxySG and a realm's off-box authentication server.

This chapter contains the following sections:

- "Controlling Access to the ProxySG"
- "Controlling Access to the Internet and Intranet"

Section A: Controlling Access to the ProxySG

Section A: Controlling Access to the ProxySG

The ProxySG has a single console account and privileged password that are created during initial configuration. The ProxySG allows you to restrict use of these credentials and to allow additional administrator access through policy.

This section contains

- "Limiting Access to the ProxySG Appliance"
- "About Password Security"
- "Limiting User Access to the ProxySG—Overview"
- "Moderate Security: Restricting Management Console Access Through the Console Access Control List"
- "Maximum Security: Administrative Authentication and Authorization Policy"

The ProxySG permits you to define a rule-based administrative access policy for SSH with password authentication, for the Management Console, and for the serial console. These policy rules can be specified either by using the Visual Policy Manager or by editing the Local Policy file. Using policy rules, you can deny access, allow access without providing credentials, or require administrators to identify themselves by entering a username and password.

If access is allowed, you can specify whether read-only or read-write access is given. You can make this policy contingent on IP address, time of day, group membership (if credentials were required), and many other conditions.

Limiting Access to the ProxySG Appliance

You can limit access to the ProxySG Appliance by:

- Restricting physical access to the system and by requiring a PIN to access the front panel.
- Restricting the IP addresses that are permitted to connect to the ProxySG CLI.
- Requiring a password to secure the serial console port.

These methods are in addition to the restrictions placed on the console account (a console account user password and user enable password). For information on using the console account, see "Changing the Username and Password through the Management Console" on page 43.

By using every possible method (physically limiting access, limiting workstation IP addresses, and using passwords), the ProxySG is very secure.

This section discusses:

- "Requiring a PIN for the Front Panel"
- "Limiting Workstation Access"
- "Securing the Serial Port"

Section A: Controlling Access to the ProxySG

Requiring a PIN for the Front Panel

On systems that have a front panel display, you can create a four-digit PIN to protect the system from unauthorized use. The PIN is hashed and stored. You can only create a PIN from the command line.

To create a front panel PIN, after initial configuration is complete:

From the (config) prompt:

```
SGOS# (config) security front-panel-pin PIN
```

where *PIN* is a four-digit number.

To clear the front-panel PIN, enter

```
SGOS# (config) security front-panel-pin 0000
```

Limits Workstation Access

During initial configuration, you have the option of preventing workstations with unauthorized IP addresses from accessing the CLI. If this option is not enabled, all workstations are allowed to access the CLI. You can also add allowed workstations later to the access control list (ACL). (For more information on limiting workstation access, see "Moderate Security: Restricting Management Console Access Through the Console Access Control List" on page 210.)

Securing the Serial Port

During initial configuration, using either the setup console or the front panel, you can restrict access to functions accessed through the serial port. You can set a password to limit access to the setup console, and require administrator login before accessing the serial console CLI.

Once the secure serial port is enabled, the ProxySG is much more secure:

- A setup console password is now required to access the setup console. If the setup console password is forgotten, the setup console is inaccessible and can no longer be used to manage network settings or recover from Management Console problems.
- A username and password is now required to use the CLI through the serial console. If the setup console password is forgotten, you can still use the serial console to connect to the ProxySG CLI.

Important: Because there is no workaround for a forgotten setup console password, Blue Coat recommends that the password be preserved on non-volatile media in a physically secure location away from the ProxySG.

To enable the secure serial port, refer to the *Quick Start Guide* for your platform.

About Password Security

In the ProxySG, console administrator passwords, the setup console password, and privileged-mode (enable) passwords are hashed and stored. It is not possible to reverse the hash to recover the plaintext passwords.

Section A: Controlling Access to the ProxySG

In addition, the `show config` and `show security` CLI commands display these passwords in their hashed form. The length of the hashed password depends on the hash algorithm used so it is not a fixed length across the board.

Passwords that the ProxySG uses to authenticate itself to outside services are encrypted using triple-DES on the appliance, and using RSA public key encryption for output with the `show config` CLI command. You can use a third-party encryption application to create encrypted passwords and copy them into the ProxySG using an encrypted-password command (which is available in several modes and described in those modes). If you use a third-party encryption application, be sure it supports RSA encryption, OAEP padding, and Base64 encoded with no new lines.

These passwords, set up during configuration of the external service, include:

- Access log FTP client passwords (primary, alternate)—For configuration information, see "Editing the FTP Client" on page 659
- Archive configuration FTP password—For configuration information, see "Archive Configuration" on page 59
- RADIUS primary and alternate secret—For configuration information, see "Defining RADIUS Realm Properties" on page 259
- LDAP search password—For configuration information, see "LDAP Search & Groups Tab (Authorization and Group Information)" on page 251
- SmartFilter download password—For configuration information, see "Configuring SmartFilter" on page 571
- SurfControl download password—For configuration information, see "Configuring SurfControl" on page 579
- Local Database password—For configuration information, see "Configuring a Local Database" on page 549 (Note that the local database often does not have a password)

Limiting User Access to the ProxySG—Overview

When deciding how to give other users read-only or read-write access to the ProxySG, sharing the basic console account settings is only one option. The following summarizes all available options:

Note: If Telnet Console access is configured, Telnet can be used to manage the ProxySG with behavior similar to SSH with password authentication.

SSL configuration is not allowed through Telnet, but is permissible through SSH.

Behavior in the following sections that applies to SSH with password authentication applies to Telnet as well. Use of Telnet is not recommended because it is not a secure protocol.

- Console account—minimum security

Section A: Controlling Access to the ProxySG

The console account username and password are evaluated when the ProxySG is accessed from the Management Console through a browser and from the CLI through SSH with password authentication. The privileged-mode password is evaluated when the console account is used through SSH with password authentication and when the CLI is accessed through the serial console and through SSH with RSA authentication. The simplest way to give access to others is sharing this basic console account information, but it is the least secure and is not recommended.

To give read-only access to the CLI, do not give out the privileged-mode password.

- Console access control list—moderate security

Using the access control list (ACL) allows you to further restrict use of the console account and SSH with RSA authentication to workstations identified by their IP address and subnet mask. When the ACL is enforced, the console account can only be used by workstations defined in the console ACL. Also, SSH with RSA authentication connections are only valid from workstations specified in the console ACL (provided it is enabled).

After setting the console account username, password, and privileged-mode password, use the CLI or the Management Console to create a console ACL. See "Moderate Security: Restricting Management Console Access Through the Console Access Control List" on page 210.

- Per-user RSA public key authentication—moderate security

Each administrator's public keys are stored on the appliance. When connecting through SSH, the administrator logs in with no password exchange. Authentication occurs by verifying knowledge of the corresponding private key. This is secure because the passwords never go over the network.

This is a less flexible option than CPL because you can't control level of access with policy, but it is a better choice than sharing the console credentials.

- Blue Coat Content Policy Language (CPL)—maximum security

CPL enables you to create an through the policy to control administrative access to the ProxySG. If the credentials supplied are not the console account username and password, policy is evaluated when the ProxySG is accessed through SSH with password authentication or the Management Console. Policy is never evaluated on direct serial console connections or SSH connections using RSA authentication.

- Using the CLI or the Management Console GUI, create an authentication realm to be used for authorizing administrative access. For administrative access, the realm must support BASIC credentials—for example, LDAP, RADIUS, Local, or NTLM with BASIC credentials enabled. For more information on realms, see Chapter 9: "Using Authentication Services" on page 233.
- Using the Visual Policy Manager, or by adding CPL rules to the Local or Central policy file, specify policy rules that: (1) require administrators to log in using credentials from the previously-created administrative realm, and (2) specify the conditions under which administrators are either denied all access, given read-only access, or given read-write access. Authorization can be based on IP address, group membership, time of day, and many other conditions. For more information, see "Defining Policies Using the Visual Policy Manager" on page 212.

Section A: Controlling Access to the ProxySG

- To prevent anyone from using the console credentials to manage the ProxySG, set the console ACL to deny all access (unless you plan to use SSH with RSA authentication). For more information, see "Moderate Security: Restricting Management Console Access Through the Console Access Control List" on page 210. You can also restrict access to a single IP address that can be used as the emergency recovery workstation.

The following chart details the various ways administrators can access the ProxySG console and the authentication and authorization methods that apply to each.

Table 8.1: ProxySG Console Access Methods/Available Security Measures

Security Measures Available	Setup Console	Serial Console	SSH with Password Authentication	SSH with RSA Authentication	Management Console
Front Panel PIN ¹					
Serial Port Password	✓				
Username and Password Evaluated (Console-Level Credentials)		✓	✓		✓
Console Access Control List Evaluated			✓ (if console credentials are offered)	✓	✓ (if console credentials are offered)
CPL <Admin> Layer Evaluated			✓ ²		✓ ³
Enable Password required to enter privileged mode (see Note 2 below)		✓	✓	✓	
CLI line-vty timeout command applies		✓	✓	✓	
Management Console Login/Logout					✓

¹The Front Panel PIN protects the ProxySG front panel from unauthorized access. For more information on limiting access to the front panel, see "Requiring a PIN for the Front Panel" on page 206.

²When using SSH (with a password) and credentials other than the console account, the enable password is actually the same as the login password. The privileged mode password set during configuration is used only in the serial console, SSH with RSA authentication, or when logging in with the console account.

³In this case, user credentials are evaluated against the policy before executing each CLI command. If you log in using the console account, user credentials are not evaluated against the policy.

Section A: Controlling Access to the ProxySG

Moderate Security: Restricting Management Console Access Through the Console Access Control List

The ProxySG allows you to limit access to the Management Console and CLI through the console ACL. An ACL, once set up, is enforced only when console credentials are used to access either the CLI or the Management Console, or when an SSH with RSA authentication connection is attempted. The following procedure specifies an ACL that lists the IP addresses permitted access.

To Create an ACL through the Management Console:

1. Select Configuration>Authentication>Console Access>Console Access.

The Console Access tab displays.

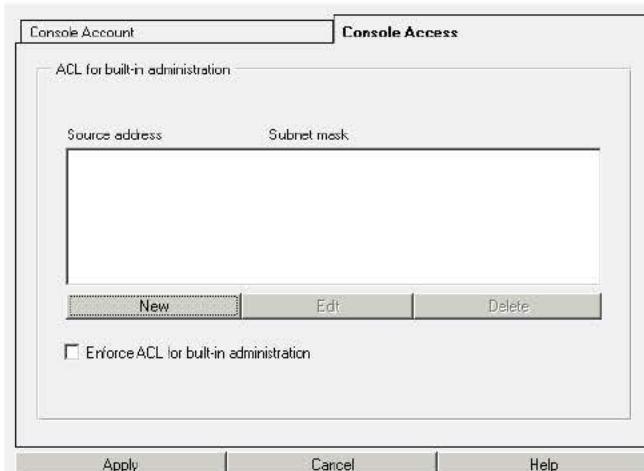


Figure 8-1: Console Access Tab

2. (Optional) To add a new address to the ACL, click New.

The Add List Item dialog is displayed.



Figure 8-2: Add List Item Dialog

- a. In the IP/Subnet fields, enter a static IP address.
- b. In the Mask fields, enter the subnet mask. To restrict access to an individual workstation, enter 255.255.255.255.

Section A: Controlling Access to the ProxySG

- c. Click OK to add the workstation to the ACL and return to the Console Access page.
- d. Repeat step 2 to add other IP addresses.
3. (Optional) To remove a source address from the ACL, select the address to remove from the Console Access page and click Delete.
4. (Optional) To change a source IP address, select the IP address to revise and click Edit. See step 2, above, for details.
5. To impose the ACL defined in the list box, select Enforce ACL for built-in administration. To allow access to the CLI or Management Console using console account credentials from any workstation, deselect the checkbox. The ACL is ignored.

Important: Before you enforce the ACL, make sure the IP address for the workstation you are using is included in the list. If you forget, or you find that you mistyped the IP address, you must correct the problem using the serial console.

6. Click Apply.

To Create an ACL through the CLI:

1. At the `(config)` command prompt, enter the following command to add workstation IP addresses to the ACL:

```
SGOS# (config) security allowed-access add ip_address [subnet_mask]
```

Note: If you omit the subnet mask, the default subnet mask of 255.255.255.255 is assumed.

2. Repeat step 1 for each workstation that you need to add to the console access list.
3. At the `(config)` command prompt, enter the following command to enforce the ACL created in step 1

```
SGOS# (config) security enforce-acl enable
```

Only those workstation IP addresses added to the ACL will be able to use the Management console account to administer the ProxySG. Make sure the IP address for the workstation you are using is included in the list.

4. To disable the ACL and open through the access to the console account user, enter the following command:

```
security enforce-acl disable
```

5. To remove an IP address and subnet mask from the ACL, enter the following command:

```
SGOS# (config) security allowed-access remove ip_address [subnet_mask]
```

Note: If you omit the subnet mask, the default subnet mask of 255.255.255.255 is assumed.

Section A: Controlling Access to the ProxySG

Maximum Security: Administrative Authentication and Authorization Policy

The ProxySG permits you to define a rule-based administrative access policy for SSH with password authentication and the Management Console. These policy rules can be specified either by using the VPM or by editing the Local policy file. Using policy rules, you can deny access, allow access without providing credentials, or require administrators to identify themselves by entering a username and password. If access is allowed, you can specify whether read-only or read-write access is given. You can make this policy contingent on IP address, time of day, group membership (if credentials were required), and many other conditions.

Setup-console access is not controlled by policy rules. For maximum security to the setup console, you can create a password to secure the serial port that connects to the ProxySG.

SSH with RSA authentication also is not controlled by policy rules. You can configure several settings that control access: the enable password, the console ACL, and per-user keys configured through the Configuration>Services>SSH>SSH Client page. (If you use the CLI, SSH commands are under config>services>ssh-console.)

Defining Administrator Authentication and Authorization Policies

The ProxySG uses CPL to define policies, including administrator, authentication, and authorization policies. CPL also allows you to give administrator privileges to users in any external authentication service.

The following summarizes the steps required to define Administrator Authentication and Authorization policies on the ProxySG:

- (Optional) If you need to give administrative access to existing users or groups, create and configure the authentication realm.
- Define the policies in the appropriate policy file where you keep the <Admin> Layer layers and rules.
- Load the policy file on the ProxySG.

When you define such policies, make sure you define them in the appropriate policy file(s). For more information on policy files and how they are used, see Chapter 12: “Managing Policy Files” on page 363.

Defining Policies Using the Visual Policy Manager

To define policies through the Management Console, use the Visual Policy Manager. When you use the VPM, policies are configured in CPL and saved in the VPM policy file. For examples of Administrator authentication or authorization policy CPL, continue with the next section. The VPM is described in detail in Chapter 13: “The Visual Policy Manager” on page 377.

Defining Policies Directly in Policy Files

To define policies manually, type CPL *rules* directly in one of the two policy files, Central or Local.

Section A: Controlling Access to the ProxySG

Important: Do not manually enter CPL rules directly into the VPM file. The file becomes corrupted.

For specific information on creating policies within the policy files, refer to the *Blue Coat Content Policy Language Guide*.

Following are the CPL elements that can be used to define administrator policies for the ProxySG.

To Define Administrator Policies by Editing a Policy File:

1. Open the policy file in a text editor.
2. Define the policies, using the correct CPL syntax.
3. Save the file.
4. Load the policy file (see "Creating and Editing Policy Files" on page 366).

Admin Transactions and <Admin> Layers

Admin transactions execute <Admin> layers. Only a restricted set of conditions, properties, and actions are permitted in <Admin> layers. Table 8.2 lists the conditions permitted in the <Admin> layer

Table 8.2: <Admin> Layer Conditions

<Admin> Network Connection Conditions	
client_address=ip_address [.subnetmask]	Tests for a match between <i>ip_address</i> and the IP address of the client transaction source.
proxy_port=number	Tests for a match between <i>number</i> and the port number for which the request is destined.
proxy_address=ip_address	Tests for a match between <i>ip_address</i> and the IP address of the network interface card for which the request is destined.
proxy_card=number	Tests for a match between <i>number</i> and the ordinal number associated with the network interface card for which the request is destined.
<Admin> General Conditions	
condition=condition.label	Tests if the specified defined condition is true.
release_id=	Tests the ProxySG release id.
<Admin> Date/Time Conditions	
date[.utc]=[date date...date]	Tests for a match between <i>date</i> and the date timestamp associated with the source of the transaction. <i>date</i> specifies a single date of the form YYYY-MM-DD or an inclusive range, as in YYYY-MM-DD...YYYY-MM-DD. By default, date is calculated based on local time. To calculate year based on the Coordinated Universal Time, include the .utc qualifier

Section A: Controlling Access to the ProxySG

Table 8.2: <Admin> Layer Conditions (Continued)

year[.utc]=[year year...year]	Tests for a match between <i>year</i> and the year timestamp associated with the source of the transaction. <i>year</i> specifies a single Gregorian calendar year of the form YYYY or an inclusive range of years, as in YYYY...YYYY. By default, year is calculated based on local time. To calculate year based on the Coordinated Universal Time, include the .utc qualifier.
month[.utc]=[month month...month]	Tests for a match between <i>month</i> and the month timestamp associated with the source of the transaction. <i>month</i> specifies a single Gregorian calendar month of the form MM or an inclusive range of months, as in MM..MM. By default, month is calculated based on local time. To calculate month based on the Coordinated Universal Time, include the .utc qualifier.
weekday[.utc]=[number number...number]	Tests for a match between <i>weekday</i> and the weekday timestamp associated with the source of the transaction. <i>weekday</i> specifies a single day of the week (where Monday=1, Tuesday=2, and Sunday=7) or an inclusive range of weekdays, as in number...number. By default, weekday is calculated based on local time. To calculate weekday based on the Coordinated Universal Time, include the .utc qualifier.
day[.utc]=[day day...day]	Tests for a match between <i>day</i> and the day timestamp associated with the source of the transaction. <i>day</i> specifies a single Gregorian calendar day of the month of the form DD or an inclusive range of days, as in DD..DD. By default, day is calculated based on local time. To calculate day based on the Coordinated Universal Time, include the .utc qualifier.
hour[.utc]=[hour hour...hour]	Tests for a match between <i>hour</i> and the hour timestamp associated with the source of the transaction. <i>hour</i> specifies a single Gregorian hour of the form HH (00, 01, and so forth, through 23) or an inclusive range of hours, as in HH..HH. By default, hour is calculated based on local time. To calculate hour based on the Coordinated Universal Time, include the .utc qualifier.
minute[.utc]=[minute minute...minute]	Tests for a match between <i>minute</i> and the minute timestamp associated with the source of the transaction. <i>minute</i> specifies a single Gregorian minute of the form MM (00, 01, and so forth, through 59) or an inclusive range of minutes, as in MM..MM. By default, minute is calculated based on local time. To calculate minute based on the Coordinated Universal Time, include the .utc qualifier.
time[.utc]=[time time...time]	Tests for a match between <i>time</i> and the time timestamp associated with the source of the transaction. <i>time</i> specifies military time of the form TTTT (0000 through 2359) or an inclusive range of times, as in TTTT..TTTT. By default, time is calculated based on local time. To calculate time based on the Coordinated Universal Time, include the .utc qualifier.

<Admin> Authorization Conditions

Section A: Controlling Access to the ProxySG

Table 8.2: <Admin> Layer Conditions (Continued)

attribute.name =value	Tests if the current transaction is authorized in a RADIUS or LDAP realm, and if the authenticated user has the specified attribute with the specified value. This trigger is unavailable if the current transaction is not authenticated.
authenticated={yes no}	Tests if authentication was requested and the credentials could be verified.
group=group_name	If authenticate=yes, the group condition tests the source of the transaction for membership in the specified groupname.
has_attribute.name=boolean	Tests if the current transaction is authorized in an LDAP realm and if the authenticated user has the specified LDAP attribute.
realm=realm_name	If authenticate=yes, the realm condition tests the source of the transaction for membership in the specified realm name.
user=username	If authenticate=yes, the user condition tests the source of the transaction for the expected username.
user_domain=windows_domain_name	(This condition is NTLM-realm specific.) If authenticate=yes, the user_domain condition tests whether the realm type is NTLM and whether the domain component of the username is the expected domain name.

<Admin> Read-only or Read-write Conditions

admin_access=read write	read tests whether the source of the transaction has read-only permission for the ProxySG console. write tests whether the source has read-write permission. When an Administrator logs into the CLI, the ProxySG executes an <Admin> transaction that includes the condition admin_access=read. If the transaction is ultimately allowed (all conditions have been met), the user will have read-only access to configuration information through the CLI. Further, when that user executes the CLI enable command, or logs into the Management Console, the ProxySG executes an <Admin> transaction with admin_access=write. If the transaction is allowed, the user will have read-write access within the CLI or the Management Console.
---------------------------	---

Table 8.3 lists the properties permitted in the <Admin> layer:

Table 8.3: <Admin> Layer Properties

<Admin> Properties

deny service(no)	Refuse service to the source of the transaction.
authenticate(realm_name)	Requests authentication of the transaction source for the specified realm.

Section A: Controlling Access to the ProxySG

Table 8.3: <Admin> Layer Properties (Continued)

authenticate.force()	If 'yes' is specified then forces authentication even if the transaction will be denied. This results in the user information being available for logging. If no, then early denial without authentication will be possible.
allow service(yes)	Permit further service to the source of the transaction.
log.suppress.field-id()	Controls suppression of the specified field-id in all facilities
log.suppress.field-id[log_list]()	Controls suppression of the specified field-id in the specified facilities.
log.rewrite.field-id()	Controls rewrites of a specific log field in all facilities.
log.rewrite.field-id[log_list]()	Controls rewrites of a specific log field in a specified list of log facilities.

Table 8.4 lists the actions permitted in the <Admin> layer:

Table 8.4: <Admin> Layer Actions

<Admin> Actions	
notify_email()	Sends an email notification to the list of recipients specified in the Event Log mail configuration when the transaction terminates.
notify_snmp()	The SNMP trap is sent when the transaction terminates.

Example Policy Using CPL Syntax

To authenticate users against an LDAP realm, use the following syntax in the Local Policy file:

```
<admin>
  authenticate(LDAP_Realm)

<admin>
  group="cn=Administrators,cn=Groups,dc=bluecoat,dc=com" allow
```

This authenticates users against the specified LDAP realm. If the users are successfully authenticated and belong to group *Administrators*, they are allowed to administer the ProxySG.

Section B: Controlling Access to the Internet and Intranet

Section B: Controlling Access to the Internet and Intranet

Once the ProxySG is secure, you can limit access to the Internet and intranet. It is possible to control access to the network without using authentication. You only need to use authentication if you want to use identity-based access controls.

This section contains:

- "Using Authentication and Proxies"
- "Using SSL with Authentication and Authorization Services"
- "Creating a Proxy Layer to Manage Proxy Operations"

Using Authentication and Proxies

Authentication means that the ProxySG requires proof of user identity in order to make decisions based on that identity. This proof is obtained by sending the client (a browser, for example) a *challenge*—a request to provide credentials. Browsers can respond to different kinds of credential challenges:

- Proxy-style challenges—Sent from proxy servers to clients that are explicitly proxied. In HTTP, the response code is 407.

An authenticating explicit proxy server sends a proxy-style challenge (407/Proxy-Authenticate) to the browser. The browser knows it is talking to a proxy and that the proxy wants proxy credentials. The browser responds to a proxy challenge with proxy credentials (Proxy-Authorization: header). The browser must be configured for explicit proxy in order for it to respond to a proxy challenge.
- Origin-style challenges—Sent from origin content servers (OCS), or from proxy servers impersonating a OCS. In HTTP, the response code is 401 Unauthorized.

In transparent proxy mode, the ProxySG uses the OCS authentication challenge (HTTP 401 and WWW-Authenticate)—acting as though it is the location from which the user initially requested a page. A transparent proxy, including a reverse proxy, must not use a proxy challenge, because the client may not be expecting it.

Once the browser supplies the credentials, the ProxySG authenticates them.

Authentication Modes

You can control the way the ProxySG interacts with the client for authentication by controlling the authentication mode. The mode specifies the challenge type and the accepted surrogate credential.

Important: Credential caching is applicable only for authentication modes involving surrogates.

Section B: Controlling Access to the Internet and Intranet

Note: *Challenge type* is the kind of challenge (for example, proxy or origin-ip-redirect) issued.

Surrogate credentials are credentials accepted in place of the user's real credentials. The purpose of surrogate credentials is to allow flexibility in limiting the frequency of authentication challenges but to ensure security in that the surrogate is associated with the same user used to create that surrogate.

- Auto: The default; the mode is automatically selected, based on the request. Chooses among proxy, origin-IP, and origin-IP-redirect, depending on the kind of connection (explicit or transparent) and the transparent authentication cookie configuration. For streaming transactions, `authenticate.mode(auto)` uses origin mode.
- Proxy: The ProxySG uses an explicit proxy challenge. No surrogate credentials are used. This is the typical mode for an authenticating explicit proxy. In some situations proxy challenges will not work; origin challenges are then issued.
- Proxy-IP: The ProxySG uses an explicit proxy challenge and the client's IP address as a surrogate credential. Proxy-IP specifies an insecure forward proxy, possibly suitable for LANs of single-user workstations. In some situations proxy challenges will not work; origin challenges are then issued.
- Origin: The ProxySG acts like an OCS and issues OCS challenges. The authenticated connection serves as the surrogate credential.
- Origin-IP: The ProxySG acts like an OCS and issues OCS challenges. The client IP address is used as a surrogate credential. Origin-IP is used to support NTLM authentication to the upstream device when the client cannot handle cookie credentials. This mode is primarily used for automatic downgrading, but it can be selected for specific situations.
- Origin-cookie: The ProxySG acts like an origin server and issues origin server challenges. A cookie is used as the surrogate credential. Origin-cookie is used in forward proxies to support pass-through authentication more securely than `origin-ip` if the client understands cookies. Only the HTTP and HTTPS protocols support cookies; other protocols are automatically downgraded to `origin-ip`.

This mode could also be used in reverse proxy situations if impersonation is not possible and the origin server requires authentication.

- Origin-cookie-redirect: The client is redirected to a virtual URL to be authenticated, and cookies are used as the surrogate credential. Note that the ProxySG does not support origin-redirects with the CONNECT method.
-

Note: During cookie-based authentication, the redirect to strip the authentication cookie from the URL is logged as a 307 (or 302) TCP_DENIED.

- Origin-IP-redirect: The client is redirected to a virtual URL to be authenticated, and the client IP address is used as a surrogate credential. Note that the ProxySG does not support origin-redirects with the CONNECT method.
- SG2: The mode is selected automatically, based on the request, and uses the SGOS 2.x-defined rules.

Section B: Controlling Access to the Internet and Intranet

- Form-IP: A form is presented to collect the user's credentials. The form is presented whenever the user's credential cache entry expires.
- Form-Cookie: A form is presented to collect the user's credentials. The cookies are set on the OCS domain only, and the user is presented with the form for each new domain. This mode is most useful in reverse proxy scenarios where there are a limited number of domains.
- Form-Cookie-Redirect: A form is presented to collect the user's credentials. The user is redirected to the authentication virtual URL before the form is presented. The authentication cookie is set on both the virtual URL and the OCS domain. The user is only challenged when the credential cache entry expires.
- Form-IP-redirect: This is similar to form-ip except that the user is redirected to the authentication virtual URL before the form is presented.

Important: Modes that use an IP surrogate credential are insecure: After a user has authenticated from an IP address, all further requests from that IP address are treated as from that user. If the client is behind a NAT, or on a multi-user system, this can present a serious security problem.

The default value is `auto`.

For more information on using authentication modes, see the *Blue Coat Content Policy Language Guide*.

Setting the Default Authenticate Mode Property

Setting the `authentication.mode` property selects a challenge type and surrogate credential combination. In `auto` mode, explicit NTLM uses connection surrogate credentials. In `sg2` mode, explicit NTLM uses IP surrogate credentials.

To Configure the NTLM Default authenticate.mode Settings:

At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) security default-authenticate-mode {auto | sg2}
```

Origin-Style Redirection

Some authentication modes redirect the browser to a *virtual authentication site* before issuing the origin-style challenge. This gives the user feedback as to which credentials are required, and makes it possible (although not required) to send the credentials over a secure connection.

Since browser requests are transparently redirected to the ProxySG, the Appliance intercepts the request for the virtual authentication site and issues the appropriate credential challenge. Thus, the challenge appears to come from the virtual site, which is usually named to make it clear to the user that ProxySG credentials are requested.

If authentication is successful, the ProxySG establishes a surrogate credential and redirects the browser back to the original request, possibly with an encoded surrogate credential attached. This allows the ProxySG to see that the request has been authenticated, and so the request proceeds. The response to that request can also carry a surrogate credential.

Section B: Controlling Access to the Internet and Intranet

To provide maximum flexibility, the virtual site is defined by a URL. Requests to that URL (only) are intercepted and cause authentication challenges; other URLs on the same host are treated normally. Thus, the challenge appears to come from a host that in all other respects behaves normally.

Note: Sharing the virtual URL with other content on a real host requires additional configuration if the credential exchange is over SSL.

You can configure the virtual site to something that is meaningful for your company. The default, which requires no configuration, is `www.cfauth.com`. See "Configuring Transparent Proxy Authentication" on page 220 to set up a virtual URL for transparent proxy.

Tip: Using CONNECT and Origin-Style Redirection

You cannot use the CONNECT method with origin-style redirection or form redirect modes. You will receive an error message similar to the following:

```
Cannot use origin-redirect for CONNECT method (explicit proxy of https URL)
```

Instead, you can add policy to either bypass authentication on the CONNECT method, or use proxy authentication. For example:

```
<proxy>
  allow http.method=CONNECT authenticate.mode(proxy) authenticate(ldap)
  allow authenticate(cert) authenticate.mode(origin-cookie-redirect)
```

Selecting an Appropriate Surrogate Credential

IP surrogate credentials are less secure than cookie surrogate credentials and should be avoided if possible. Note that if multiple clients share an IP address (such as when they are behind a NAT firewall or on a multi-user system), the IP surrogate mechanism cannot distinguish between those users.

Configuring Transparent Proxy Authentication

The following sections provide general instructions on configuring for transparent proxy authentication.

In addition to configuring transparent proxy authentication, you must also enable a transparent proxy port before the transparent proxy is functional. To enable a transparent proxy port, see "Creating and Editing Services" on page 121.

To Set Transparent Proxy Options through the Management Console:

1. Select Configuration>Authentication>Transparent Proxy.

The Transparent Proxy tab displays.

Section B: Controlling Access to the Internet and Intranet



Figure 8-3: Transparent Proxy Tab

2. Select the transparent proxy method—cookie-based or IP address-based. The default is **Cookie**. If you select **Cookie**, the **Cookie Type** radio buttons are available. Click either **Session**, for cookies that will be deleted at the end of a session, or **Persistent**, for cookies that will remain on a client machine until the cookie TTL (Time To Live) is reached or the credentials cache is flushed. The default is **Session**. If you select **Persistent Cookies**, enter the **Cookie TTL**. If you choose **IP address-based**, enter the **IP address TTL**. The default for each is 15 minutes.

Note: A value of 0 (zero) for the IP address TTL re-prompts the user for credentials once the specified cache duration for the particular realm has expired.

For authentication modes that make use of IP surrogate credentials, once the IP address TTL expires the proxy re-challenges all client requests that do not contain credentials for which an IP surrogate credential cache entry previously existed.

If at this point the client supplied a different set of credentials than previously used to authenticate—for which an entry in the user credential cache still exists—the proxy fails authentication. This is to prevent any other client to potentially gain network access by impersonating another user by supplying his or her credentials. However, once the user credential cache entry's TTL has expired, you can supply a different set of credentials than previously used for authentication.

3. Select the **Virtual URL**. The default is www.cfauth.com. Blue Coat recommends you change the virtual hostname to something meaningful to you, preferably the IP address of the **ProxySG**, unless you are using secure credentials over SSL. Using the IP address of the **ProxySG** enables you to be sure that the correct **ProxySG** is addressed in a cluster configuration.
4. Click **Apply**.

Section B: Controlling Access to the Internet and Intranet

To Set Transparent Proxy Options through the CLI:

1. At the `(config)` command prompt, enter the following command:

```
SGOS# (config) security transparent-proxy-auth method {cookie | ip}
```

- a. If you select cookie-based transparent proxy authentication, enter the following command to specify persistent cookies or cookies that persist for the current session only:

```
SGOS# (config) security transparent-proxy-auth cookie {persistent | session}
```

- b. If you select persistent cookies, enter the following command to specify the minutes that the cookie persists:

```
SGOS# (config) security transparent-proxy-auth time-to-live persistent-cookie minutes
```

- c. If you choose IP-based transparent proxy authentication, enter the following command to specify that the user be re-prompted for credentials after the number of TTL minutes specified:

```
SGOS# (config) security transparent-proxy-auth time-to-live ip minutes
```

A value of 0 (zero) for the IP address TTL re-prompts the user for credentials once the specified cache duration for the particular realm has expired.

2. (Optional step for single ProxySG scenarios, only needed if specifying a different virtual URL than supplied by Blue Coat—www.cfauth.com) To specify the virtual URL for cookie-based authentication, enter the following command:

```
SGOS# (config) security transparent-proxy-auth cookie virtual-url url
```

3. (Optional, if you choose cookie-based) Add the virtual host domain to the DNS service for your organization so that browsers, when redirected to the virtual URL, can resolve the hostname in the URL. (If you use the virtual hostname provided by Blue Coat—www.cfauth.com—you do not need to add the hostname to the DNS service.)

Using SSL with Authentication and Authorization Services

Blue Coat recommends that you use SSL during authentication to secure your user credentials. Blue Coat now supports SSL between the client and the ProxySG and between the ProxySG to LDAP and NTLM authentication servers.

SSL Between the Client and the ProxySG

To configure SSL for to use origin-cookie-redirect or origin-ip-redirect challenges, you must:

- Specify a virtual URL with the HTTPS protocol (for example, `https://virtual_address`).
- Create a keyring and certificate on the ProxySG.
- Create an HTTPS service to run on the port specified in the virtual URL and to use the keyring you just created.

Section B: Controlling Access to the Internet and Intranet

Note: You can only use SSL between the client and the ProxySG for origin-style challenges on transparent connections (SSL for explicit proxy authentication is not supported).

In addition, if you use a forward proxy, the challenge type must use redirection; it cannot be an origin or origin-ip challenge type.

When redirected to the virtual URL, the user is prompted to accept the certificate offered by the ProxySG (unless the certificate is signed by a trusted certificate authority). If accepted, the authentication conversation between the ProxySG and the user will be encrypted using the certificate.

Note: If the hostname does not resolve to the IP address of the ProxySG, then the network configuration must redirect traffic for that port to the Appliance. Also, if you use the IP address as the virtual hostname, you might have trouble getting a certificate signed by a CA-Certificate authority (which may not be important).

For information on creating a keyring and a certificate, see "Configuring HTTPS Termination" on page 176.

You can use SSL between the ProxySG and NTLM and LDAP authentication servers. For more information, see Chapter 9: "Using Authentication Services" on page 233.

Creating a Proxy Layer to Manage Proxy Operations

Once hardware configuration is complete and the system configured to use transparent or explicit proxies, use CPL or VPM to provide on-going management of proxy operations.

Using CPL

Below is a table of all commands available for use in proxy layers of a policy. If a condition, property, or action does not specify otherwise, it can be used only in <Proxy> layers. For information on creating effective CPL, refer to the *Blue Coat Content Policy Language Guide*.

Table 8.5: <Proxy> Layer Conditions

<Proxy> Layer Conditions	Meaning
admin.access=	Tests the administrative access requested by the current transaction. Can also be used in <Admin> layers.
attribute.name=	Tests if the current transaction is authenticated in a RADIUS or LDAP realm, and if the authenticated user has the specified attribute with the specified value. Can also be used in <Admin> layers.
authenticated=	Tests if authentication was requested and the credentials could be verified; otherwise, false. Can also be used in <Admin> layers.
bitrate=	Tests if a streaming transaction requests bandwidth within the specified range or an exact match. Can also be used in <Cache> layers.

Section B: Controlling Access to the Internet and Intranet**Table 8.5: <Proxy> Layer Conditions (Continued)**

category=	Tests if the content categories of the requested URL match the specified category, or if the URL has not been categorized. Can also be used in <Cache> layers.
client_address=	Tests the IP address of the client. Can also be used in <Admin> layers.
client.connection.negotiated_cipher=	Test the cipher suite negotiated with a securely connected client. Can also be used in <Exception> layers.
client.connection.negotiated_cipher.strength=	Test the cipher strength negotiated with a securely connected client. Can also be used in <Exception> layers.
client.host=	Test the hostname of the client (obtained through RDNS). Can also be used in <Admin>, <Forward>, and <Exception> layers.
client.host.has_name=	Test the status of the RDNS performed to determine 'client.host'. Can also be used in <Admin>, <Forward>, and <Exception> layers.
client_protocol=	Tests true if the client transport protocol matches the specification. Can also be used in <Exception> layers.
condition=	Tests if the specified defined condition is true. Can be used in all layers.
console_access=	(This trigger was formerly admin=yes no.) Tests if the current request is destined for the admin layer. Can also be used in <Cache> and <Exception> layers.
content_management=	(This trigger was formerly content_admin=yes no.) Tests if the current request is a content-management transaction. Can also be used in <Exception> and <Forward> layers.
date[.utc]=	Tests true if the current time is within the startdate..enddate range, inclusive. Can be used in all layers.
day=	Tests if the day of the month is in the specified range or an exact match. Can be used in all layers.
exception.id=	Indicates that the requested object was not served, providing this specific exception page. Can also be used in <Exception> layers.
ftp.method=	Tests ftp request methods against any of a well-known set of FTP methods. Can also be used in <Cache> and <Exception> layers.
group=	Tests if the authenticated condition is set to yes, the client is authenticated, and the client belongs to the specified group. Can also be used in <Admin> layers.
has_attribute.name=	Tests if the current transaction is authenticated in an LDAP realm and if the authenticated user has the specified LDAP attribute. Can also be used in <Admin> layers.

Section B: Controlling Access to the Internet and Intranet

Table 8.5: <Proxy> Layer Conditions (Continued)

hour=	Tests if the time of day is in the specified range or an exact match. Can be used in all layers.
http.method=	Tests HTTP request methods against any of a well known set of HTTP methods. Can also be used in <Cache> and <Exception> layers.
http.method.regex=	Test the HTTP method using a regular expression. Can also be used in <Exception> layers.
http.request_line.regex=	Test the HTTP protocol request line. Can also be used in <Exception> layers.
http.request.version=	Tests the version of HTTP used by the client in making the request to the ProxySG. Can also be used in <Cache> and <Exception> layers.
http.response_code=	Tests true if the current transaction is an HTTP transaction and the response code received from the origin server is as specified. Can also be used in <Cache> and <Exception> layers.
http.response.version=	Tests the version of HTTP used by the origin server to deliver the response to the ProxySG. Can also be used in <Cache> and <Exception> layers.
http.transparent_authentication=	This trigger evaluates to true if HTTP uses transparent proxy authentication for this request. Can also be used in <Cache> and <Exception> layers.
im.buddy_id=	Tests the buddy_id associated with the IM transaction. Can also be used in <Exception> layers.
im.chat_room.conference=	Tests whether the chat room associated with the transaction has the conference attribute set. Can also be used in <Exception> layers.
im.chat_room.id=	Tests the chat room ID associated with the transaction. Can also be used in <Exception> layers.
im.chat_room.invite_only=	Tests whether the chat room associated with the transaction has the invite_only attribute set. Can also be used in <Exception> layers.
im.chat_room.type=	Tests whether the chat room associated with the transaction is public or private. Can also be used in <Exception> layers.
im.chat_room.member=	Tests whether the chat room associated with the transaction has a member matching the specified criterion. Can also be used in <Exception> layers.
im.chat_room.voice_enabled=	Tests whether the chat room associated with the transaction is voice enabled. Can also be used in <Exception> layers.
im.client=	Test the type of IM client in use. Can also be used in <Exception>, <Forward>, and <Cache> layers.
im.file.extension=	Tests the file extension. Can also be used in <Exception> layers.
im.file.name=	Tests the file name (the last component of the path), including the extension. Can also be used in <Exception> layers.

Section B: Controlling Access to the Internet and Intranet**Table 8.5: <Proxy> Layer Conditions (Continued)**

im.file.path=	Tests the file path against the specified criterion. Can also be used in <Exception> layers.
im.file.size=	Performs a signed 64-bit range test. Can also be used in <Exception> layers.
im.message.reflected	Test whether IM reflection occurred. Can also be used in <Exception> and <Forward> layers.
im.message.route=	Tests how the IM message reaches its recipients. Can also be used in <Exception> layers.
im.message.size=	Performs a signed 64-bit range test. Can also be used in <Exception> layers.
im.message.text.substring=	Performs a signed 64-bit range test. Can also be used in <Exception> layers.
im.message.opcode=	Tests the value of an opcode associated with an im.method of send_unknown or receive_unknown.
im.message.type=	Tests the message type. Can also be used in <Exception> layers.
im.method=	Tests the method associated with the IM transaction. Can also be used in <Cache> and <Exception> layers.
im.user_id=	Tests the user_id associated with the IM transaction. Can also be used in <Exception> layers.
live=	Tests if the streaming content is a live stream. Can also be used in <Cache> layers.
minute=	Tests if the minute of the hour is in the specified range or an exact match. Can be used in all layers.
month=	Tests if the month is in the specified range or an exact match. Can be used in all layers.
proxy_address=	Tests the IP address of the network interface card (NIC) on which the request arrives. Can also be used in <Admin> layers.
proxy_card=	Tests the ordinal number of the network interface card (NIC) used by a request. Can also be used in <Admin> layers.
proxy_port=	Tests if the IP port used by a request is within the specified range or an exact match. Can also be used in <Admin> layers.
raw_url	Test the value of the raw request URL. Can also be used in <Exception> layers.
raw_url.host	Test the value of the 'host' component of the raw request URL. Can also be used in <Exception> layers.
raw_url.path	Test the value of the 'path' component of the raw request URL. Can also be used in <Exception> layers.

Section B: Controlling Access to the Internet and Intranet

Table 8.5: <Proxy> Layer Conditions (Continued)

raw_url.pathquery	Test the value of the 'path and query' component of the raw request URL. Can also be used in <Exception> layers.
raw_url.port	Test the value of the 'port' component of the raw request URL. Can also be used in <Exception> layers.
raw_url.query	Test the value of the 'query' component of the raw request URL. Can also be used in <Exception> layers.
realm=	Tests if the authenticated condition is set to yes, the client is authenticated, and the client has logged into the specified realm. an also be used in <Admin> layers.
release_id=	Tests the ProxySG release ID. Can be used in all layers.
request_header_address. header_name=	Tests if the specified request header can be parsed as an IP address. Can also be used in <Cache> layers.
request_header.header_ name=	Tests the specified request header (<i>header_name</i>) against a regular expression. Can also be used in <Cache> layers.
request.header.header_ name.count	Test the number of header values in the request for the given header_name. Can also be used in <Exception> layers.
request.header.header_ name.length	Test the total length of the header values for the given header_name. Can also be used in <Exception> layers.
request.header.Referer.u rl.host.has_name=	Test whether the Referer URL has a resolved DNS hostname. Can also be used in <Exception> layers.
request.header.Referer.u rl.is_absolute	Test whether the Referer URL is expressed in absolute form. Can also be used in <Exception> layers.
request.raw_headers.coun t	Test the total number of HTTP request headers. Can also be used in <Exception> layers.
request.raw_headers. length	Test the total length of all HTTP request headers. Can also be used in <Exception> layers.
request.raw_headers.rege x	Test the value of all HTTP request headers with a regular expression. Can also be used in <Exception> layers.
request.x_header.header_ name.count	Test the number of header values in the request for the given <i>header_name</i> . Can also be used in <Exception> layers.
request.x_header.header_ name.length	Test the total length of the header values for the given <i>header_name</i> . Can also be used in <Exception> layers.
response_header.header_ name=	Tests the specified response header (<i>header_name</i>) against a regular expression. Can also be used in <Cache> layers.
response_x_header.header _name=	Tests the specified response header (<i>header_name</i>) against a regular expression. Can also be used in <Cache> layers.

Section B: Controlling Access to the Internet and Intranet**Table 8.5: <Proxy> Layer Conditions (Continued)**

server_url[.case_sensitive .no_lookup]=	Tests if a portion of the requested URL exactly matches the specified pattern. Can also be used in <Forward> layers.
socks.accelerated=	Controls the SOCKS proxy handoff to other protocol agents.
socks.method=	Tests the protocol method name associated with the transaction. Can also be used in <Cache> and <Exception> layers.
socks.version=	Switches between SOCKS 4/4a and 5. Can also be used in <Exception> and <Forward> layers.
streaming.content=	(This trigger has been renamed from streaming.) Can also be used in <Cache>, <Exception>, and <Forward> layers.
time=	Tests if the time of day is in the specified range or an exact match. Can be used in all layers.
tunneled=	
url.domain=	Tests if the requested URL, including the domain-suffix portion, matches the specified pattern. Can also be used in <Forward> layers.
url.extension=	Tests if the filename extension at the end of the path matches the specified string. Can also be used in <Forward> layers.
url.host=	Tests if the host component of the requested URL matches the IP address or domain name. Can also be used in <Forward> layers.
url.host.has_name	Test whether the request URL has a resolved DNS hostname. Can also be used in <Exception> layers
url.is_absolute	Test whether the request URL is expressed in absolute form. Can also be used in <Exception> layers
url.host.is_numeric=	This is true if the URL host was specified as an IP address. Can also be used in <Forward> layers.
url.host.no_name=	This is true if no domain name can be found for the URL host. Can also be used in <Forward> layers.
url.host.regex=	Tests if the specified regular expression matches a substring of the domain name component of the request URL. Can also be used in <Forward> layers.
url.host.suffix=	Can also be used in <Forward> layers.
url.path=	Tests if a prefix of the complete path component of the requested URL, as well as any query component, matches the specified string. Can also be used in <Forward> layers.
url.path.regex=	Tests if the regex matches a substring of the path component of the request URL. Can also be used in <Forward> layers.
url.port=	Tests if the port number of the requested URL is within the specified range or an exact match. Can also be used in <Forward> layers.

Section B: Controlling Access to the Internet and Intranet

Table 8.5: <Proxy> Layer Conditions (Continued)

url.query.regex=	Tests if the regex matches a substring of the query string component of the request URL. Can also be used in <Forward> layers.
url.regex=	Tests if the requested URL matches the specified pattern. Can also be used in <Forward> layers.
url.scheme=	Tests if the scheme of the requested URL matches the specified string. Can also be used in <Forward> layers.
user=	Tests the authenticated user name of the transaction. Can also be used in <Admin> layers.
user_domain=	Tests if the authenticated condition is set to yes, the client is authenticated, the logged-into realm is an NTLM realm, and the domain component of the user name is the specified domain. Can also be used in <Admin> layers.
weekday=	Tests if the day of the week is in the specified range or an exact match. Can be used in all layers.
year=	Tests if the year is in the specified range or an exact match. Can be used in all layers.

Table 8.6: <Proxy> Layer Properties

<Proxy> Layer Properties	Meaning
action.action_label()	Selectively enables or disables a specified define action block. Can also be used in <Cache> layers.
allow	Allows the transaction to be served. Can be used in all layers except <Exception> and <Forward> layers.
always_verify()	Determines whether each request for the objects at a particular URL must be verified with the origin server.
authenticate()	Identifies a realm that must be authenticated against. Can also be used in <Admin> layers.
authenticate.force()	Either disables proxy authentication for the current transaction (using the value no) or requests proxy authentication using the specified authentication realm. Can also be used in <Admin> layers.
authenticate.form()	When forms-based authentication is in use, authenticate.form() selects the form used to challenge the user.
authenticate.mode (auto) authenticate.mode (sg2)	Setting the authentication.mode property selects a challenge type and surrogate credential combination. In auto mode, explicit NTLM uses connection surrogate credentials. In sg2.mode, explicit NTLM uses IP surrogate credentials.
authenticate.redirect_stored_requests	Sets whether requests stored during forms-based authentication can be redirected if the upstream host issues a redirecting response.
bypass_cache()	Determines whether the cache will be bypassed for a request.

Section B: Controlling Access to the Internet and Intranet

Table 8.6: <Proxy> Layer Properties (Continued)

check_authorization()	In connection with CAD (Caching Authenticated Data) and CPAD (Caching Proxy Authenticated Data) support, check_authorization() is used when you know that the upstream device will sometimes (not always or never) require the user to authenticate and be authorized for this object. Can also be used in <Cache> layers.
delete_on_abandonment()	If set to yes, then if all clients requesting an object close their connections prior to the object being delivered, the object fetch from the origin server will be abandoned. Can also be used in <Cache> layers.
deny	Denies service. Can be used in all layers except <Exception> and <Forward> layers.
dynamic_bypass()	Used to indicate that a particular transparent request should not be handled by the proxy, but instead be subjected to our dynamic bypass methodology.
exception()	Indicates not to serve the requested object, but instead serve this specific exception page. Can be used in all layers except <Exception> layers.
ftp.server_connection()	Determines when the control connection to the server is established.
ftp.welcome_banner()	Sets the welcome banner for a proxied FTP transaction.
http.client.recv.timeout	Sets the socket timeout for receiving bytes from the client.
http.request.version()	The http.request.version() property sets the version of the HTTP protocol to be used in the request to the origin content server or upstream proxy. Can also be used in <Cache> layers.
http.response.parse_meta_tag. Cache-Control()	Controls whether the 'Cache-Control' META Tag is parsed in an HTML response body. Can also be used in <Cache> layers.
http.response.parse_meta_tag. Expires	Controls whether the 'Expires' META Tag is parsed in an HTML response body. Can also be used in <Cache> layers.
http.response.parse_meta_tag. Pragma.no-cache	Controls whether the 'Pragma: no-cache' META Tag is parsed in an HTML response body. Can also be used in <Cache> layers.
http.response.version()	The http.response.version() property sets the version of the HTTP protocol to be used in the response to the client's user agent.
http.server.recv.timeout()	Sets the socket timeout for receiving bytes from the upstream host. Can also be used in <Forward> layers.
im.block_encryption	Prevents the encryption of AOL IM messages by modifying messages during IM login time.
im.reflect	Sets whether IM reflection should be attempted.
im.strip_attachments()	Determines whether attachments are stripped from IM messages.
im.transport	Sets the type of upstream connection to make for IM traffic.

Section B: Controlling Access to the Internet and Intranet**Table 8.6: <Proxy> Layer Properties (Continued)**

<code>log.suppress.field-id()</code>	The <code>log.suppress.field-id()</code> controls suppression of the specified field-id in all facilities (individual logs that contain all properties for that specific log in one format). Can be used in all layers.
<code>log.suppress.field-id [log_list]()</code>	The <code>log.suppress.field-id [log_list]()</code> property controls suppression of the specified field-id in the specified facilities. Can be used in all layers.
<code>log.rewrite.field-id()</code>	The <code>log.rewrite.field-id()</code> property controls rewrites of a specific log field in all facilities. Can be used in all layers.
<code>log.rewrite.field-id [log_list]()</code>	The <code>log.rewrite.field-id [log_list]()</code> property controls rewrites of a specific log field in a specified list of log facilities. Can be used in all layers.
<code>reflect_ip()</code>	Determines how the client IP address is presented to the origin server for explicitly proxied requests. Can also be used in <Forward> layers.
<code>request.filter_service()</code>	Websense is the built in service name for the off-box content filtering service. Can also be used in <Cache> layers.
<code>request.icap_service()</code>	Determines whether a request from a client should be processed by an external ICAP service before going out.
<code>shell.prompt</code>	Sets the prompt for a proxied Shell transaction.
<code>shell.realm_banner</code>	Sets the realm banner for a proxied Shell transaction.
<code>shell.welcome_banner</code>	Sets the welcome banner for a proxied Shell transaction.
<code>socks.accelerate()</code>	The <code>socks.accelerate</code> property controls the SOCKS proxy handoff to other protocol agents.
<code>socks.authenticate()</code>	The same realms can be used for SOCKS proxy authentication as can be used for regular proxy authentication.
<code>socks.authenticate.force()</code>	The <code>socks.authenticate.force()</code> property forces the realm to be authenticated through SOCKS.

Table 8.7: <Proxy> Layer Actions

<Proxy> Layer Actions	Meaning
<code>log_message()</code>	Writes the specified string to the ProxySG event log. Can be used in all layers except <Admin>.
<code>notify_email()</code>	Sends an email notification to the list of recipients specified in the Event Log mail configuration. Can be used in all layers.
<code>notify_snmp()</code>	The SNMP trap is sent when the transaction terminates. Can be used in all layers.
<code>redirect()</code>	Ends the current HTTP transaction and returns an HTTP redirect response to the client.

Section B: Controlling Access to the Internet and Intranet

Table 8.7: <Proxy> Layer Actions (Continued)

transform	Invokes the active content or URL rewrite transformer.
-----------	--

Chapter 9: Using Authentication Services

Determining and configuring the type of security (such as LDAP, local list, and NTLM) to implement on your network (authorization) is a critical part of managing enterprise security.

Understanding Realms

The ProxySG provides a flexible authentication architecture that supports multiple services with multiple backend servers (for example, LDAP directory servers together with NT domains with no trust relationship) within each authentication scheme with the introduction of the *realm*.

A *realm* authenticates and authorizes users for access to ProxySG services using either explicit proxy or transparent proxy mode, discussed in "Configuring Proxies" on page 137.

Multiple authentication realms can be used on a single ProxySG. Multiple realms are essential if the enterprise is a managed service provider or the company has merged with or acquired another company. Even for companies using only one protocol, multiple realms might be necessary, such as the case of a company using an LDAP server with multiple authentication boundaries. You can use realm sequencing to search the multiple realms all at once.

A realm configuration includes:

- Realm name
- Authentication service—(NTLM, LDAP, RADIUS, Local, Certificate, Sequences, Netegrity SiteMinder®)
- External server configuration—Backend server configuration information, such as host, port, and other relevant information based on the selected service.
- Authentication schema—The definition used to authenticate users.
- Authorization schema—The definition used to authorize users for membership in defined groups and check for attributes that trigger evaluation against any defined policy rules.

Note: One-time passwords for any realm type are not supported.

SSL Between the ProxySG and the Authentication Server

SSL communication between the ProxySG and LDAP and NTLM authentication servers is supported. In addition, you can also use SSL between the client and the ProxySG. For more information on using SSL between the client and the ProxySG, see "SSL Between the Client and the ProxySG" on page 222.

Configuring a realm to use SSL between the ProxySG and the authentication server is performed on a per-realm basis. Part of the SSL configuration is specifying whether to verify the server's certificate. If the server certificate is to be verified, then the server's certificate must be signed by a Certificate Authority that the ProxySG trusts, and the common name in the server certificate must match the server host as specified in the realm configuration.

The realms use the default SSL client defined on the ProxySG for SSL communications to the authentication servers.

Note: If the browser is configured for on-line checking of certificate revocation, the status check must be configured to bypass authentication.

The chapter contains the following sections:

- "NTLM Realm Authentication and Authorization"
- "LDAP Realm Authentication and Authorization"
- "RADIUS Realm Authentication and Authorization"
- "Local Realm Authentication and Authorization"
- "Certificate Realm Authentication"
- "Sequence Realm Authentication"
- "Netegrity SiteMinder"
- "Managing the Credential Cache"

Section A: NTLM Realm Authentication and Authorization

Section A: NTLM Realm Authentication and Authorization

Windows NT LAN Manager (NTLM) is the authentication protocol used on Windows NT networks.

NTLM is a Microsoft-proprietary protocol that authenticates users and computers based on an authentication challenge and response. When an NTLM realm is used and a resource is requested by the client from the ProxySG, the appliance contacts the user's or computer's account domain to verify identity and then requests an access token. The access token is generated by the domain controller and passed to (and if valid, accepted by) the ProxySG.

Refer to the Microsoft Web site for detailed information about the NTLM protocol and a list of which versions of the Microsoft operating systems use NTLM.

This section discusses the following topics:

- "How Blue Coat Works with NTLM"
- "Creating an NTLM Realm"
- "NTLM Servers"
- "Defining NTLM Realm General Properties"
- "Creating the CPL"

How Blue Coat Works with NTLM

Blue Coat uses a proprietary NTLM agent to better manage NTLM connections.

For NTLM, a single BCAAA (Blue Coat Authentication and Authorization Agent) can support multiple ProxySG Appliances; however, only one agent is permitted per realm.

Important: You must use the 3.2 release of BCAAA with SGOS 3.2. You can also use BCAAA in place of the deprecated CAASNT service for SGOS 2.x and SGOS 3.x. You cannot use CAASNT with SGOS 3.2 and higher.

BCAAA must be installed on a domain controller or member server. If the server where the BCAAA is installed and its domain have a trust relationship with other domains, the user is authenticated automatically by the other domains.

Creating an NTLM Realm

To create an NTLM realm, you must provide at least the primary host of the NTLM server for that realm.

To Create an NTLM Realm through the Management Console:

1. Select Configuration>Authentication>NTLM>NTLM Realms.

The NTLM Realms tab displays.

Section A: NTLM Realm Authentication and Authorization

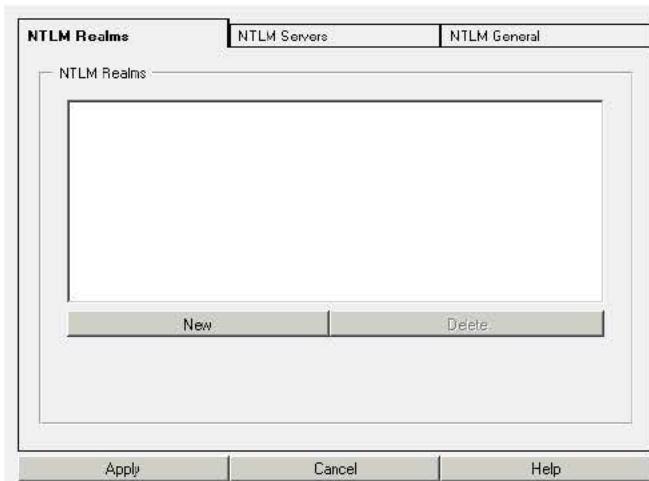


Figure 9-1: NTLM Realms Tab

2. Click New; the Add NTLM Realm dialog displays.

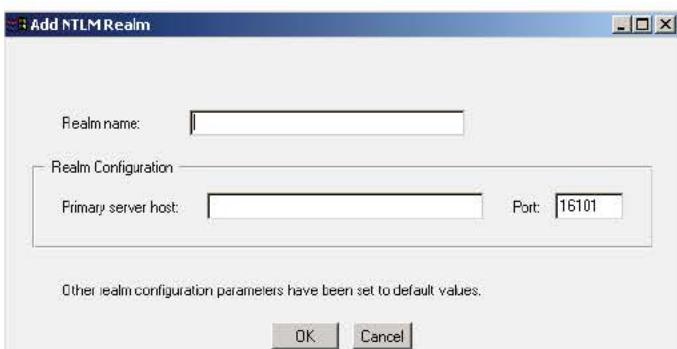


Figure 9-2: Add NTLM Realm

3. In the **Realm name** field, enter a realm name. The name can be 32 characters long and composed of alphanumeric characters and underscores. The name *must* start with a letter.
4. Identify the primary server host. You must enter a valid host or an error message is generated.
5. (Optional) The default port is 16101. You can change the port number if the primary server is listening on a different port.
6. Click OK; click Apply.

NTLM Servers

Once you have created an NTLM realm, you can use the NTLM Servers tab to change the current default settings.

1. Select Configuration>Authentication>NTLM>NTLM Servers.

The NTLM Servers tab displays.

Section A: NTLM Realm Authentication and Authorization

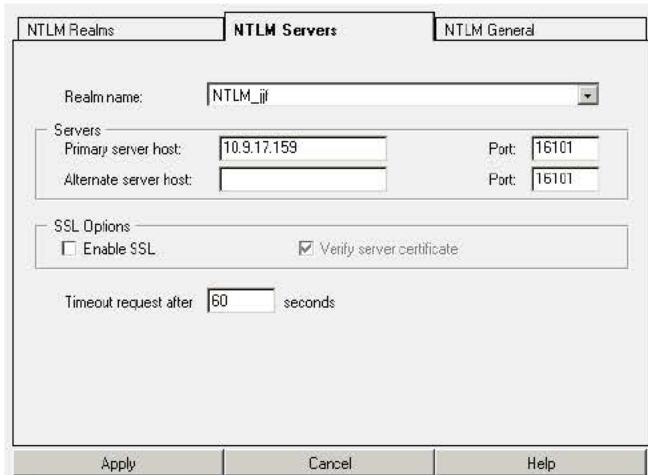


Figure 9-3: NTLM Servers Tab

2. From the Realm Name drop-down list, select the NTLM realm for which you want to change server properties.

Note: You must have defined at least one NTLM realm (using the NTLM Realms tab) before attempting to set NTLM server properties. If the message **Realms must be added in the NTLM Realms tab before editing this tab** is displayed in red at the bottom of this page, you do not currently have any NTLM realms defined.

3. Specify the host and port for the primary NTLM server. The default port is 16101.
4. (Optional) Specify the host and port for the alternate NTLM server. The default port is 16101.
5. (Optional) Under SSL Options, click the SSL enable checkbox to enable SSL.
6. (Optional) By default, if SSL is enabled, the BCAAA certificate is verified. If you do not want to verify the BCAAA certificate, deselect this checkbox.
7. In the Timeout Request field, type the number of seconds the ProxySG allows for each request attempt before timing out. (The default request timeout is 60 seconds.)
8. Click **Apply**. Repeat the above steps for additional NTLM realms, up to a total of 40.

To Create and Define an NTLM Realm through the CLI:

1. At the **(config)** prompt, enter the following command to create an NTLM realm:

```
SGOS#(config) security ntlm create-realm realm_name primary_host [primary_port]
```

where:

realm_name The name of the NTLM realm.

primary_host The host for the primary NTLM server.

primary_port The port for the primary NTLM server. The default port is 16101.

Section A: NTLM Realm Authentication and Authorization

2. To redefine the NTLM realm configuration for the realm you just created, enter the following commands:

```
SGOS#(config) security ntlm edit-realm realm_name
```

```
SGOS#(config ntlm realm_name) primary-server primary_host [primary_port]
```

and optionally,

```
SGOS#(config ntlm realm_name) alternate-server alternate_host [alternate_port]
```

where:

primary_host The host for the primary NTLM server.

primary_port The port for the primary NTLM server. The default port is 16101.

alternate_host The host for the alternate NTLM server.

alternate_port The port for the alternate NTLM server. The default port is 16101.

3. To enable SSL for this realm and to have the BCAAA certificate verified, enter:

```
SGOS#(config ntlm realm_name) ssl enable
```

```
SGOS#(config ntlm realm_name) ssl-verify-server enable
```

Defining NTLM Realm General Properties

The NTLM General tab allows you to specify the display name, whether to support Basic and NTLM credentials, the credential cache duration and a virtual URL.

To Configure General Settings through the Management Console:

1. Select Configuration>Authentication>NTLM>NTLM General.

The NTLM General tab displays.

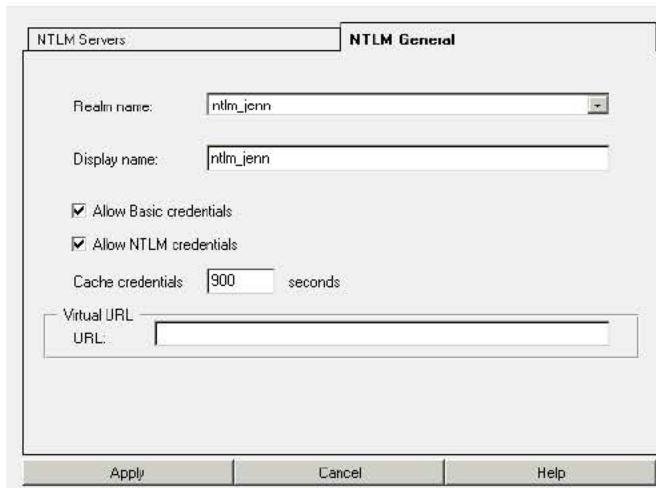


Figure 9-4: NTLM General Tab

Section A: NTLM Realm Authentication and Authorization

2. From the Realm Name drop-down list, select the NTLM realm for which you want to change properties.

Note: You must have defined at least one NTLM realm (using the NTLM Realms tab) before attempting to set NTLM general properties. If the message `Realms must be added in the NTLM Realms tab before editing this tab` is displayed in red at the bottom of this page, you do not currently have any NTLM realms defined.

3. If needed, change the NTLM realm display name. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
4. You can enable or disable support for Basic credentials in the realm by selecting or deselecting the Allow Basic credentials checkbox.

Note: Note that at least one Basic or NTLM credential must be supported. Also, if the NTLM realm is part of a sequence realm and is not the first realm in the sequence with try NTLM authentication only once enabled that Basic credentials cannot be disabled in the NTLM realm.

5. You can enable or disable support for NTLM credentials in the realm by selecting or deselecting the Allow NTLM credentials checkbox. Note that at least one of Basic or NTLM credentials must be supported.
6. Specify the length of time, in seconds, that user and administrator credentials received from the NTLM server are cached. Credentials can be cached for up to 3932100 seconds. The default cache duration is 900 seconds (15 minutes).

Note: If you specify 0, traffic is increased to the NTLM server because each authentication request generates an authentication and authorization request to the server.

7. You can specify a virtual URL based on the individual realm. For more information on the virtual URL, see Chapter 8: “Security and Authentication” on page 203.
8. Click Apply.

To Configure General Settings through the CLI:

At the `(config)` command prompt, enter the following commands to configure general settings:

```
SGOS# (config ntlm realm_name) cache-duration seconds
SGOS# (config ntlm realm_name) credentials-basic enable|disable
SGOS# (config ntlm realm_name) credentials-ntlm enable|disable
SGOS# (config ntlm realm_name) display-name name
SGOS# (config ntlm realm_name) virtual-url url
```

where:

<code>cache-duration</code> <i>seconds</i>	Specifies the length of time in seconds that user and administrator credentials received from the NTLM server are cached. Credentials can be cached for up to 3932100 seconds. The default value is 900 seconds (15 minutes).
--	---

Section A: NTLM Realm Authentication and Authorization

credentials-	enable disable	Enables or disables Basic credential support.
credentials-	enable disable	Enables or disables NTLM credential support.
display-name	name	The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
virtual-url	url	The URL to redirect to when the user needs to be challenged for credentials. see Chapter 8: "Security and Authentication" on page 203 for more details.

Creating the CPL

You can create CPL policies now that you have completed NTLM realm configuration. Be aware that the examples below are just part of a comprehensive authentication policy. By themselves, they are not adequate for your purposes.

The examples below assume the default policy condition is *allow*. On new SGOS 3.x systems, the default policy condition is *deny*.

Note: See the *Blue Coat Content Policy Language Guide* for details about CPL and how transactions trigger the evaluation of policy file layers.

- Every NTLM-authenticated user is allowed access the ProxySG.

```
<Proxy>
    authenticate (NTLMRealm)
```
- Group membership is the determining factor in granting access to the ProxySG.

```
<Proxy>
    authenticate (NTLMRealm)
<Proxy>
    group="Domain\internetusers"
    deny
```

Tips and Boundary Conditions

- Forms authentication modes cannot be used with an NTLM realm that allows only NTLM credentials or a Certificate realm. If a form mode is in use and the authentication realm is either, you will receive a configuration error.
- For Windows Internet Explorer NTLM users who want true single-sign-on (allowing Internet Explorer to provide your credentials automatically when challenged), you must set the virtual URL to a hostname that is resolvable to the IP address of the ProxySG by the client machines. Dots (for example, 10.1.1.1) are not allowed.

To define the information in Internet Explorer, go to Internet Options>Security>Local intranet>Sites>Advanced...>Web sites. (If you are an XP user, go to Internet Options>Security>Internet>Custom Level, then check Automatic logon with current username and password.)

Section A: NTLM Realm Authentication and Authorization

For Windows Internet Explorer 6.x users, add the virtual host address to Internet Options>Privacy>Web Sites>Managed Web Sites>Always Allow.

Section B: LDAP Realm Authentication and Authorization

Section B: LDAP Realm Authentication and Authorization

Many companies and organizations use the Lightweight Directory Access Protocol (LDAP) as the directory protocol of choice, enabling software to find an individual user without knowing where that user is located in the network topography.

This section discusses the following topics:

- "Overview"
- "Creating an LDAP Realm"
- "LDAP Servers"
- "Defining LDAP Base Distinguished Names"
- "LDAP Search & Groups Tab (Authorization and Group Information)"
- "Customizing LDAP Objectclass Attribute Values"
- "Defining Sequence Realm General Properties"
- "Creating the CPL"

Overview

Blue Coat supports both LDAP v2 and LDAP v3, but recommends LDAP v3 because it uses Transport Layer ProxySG (TLS) and SSL to provide a secure connection between the ProxySG and the LDAP server.

An LDAP directory, either version 2 or version 3, consists of a simple tree hierarchy. An LDAP directory might span multiple LDAP servers. In LDAP v3, servers can return referrals to other servers back to the client, allowing the client to follow those referrals if desired.

Directory services simplify administration; any additions or changes made once to the information in the directory are immediately available to all users and directory-enabled applications, devices, and ProxySG Appliances.

The ProxySG supports the use of external LDAP database servers to authenticate and authorize users on a per-group or per-attribute basis.

LDAP group-based authentication for the ProxySG can be configured to support any LDAP-compliant directory including:

- Microsoft Active Directory Server
- Novell NDS/eDirectory Server
- Netscape/Sun iPlanet Directory Server
- Other

The ProxySG also provides the ability to search for a single user in a single root of an LDAP directory information tree (DIT), and to search in multiple Base Distinguished Names (DNs).

You can configure a LDAP realm to use SSL when communicating to the LDAP server.

Section B: LDAP Realm Authentication and Authorization

Configuring LDAP involves the following steps:

- Creating a realm (up to 40) and configuring basic settings.
- Configuring an LDAP server
- Defining LDAP Base Distinguished Names
- Defining Authorization and Group information
- Configuring general LDAP realm settings
- Creating policy

Creating an LDAP Realm

To Create an LDAP Realm through the Management Console:

1. Select Configuration>Authentication>LDAP>LDAP Realms.

The LDAP Realms tab displays.

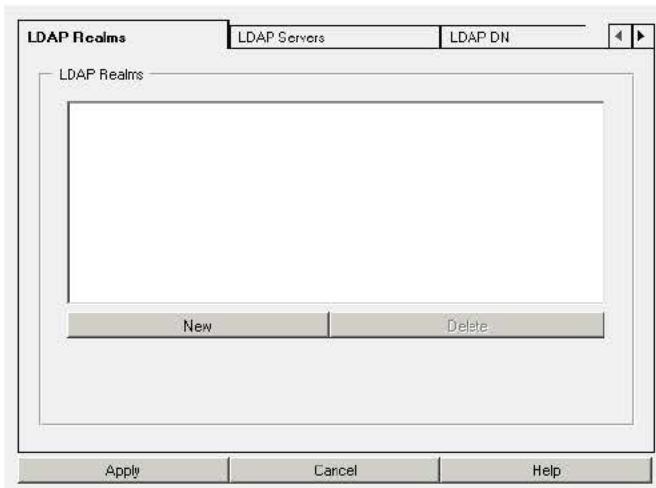


Figure 9-5: LDAP Realms Tab

Section B: LDAP Realm Authentication and Authorization

2. Click New; the Add LDAP Realm dialog displays.

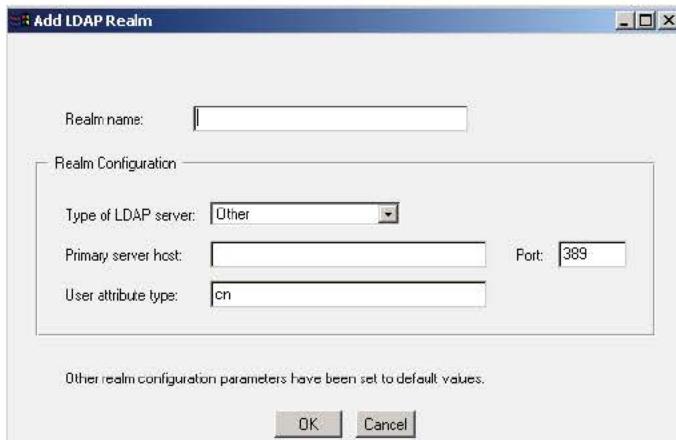


Figure 9-6: Add LDAP Realm

3. In the Real name field, enter a realm name. The name can be 32 characters long and composed of alphanumeric characters and underscores. The name *must* start with a letter.
4. From the Type of LDAP server drop-down list, select the specific LDAP server.
5. Specify the host and port for the primary LDAP server. The host must be entered. The default port number is 389.
6. In the User attribute type field, specify the default user attribute type for the type of LDAP server.

Microsoft Active Directory Server	sAMAccountName=
Novell NDS/eDirectory Server/Other	cn=
Netscape/iPlanet Directory Server	uid=

7. Click OK; click Apply.

LDAP Servers

Once you have created an LDAP realm, you can use the LDAP Servers tab to change the current default settings.

To Edit LDAP Server Properties through the Management Console:

Note that the default values exist. You do not need to change these values if the default settings are acceptable.

1. Select Configuration>Authentication>>LDAP>LDAP Servers.

The LDAP Servers tab displays.

Section B: LDAP Realm Authentication and Authorization

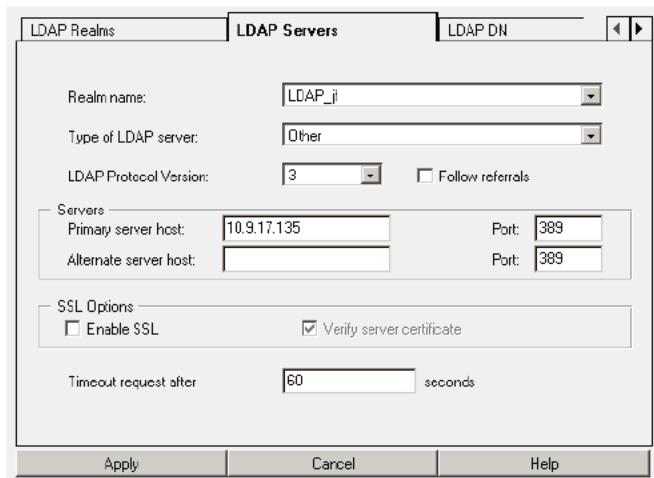


Figure 9-7: LDAP Servers Tab

2. From the Realm Name drop-down list, select the LDAP realm for which you want to change server properties.

Note: You must have defined at least one LDAP realm (using the LDAP Realms tab) before attempting to set LDAP server properties. If the message `Realms must be added` in the LDAP Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any LDAP realms defined.

3. From the Type of LDAP server drop-down list, select the specific LDAP server.
4. From the LDAP Protocol Version drop-down list, select v2 for LDAP v2 support. LDAP v3 is the default.

If you use LDAP v3, you can click the Follow referrals checkbox to allow the client to follow referrals to other servers. (This feature is not available with LDAP v2.) The default is Disabled.

Section B: LDAP Realm Authentication and Authorization

5. Specify the host and port for the primary LDAP server. The host must be entered. The default port number is 389.
6. (Optional) Specify the host and port for the alternate LDAP server. The default port is 389.
7. (Optional) Under SSL Options, click Enable SSL to enable SSL. You can only select this option if you are using LDAP v3.
8. (Optional) By default, if SSL is enabled, the LDAP server certificate is verified. If you do not want to verify the server certificate, disable this setting.
9. (Optional) Change the timeout request for the server from its default of 60 seconds.
10. Click Apply. Repeat the above steps for additional LDAP realms, up to a total of 40.

To Define a Realm and Edit LDAP Server Properties through the CLI:

1. At the `(config)` command prompt, enter the following command to create an LDAP realm:

```
SGOS# (config) security ldap create-realm {ad | iplanet | nds | other} realm_name
[base_dn] primary_host [primary_port]
```

where:

<code>{ad iplanet nds other}</code>	The type of LDAP realm to create. ad specifies a Microsoft Active Directory realm; iplanet specifies a Netscape/Sun iPlanet realm; nds specifies a Novell NDS/eDirectory realm; other specifies a realm of any other type.
<code>realm_name</code>	The name of the new LDAP realm.
<code>base_dn</code>	The distinguished name (DN) that will be used as the unique key for the LDAP group database; the distinguished name of the key entry and all entries below it in the directory tree. You can specify additional Base DNs after the realm has been created. For example: ou=insideSales, o=toolsdivision. A Base DN can be up to 128 characters long. (In Netscape/iPlanet Directory Server, Base DN is also known as the Root DN.) See Table 9.1 for sample DN entries.
<code>primary_host</code>	Note that at least one base DN is required for authentication to succeed, although you can create a realm without a base DN.
<code>primary_port</code>	The host for the primary LDAP server.
	The port for the primary LDAP server. The default port is 389.

2. To redefine the newly-created LDAP realm authentication properties, enter the following commands:

```
SGOS# (config) security ldap edit-realm realm_name
SGOS# (config ldap realm_name) primary-server host [port]
```

and, optionally:

```
SGOS# (config ldap realm_name) alternate-server host [port]
SGOS# (config ldap realm_name) distinguished-name base-dn clear
SGOS# (config ldap realm_name) distinguished-name base-dn add base_DN
SGOS# (config ldap realm_name) protocol-version 2 | 3
SGOS# (config ldap realm_name) referrals-follow enable | disable
```

Section B: LDAP Realm Authentication and Authorization

```
SGOS# (config ldap realm_name) spoof-authentication none | origin | proxy
SGOS# (config ldap realm_name) ssl enable | disable
SGOS# (config ldap realm_name) ssl-verify-server enable | disable
SGOS# (config ldap realm_name) exit
SGOS# (config ldap realm_name) timeout seconds
```

where

alternate-server	<i>host [port]</i>	The host for the secondary LDAP server. The port can also be added, if you need it to be other than the default (389).
distinguished name base-dn	<i>clear add base_DN</i>	Clears the existing base_DN or adds the specified base_DN. The distinguished name (DN) that will be used as the unique key for the LDAP group database; the distinguished name of the key entry and all entries below it in the directory tree. You can specify additional Base DNs after the realm has been created. For example: ou=insidesales, o=toolsdivision. A Base DN can be up to 128 characters long. (In Netscape/iPlanet Directory Server, Base DN is also known as the Root DN.) See Table 9.1 for sample DN entries.
protocol-version	<i>2 3</i>	Note that at least one base DN is required for authentication to succeed, although you can create a realm without a base DN.
referrals-follow	<i>enable disable</i>	The LDAP version you want to use. LDAP v3 is the default, allowing you to use the referrals-follow argument and to use SSL.
spoof-authentication	<i>none origin proxy</i>	Allows the client to follow referrals to other servers. This argument is not available if you use LDAP v2.
ssl	<i>enable disable</i>	Enables/disables the forwarding of authenticated credentials to the origin content server or for proxy authentication. You can only choose one. <ul style="list-style-type: none"> • If set to <i>origin</i>, the spoofed header will be an Authorization: header. • If set to <i>proxy</i>, the spoofed header will be a Proxy-Authorization: header. • If set to <i>none</i>, no spoofing will be done.
ssl-verify-server	<i>enable disable</i>	Flush the entries for a realm if the spoof-authentication value is changed to ensure that the spoof-authentication value is immediately applied.
		Enables or disables SSL. This argument is not available if you use LDAP v2.
		By default, if SSL is enabled, the LDAP server certificate is verified. If you do not want to verify the server certificate, disable this setting.

Section B: LDAP Realm Authentication and Authorization

```
SGOS#(config ldap    seconds
      realm_name) timeout
```

Note that this command is not in the edit-realm submode. Changes the timeout request for the server from its default of 60 seconds.

3. (Optional) Once in the edit-realm submode, use the ? command to view all of the edit-realm commands available.

Defining LDAP Base Distinguished Names

The ProxySG allows you to specify multiple Base Distinguished Names (DNs) to search per realm, along with the ability to specify a specific branch of a Base DN.

A *Base DN* identifies the entry that is starting point of the search. You must specify at least one non-null base-DN for LDAP authentication to succeed.

You must enter complete DNs. Table 9.1 lists some examples of distinguished name attributes.

Table 9.1: Distinguished Name Attributes

DN Attribute Syntax	Parameter Description
c=country	Country in which the user or group resides. Examples: c=US, c=GB.
cn=common name	Full name of person or object defined by the entry. Examples: cn=David Smith, cn=Administrators, cn=4th floor printer
mail=email address	User or group email address.
givenName=given name	User's first name.
l=locality	Locality in which the user or group resides. This can be the name of a city, country, township, or other geographic regions. Examples: l=Seattle, l=Pacific Northwest, l=King County
o=organization	Organization to which the user or group is a member. Examples: o=Blue Coat Inc, o=UW
ou=organizational unit	Unit within an organization. Examples: ou=Sales, ou=IT, ou=Compliance
st=state or province	State or province in which the user or group resides. Examples: st=Washington, st=Florida
userPassword=password	Password created by a user.
streetAddress=street address	Street number and address of user or group defined by the entry. Example: streetAddress= 650 Almanor Avenue Sunnyvale, California 94085-3515
sn=surname	User's last name.
telephoneNumber=telephone	User or group telephone number.
title=title	User's job title.
uid=user ID	Name that uniquely identifies the person or object defined by the entry. Examples: uid=ssmith, uid=kjones

To Define Searchable LDAP Base DNs through the Management Console:

1. Select Configuration>Authentication>LDAP>LDAP DN.

Section B: LDAP Realm Authentication and Authorization

The LDAP DN tab displays.

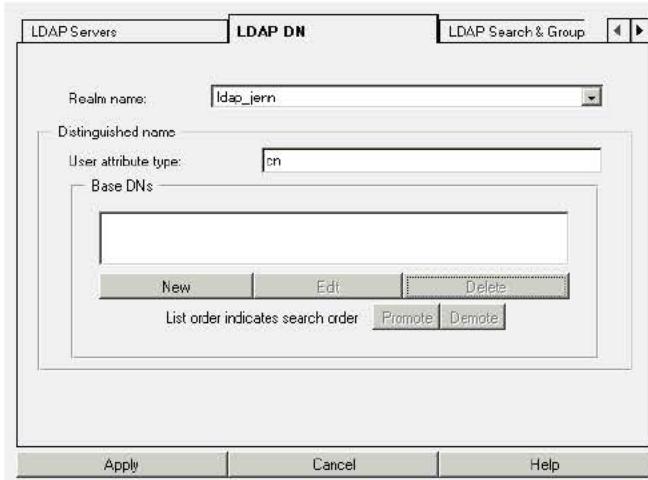


Figure 9-8: LDAP DN Tab

- From the Realm Name drop-down list, select the LDAP realm for which you want to change DN properties.

Note: You must have defined at least one LDAP realm (using the LDAP Realms tab) before attempting to set LDAP DN properties. If the message `Realms must be added in the LDAP Realms tab before editing this tab` is displayed in red at the bottom of this page, you do not currently have any LDAP realms defined.

- In the User attribute type field, the ProxySG has entered the default user attribute type for the type of LDAP server you specified when creating the realm.

Microsoft Active Directory Server	<code>sAMAccountName=</code>
Novell NDS/eDirectory Server/Other	<code>cn=</code>
Netscape/iPlanet Directory Server	<code>uid=</code>

If you entered information correctly when creating the realm, you do not need to change the User attribute type in this step. If you do need to change or edit the entry, do so directly in the field.

- Enter as many Base DNs as you need for the realm. Assume, for example, that Sample_Company has offices in New York and Lisbon, each with its own Base DN.



Figure 9-9: Simplified Directory Information Trees

Section B: LDAP Realm Authentication and Authorization

To specify entries for the Base DNs field, click New, enter the Base DN, and click OK. Repeat for multiple Base DNs. To search all of Sample_Company, enter o values:



Figure 9-10: Searching SampleCompany

To search the manufacturing organizations, rather than starting at the top, enter ou and o values:



Figure 9-11: Searching Part of SampleCompany

You can add, edit, and delete Base DNs for a ProxySG to search. You can also select an individual DN and move it up or down in the list with the Promote and Demote buttons. The ProxySG searches multiple DNs in the order listed, starting at the top and working down.

5. Click Apply to save the changes.

To Define One or More Searchable LDAP Base DNs through the CLI:

1. To define a Base DN, enter the following command:

```
SGOS#(config ldap realm_name) distinguished-name base-dn add base-dn
```

where base-dn is a string up to 128 characters long in the format appropriate to the type of LDAP server represented by the realm name. The base-dn should be the Fully-Qualified Domain Name (FQDN) of the base of the search.

Repeat this step for each additional Base DN you want added to the list. Entries in the list start with the first Base DN created; subsequent additions are appended to the list. The list is searched from the top down.

2. (Optional) To remove a Base DN:

```
SGOS#(config ldap realm_name) distinguished-name base-dn remove base_dn
```

3. (Optional) To remove all Base DNs and clear the list:

```
SGOS#(config ldap realm_name) distinguished-name base-dn clear
```

4. (Optional) To move a Base DN up or down in the list of Base DNs:

```
SGOS#(config ldap realm_name) distinguished-name base-dn {promote | demote} base_dn
```

Section B: LDAP Realm Authentication and Authorization

where `promote` moves the specified Base DN up one level in the list and `demote` moves it down one level. You need to issue the command for each level you want to move the Base DN.

LDAP Search & Groups Tab (Authorization and Group Information)

After creating an LDAP realm, providing at least the required fields of the LDAP server for that realm, and defining base DNs for the realm, you must define authorization properties for each LDAP realm you created.

Note: Authorization decisions are completely handled by policy. The groups that the ProxySG looks up and queries are derived from the groups specified in policy in `group=` conditions, `attribute=` conditions, and `has Attribute` conditions. If you do not have any of those conditions, then Blue Coat does not look up any groups or attributes to make policy decisions based on authorization.

To Define LDAP Realm Authorization Properties through the Management Console:

1. Select Configuration>Authentication>LDAP>LDAP Search & Groups.

The LDAP Search & Groups tab displays.

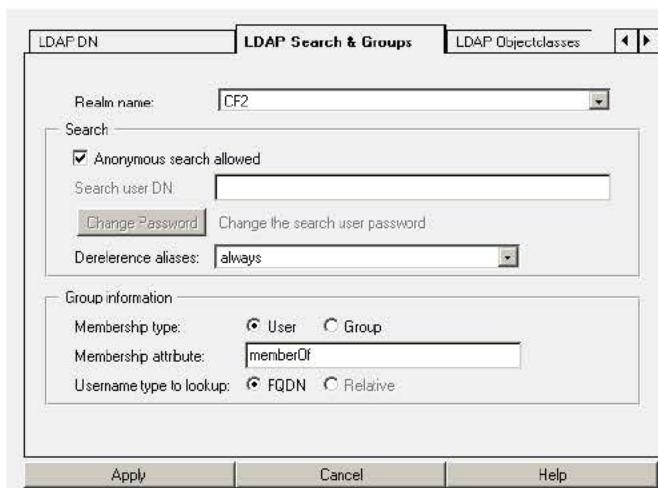


Figure 9-12: LDAP Search & Groups Tab

2. From the Realm Name drop-down list, select the LDAP realm for which you want to specify authorization information.

Note: You must have defined at least one LDAP realm (using the LDAP Realms tab) before attempting to set LDAP Search & Group properties. If the message Realms must be added in the LDAP Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any LDAP realms defined.

Section B: LDAP Realm Authentication and Authorization

3. Specify whether to allow anonymous search or to enforce user authentication before allowing a search.

Some directories require a valid user to be able to perform an LDAP search; they do not allow *anonymous bind*. (Active Directory is one such example.) For these directories, you must specify a valid fully-qualified distinguished username and the password that permits directory access privileges. (For example, `cn=user1,cn=users,dc=bluecoat,dc=com` is a possible fully-qualified distinguished name.)

To permit users to anonymously bind to the LDAP service, select **Anonymous Search Allowed**. For example, with Netscape/iPlanet Directory Server, when anonymous access is allowed, no username or password is required by the LDAP client to retrieve information.

The LDAP directory attributes available for an anonymous client are typically a subset of those available when a valid user distinguished name and password have been used as search credentials.

To enforce user authentication before binding to the LDAP service, deselect **Anonymous Search Allowed**, and set the **Search User DN** and **Search User Password**. Enter a user distinguished name in the **Search User DN** field. This username can identify a single user or a user object that acts as a proxy for multiple users (a pool of administrators, for example). A search user distinguished name can be up to 512 characters long.

You can set or change the user password by clicking **Change Password**. This password can be up to 64 alphanumeric characters long.

You might want to create a separate user (such as Blue Coat, for example) instead of using an Administrator distinguished name and password.

The **Dereference level** field has four values—**always**, **finding**, **never**, **searching**—that allow you to specify when to search for a specific object rather than search for the object's alias. The default is **Always**.

4. Group Information

Membership type and **Membership attribute**: The ProxySG enters the appropriate default:

- Microsoft Active Directory:
Membership type: `user`
Membership attribute type: `memberOf`
- Netscape/Sun iPlanet:
Membership type: `group`
Membership attribute type: `uniqueMember`
- Novell NDS eDirectory/Other
Membership type: `user`
Membership attribute type: `member`

Username type to lookup: Select either **FQDN** or **Relative**. Only one can be selected at a time.

- Relative can only be selected in the membership type is **Group**.
- FQDN indicates that the lookup is done only on the user object. FQDN can be selected when the membership type is either **Group** or **User**.

Section B: LDAP Realm Authentication and Authorization

5. Click Apply.

To Define LDAP Realm Authorization Properties through the CLI:

1. Define the search criteria for the LDAP realm:

```
SGOS#(config ldap realm_name) search {anonymous {disable | enable} | dereference {always | finding | never | searching} | password password | encrypted-password | user-dn user_dn}
```

where:

<i>anonymous</i>	<i>disable</i> <i>enable</i>	If disabled, users will not be permitted to anonymously bind to the LDAP service. If enabled, users will be permitted to anonymously bind to the LDAP service. When anonymous access is allowed, no password is required by the LDAP client to retrieve information, however, one can be specified, if extra security is desirable.
<i>dereference</i>	<i>always</i> <i>finding</i> <i>searching</i> <i>never</i>	The LDAP directory attributes available for an anonymous client are typically a subset of those available to clients that have been authenticated through a user distinguished name and password.
<i>password</i> <i>encrypted-</i> <i>password</i>	<i>password</i> <i>encrypted_-</i> <i>password</i>	Sets dereference options. <i>always</i> dereference aliases is the default. <i>finding</i> dereferences aliases only during name resolution. <i>searching</i> dereferences aliases only after name resolution. <i>never</i> means that aliases will never be dereferenced.
<i>user_dn</i>	<i>user_dn</i>	Specifies the user password (or encrypted password) associated with the user distinguished name. The non-encrypted (or clear-text) password can be up to 64 alphanumeric characters long. The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted. If you choose to use a third-party encryption application, be sure it supports RSA encryption, OAEP padding andBase64 encoded with no newlines.
		Specifies a user distinguished name. This username can identify a single user or a user object that acts as a proxy for multiple users (a pool of administrators, for example). Search user distinguished name can be up to 512 characters long.

2. To define LDAP realm membership properties:

```
SGOS#(config ldap realm_name) membership-attribute membership_attribute
```

where *membership_attribute* is the name of the attribute that has the group information. (For Active Directory, the attribute name is `memberOf`. For iPlanet, the attribute name is `uniqueMember`. For Novell Directory service, the attribute name is `member`.)

```
SGOS#(config ldap realm_name) membership-type {group | user}
```

where `group` specifies that this realm is composed of individual members belonging to a group defined elsewhere, and `user` specifies that this realm is composed of individual disparate members whose only link to each other is membership in this group.

Section B: LDAP Realm Authentication and Authorization

SGOS# (config ldap *realm_name*) **membership-username** (full | relative)

where **full** specifies that the user's FQDN will be used during membership lookups, and **relative** specifies that the user's relative username will be used during membership lookups. Only one can be selected at a time.

Boundary Condition

Only one LDAP search user DN can be configured per LDAP realm. As a result, if a search user DN is defined and if the LDAP server returns a referral to another server, that second server must also support binding as the LDAP search user DN in order for authentication to succeed. This is not an issue if anonymous binds are used for both servers.

Customizing LDAP Objectclass Attribute Values

The **objectclass** attributes on an LDAP object define the type of object an entry is. For example, a user entry might have an **objectclass** attribute value of *person* while a group entry might have an **objectclass** attribute value of *group*.

The **objectclass** attribute values defined on a particular entry can differ among LDAP servers. The **objectclass** attribute values are attribute values only, they are not DNs of any kind.

Currently, the **objectclass** attribute values are used by Blue Coat during a VPM browse of an LDAP server. If an administrator wants to browse the groups in a particular realm, the ProxySG searches the LDAP server for objects that have **objectclass** attribute values matching those in the group list and in the container list. The list of **objectclass** attribute values in the container list is needed so that containers that contain groups can be fetched and expanded correctly.

To Customize LDAP Objectclass Attribute Values through the Management Console:

1. Select Configuration>Authentication>LDAP>LDAP Objectclasses.

The LDAP Objectclasses tab displays.

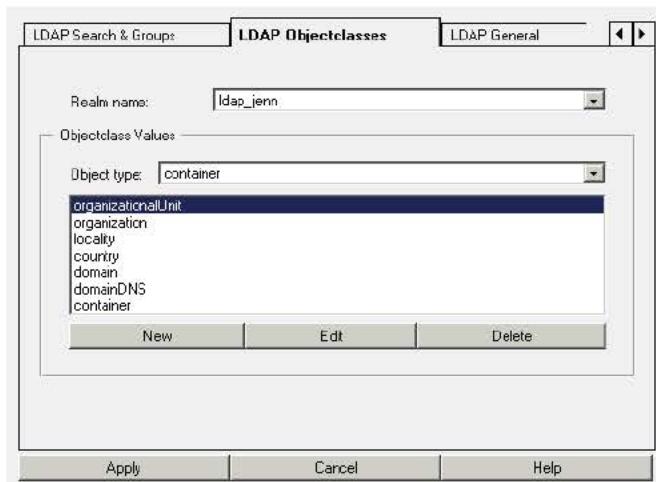


Figure 9-13: LDAP Objectclasses Tab

Section B: LDAP Realm Authentication and Authorization

2. From the Realm name drop-down list, select the LDAP realm whose objectclasses you want to modify.
3. From the Object type drop-down list, select the type of object: container, group, or user.
4. To create or edit an object for the specified objectclass, click New or Edit. (The only difference is whether you are adding or editing an objectclass value.)

The Add/Edit Objectclass Value dialog displays.

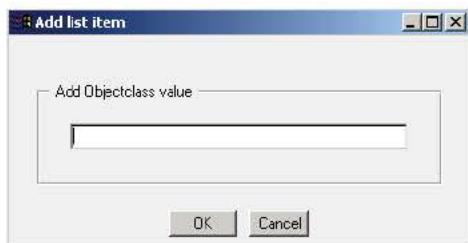


Figure 9-14: Add Objectclass Value

5. Enter or edit the objectclass, and click OK; click Apply. For example, objectclass=organization.

Defining LDAP General Realm Properties

The LDAP General tab allows you to indicate whether an LDAP server is configured to expect case-sensitive usernames and passwords, the length of time that credentials are cached, the display name, and if you want to use a special virtual host for this realm.

To Configure General LDAP Settings through the Management Console:

1. Select Configuration>Authentication>LDAP>LDAP General.

The LDAP General tab displays.

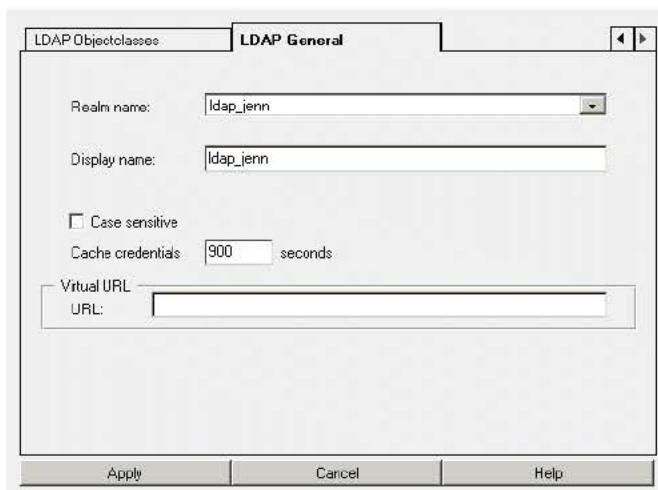


Figure 9-15: LDAP General Tab

Section B: LDAP Realm Authentication and Authorization

2. From the Realm Name drop-down list, select the LDAP realm for which you want to change properties.

Note: You must have defined at least one LDAP realm (using the LDAP Realms tab) before attempting to set LDAP general properties. If the message Realms must be added in the LDAP Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any LDAP realms defined.

3. If needed, give the LDAP realm a display name. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
4. If the LDAP server is configured to expect case-sensitive usernames and passwords, select Case sensitive.
5. Specify the length of time in seconds that user and administrator credentials received from the LDAP server are cached. Credentials can be cached for up to 3932100 seconds. The default value is 900 seconds (15 minutes).

Note: If you specify 0, this increases traffic to the LDAP server because each authentication request generates an authentication and authorization request to the server.

6. You can specify a virtual URL based on the individual realm. For information on the virtual URL, see Chapter 8: "Security and Authentication" on page 203.

To Configure General Settings through the CLI:

At the (config) prompt, enter the following command to configure general settings:

```
SGOS# (config ldap realm_name) cache-duration seconds
SGOS# (config ldap realm_name) case-sensitive {enable | disable}
SGOS# (config ldap realm_name) virtual-url url
SGOS# (config ldap realm_name) display-name name
```

where:

cache-duration	seconds	Specifies the length of time in seconds that user and administrator credentials received from the LDAP server are cached. Credentials can be cached for up to 3932100 seconds. The default value is 900 seconds (15 minutes). If you specify 0, cached user and administrator credentials are not re-used.
case-sensitive	enable disable	Enable this setting if the LDAP server is configured to expect case-sensitive usernames and passwords.
virtual-url	url	The URL to redirect to when the user needs to be challenged for credentials. See Chapter 8: "Security and Authentication" on page 203.
display-name	name	The default value for the display name is the realm name. The display name cannot be longer than 128 characters and cannot be null.

Section B: LDAP Realm Authentication and Authorization

Creating the CPL

Be aware that the examples below are just part of a comprehensive authentication policy. By themselves, they are not adequate for your purposes.

Note: Refer to the *Blue Coat Content Policy Language Guide* for details about CPL and how transactions trigger the evaluation of policy file layers.

Be aware that the default policy condition for these examples is *allow*. The default policy condition on new SGOS 3.x systems is *deny*.

- Every LDAP-authenticated user is allowed access the ProxySG.

```
<Proxy>
    authenticate (LDAPRealm)
```

- Group membership is the determining factor in granting access to the ProxySG.

```
<Proxy>
    authenticate (LDAPRealm)
<Proxy>
    group="cn=proxyusers, ou=groups, o=myco"
    deny
```

- A subnet definition determines the members of a group, in this case, members of the Human Resources department.

```
<Proxy>
    authenticate (LDAPRealm)
<Proxy>
    Define subnet HRSubnet
        192.168.0.0/16
        10.0.0.0/24
    End subnet HRSubnet
    [Rule] client_address=HRSubnet
        url.domain=monster.com
        url.domain=hotjobs.com
        deny
    .
    .
    .
    [Rule]
        deny
```

Section C: RADIUS Realm Authentication and Authorization

Section C: RADIUS Realm Authentication and Authorization

RADIUS is often the protocol of choice for ISPs or enterprises with very large numbers of users. Like LDAP, RADIUS was designed to handle these large numbers through centralized user administration that eases the repetitive tasks of adding and deleting users and their authentication information. Unlike LDAP, RADIUS inherently provides some protection against sniffing.

This section discusses the following topics:

- "Creating a RADIUS Realm"
- "Defining RADIUS Realm Properties"
- "Defining RADIUS Realm General Properties"
- "Creating the CPL"

Creating a RADIUS Realm

To Create a RADIUS Realm through the Management Console:

1. Select Configuration>Authentication>RADIUS>RADIUS Realms.

The RADIUS Realms tab displays.

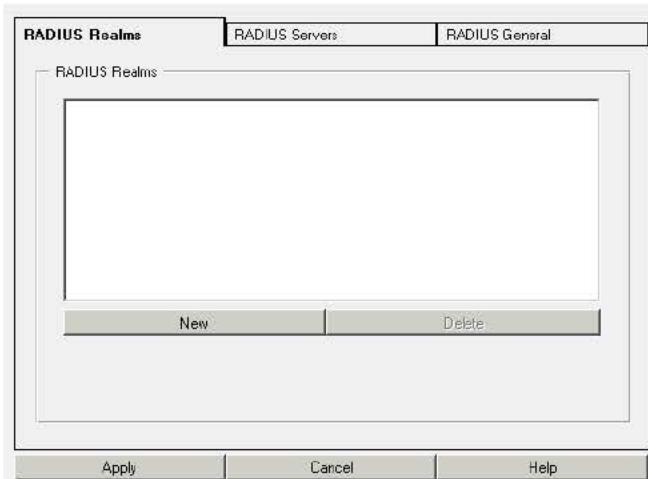


Figure 9-16: RADIUS Realms Tab

Section C: RADIUS Realm Authentication and Authorization

2. Click New; the Add RADIUS Realm dialog displays.

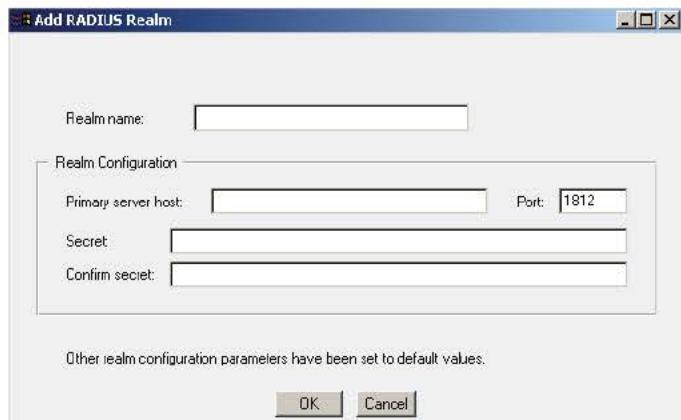


Figure 9-17: Add RADIUS Realm

3. In the Realm name field, enter a realm name. The name can be up to 32 characters long and composed of alphanumeric characters and underscores. The name *must* start with a letter.
4. Specify the host and port for the primary RADIUS server. The default port is 1812.
5. Specify the RADIUS secret. RADIUS secrets can be up to 64 characters long and are always case sensitive.
6. Confirm the secret.
7. Click OK; click Apply.

Defining RADIUS Realm Properties

Once you have created a RADIUS realm, you can change the primary host, port, and secret of the RADIUS server for that realm.

To Re-define RADIUS Server Properties through the Management Console:

Note: To make these settings through the CLI, see "To Create and Define a RADIUS Realm through the CLI" on page 262.

1. Select Configuration>Authentication>RADIUS>RADIUS Servers.
The RADIUS Servers tab displays.

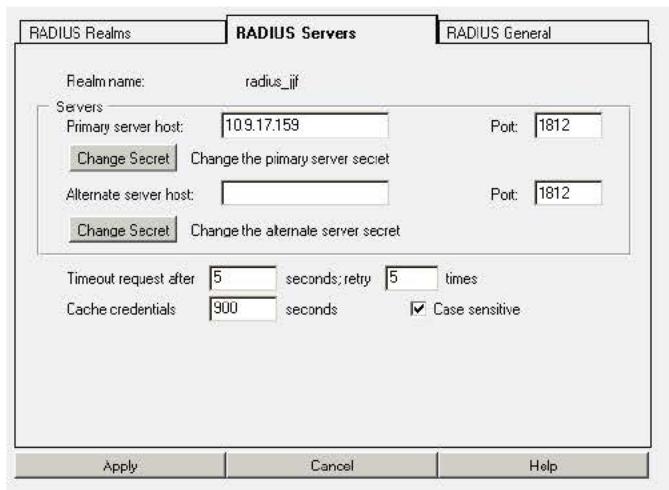
Section C: RADIUS Realm Authentication and Authorization

Figure 9-18: RADIUS Servers Tab

Note: You must have defined a RADIUS realm (using the RADIUS Realms tab) before attempting to set RADIUS server properties. If the message **Realms** must be added in the RADIUS Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have a RADIUS realm defined.

2. Specify the host and port for the primary RADIUS server. The default port is 1812. (To create or change the RADIUS secret, click Change Secret. RADIUS secrets can be up to 64 characters long and are always case sensitive.)
3. (Optional) Specify the host and port for the alternate RADIUS server. The default port is 1812. (To create or change the RADIUS secret, click Change Secret. RADIUS secrets can be up to 64 characters long and are always case sensitive.)
4. In the Timeout Request field, enter the number of seconds the ProxySG allows for each request attempt before timing out. The default request timeout is 5 seconds. In the Retry field, enter the number of attempts permitted. The default number of retries is 5.
5. Specify the length of time, in seconds, that user credentials received from the RADIUS server are cached. Credentials can be cached for up to 3932100 seconds. The default is 900 seconds (15 minutes).

Note: If you specify 0, traffic is increased to the RADIUS server because each authentication request generates an authentication and authorization request.

Section C: RADIUS Realm Authentication and Authorization

6. If the RADIUS server is configured to expect case-sensitive usernames and passwords, select Case sensitive.
7. Click Apply.

Important: If the user record contains Check-list ServiceType attributes, then at least one of the ServiceType values must match the service-type of the RADIUS server as configured on the ProxySG. To set the RADIUS server service-type, see "To Create and Define a RADIUS Realm through the CLI:" on page 262.

Defining RADIUS Realm General Properties

The RADIUS General tab allows you to specify the display name and a virtual URL.

To Configure General Settings through the Management Console:

1. Select Configuration>Authentication>RADIUS>RADIUS General.

The RADIUS General tab displays.

RADIUS Realms	RADIUS Servers	RADIUS General
Realm name:	radius_jif	
Display name:	radius_jif	
Virtual URL	URL: [empty]	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>		

Figure 9-19: RADIUS General Tab

2. From the Realm Name drop-down list, select the RADIUS realm for which you want to change properties.

Note: You must have defined at least one RADIUS realm (using the RADIUS Realms tab) before attempting to set RADIUS general properties. If the message Realms must be added in the RADIUS Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any RADIUS realms defined.

Section C: RADIUS Realm Authentication and Authorization

3. If needed, change the RADIUS realm display name. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
4. (Optional) You can specify a virtual URL based on the individual realm. For more information on the virtual URL, see Chapter 8: "Security and Authentication" on page 203.
5. Click Apply.

To Create and Define a RADIUS Realm through the CLI:

1. At the (config) prompt, enter the following command to create a RADIUS realm:

```
SGOS# (config) security radius create-realm realm_name secret primary-server_host [primary-server_port]  
-or-  
SGOS# (config) security radius create-realm-encrypted realm_name encrypted_secret primary_host [primary_port]
```

where:

<i>realm_name</i>	The name of the RADIUS realm.
<i>secret</i> <i>encrypted_secret</i>	The shared secret (or encrypted secret) associated with the primary RADIUS server. (RADIUS secrets can be up to 64 characters long and are always case sensitive.)
	The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted. If you choose to use a third-party encryption application, be sure it supports RSA encryption, OAEP padding and Base64 encoded with no new lines.
<i>primary_host</i>	The host for the primary RADIUS server.
<i>primary_port</i>	The port for the primary RADIUS server. The default port is 1812.

2. To set the newly-created RADIUS realm primary and alternate hosts and passwords, enter the following commands:

```
SGOS# (config) security radius edit-realm realm_name  
SGOS# (config radius realm_name) primary-server primary_host [primary_port]  
SGOS# (config radius realm_name) primary-server service-type type  
SGOS# (config radius realm_name) primary-server secret secret  
-or-  
SGOS# (config radius realm_name) primary-server encrypted-secret encrypted_secret
```

and optionally:

```
SGOS# (config radius realm_name) alternate-server alternate_host [alternate_port]  
SGOS# (config radius realm_name) alternate-server secret secret  
-or-  
SGOS# (config radius realm_name) alternate-server encrypted-secret  
encrypted_secret  
SGOS# (config radius realm_name) alternate-server service-type type
```

Section C: RADIUS Realm Authentication and Authorization

where:

*secret|
encrypted_secret* The shared secret (or encrypted secret) associated with the primary or alternate RADIUS server. (RADIUS secrets can be up to 64 characters long and are always case sensitive.)

The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted. If you choose to use a third-party encryption application, be sure it supports RSA encryption, OAEP padding andBase64 encoded with no newlines.

type *type* stands for the service type, which can be one of the following:

1. Login
2. Framed
3. Callback Login
4. Callback Framed
5. Outbound
6. Administrative
7. NAS Prompt
8. Authenticate Only
9. Callback NAS Prompt
10. Call Check
11. Callback Administrative

If the user record contains Check-list ServiceType attributes, then at least one of the ServiceType values must match the service-type of the RADIUS server as configured on the ProxySG.

primary_server The host for the primary RADIUS server.

primary_port The port for the primary RADIUS server. The default port is 1812.

alternate_host The host for the alternate RADIUS server.

alternate_port The port for the alternate RADIUS server. The default port is 1812.

3. To complete configuration of the RADIUS realm, enter the following commands:

```
SGOS#(config radius realm_name) timeout seconds
SGOS#(config radius realm_name) server-retry count
SGOS#(config radius realm_name) cache-duration seconds
SGOS#(config radius realm_name) case-sensitive enable | disable
SGOS#(config radius realm_name) display-name name
SGOS#(config radius realm_name) spoof-authentication none | origin | proxy
```

where:

<i>timeout</i>	<i>seconds</i>	The length of time permitted for RADIUS requests to be received before timing out. The default is 5 seconds
----------------	----------------	---

<i>server-retry</i>	<i>count</i>	The maximum number of attempts to access the server.
---------------------	--------------	--

<i>cache-duration</i>	<i>seconds</i>	The length of time that credentials should be cached for this RADIUS realm. The default is 900 seconds (15 minutes)
-----------------------	----------------	---

<i>display-name</i>	<i>name</i>	The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
---------------------	-------------	--

Section C: RADIUS Realm Authentication and Authorization

spoof-authentication none | origin
| proxy

Enables/disables the forwarding of authenticated credentials to the origin content server or for proxy authentication. You can only choose one.

- If set to *origin*, the spoofed header will be an *Authorization*: header.
- If set to *proxy*, the spoofed header will be a *Proxy-Authorization*: header.
- If set to *none*, no spoofing will be done.

Flush the entries for a realm if the spoof-authentication value is changed to ensure that the spoof-authentication value is immediately applied.

Creating the CPL

Be aware that the examples below are just part of a comprehensive authentication policy. By themselves, they are not adequate for your purposes.

Note: Refer to the *Blue Coat Content Policy Language Guide* for details about CPL and how transactions trigger the evaluation of policy file layers.

- Every RADIUS-authenticated user is allowed access the ProxySG.

```
<Proxy>
    authenticate (RADIUSRealm)
<Proxy>
    allow hasAttribute.servicetype=yes
    deny
```

Section D: Local Realm Authentication and Authorization

Section D: Local Realm Authentication and Authorization

Using a Local realm is appropriate when the network topography does not include external authentication or when you want to add users and administrators to be used by the ProxySG only.

The Local realm (you can create up to 40) uses a *Local User List*, a collection of users and groups stored locally on the ProxySG. You can create up to 50 different Local User Lists. Multiple Local realms can reference the same list at the same time, although each realm can only reference one list at a time. The default list used by the realm can be changed at any time.

This section discusses the following topics:

- "Creating a Local Realm"
- "Changing Local Realm Properties"
- "Defining the Local User List"
- "Creating the CPL"

Creating a Local Realm

To Create a Local Realm through the Management Console:

1. Select Configuration>Authentication>Local >Local Realms.

The Local Realms tab displays.

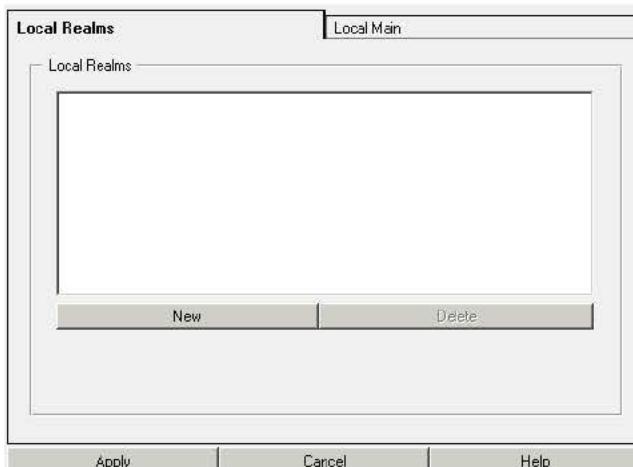


Figure 9-20: Local Realms Tab

Section D: Local Realm Authentication and Authorization

2. Click New; the Add Local Realm dialog displays.



Figure 9-21: Add Local Realm

3. In the Realm name field, enter a realm name. The name can be 32 characters long and composed of alphanumeric characters and underscores. The name must start with a letter.
4. Click OK; click Apply.

To Create a Local Realm through the CLI:

Up to 40 Local realms can be configured per ProxySG.

At the (config) command prompt, enter the following command to create a Local realm:

```
SGOS#(config) security local create-realm realm_name  
where realm_name is the name of the new Local realm.
```

Changing Local Realm Properties

Once you have created a Local realm, you can modify the properties through the Management Console or the CLI.

To Define or Change Local Realm Properties through the Management Console:

1. Select Configuration>Authentication>Local >Local Main.

The Local Main tab displays.

Section D: Local Realm Authentication and Authorization

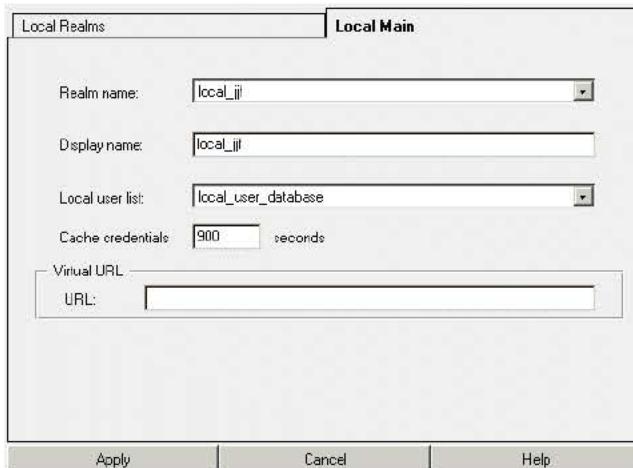


Figure 9-22: Local Main Tab

Note: You must define a Local realm (using the Local Realms tab) before attempting to set realm properties. If the message `Realms must be added in the Local Realms tab before editing this tab` is displayed in red at the bottom of this page, you do not have a Local realm defined.

2. **Display name:** The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
3. **Local User List:** Specify the local user list you want to use from the drop-down list.
4. **Specify the length of time, in seconds, that user and administrator credentials received from the Local password file should be cached.** Credentials can be cached for up to 3932100 seconds. The default is 900 seconds (15 minutes).
5. **You can specify a virtual URL based on the individual realm.** For information on using virtual URLs, see Chapter 8: “Security and Authentication” on page 203.
6. **Click Apply.**

To Define or Change Local Realm Properties through the CLI:

1. From the `(config)` prompt, enter the following commands to modify realm properties:

```
SGOS#(config) security local edit-realm realm_name
SGOS#(config local realm_name) cache-duration 600
SGOS#(config local realm_name) display-name name
SGOS#(config local realm_name) local-user-list list_name
SGOS#(config local realm_name) rename new_name
SGOS#(config local realm_name) spoof-authentication none | origin | proxy
SGOS#(config local realm_name) virtual-url url
```

Section D: Local Realm Authentication and Authorization

where:

cache-duration	seconds	The number of seconds that user and administrator credentials received from the Local password file should be cached. The default is 900 seconds (15 minutes).
display-name	name	The display name for a realm, presented to the user as part of the authentication challenge, is equivalent to the <i>display-name</i> option in the CPL authenticate action. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
local-user-list	list_name	The list you want to associate with this realm. The list must exist before it is added. The local user list is set to the default list when the realm is created. For more information on creating a local list, see "Defining the Local User List" on page 268.
rename	new_name	Allows you to change the display name of an existing realm.
spoof-authentication	none origin proxy	Enables/disables the forwarding of authenticated credentials to the origin content server or for proxy authentication. You can only choose one. <ul style="list-style-type: none"> • If set to <i>origin</i>, the spoofed header will be an Authorization: header. • If set to <i>proxy</i>, the spoofed header will be a Proxy-Authorization: header. • If set to <i>none</i>, no spoofing will be done. Flush the entries for a realm if the spoof-authentication value is changed to ensure that the spoof-authentication value is immediately applied.
virtual-url	url	The URL to redirect to when the user needs to be challenged for credentials. See Chapter 8: "Security and Authentication" on page 203 for more details.

2. (Optional) View the configuration:

```
SGOS#(config local realm_name) view
  Realm name:      local1
  Display name:    local1
  Local user list: list20
  Cache duration:  600
  Virtual URL:    10.9.87.85
```

Defining the Local User List

Defining the local user list involves the following steps:

- Create a list or customize the default list for your needs.
- Upload a user list or add users and groups through theProxySG.
- (Optional but recommended) Enhance security settings for the user list.

Section D: Local Realm Authentication and Authorization

- Associate the list with the realm through CPL.

Creating a Local User List

The user list *local_user_database* is created on a new system or after an upgrade. It is empty on a new system. If a password file existed on the ProxySG before an upgrade, then the list contains all users and groups from the password file; the initial default user list is *local_user_database*. If a new user list is created, the default can be changed to point to it instead by invoking the `security local-user-list default list listname` command. You can create up to 50 new lists with 10,000 users each.

Lists can be uploaded or you can directly edit lists through the CLI. If you want to upload a list, it must be created as a text file using the *.htpasswd* format of the ProxySG.

Each user entry in the list consists of:

- User name
- List of groups
- Hashed password
- Enabled/disabled boolean searches

A list that has been populated looks like this:

```
SGOS# (config) security local-user-list edit listname
SGOS# (config local-user-list listname) view
list20
Lockout parameters:
  Max failed attempts: 60
  Lockout duration:    3600
  Reset interval:      7200
Users:
admin1
  Hashed Password: $1$TvEzpZE$Z2A/OuJU3w5LnEONDHkmg.
  Enabled: true
  Groups:
    group1
admin2
  Hashed Password: $1$sKJvNB3r$xsInBU./2hhBz6xDAHpND.
  Enabled: true
  Groups:
    group1
    group2
admin3
  Hashed Password: $1$duuCUT30$keSdIkZVS4RyFz47G78X20
  Enabled: true
  Groups:
    group2
Groups:
  group1
  group2
```

Section D: Local Realm Authentication and Authorization

To create a new empty local user list:

```
SGOS# (config) security local-user-list create listname
```

User Name

The user name must be case-sensitively unique, and can be no more than 64 characters long. All characters are valid, except for a colon (:).

A new local user is enabled by default and has an empty password.

List of Groups

You cannot add a user to a group unless the group has previously been created in the list. The group name must be case-sensitively unique, and can be no more than 64 characters long. All characters are valid, except for colon (:).

The groups can be created in the list; however, their user permissions are defined through policies only.

Hashed Password

The hashed password must be a valid UNIX DES or MD5 password whose clear-text equivalent cannot be more than 64 characters long.

To populate the local user list using an off-box .htpasswd file, continue with the next section. To populate the local user list using the ProxySG CLI, go to "Creating a Local User List" on page 269.

How to Populate a List using the .htpasswd File

To add users to a text file in .htpasswd format, enter the following UNIX htpasswd command:

```
prompt> htpasswd [-c] .htpasswd username
```

The -c option creates a new .htpasswd file and should only be used for the very first .htpasswd command. You can overwrite any existing .htpasswd file by using the -c option.

After entering this command, you are prompted to enter a password for the user identified by *username*. The entered password is hashed and added to the user entry in the text file. If the -m option is specified, the password is hashed using MD5; otherwise, UNIX DES is used

Important: Because the -c option overwrites the existing file, do not use the option if you are adding users to an existing .htpasswd file.

Once you have added the users to the .htpasswd file, you can manually edit the file to add user groups. When the .htpasswd file is complete, it should have the following format:

```
user:encrypted_password:group1,group2,...  
user:encrypted_password:group1,group2,...
```

Section D: Local Realm Authentication and Authorization

Note: You can also modify the users and groups once they are loaded on the ProxySG. To modify the list once it is on the ProxySG, see "Populating a Local User List through the ProxySG" on page 271.

How to Upload the .htpasswd File

When the .htpasswd file is uploaded, the entries from it either replace all entries in the default local user list or append to the entries in the default local user list. One default local user list is specified on the ProxySG.

To set the default local user list use the command `security local-user-list default list listname`. The list specified must exist.

To specify that the uploaded .htpasswd file replace all existing user entries in the default list, enter `security local-user-list default append-to-default disable` before uploading the .htpasswd file.

To specify that the .htpasswd file entries should be appended to the default list instead, enter `security local-user-list default append-to-default enable`.

Uploading the .htpasswd File:

The .htpasswd file is loaded onto the ProxySG with a Perl script found at:

`http://download.bluecoat.com/release/tools/set_auth.zip`

Unzip the file, which contains the `set_auth.pl` script.

Note: To use the `set_auth.pl` script, you must have Perl binaries on the system where the script is running.

To Load the .htpasswd File:

`prompt> set_auth.pl username password path_to_.htpasswd_file_on_local_machine ip_address_of_the_ProxySG`

where `username` and `password` are valid administrator credentials for the ProxySG.

Populating a Local User List through the ProxySG

You can populate a local user list from scratch or modify a local user list that was populated by loading an .htpasswd file.

To Create a New, Empty Local User List:

`SGOS#(config) security local-user-list create listname`

To Modify an Existing Local User List (Can be Empty or Contain Users):

- From the `(config)` prompt, enter:

`SGOS#(config) security local-user-list edit listname`
`SGOS#(config local-user-list listname)`

Section D: Local Realm Authentication and Authorization

2. To add users and groups to the list, enter the following commands, beginning with groups, since they must exist before you can add them to a user account.

```
SGOS#(config local-user-list listname) group create group1
ok
SGOS#(config local-user-list listname) group create group2
ok
SGOS#(config local-user-list listname) group create group3
ok
SGOS#(config local-user-list listname) user create username
```

3. Add the user information to the user account.

```
SGOS#(config local-user-list listname) user edit username
SGOS#(config local-user-list listname username) group add groupname1
SGOS#(config local-user-list listname username) group add groupname2
SGOS#(config local-user-list listname username) password password
-or-
SGOS#(config local-user-list listname username) hashed-password hashed-password
```

Note: If you enter a clear-text password, the ProxySG hashes the password. If you enter a hashed password, the ProxySG does not hash it again.

4. (Optional) The user account is enabled by default. To disable a user account:

```
SGOS#(config local-user-list listname username) disable
ok
```

5. Repeat the above steps for each user you want added to the list.

To View the Results of an Individual User Account:

Remain in the user account submode and enter the following command:

```
SGOS#(config local-user-list listname username) view
admin1
Hashed Password: $1$TvEzpZE$Z2A/OuJU3w5LnEONDHkmg.
Enabled: true
Failed Logins: 6
Groups:
group1
```

Note: If a user has no failed logins, the statistic does not display.

To View the Users in the Entire List:

Exit the user account submode and enter:

```
SGOS#(config local-user-list listname username) exit
SGOS#(config local-user-list listname) view
list20
Lockout parameters:
Max failed attempts: 60
Lockout duration: 3600
```

Section D: Local Realm Authentication and Authorization

```

Reset interval:      7200
Users:
admin1
  Hashed Password: $1$TvEzpZE$Z2A/OuJU3w5LnEONDHkmg.
  Enabled: true
  Groups:
    group1
admin2
  Hashed Password: $1$sKJvNB3r$xsInBU./2hhBz6xDAHpND.
  Enabled: true
  Groups:
    group1
    group2
admin3
  Hashed Password: $1$duuCuT30$keSdIkZVS4RyFz47G78X20
  Enabled: true
  Groups:
    group2
Groups:
  group1
  group2

```

To View all the Lists on the ProxySG:

```

SGOS#(config) show security local-user-list
Default List: local_user_database
Append users loaded from file to default list: false
local_user_database
Lockout parameters:
  Max failed attempts: 60
  Lockout duration:     3600
  Reset interval:       7200
  Users:
  Groups:

test1
Lockout parameters:
  Max failed attempts: 60
  Lockout duration:     3600
  Reset interval:       7200
  Users:
  Groups:

```

To Delete Groups Associated with a User:

```
SGOS#(config local-user-list listname username) group remove group_name
```

To Delete Users from a List:

```

SGOS#(config local-user-list listname) user delete username
This will permanently delete the object. Proceed with deletion?
(y or n) y
ok

```

Section D: Local Realm Authentication and Authorization

To Delete all Users from a List:

```
SGOS# (config local-user-list listname) user clear
ok
```

The groups remain but have no users.

To Delete all Groups from a List:

```
SGOS# (config local-user-list listname) group clear
ok
```

The users remain but do not belong to any groups.

Enhancing Security Settings for the Local User List

You can configure a local user database so that each user account is automatically disabled if too many failed login attempts occur for the account in too short a period, indicating a brute-force password attack on the ProxySG. The security settings are available through the CLI only.

Available security settings are:

- Maximum failed attempts: The maximum number of failed password attempts allowed for an account. When this threshold is reached, the account will be disabled (locked). If this is zero, there is no limit. The default is 60 attempts.
- Lockout duration: The time after which a locked account will be re-enabled. If this is zero, the account will not automatically re-enable, but will instead stay locked until manually enabled. The default is 3600 seconds (one hour).
- Reset interval: The time after which a failed password count will be reset after the last failed password attempt. If this is zero, the failed password count will be reset only when the account is enabled or when its password is changed. The default is 7200 seconds (two hours).

These values are enabled by default on the system for all user account lists. You can change the defaults for each list that exists on the system.

To Change the Security Settings for a Specific User Account List

1. Enter the following commands from the (config) prompt:

```
SGOS# (config) security local-user-list edit listname
SGOS# (config local-user-list listname) lockout-duration seconds
SGOS# (config local-user-list listname) max-failed-attempts attempts
SGOS# (config local-user-list listname) reset-interval seconds
```

2. (Optional) View the settings:

```
SGOS# (config local-user-list listname) view
listname
Lockout parameters:
  Max failed attempts: 45
  Lockout duration:    3600
  Reset interval:      0
```

Section D: Local Realm Authentication and Authorization

3. (Optional) To disable any of these settings:

```
SGOS# (config local-user-list listname) no [lockout-duration |  
max-failed-attempts | reset-interval]
```

Creating the CPL

Be aware that the examples below are just part of a comprehensive authentication policy. By themselves, they are not adequate for your purposes. (The default policy in these examples is deny.)

Note: Refer to the *Blue Coat Content Policy Language Guide* for details about CPL and how transactions trigger the evaluation of policy file layers.

- Every Local-authenticated user is allowed access the ProxySG.

```
<Proxy>  
    authenticate (LocalRealm)
```

- Group membership is the determining factor in granting access to the ProxySG.

```
<Proxy>  
    authenticate (LocalRealm)  
<Proxy>  
    group="group1" allow
```

- A subnet definition determines the members of a group, in this case, members of the Human Resources department.

```
<Proxy>  
    authenticate (LocalRealm)  
<Proxy>  
    Define subnet HRSUBNET  
        192.168.0.0/16  
        10.0.0.0/24  
    End subnet HRSUBNET  
    [Rule] client_address=HRSUBNET  
        url.domain=monster.com  
        url.domain=hotjobs.com  
        deny  
    .  
    .  
    .  
    [Rule]  
        deny
```

Section E: Certificate Realm Authentication

Section E: Certificate Realm Authentication

Certificate realms are used to authenticate users. If the users are members of an LDAP or Local group, the Certificate Realm can also forward the user credentials to the specified authorization realm, which determines the user's authorization (permissions).

This section discusses the following topics:

- "How Certificate Realm Works"
- "Creating a Certificate Realm"
- "Defining a Certificate Realm"
- "Defining Certificate Realm General Properties"
- "Revoking User Certificates"

How Certificate Realm Works

Once an SSL session has been established, the user is asked to select the certificate to send to the ProxySG. If the certificate was signed by a Certificate Signing Authority that the ProxySG trusts, including itself, then the user is considered authenticated. The user name for the user is the one extracted from the certificate during authentication.

At this point the user is authenticated. If an authorization realm has been specified, such as LDAP or Local, the certificate realm then passes the user name to the specified authorization realm, which figures out which groups the user belongs to.

Note: If you authenticate with a certificate realm, you cannot also challenge for a password.

Certificate realms do not require an authorization realm. If no authorization realm is configured, the user is not a member of any group. The effect this has on the user depends on the authorization policy. If the policy does not make any decisions based on groups, then you do not need to specify an authorization realm. Also, if your policy is such that it works as desired when all certificate realm-authenticated users are not in any group, you do not have to specify an authorization realm.

To use a Certificate Realm, you must:

- Configure SSL between the client and ProxySG (for more information, see "SSL Between the Client and the ProxySG" on page 222)
- Enable verify-client on the HTTPS service that will be used (for more information, see "HTTPS" on page 127).
- Verify that the certificate authority that signed the client's certificates is in the ProxySG *trusted* list.

Creating a Certificate Realm

To Create a Certificate Realm through the Management Console:

1. Select Configuration>Authentication>Certificate>Certificate Realms.

Section E: Certificate Realm Authentication

The Certificate Realms tab displays.

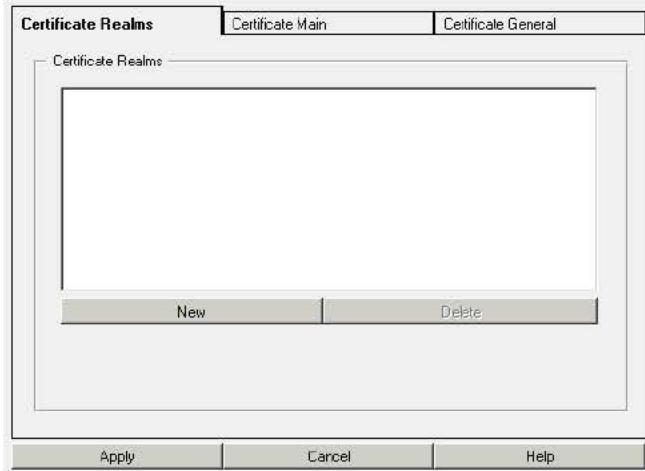


Figure 9-23: Certificate Realms Tab

2. Click New; the Add Certificate Realm dialog displays.



Figure 9-24: Add Certificate Realm

3. In the Realm name field, enter a realm name. The name can be 32 characters long and composed of alphanumeric characters and underscores. The name *must* start with a letter.
4. Click OK; click Apply.

To Create a Certificate Realm through the CLI:

Up to 40 Certificate realms can be configured per ProxySG.

At the (config) command prompt, enter the following command to create a Certificate realm:

```
SGOS# (config) security certificate create-realm realm_name
where realm_name is the name of the new Certificate realm.
```

Section E: Certificate Realm Authentication

Defining a Certificate Realm

To Define Certificate Authentication Properties through the Management Console

Note: You can also define certificate authentication properties through the CLI. For information, see "To Create and Define a Certificate Realm through the CLI:" on page 280:

1. Select Configuration>Authentication>Certificate>Certificate Main.

The Certificate Main tab displays.

Certificate Realms	Certificate Main	Certificate General
Realm name:	certificate_if	
Authorization Realm Name:	None	
Username attribute:	CN	
Container attribute list:		
<input checked="" type="checkbox"/> Append Base DN		
Base DN:		
Cache credentials:	900	seconds

Buttons at the bottom: Apply, Cancel, Help

Figure 9-25: Certificate Main Tab

2. From the Realm Name drop-down list, select the Certificate realm for which you want to change realm properties.

Note: You must have defined at least one Certificate realm (using the Certificate Realms tab) before attempting to set Certificate realm properties. If the message `Realms must be added in the Certificate Realms tab before editing this tab` is displayed in red at the bottom of this page, you do not currently have any Certificate realms defined.

3. (Optional) From the Authorization Realm Name drop-down list, select the LDAP or Local realm you want to use to authorize users.
4. From the username attribute field, enter the attribute that specifies the common name in the subject of the certificate. CN is the default.
5. (Optional, if you are configuring a Certificate realm with LDAP authorization) Enter the list of attributes (the container attribute field) that should be used to construct the user's distinguished name.

For example, `$(OU) $(O)` substitutes the OU and O fields from the certificate.

Section E: Certificate Realm Authentication

6. (Optional, if you are configuring a Certificate realm with LDAP authorization) Select or deselect Append Base DN.
7. (Optional, if you are configuring a Certificate realm with LDAP authorization) Enter the Base DN where the search starts. If no BASE DN is specified and Append Base DN is enabled, the first Base DN defined in the LDAP realm used for authorization is appended.
8. Cache credentials: Specify the length of time, in seconds, that user and administrator credentials received from the Local password file should be cached. Credentials can be cached for up to 3932100 seconds. The default is 900 seconds (15 minutes).

Defining Certificate Realm General Properties

The Certificate General tab allows you to specify the display name and a virtual URL.

To Configure Certificate Realm General Settings through the Management Console:

1. Select Configuration>Authentication>Certificate>Certificate General.

The Certificate General tab displays.

Certificate Realms	Certificate Main	Certificate General
Realm name:	certificate	
Display name:	certificate	
Virtual URL	URL:	
<input type="button" value="Apply"/> <input type="button" value="Cancel"/> <input type="button" value="Help"/>		

Figure 9-26: Certificate General Tab

2. From the Realm name drop-down list, select the Certificate realm for which to change properties.

Note: You must have defined at least one Certificate realm (using the Certificate Realms tab) before attempting to set Certificate general properties. If the message Realms must be added in the Certificate Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any Certificate realms defined.

Section E: Certificate Realm Authentication

3. If needed, change the Certificate realm display name. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
4. You can specify a virtual URL based on the individual realm. For more information on the virtual URL, see Chapter 8: "Security and Authentication" on page 203.
5. Click **Apply**.

To Create and Define a Certificate Realm through the CLI:

1. At the `(config)` prompt:

```
SGOS# (config) security certificate create-realm realm_name
```

2. To define an authorization realm for the Certificate realm configuration for the realm you just created, enter the following commands:

```
SGOS# (config) security certificate edit-realm realm_name
SGOS# (config certificate realm_name) authorization {append-base-dn {enable | disable | dn dn_to_append} | container-attr-list list | realm-name realm | username-attribute attribute}
```

where:

<code>append-base-dn</code>	<code>enable</code> <code>disable</code> <code>dn</code> <code>dn_to_append</code>	Used only if an LDAP authorization realm is present.
<code>container-attr-list</code>	<code>list</code>	Used only if an LDAP authorization realm is present. If the CLI contains spaces, quotes must be used, as in "ou=Research and Development, ou=Sales, o=Blue Coat".
<code>realm-name</code>	<code>realm_name</code>	The name of the LDAP or Local realm that will be used for authorization. The realm name must already exist.
<code>username-attribute</code>	<code>attribute</code>	The attribute that specifies the common name in the subject of the certificate. CN is the default.

3. Enter the following commands to modify Certificate realm properties:

```
SGOS# (config certificate realm_name) cache-duration 600
SGOS# (config certificate new_realm_name) virtual-url cfauth.com
SGOS# (config certificate new_realm_name) display-name display_name
```

where:

<code>cache-duration</code>	<code>seconds</code>	The number of seconds that user and administrator credentials received from the Credential realm should be cached. The default is 900 seconds (15 minutes).
<code>virtual-url</code>	<code>url</code>	The URL to redirect to when the user needs to be challenged for credentials. See Chapter 8: "Security and Authentication" on page 203 for more details.
<code>display-name</code>	<code>display_name</code>	The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.

Section E: Certificate Realm Authentication

4. (Optional) View the results:

```
SGOS# (config certificate certificate-name) view
Realm name:           certificate-name
Display name:         certificate-name
Cache duration:       900
Virtual URL:          cfauth.com
Authorization realm:  ldap-realm
Username attribute:   cn
Container attr. list: ou=Sales,ou=Manufacturing
Append DN:            enabled
Base DN:
```

Revoking User Certificates

Using policy you can revoke certain certificates by writing policy that denies access to users who have authenticated with a certificate you want to revoke. You must maintain this list on the ProxySG; it is not updated automatically.

A certificate is identified by its issuer (the Certificate Signing Authority that signed it) and its serial number, which is unique to that CA.

Using that information, you can use the following strings to create a policy to revoke user certificates:

- `user.x509.serialNumber`—This is a string representation of the certificate's serial number in HEX. The string is always an even number of characters long, so if the number needs an odd number of characters to represent in hex, there is a leading zero. Comparisons are case insensitive.
- `user.x509.issuer`—This is an RFC2253 LDAP DN. Comparisons are case sensitive.
- (optional) `user.x509.subject`: This is an RFC2253 LDAP DN. Comparisons are case sensitive.

Example

If you have only one Certificate Signing Authority signing user certificates, you do not need to test the issuer. In the <Proxy> layer of the Local Policy file:

```
<proxy>
  deny user.x509.serialnumber=11
  deny user.x509.serialNumber=0F
```

If you have multiple Certificate Signing Authorities, test both the issuer and the serial number. In the <Proxy> layer of the Local Policy file:

```
<proxy>
  deny user.x509.issuer="Email=name,CN=name,OU=name,O=company,L=city,ST=state or
  province,C=country" user.x509.serialnumber=11\
  deny user.x509.issuer="CN=name,OU=name,O=company, L=city,ST=state or
  province,C=country" \
  deny user.x509.serialnumber=2CB06E9F0000000000B
```

Section E: Certificate Realm Authentication

Creating the Certificate Authorization Policy

When you complete Certificate realm configuration, you can create CPL policies. Be aware that the examples below are just part of a comprehensive authentication policy. By themselves, they are not adequate.

Note: Refer to the *Blue Coat Content Policy Language Guide* for details about CPL and how transactions trigger the evaluation of policy file <Proxy> and other layers.

Be aware that the default policy condition for these examples is *allow*. On new SGOS3.x systems, the default policy condition is *deny*.

- Every Certificate realm authenticated user is allowed access the ProxySG.

```
<Proxy>
    authenticate (CertificateRealm)
```

- A subnet definition determines the members of a group, in this case, members of the Human Resources department. (They are allowed access to the two URLs listed. Everyone else is denied permission.)

```
<Proxy>
    authenticate (CertificateRealm)
<Proxy>
    Define subnet HRSUBNET
        192.168.0.0/16
        10.0.0.0/24
    End subnet HRSUBNET
    [Rule] client_address=HRSUBNET
        url.domain=monster.com
        url.domain=hotjobs.com
        deny
    .
    .
    .
    [Rule]
        deny
```

Tips

If you use a certificate realm and see an error message similar to the following

```
Realm configuration error for realm "cert": connection is not SSL .
```

This means that certificate authentication was requested for a transaction, but the transaction was not done on an SSL connection, so no certificate was available.

This can happen in three ways:

- The authenticate mode is either `origin-IP-redirect/origin-cookie-redirect` or `origin-IP/origin-cookie`, but the virtual URL does not have an https: scheme. This is likely if authentication through a certificate realm is selected with no other configuration, since the default configuration does not use SSL for the virtual URL.

Section E: Certificate Realm Authentication

- In a server accelerator deployment, the authenticate mode is origin and the transaction is on a non-SSL port.
- The authenticate mode is `origin-IP-redirect/origin-cookie-redirect`, the user has authenticated, the credential cache entry has expired, and the next operation is a POST or PUT from a browser that does not handle 307 redirects (that is, from a browser other than Internet Explorer). The workaround is to visit another URL to refresh the credential cache entry and then try the POST again.

Section F: Sequence Realm Authentication

Section F: Sequence Realm Authentication

Once a realm is configured, you can associate it with other realms to allow Blue Coat to search for the proper authentication credentials for a specific user. That is, if the credentials are not acceptable to the first realm, they are sent to the second, and so on until a match is found or all the realms are exhausted. This is called *sequencing*.

This section discusses the following topics:

- "Adding Realms to a Sequence Realm""
- "Creating a Sequence Realm"

Adding Realms to a Sequence Realm"

Keep in mind the following rules for using realm sequences:

- Ensure the realms to be added to the sequence are customized to your needs. Check each realm to be sure that the current values are correct. For NTLM, verify that the Allow Basic Credentials checkbox is set correctly.
- All realms in the realm sequence must exist and cannot be deleted or renamed while the realm sequence references them.
- Only one NTLM realm is allowed in a realm sequence.
- If an NTLM realm is in a realm sequence, it must be either the first or last realm in the list.
- If an NTLM realm is in a realm sequence and the NTLM realm does not support Basic credentials, the realm must be the first realm in the sequence and try NTLM authentication once must be enabled.
- Multiple BASIC realms are allowed.
- Connection-based realms, such as Certificate, are not allowed in the realm sequence.
- A realm can only exist once in a particular realm sequence.
- A realm sequence cannot have another realm sequence as a member.
- If a realm is down, an exception page is returned. Authentication is not tried against the other later realms in the sequence.

Creating a Sequence Realm

To Create a Sequence Realm through the Management Console:

1. Select Configuration>Authentication>Sequences>Sequence Realms.

The Sequence Realms tab displays.

Section F: Sequence Realm Authentication

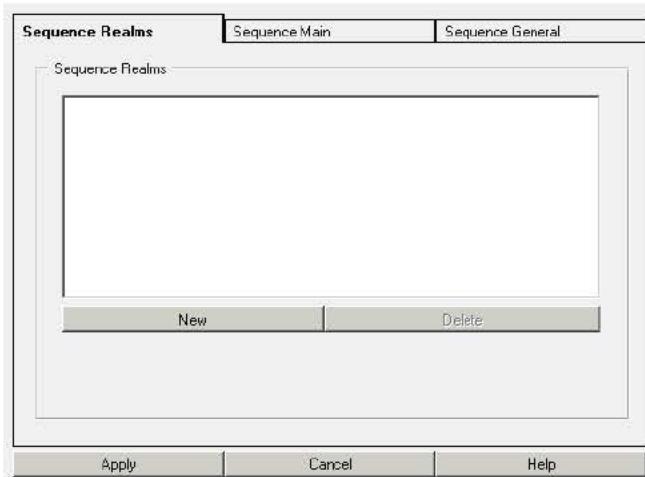


Figure 9-27: Sequence Realms Tab

2. Click New; the Add Sequence Realm dialog displays.

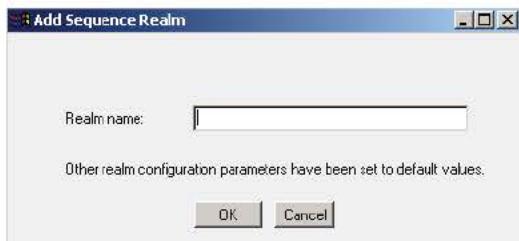


Figure 9-28: Add Sequence Realm

3. In the Realm name, enter a realm name. The name can be 32 characters long and composed of alphanumeric characters and underscores. The name must start with a letter.
4. Click OK.
5. Click Apply.

To Create a Sequence Realm through the CLI:

Up to 40 Sequence realms can be configured per ProxySG.

At the (config) command prompt, enter the following command to create a Certificate realm:

```
SGOS#(config) security sequence create-realm realm_name
where realm_name is the name of the new Sequence realm.
```

Adding Realms to a Sequence Realm

To Add Realms to a Sequence Realm through the Management Console:

1. Select Configuration>Authentication>Sequences>Sequence Main.

Section F: Sequence Realm Authentication

The Sequences tab displays with the Sequence realm that you want to add realms to.

Note: You must have defined at least one sequence realm (using the Sequence Realms tab) before attempting to set Sequence general properties. If the message Realms must be added in the Sequence Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any Sequence realms defined.

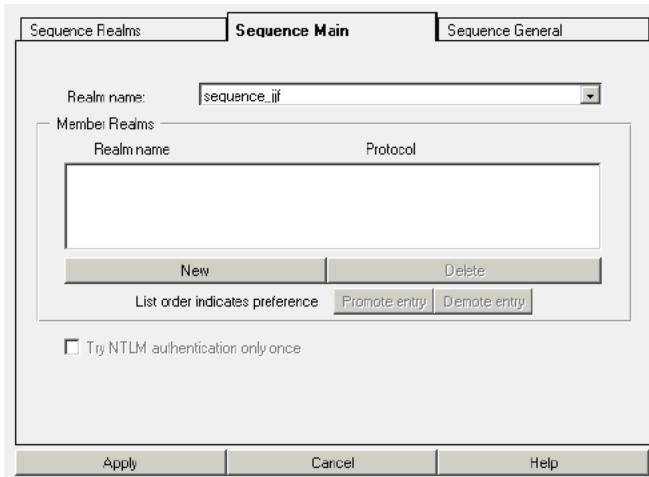


Figure 9-29: Sequence Main Tab

2. Click New to add an existing realm to the realm sequence from the drop-down list. Remember that each realm can be used only once in a realm sequence.



Figure 9-30: Add Member Realm

3. From the drop-down list, select the Sequence realm you wanted added to the realm sequence.
4. Click OK.

You are returned to the main Sequences menu.

Section F: Sequence Realm Authentication

5. Click **Apply**.
6. Repeat from step 2 until you have added all necessary realms.
7. To change the order that the realms are checked, use the promote/demote buttons. Note that when you add an NTLM realm, it is placed first in the list and you can allow the realm sequence to try NTLM authentication only once. If you demote the NTLM entry, it becomes last in the sequence and the default of checking NTLM multiple times is enabled.
8. Click **Apply**.

To Add Authentication Realms to a Sequence Realm through the CLI:

1. From the (config) prompt, add existing realms to the new specified sequence realm name:

```
SGOS#(config) security sequence edit-realm realm_sequence_name
SGOS#(config sequence realm_sequence_name) realm add realm_name
```

2. Repeat the **realm add realm_name** command until all necessary realms have been added.
3. (Optional) Give the new sequence realm a display name. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.

```
SGOS#(config sequence realm_sequence_name) display-name display_name
```

Defining Sequence Realm General Properties

The Sequence General tab allows you to specify the display name and a virtual URL.

To Manage Authentication Realms in a Sequence Realm through the Management Console:

1. Select Configuration>Authentication>Sequences>Sequence General.

The Sequence General tab displays.

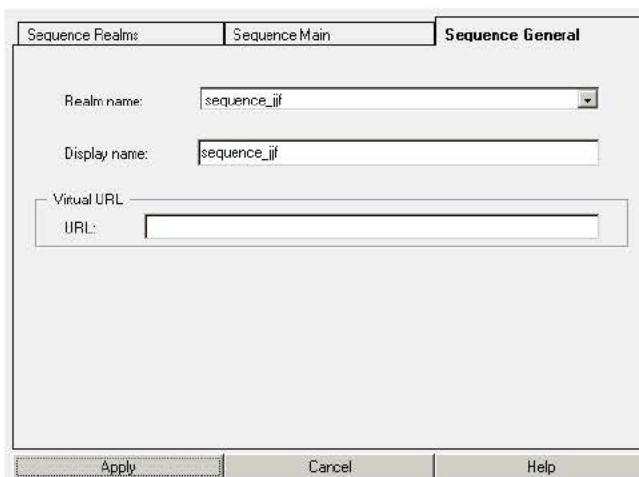


Figure 9-31: Sequence General Tab

Section F: Sequence Realm Authentication

2. From the Realm name drop-down list, select the Sequence realm for which you want to change properties.

Note: You must have defined at least one sequence realm (using the Sequence Realms tab) before attempting to set Sequence general properties. If the message `Realms must be added in the Sequence Realms tab before editing this tab` is displayed in red at the bottom of this page, you do not currently have any Sequence realms defined.

3. If needed, change the Sequence realm display name. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
4. You can specify a virtual URL based on the individual realm sequence. For more information on the virtual URL, see Chapter 8: "Security and Authentication" on page 203.
5. Click **Apply**.

To Manage Authentication Realms in a Sequence Realm through the CLI:

1. When you add an NTLM realm it is placed first in the list, and you have the option of allowing the realm sequence to try NTLM authentication only once. If you demote the NTLM entry, it becomes last in the sequence and the default of checking NTLM multiple times is enabled.

```
SGOS#(config sequence realm_sequence_name) ntlm-only-once-enable  
% An NTLM realm must be the first member of the realm sequence before specifying  
to try NTLM authentication only once  
SGOS#(config sequence realm_sequence_name) realm promote ntlm1  
SGOS#(config sequence realm_sequence_name) ntlm-only-once-enable
```

2. (Optional) You can specify a virtual URL based on the individual realm sequence. For information on the virtual URL, see "Security and Authentication" on page 203.

```
SGOS#(config sequence realm_sequence_name) virtual-url 10.25.36.47  
ok
```

3. View the configuration.

- a. To view the configuration of the current realm sequence, remain in the submode and enter:

```
SGOS#(config sequence realm_sequence_name) view  
Realm name: seq1  
Display name:seq1  
Virtual URL: 10.25.36.47  
Try NTLM only once: yes  
Member realms:  
radius1  
test  
ldap1
```

- b. To view the configurations of all realm-sequence-names, exit the `edit-realm` submode, and enter:

Section F: Sequence Realm Authentication

```
SGOS#(config sequence realm_sequence_name) exit
SGOS#(config) security sequence view
Realm name:           seq1
Display name:seq1
Virtual URL:          10.25.36.47
Try NTLM only once:   yes
Member realms:
  ntlm1
  radius1
  test
  ldap1
Realm name:           seq2
Virtual URL:
Try NTLM only once:   no
Member realms:
  ldap1
  ldap2
```

Section G: Netegrity SiteMinder

Section G: Netegrity SiteMinder

The ProxySG can be configured to consult a SiteMinder policy server for authentication and session management decisions. This requires that a SiteMinder realm be configured on the ProxySG and policy written to use that realm for authentication.

Important: Use of this feature is subject to obtaining the appropriate license. The license check is on the ProxySG.

Access to the SiteMinder policy server is done through the Blue Coat Authentication and Authorization Agent (BCAAA), which must be installed on a Windows 2000 system or higher with access to the SiteMinder policy servers.

Understanding SiteMinder Interaction with Blue Coat

Within the SiteMinder system, BCAA acts as a custom Web agent. It communicates with the SiteMinder policy server to authenticate the user and to obtain a SiteMinder session token, response attribute information, and group membership information.

Custom header and cookie response attributes associated with OnAuthAccept and OnAccessAccept attributes are obtained from the policy server and forwarded to the ProxySG. They can (as an option) be included in requests forwarded by the ProxySG.

Within the ProxySG system, BCAA acts as its agent to communicate with the SiteMinder server. The ProxySG provides the user information to be validated to BCAA, and receives the session token and other information from BCAA.

Each ProxySG SiteMinder realm used causes the creation of a BCAA process on the Windows host computer running BCAA. A single host computer can support multiple ProxySG realms (from the same or different ProxySG Appliances); the number depends on the capacity of the BCAA host computer and the amount of activity in the realms.

Note: The BCAA service is not supported on Solaris in this release. However, Blue Coat can communicate with SiteMinder, regardless of the system it runs on.

Configuration of the ProxySG SiteMinder realm must be coordinated with configuration of the SiteMinder policy server. Each must be configured to be aware of the other. In addition, certain SiteMinder responses must be configured so that BCAA gets the information the ProxySG needs.

Configuring the SiteMinder Policy Server

Note: Blue Coat assumes you are familiar with configuration of SiteMinder policy servers and Web agents.

Since BCAA is a Web agent in the SiteMinder system, it must be configured on the SiteMinder policy server. Configuration of BCAA on the host computer is not required; the agent obtains its configuration information from the ProxySG.

Section G: Netegrity SiteMinder

A suitable Web agent must be created and configured on the SiteMinder server. This must be configured to support 4.x agents, and a shared secret must be chosen and entered on the server (it must also be entered in the ProxySG SiteMinder realm configuration).

SiteMinder protects resources identified by URLs. A ProxySG realm is associated with a single protected resource. This could be an already existing resource on a SiteMinder server, (typical for a reverse proxy arrangement) or it could be a resource created specifically to protect access to ProxySG services (typical for a forward proxy).

Important: The request URL is not sent to the SiteMinder policy server as the requested resource; the requested resource is the entire ProxySG realm. Access control of individual URLs is done on the ProxySG using CPL or VPM.

The SiteMinder realm that controls the protected resource must be configured with a compatible authentication scheme. The supported schemes are Basic (in clear and over SSL), Forms (in clear and over SSL), and X.509 certificates. Configure the SiteMinder realm with one of these authentication schemes.

Note: Only the following X.509 Certificates are supported: X.509 Client Cert Template, X.509 Client Cert and Basic Template, and X.509 Client Cert and Form Template.

ProxySG requires information about the authenticated user to be returned as a SiteMinder response. The responses should be sent by an `OnAuthAccept` rule used in the policy that controls the protected resource.

The responses must include the following:

- A Web-Agent-HTTP-Header-variable named `BCSI_USERNAME`. It must be a user attribute; the value of the response must be the simple user name of the authenticated user. For example, with an LDAP directory this might be the value of the `cn` attribute or the `uid` attribute.
- A Web-Agent-HTTP-Header-variable named `BCSI_GROUPS`. It must be a user attribute and the value of the response must be `SM_USERGROUPS`.

Note that if the policy server returns an LDAP FQDN as part of the authentication response, the ProxySG will use that LDAP FQDN as the FQDN of the user.

Once the SiteMinder agent object, configuration, realm, rules, responses and policy have been defined, the ProxySG can be configured.

Additional SiteMinder Configuration Notes

Note: Additional configuration might be needed on the SiteMinder server depending on specific features being used.

- If using single-sign-on (SSO) with off-box redirection (such as to a forms login page), the forms page must be processed by a 5.x or later Web Agent, and that agent must be configured with `fcccompatmode=no`. Note that this precludes that agent from doing SSO with 4.x agents.

Section G: Netegrity SiteMinder

- For SSO to work with other Web agents, the other agents must have the `AcceptTPCookie=YES` as part of their configuration. This is described in the SiteMinder documentation.
- Blue Coat does not extract the issuerDN from X.509 certificates in the same way as the SiteMinder agent. Thus, a separate certificate mapping might be needed for the SGOS agent and the SiteMinder agents.

For example, the following was added to the SiteMinder policy server certificate mappings:

```
CN=Waterloo Authentication and Security Team,OU=Waterloo R&D, O=Blue Coat\,
Inc., L=Waterloo, ST=ON, C=CA
```

- In order to use off-box redirection (such as an SSO realm), all agents involved must have the setting `EncryptAgentName=no` in their configurations.
- The ProxySG Appliance's credential cache only caches the user's authentication information for the smaller of the time-to-live (TTL) configured on the ProxySG and the session TTL configured on the SiteMinder policy server.

Note: Credential caching is applicable only for authentication modes involving surrogates.

Configuring the ProxySG Realm

The ProxySG realm must be configured so that it can:

- Find the Blue Coat agent(s) that will act on its behalf (hostname or IP address, port, SSL options, and the like).
- Provide BCAAA with the information necessary to allow it to identify itself as a Web agent (agent name, shared secret).
- Provide BCAAA with the information that allows it to find the SiteMinder policy server (IP address, ports, connection information.)
- Provide BCAAA with the information that it needs to do authentication and collect authorization information (protected resource name), and general options (server fail-over and off-box redirection)

For more information on configuring the ProxySG SiteMinder realm, see "Creating a SiteMinder Realm" on page 293.

Note: All ProxySG and agent configuration is done on the ProxySG. The ProxySG sends the necessary information to BCAAA when it establishes communication.

Participating in a Single Sign-On (SSO) Scheme

The ProxySG can participate in SSO with other systems that use the same SiteMinder policy server. Users must supply their authentication credentials only once to any of the systems participating. Participating in SSO is not a requirement, the Proxy SG can use the SiteMinder realm as an ordinary realm.

Section G: Netegrity SiteMinder

When using SSO with SiteMinder, the SSO token is carried in a cookie (SMSESSION). This cookie is set in the browser by the first system that authenticates the user; other systems obtain authentication information from the cookie and so do not have to challenge the user for credentials. The ProxySG sets the SMSESSION cookie if it is the first system to authenticate a user, and authenticates the user based on the cookie if the cookie is present.

Since the SSO information is carried in a cookie, all the servers participating must be in the same cookie domain, including the ProxySG. This imposes restrictions on the `authenticate.mode()` used on the ProxySG.

- A reverse proxy can use any `origin` mode.
- A forward proxy must use one of the `origin-redirect` modes (such as `origin-cookie-redirect`). Note that, when using `origin-*-redirect` modes, the virtual URL's hostname must be in the same cookie domain as the other systems. It cannot be an IP address and the default `www.cfauth.com` does not work either.

When using `origin-*-redirect`, the SSO cookie is automatically set in an appropriate response after the ProxySG authenticates the user. When using `origin` mode (in a reverse proxy), setting this cookie must be explicitly specified by the administrator. The policy substitution variable `$({x-agent-sso-cookie})` expands to the appropriate value of the `set-cookie: header`.

Avoiding ProxySG Challenges

In some SiteMinder deployments all credential challenges are issued by a central authentication service (typically a Web server that challenges through a form). Protected services do not challenge and process request credentials; instead, they work entirely with the SSO token. If the request does not include an SSO token, or the SSO token is not acceptable, the request is redirected to the central service, where authentication occurs. Once authentication is complete, the request is redirected to the original resource with a response that sets the SSO token.

If the SiteMinder policy server is configured to use a forms-based authentication scheme, the above happens automatically. However, in this case, the ProxySG realm can be configured to redirect to an off-box authentication service always. The URL of the service is configured in the scheme definition on the SiteMinder policy server. The ProxySG realm is then configured with `always-redirect-offbox` enabled.

Note that the ProxySG must not attempt to authenticate a request for the off-box authentication URL. If necessary, `authenticate(no)` can be used in policy to prevent this.

Creating a SiteMinder Realm

To Create a SiteMinder Realm through the Management Console:

1. Select Configuration>Authentication>Netegrity SiteMinder>SiteMinder Realms.
The SiteMinder Realms tab displays.

Section G: Netegrity SiteMinder

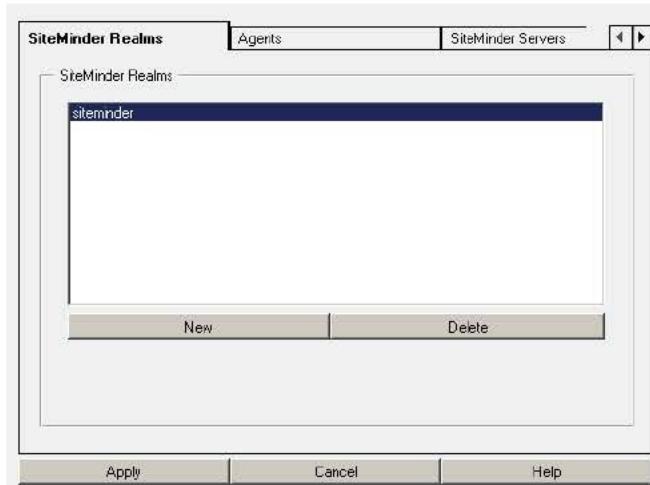


Figure 9-32: SiteMinder Realms Tab

2. Click New; the Add SiteMinder Realm dialog displays.



Figure 9-33: Add SiteMinder Realm

3. In the Realm name field, enter a realm name. The name can be 32 characters long and composed of alphanumeric characters and underscores. The name *must* start with a letter. The name should be meaningful to you, but it does not have to be the name of the SiteMinder policy server.
4. Click OK.
5. Click Apply.

To Create a SiteMinder Realm through the CLI:

At the (config) prompt, enter the following command to create a SiteMinder realm:

```
SGOS#(config) security siteminder create-realm realm_name  
where realm_name is the name of the SiteMinder realm.
```

Agents

You must configure the SiteMinder realm so that it can find the Blue Coat Authentication and Authorization Agent (BCAAA).

Section G: Netegrity SiteMinder

To Edit a SiteMinder Agent through the Management Console:

1. Select Configuration>Authentication>Netegrity SiteMinder>Agents.

The Agents tab displays.

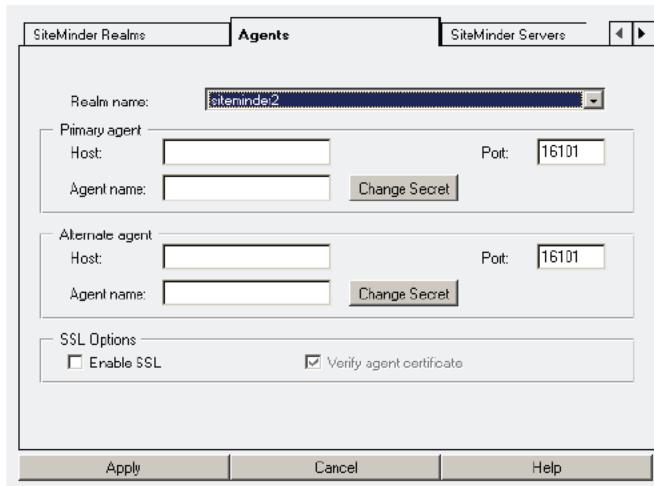


Figure 9-34: SiteMinder Agents Tab

2. Select the realm name to edit from the drop-down list.

Note: You must have defined at least one SiteMinder realm (using the SiteMinder Realms tab) before attempting to configure SiteMinder agents. If the message Realms must be added in the SiteMinder Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any SiteMinder realms defined.

Section G: Netegrity SiteMinder

3. In the Primary agent section, enter the hostname or IP address where the agent resides.
4. Change the port from the default of 16101 if necessary.
5. Enter the agent name in the Agent name field. The agent name is the name of the agent as configured on the SiteMinder policy server.
6. You must create a secret for the Agent that matches the secret created on the SiteMinder policy server. Click Change Secret. SiteMinder secrets can be up to 64 characters long and are always case sensitive.
7. (Optional) Enter an alternate agent host and agent name in the Alternate agent section.
8. (Optional) Click Enable SSL to enable SSL between the ProxySG and the BCAAA.
9. (Optional) By default, if SSL is enabled, the SiteMinder BCAAA certificate is verified. If you do not want to verify the agent certificate, disable this setting.

To Edit a SiteMinder Agent through the CLI:

1. To define the primary and alternate agent configuration for the realm you just created, enter the following commands at the (config) prompt:

```
SGOS# (config) security siteminder edit-realm realm_name
SGOS# (config siteminder realm_name) primary-agent agent-name agent_name
SGOS# (config siteminder realm_name) primary-agent host host_name_or_IP
SGOS# (config siteminder realm_name) primary-agent port port_number
SGOS# (config siteminder realm_name) primary-agent encrypted-shared-secret
encrypted_shared_secret
-or-
SGOS# (config siteminder realm_name) primary-agent shared-secret shared_secret
SGOS# (config siteminder realm_name) alternate-agent agent-name agent_name
SGOS# (config siteminder realm_name) alternate-agent host host_name_or_IP_address
SGOS# (config siteminder realm_name) alternate-agent port port_number
SGOS# (config siteminder realm_name) alternate-agent encrypted-shared-secret
encrypted_shared_secret
-or-
SGOS# (config siteminder realm_name) alternate-agent shared-secret shared_secret
```

where:

primary-agent/
alternate agent

These commands allow you to configure either the primary or alternate agent for the SiteMinder realm.

agent-name

agent_name

The name of the agent.

host

host_name_or_IP_address

The host ID or the IP address of the system that contains the agent.

port

port_number

The port where the agent listens.

Section G: Netegrity SiteMinder

```
encrypted-shared-secret secret
/shared-secret
```

The shared secret (or encrypted secret) associated with the primary or alternate agent. (Secrets can be up to 64 characters long and are always case sensitive.)

The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted. If you choose to use a third-party encryption application, be sure it supports RSA encryption, OAEP padding, and Base64 encoded with no newlines.

2. To enable SSL for this realm and to have the BCAAA certificate verified, enter:

```
SGOS# (config siteminder realm_name) ssl enable
SGOS# (config siteminder realm_name) ssl-verify-agent enable
```

SiteMinder Servers

Once you create a SiteMinder realm, use the SiteMinder Servers tab to create and edit the list of SiteMinder policy servers consulted by the realm.

To Edit SiteMinder Policy Servers through the Management Console:

1. Select Configuration>Authentication>Netegrity SiteMinder>SiteMinder Servers.

The SiteMinder Servers tab displays.

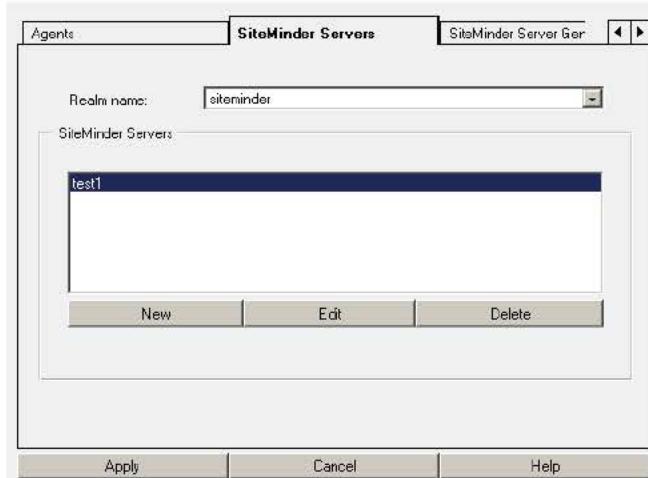


Figure 9-35: SiteMinder Servers Tab

Section G: Netegrity SiteMinder

2. From the Realm Name drop-down list, select the SiteMinder realm for which you want to add servers or change server properties.

Note: You must have defined at least one SiteMinder realm (using the SiteMinder Realms tab) before attempting to set SiteMinder policy server properties. If the message **Realms must be added in the SiteMinder Realms tab before editing this tab** is displayed in red Click **Apply**. Repeat the above steps for additional SiteMinder realms, up to a total of 40.

3. To create a new SiteMinder policy server, click **New**.

The Add List dialog displays.



Figure 9-36: SiteMinder Add List Item Dialog

- a. Enter the name of the server in the dialog. This name is used only to identify the server in the ProxySG Appliance's configuration; it usually is the real hostname of the SiteMinder policy server.
 - b. Click **OK**.
4. To edit an existing SiteMinder policy server, click **Edit**.

The Edit dialog displays.

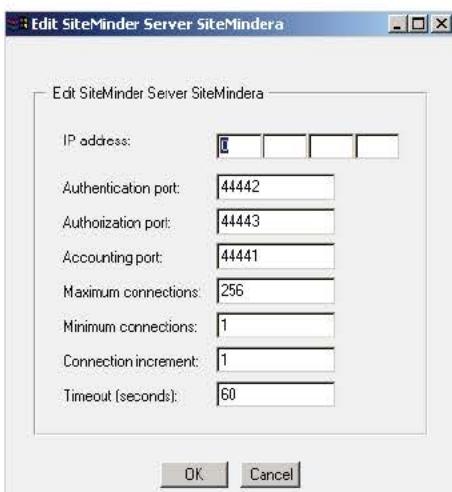


Figure 9-37: SiteMinder Edit Server Dialog

Section G: Netegrity SiteMinder

- a. Enter the IP address of the SiteMinder policy server in the IP address field.
 - b. Enter the correct port number for the Authentication, Authorization, and Accounting ports. The ports should be the same as the ports configured on their SiteMinder policy server. The valid port range is 1-65535.
 - c. The maximum number of connections is 32768; the default is 256.
 - d. The connection increment specifies how many connections to open at a time if more are needed and the maximum is not exceeded. One is the default.
 - e. The timeout value has a default of 60 seconds, which can be changed.
5. Click OK.
 6. Click Apply.

To Edit SiteMinder Policy Servers through the CLI:

To create and edit the SiteMinder policy server for the realm you just created, enter the following commands:

Note: The only required option is the IP address. The other options need only be used if you want to change the defaults.

```
SGOS#(config) security siteminder edit-realm realm_name
SGOS#(config siteminder realm_name) siteminder-server create server_name
SGOS#(config siteminder realm_name) siteminder-server edit server_name
SGOS#(config siteminder realm_name server_name) ip-address ip_address
SGOS#(config siteminder realm_name server_name) authentication-port port_number
SGOS#(config siteminder realm_name server_name) authorization-port port_number
SGOS#(config siteminder realm_name server_name) accounting-port port_number
SGOS#(config siteminder realm_name server_name) connection-increment number
SGOS#(config siteminder realm_name server_name) max-connections number
SGOS#(config siteminder realm_name server_name) min-connections number
SGOS#(config siteminder realm_name server_name) timeout seconds
```

where:

siteminder-server	create server_name edit server_name delete	You can create a SiteMinder policy server, edit it, or delete it.
edit server_name	ip-address ip_address	The IP address of the SiteMinder policy server.
edit server_name	authentication-port port_number	The default is 44442. The ports should be the same as the ports configured on the SiteMinder policy server. The valid port range is 1-65535.
edit server_name	authorization-port port_number	The default is 44443. The ports should be the same as the ports configured on the SiteMinder policy server. The valid port range is 1-65535.
edit server_name	accounting-port port_number	The default is 44441. The ports should be the same as the ports configured on the SiteMinder policy server. The valid port range is 1-65535.

Section G: Netegrity SiteMinder

edit server_name	connection-increment number	The default is 1. The connection increment specifies how many connections to open at a time if more are needed and the maximum is not exceeded.
edit server_name	max-connections number	The default is 256. The maximum number of connections is 32768.
edit server_name	min-connections number	The default is 1.
edit server_name	timeout seconds	The default is 60.

To View the SiteMinder Policy Server Configuration:

```
SGOS# (config siteminder realm_name server_name) view
  Server name:          test
  IP address:           10.25.36.47
  Min connections:     1
  Max connections:     256
  Connection inc:      1
  Timeout:              60
  Authentication Port: 44442
  Authorization Port: 44443
  Accounting Port:    44441
```

Defining SiteMinder Server General Properties

The SiteMinder Server General tab allows you to specify the protected resource name, the server mode, and whether requests should always be redirected off box.

To Configure General Settings through the Management Console:

1. Select Configuration>Authentication>Netegrity SiteMinder>SiteMinder Server General.

The SiteMinder Server General tab displays.

Section G: Netegrity SiteMinder

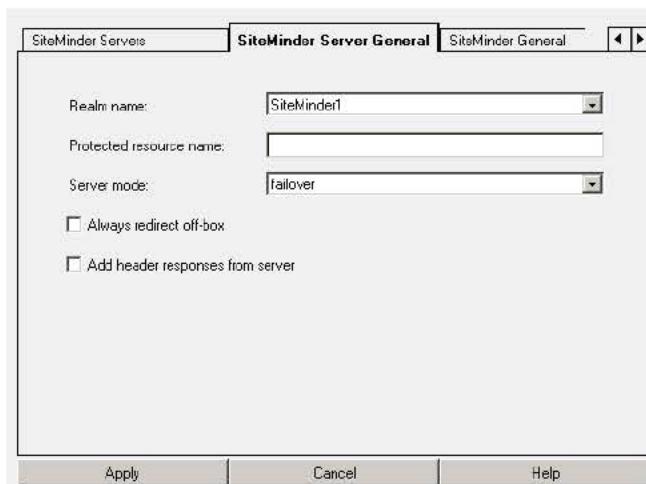


Figure 9-38: SiteMinder Server General Tab

2. From the Realm Name drop-down list, select the SiteMinder realm for which you want to change properties.

Note: You must have defined at least one SiteMinder realm (using the SiteMinder Realms tab) before attempting to set SiteMinder general properties. If the message **Realms must be added** in the SiteMinder Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any SiteMinder realms defined.

3. Enter the protected resource name. The protected resource name is the same as the resource name on the SiteMinder policy server that has rules and policy defined for it.
4. In the Server mode drop-down list, select either failover or round-robin. Failover mode falls back to one of the other servers if the primary one is down. Round-robin modes specifies that all of the servers should be used together in a round-robin approach. Failover is the default.

Note: The server mode describes the way the agent (BCAAA) interacts with the SiteMinder policy server, not the way that ProxySG interacts with BCAA.

5. To force authentication challenges to always be redirected to an off-box URL, check the Always redirect off-box checkbox.

Note: All SiteMinder Web agents involved must have the setting `EncryptAgentName=no` in their configurations to go off-box for any reason.

If using SiteMinder forms for authentication, the ProxySG always redirects the browser to the forms URL for authentication. You can force this behavior for other SiteMinder schemes by configuring the always redirect off-box property on the realm.

Section G: Netegrity SiteMinder

6. If your Web applications need information from the SiteMinder policy server responses, you can check the Add Header Responses checkbox. When this is checked, responses from the policy server obtained during authentication are added to each request forwarded by the ProxySG. Note that header responses will replace any existing header of the same name; if no such header exists, the header will be added. Cookie responses will replace a cookie header with the same cookie name; if no such cookie header exists, one will be added.
7. Click Apply.

To Configure General Settings through the CLI:

At the (config) command prompt, enter the following commands to configure general server settings:

```
SGOS#(config siteminder realm_name) protected-resource-name
protected_resource_name
SGOS#(config siteminder realm_name) server-mode failover| round-robin
(optional) SGOS#(config siteminder realm_name) always-redirect-offbox enable | disable
(optional) SGOS#(config siteminder realm_name) add-header-responses enable | disable
```

where:

protected-resource-name	protected_resource_name	The resource name on the SiteMinder policy server that has rules and policy defined for it.
server-mode	failover round-robin	Behavior of the server. Failover mode falls back to one of the other servers if the primary one is down. Round-robin modes specifies that all of the servers should be used together in a round-robin approach. Failover is the default.
always-redirect-offbox	enable disable	If using SiteMinder forms for authentication, the ProxySG always redirects the browser to the forms URL for authentication. You can force this behavior for other SiteMinder schemes by configuring the always redirect off-box property on the realm. All agents involved must have the setting EncryptAgentName=no in their configurations to go off-box for any reason.

Section G: Netegrity SiteMinder

add-header-responses	enable disable	Enable if your Web applications need information from the SiteMinder policy server responses. Note that header responses will replace any existing header of the same name; if no such header exists, the header will be added. Cookie responses will replace a cookie header with the same cookie name; if no such cookie header exists, one will be added.
----------------------	------------------	--

SiteMinder General

The SiteMinder General tab allows you to set a display name, cache credentials, timeout value, and create a virtual URL.

To Manage General Settings for the SiteMinder Realm:

1. Select Authentication>Netegrity SiteMinder>SiteMinder General.

The SiteMinder General tab displays.

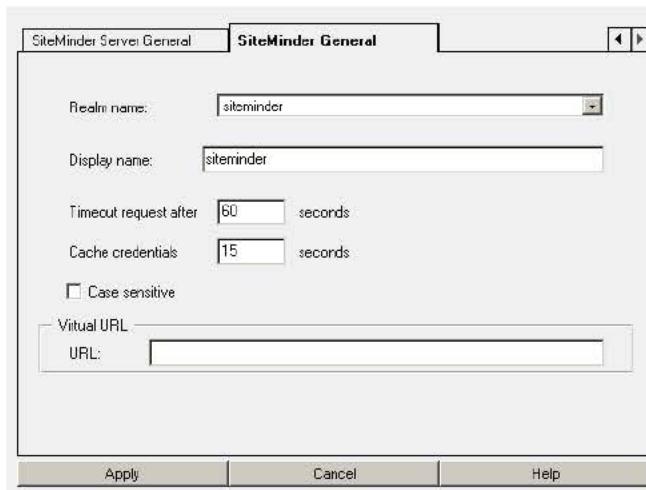


Figure 9-39: SiteMinder General Tab

2. From the Realm Name drop-down list, select the SiteMinder realm for which you want to change properties.

Note: You must have defined at least one SiteMinder realm (using the SiteMinder Realms tab) before attempting to set SiteMinder general properties. If the message Realms must be added in the SiteMinder Realms tab before editing this tab is displayed in red at the bottom of this page, you do not currently have any SiteMinder realms defined.

Section G: Netegrity SiteMinder

3. If needed, change the SiteMinder realm display name. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
4. Specify the length of time, in seconds, that user and administrator credentials received from the SiteMinder policy server are cached. Credentials can be cached for up to 3932100 seconds. The default cache-duration is 900 seconds (15 minutes).
5. If you want group comparisons for SiteMinder groups to be case sensitive, select Case sensitive.
6. The virtual hostname must be in the same cookie domain as the other servers participating in the SSO. It cannot be an IP address or the default, www.cfauth.com.
7. Click Apply.

To Set SiteMinder General Settings through the CLI:

At the (config) command prompt, enter the following commands to configure general server settings:

```
SGOS#(config siteminder realm_name) cache-duration seconds  
SGOS#(config siteminder realm_name) case-sensitive enable | disable  
SGOS#(config siteminder realm_name) display-name name  
SGOS#(config siteminder realm_name) virtual-url URL
```

where:

cache-duration seconds	Specifies the length of time in seconds that user and administrator credentials received from the SiteMinder policy server are cached. Credentials can be cached for up to 3932100 seconds. The default value is 900 seconds (15 minutes).
case-sensitive enable disable	Specifies whether the SiteMinder policy server is configured to expect case-sensitive usernames and passwords.
display-name name	Equivalent to the display-name option in the CPL authenticate action. The default value for the display name is the realm name. The display name cannot be longer than 128 characters and it cannot be null.
virtual-url url	The URL to redirect to when the user needs to be challenged for credentials. see Chapter 8: "Security and Authentication" on page 203 for more details.

Creating the CPL

You can create CPL policies now that you have completed SiteMinder realm configuration. Be aware that the examples below are just part of a comprehensive authentication policy. By themselves, they are not adequate for your purposes.

The examples below assume the default policy condition is *allow*. On new SGOS 3.x systems, the default policy condition is *deny*.

Note: See the *Blue Coat Content Policy Language Guide* for details about CPL and how transactions trigger the evaluation of policy file <Proxy> and other layers.

Section G: Netegrity SiteMinder

- Every SiteMinder-authenticated user is allowed access the ProxySG.

```
<Proxy>
```

```
    authenticate (SiteMinderRealm)
```

- Group membership is the determining factor in granting access to the ProxySG.

```
<Proxy>
```

```
    authenticate (LDAPRealm)
```

```
<Proxy>
```

```
    group="cn=proxyusers, ou=groups, o=myco"
```

```
    deny
```

Section H: Forms-Based Authentication

Section H: Forms-Based Authentication

You can use forms-based authentication exceptions to control what your users see during authentication. You can:

- Specify the realm the user is to authenticate against.
- Specify that the credentials requested are for the ProxySG. This avoids confusion with other authentication challenges.
- Make the form comply with company standards and provide other information, such as a help link.

The authentication form (an HTML document) is served when the user makes a request and requires forms-based authentication. If the user successfully authenticates to the ProxySG, the ProxySG redirects the user back to the original request.

If the user does not successfully authenticate against the ProxySG and the error is user-correctable, the user will be presented with the authentication form again.

Note: You can configure and install the authentication form and several properties through the Management Console and the CLI, but you must use policy to dictate the authentication form's use.

With forms-based authenticating, you can set limits on the maximum request size to store and define the request object expiry time. You can also specify whether to verify the client's IP address against the original request and whether to allow redirects to the original request.

To create and put into use forms-based authentication, you must complete the following steps:

- Create a new form or edit the existing authentication form exception
- Set storage options
- Set CPL policies

Understanding Authentication Forms

You can customize the default authentication form exception or you can use it as a template to create other authentication forms. (You can create as many authentication form exceptions as needed. The form must be a valid HTML document that contains valid form syntax.)

The default authentication form contains the following:

- **Title** and sentence instructing the user to enter ProxySG credentials for the appropriate realm.
- **Domain:** Text input with maximum length of 64 characters. The name of the input must be PROXY_SG_DOMAIN, and you can specify a default value of \${x-cs-auth-domain} so that the user's domain is prepopulated on subsequent attempts (after a failure).

The input field is optional, used only if the authentication realm is an NTLM realm. If it is used, the value is prepended to the username value with a backslash.

Section H: Forms-Based Authentication

- **Username:** Text input with maximum length of 64 characters. The name of the input must be PROXY_SG_USERNAME, and you can specify a default value of \$(cs-username) so the username is prepopulated on subsequent attempts (after a failure).
- **Password:** The password should be of type PASSWORD with a maximum length of 64 characters. The name of the input must be PROXY_SG_PASSWORD.
- **Request ID:** If the request contains a body, then the request is stored on the ProxySG until the user is successfully authenticated.

The request ID should be of type HIDDEN. The input name must be PROXY_SG_REQUEST_ID, and the value must be \$(x-cs-auth-request-id). The information to identify the stored request is saved in the request id variable.

- **Submit button.** The submit button is required to submit the form to the ProxySG.
- **Clear form button.** The clear button is optional and resets all form values to their original values.
- **Form action URI:** The value is the authentication virtual URL plus the query string containing the base64 encoded original URL \$(x-cs-auth-form-action-url).
- Form METHOD of POST. The form method must be POST. The ProxySG will not process forms submitted with GET.

The ProxySG only parses the following input fields during form submission:

- PROXY_SG_USERNAME (required)
- PROXY_SG_PASSWORD (required)
- PROXY_SG_REQUEST_ID (required)
- PROXY_SG_DOMAIN. (optional) If specified, its value will be prepended to the username and separated with a backslash.

The default authentication form looks similar to the following:

```
<HTML>
<HEAD>
<TITLE>Enter Proxy Credentials for Realm $(cs-realm)</TITLE>
</HEAD>
<BODY>
<H1>Enter Proxy Credentials for Realm $(cs-realm)</H1>
<P>Reason for challenge: $(exception.last_error)
<P>
<FORM METHOD="POST" ACTION=$(x-cs-auth-form-action-url)>
$(x-cs-auth-form-domain-field)
<P>Username: <INPUT NAME="PROXY_SG_USERNAME" MAXLENGTH="64"
VALUE=$(cs-username)></P>
<P>Password: <INPUT TYPE="PASSWORD" NAME="PROXY_SG_PASSWORD" MAXLENGTH="64"></P>
<INPUT TYPE="HIDDEN" NAME="PROXY_SG_REQUEST_ID" VALUE=$(x-cs-auth-request-id)>
<P><INPUT TYPE="SUBMIT" VALUE="Submit"> <INPUT TYPE="RESET"></P>
</FORM>
<P>$(exception.contact)
</BODY>
</HTML>
```

Section H: Forms-Based Authentication

If the realm is an NTLM realm, the \$(x-cs-auth-form-domain-field) substitution expands to:

```
<P>Domain: <INPUT NAME=PROXY_SG_DOMAIN MAXLENGTH=64 VALUE=$(x-cs-auth-domain)>
```

If you specify \$(x-cs-auth-form-domain-field), you do not need to explicitly add the domain input field.

User/Realm CPL Substitutions for Authentication Forms

CPL user/realm substitutions that are common in authentication form exceptions are listed below. The syntax for a CPL substitution is:

\$(CPL_substitution)

group	user-name	x-cs-auth-request-id
groups	user.x509.issuer	x-cs-auth-domain
realm	user.x509.serialNumber	x-cs-auth-form-domain-field
user	user.x509.subject	x-cs-auth-form-action-url
cs-realm	x-cs-auth-request-id	

Note: Any substitutions that are valid in CPL and in other exceptions are valid in authentication form exceptions.

For a discussion of using CPL and a complete list of CPL substitutions, as well as a description of each substitution, refer to the *Blue Coat Content Policy Language Guide*.

Tip

There is no realm restriction on the number of authentication form exceptions you can create. You can have as many forms as you want, although you might want to make them as generic as possible to cut down on maintenance.

Creating and Editing an Authentication Form

You can create a new authentication form or you can edit the existing one. If you create a new form, the new form uses the default authentication form as a template. If you edit the default form, all forms created after that contain the modification.

To Create or Edit an Authentication Form through the Management Console:

1. Select Configuration>Authentication>Forms.

The Authentication Forms tab displays.

Section H: Forms-Based Authentication

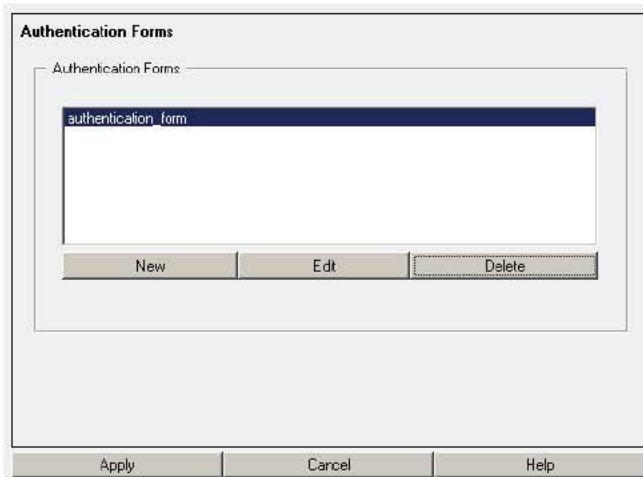


Figure 9-40: Authentication Forms

Click Edit to edit the default authentication form; click New to create a new authentication form based on the existing default settings.

2. If you click New, the Add Authentication Form dialog displays.

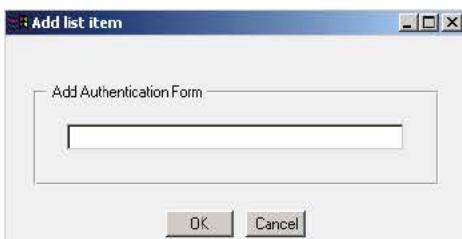


Figure 9-41: Authentication Form Dialog

3. Enter the form name. Click OK.
4. If you highlight the form you want to edit and click Edit, the Edit Authentication *authentication form name* dialog displays.



Figure 9-42: Edit Authentication Form Dialog

5. From the drop-down list, select the method to use to install the authentication form; click Install.
- Remote URL:

Section H: Forms-Based Authentication

Enter the fully-qualified URL, including the filename, where the authentication form is located. To view the file before installing it, click View. Click Install. To view the results, click Results; to close the dialog when through, click OK.

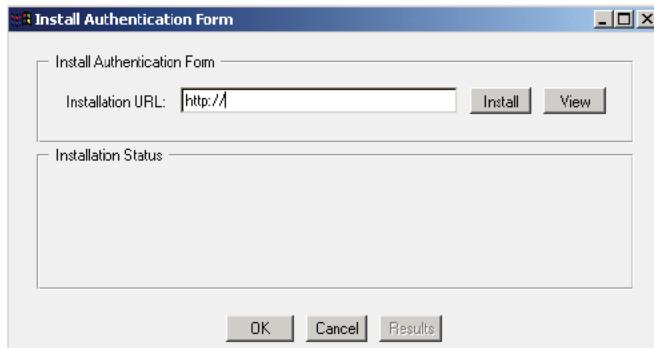


Figure 9-43: Specifying the Remote Location of an Authentication Form

Local File:

Click Browse to bring up the Local File Browse window. Browse for the file on the local system. Open it and click Install. When the installation is complete, a results window opens. View the results; to close the window, click Close.

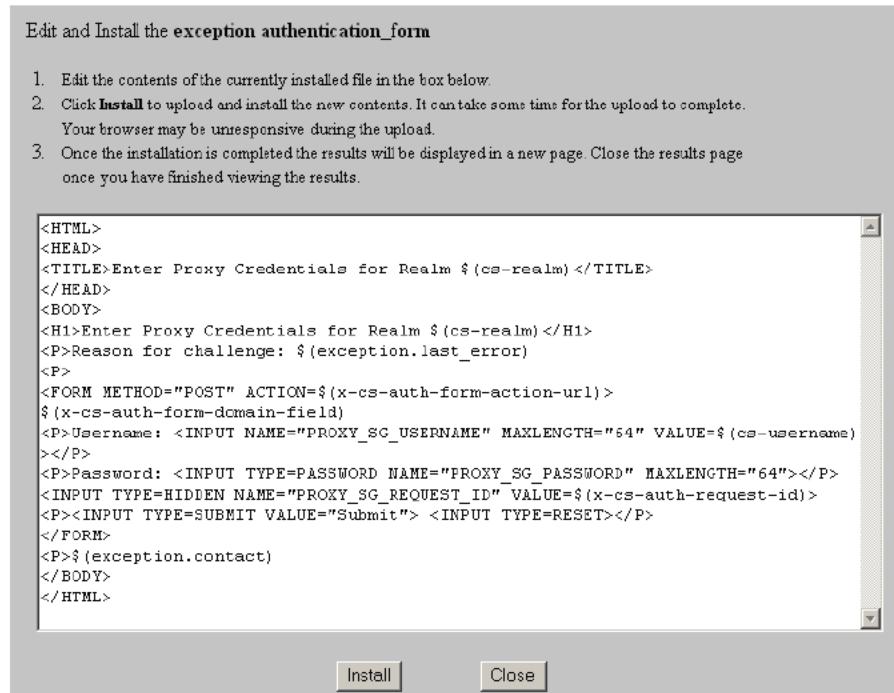


Figure 9-44: Specifying the Local Location of an Authentication Form

Section H: Forms-Based Authentication

□ **Text Editor:**

The current authentication form is displayed in the text editor. You can edit the form in place. Click **Install** to upload and install the new contents. It can take some time for the upload to complete. Your browser may be unresponsive during the upload. View the results; to close the window, click **Close**.

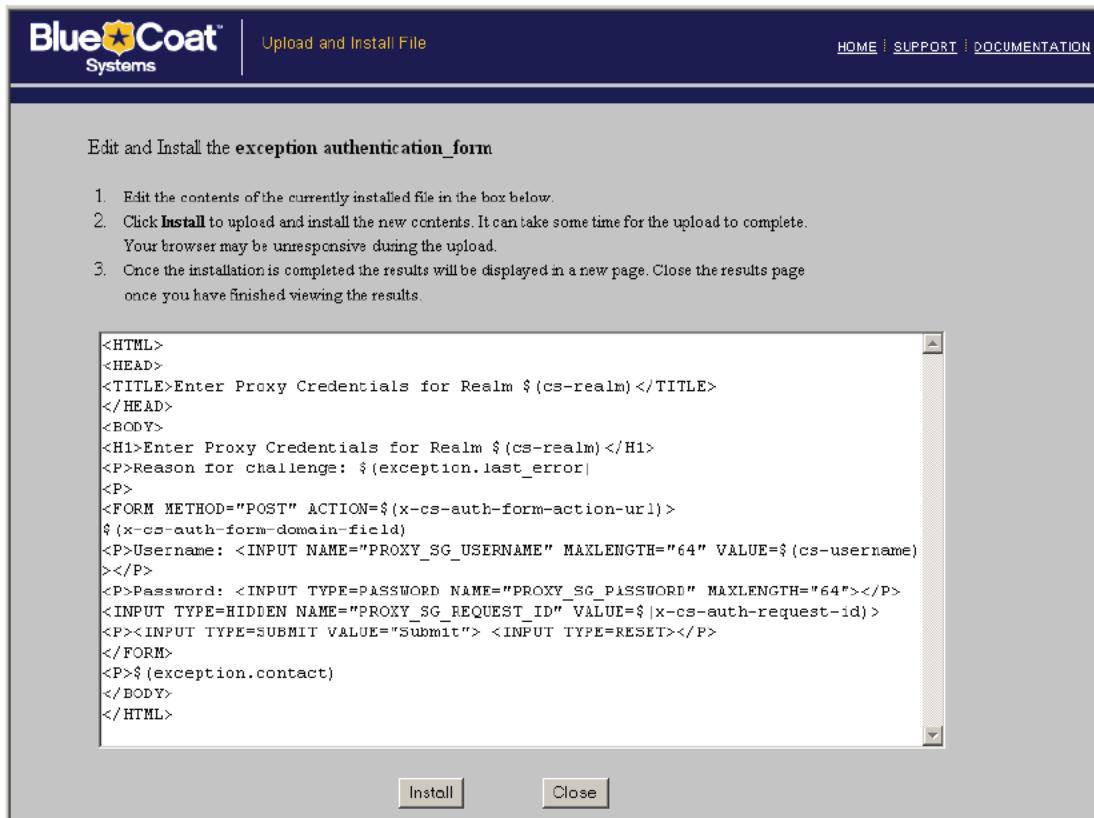


Figure 9-45: Using the ProxySG Text Editor

To Create an Authentication Form through the CLI:

Remember that if you create a new form, the new form uses the default authentication form as a template. If you edit the default form, all forms created after that will also have the modification.

To create a new form, enter the following command from the (config) prompt:

```
SGOS#(config) security authentication-form create form_name
      ok
```

To view the authentication forms on the system, enter the following command:

```
SGOS#(config) show security authentication-form
Authentication forms:
authentication_form
authentication_test
```

Section H: Forms-Based Authentication

To Edit an Authentication Form through the CLI:

You cannot edit an authentication form in place through the CLI. You can replace a form though using either remote download or through the ProxySG Appliance's inline commands.

To Edit an Authentication Form using Inline Commands:

```
SGOS# (config) security authentication-form inline form_name end-of-file_marker  
-or-  
SGOS# inline authentication-form form_name end-of-file_marker
```

Remember that any form you modify must contain the username, password and request ID. A form that is missing these values will result in the user receiving an error page when the authentication form is submitted. For more information on required fields in a new authentication form, see "Understanding Authentication Forms" on page 306.

Note: You can also import the entire set of forms through the `inline authentication-forms` command.

Notes on using inline commands:

- If you make a mistake on the current line of the script you are typing, you can backspace to correct the problem.
- If you notice a mistake on a previous line, you must quit the script (by using `Ctrl<c>`) and start over.
- The inline script overwrites the existing template.

To Create and Download an Authentication Form using a Text Editor:

1. Create the authentication form as a text file.
2. Place the form on a server that is accessible to the ProxySG.
3. Enter the following commands to give the ProxySG the file's location and to download the file:

```
SGOS# (config) security authentication-form path [form_name] path  
SGOS# (config) security authentication-form load form_name  
-or-  
SGOS#load authentication-form form_name
```

Note: You can also download the entire set of forms through the `security authentication-form path` and `load authentication-forms` commands.

To Delete an Authentication Form:

From the `(config)` prompt, enter the following commands:

```
SGOS# (config) security authentication-form delete form_name
```

Section H: Forms-Based Authentication

Setting Storage Options

When a request requiring the user to be challenged with a form contains a body, the request is stored on the ProxySG while the user is being authenticated. Storage options include

- the maximum request size
- the expiration of the request
- whether to verify the IP address of the client requesting against the original request
- whether to allow redirects from the origin server

The storage options are global, applying to all form exceptions you use.

The global allow redirects configuration option can be overridden on a finer granularity in policy using the `authenticate.redirect_stored_requests (yes|no)` action.

To Set Storage Options through the Management Console:

1. Select Configuration>Authentication>Request Storage.

The Request Storage tab displays.

The screenshot shows a dialog box titled "Request Storage". It contains the following fields and settings:

- Maximum request size to store (Megabytes): 50
- Request object expiry time (seconds): 300
- Verify the IP address against the original request
- Allow redirects

At the bottom of the dialog box are three buttons: "Apply", "Cancel", and "Help".

Figure 9-46: Request Storage Tab

Section H: Forms-Based Authentication

2. In the Maximum request size to store (Megabytes) field, enter the maximum POST request size allowed during authentication. The default is 50 megabytes.
3. In the Request object expiry time (seconds) field, enter the amount of time before the stored request expires. The default is 300 seconds (five minutes). The expiry time should be long enough for the user to fill out and submit the authentication form.
4. If you don't want the ProxySG to Verify the IP address against the original request, doubleclick the checkbox to deselect the option. The default is to verify the IP address.
5. If you want to Allow redirects from the origin servers, click the checkbox. The default is to not allow redirects from origin servers.

Note: During authentication, the user's POST is redirected to a GET request. The client will therefore automatically follow redirects from the origin server. Since the ProxySG is converting the GET to a POST and adding the post data to the request before contacting the origin server, the administrator needs to explicitly specify that redirects to these POSTs requests can be automatically followed.

6. Click Apply.

To Set Storage Options through the CLI:

From the (config) prompt, enter the following commands to select storage options:

```
SGOS# (config) security request-storage max-size megabytes
SGOS# (config) security request-storage expiry-time seconds
SGOS# (config) security request-storage verify-ip enable | disable
SGOS# (config) security request-storage allow-redirects enable | disable
```

where

max-size	megabytes	Sets the maximum POST request size during authentication. The default is 50 megabytes.
expiry-time	seconds	Sets the amount of time before the stored request expires. The default is 300 seconds (five minutes)
verify-ip	enable disable	Enables or disables the verify-ip option. The default is to enable the ProxySG to verify the IP address against the original request.
allow-redirects	enable disable	Specifies whether to allow redirects. The default is disable.

Using CPL with Forms-Based Authentication

To use forms-based authentication, you must create policies that enable it and also control which form will be used in which situations. A form must exist before it can be referenced in policy.

- Which form to use during authentication is specified in policy using the CPL condition `authenticate.form(form_name)`.

Section H: Forms-Based Authentication

Note: The `authenticate.form(form.name)` condition can be used with the form authentication modes only. If no form is specified the form defaults to `authentication_form`.

- Using the `authentication.mode()` property selects a combination of challenge type and surrogate credentials. The `authentication.mode()` property offers several options specifically for forms-based authentication:
 - Form-IP—The user's IP is used as a surrogate credential. The form is presented whenever the user's credential cache entry expires.
 - Form-Cookie—Cookies are used as surrogate credentials. The cookies are set on the OCS domain only, and the user is presented with the form for each new domain. This mode is most useful in reverse proxy scenarios where there are a limited number of domains.
 - Form-Cookie-Redirect—The user is redirected to the authentication virtual URL before the form is presented. The authentication cookie is set on both the virtual URL and the OCS domain. The user is only challenged when the credential cache entry expires.
 - Form-IP-redirect —This is similar to form-ip except that the user is redirected to the authentication virtual URL before the form is presented.
- If you authenticate users who have third-party cookies explicitly disabled, you can use the `authenticate.use_url_cookie()` property.
- Since the `authentication.mode()` property will be defined as a form mode (above) in policy, you don't need to adjust the default authenticate mode through the CLI.
- Using the `authenticate.redirect_stored_requests(yes|no)` action allows granularity in policy over the global allow redirect config option.

For information on using these CPL conditions and properties, refer to the *Blue Coat Content Policy Language Guide*.

Tips and Boundary Conditions

- If the user is supposed to be challenged with a form on a request for an image or video, the ProxySG returns a 403 error page instead of the form. If the reason for the challenge is that the user's credentials have expired and the object is from the same domain as the container page, then reloading the container page should result in the user receiving the authentication form and being able to authenticate. However, if the client browser loads the container page using an existing authenticated connection, the user might still not receive the authentication form.

Closing and reopening the browser should fix the issue. Requesting a different site might also cause the browser to open a new connection and the user will be returned the authentication form.

If the container page and embedded objects have a different domain though and the authentication mode is "form-cookie", reloading or closing and reopening the browser might not fix the issue as the user is never returned a cookie for the domain the object belongs to. In these scenarios, it is recommended that policy be written to either bypass authentication for that domain or to use a different authentication mode such as "form-cookie-redirect" for that domain.

Section H: Forms-Based Authentication

- Forms-based authentication works with HTTP browsers only.
- Since forms only support BASIC authentication, authentication-form exceptions cannot be used with a Certificate realm or with an NTLM realm that allows only NTLM credentials. If a form is in use and the authentication realm is either NTLM credentials or a Certificate realm, the user receives a configuration error.
- User credentials are sent in cleartext. However, they can be sent securely using SSL if the virtual URL is HTTPS.
- Since not all user requests support forms (such as WebDAV and streaming), you should create policy to bypass authentication or use a different authentication mode with the same realm for those requests.

Section I: Managing the Credential Cache

Section I: Managing the Credential Cache

When you have configured all your realms, you can view your realms and manage the credentials cache for a specific realm.

Credential caching is applicable only for authentication modes involving surrogates. For more information about surrogates, see "Authentication Modes" on page 217.

Note: XFTP users are not prompted for proxy authentication if the credentials are in the cache and the credentials have not expired.

To Manage the Credential Cache through the Management Console:

1. Select Configuration>Authentication>Realms.

The Realms tab displays, with all realms that you have created.

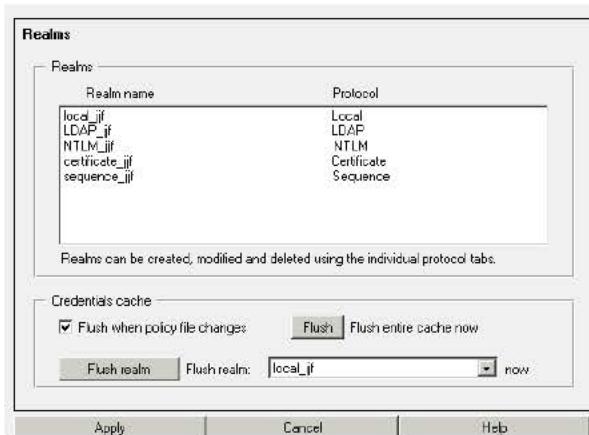


Figure 9-47: Viewing All Realms on the ProxySG

2. To manage the credential cache:

- To purge the credentials cache when you make policy changes, select **Flush When Policy File Changes** (this option is selected by default).
- To flush the entire credentials cache immediately, click **Flush** and confirm.
- To flush only the entries for a particular realm in the credentials cache, select the realm from the drop-down list, click **Flush Realm** and confirm.

All of these actions force users to be re-authenticated.

3. Click **Apply**.

Section I: Managing the Credential Cache

To Manage the Credential Cache through the CLI:

From the `(config)` command prompt, enter the following command:

```
SGOS# (config) security flush-credentials <enter> [on-policy-change {enable | disable} | realm realm]
```

where:

<enter>	Press <Enter> to flush the credential cache now.
on-policy-change enable disable	Flush the cache only if the policy changes.
realm realm	Flush the credential cache for the specified realm.

Section I: Managing the Credential Cache

Section I: Managing the Credential Cache

Chapter 10: External Services

This chapter describes how to configure the ProxySG to interact with external ICAP and Websense servers to provide content scanning, content transformation, and content filtering services.

This chapter contains the following sections:

- "Section A: ICAP"—Describes the ICAP protocol and describes how to create and manage ICAP services on the ProxySG.
- "Section B: Websense"—Describes how to create a Websense service
- "Section C: Service Groups"—Describes how to create service groups of ICAP or Websense entries and configure load balancing.
- "Section D: Displaying External Service and Group Information"—Describes how to display external service configurations through the CLI.

Related Topics:

- Chapter 11: "Health Checks"
- Chapter 17: "Content Filtering"

Section A: ICAP

Section A: ICAP

This section describes the Internet Content Adaptation Protocol (ICAP) solution of content scanning and modification.

When integrated with a supported ICAP server, the ProxySG provides content scanning, filtering, and repair service for Internet-based malicious code. ICAP is an evolving architecture that allows an enterprise to dynamically scan and change Web content. To eliminate threats to the network and to maintain caching performance, the ProxySG sends objects to the integrated ICAP server for checking and saves the scanned objects in its object store. With subsequent content requests, the appliance serves the scanned object rather than rescan the same object for each request.

Configuring ICAP on the ProxySG involves the following steps:

1. Install the ICAP server.
2. Configure the ProxySG to use ICAP and configure basic features.
3. Define scanning policies, then load the policy file on the ProxySG.

Supported ICAP Servers

The ProxySG supports the following ICAP servers:

- Blue Coat ProxyAV, version 2.x.
- Symantec AntiVirus Scan Engine (SAVSE) 4.0, version 4.04.46; ICAP 1.0
- Trend Micro InterScan WebProtect (ISWP) 1.5, build_SOL_1266; ICAP 1.0
- WebWasher 4.4, build 552; ICAP 1.0
- Finjan Vital Security for Web v7.0; Service Pack 2; build 4.552; ICAP 1.0

Note: While SGOS 2.x supported ICAP v0.95 servers and services, SGOS 3.2.x does not. Upon upgrading to SGOS 3.2.x, any configured v0.95 services become inactive.

ICAP v1.0 Features

This section describes features of the ICAP v1.0 protocol.

Sense Settings

The Sense Settings feature allows the ProxySG to query any identified ICAP server running v1.0, detect the parameters, and configure the ICAP service as appropriate. See "Creating an ICAP Service" on page 325.

Section A: ICAP

ISTags

An ICAP v1.0 server is required to return in each response an ICAP header ISTag indicating the current state of the ICAP server. This eliminates the need to designate artificial pattern version numbers, as is required in v0.95.

Note: Backing out a virus pattern on the ICAP server can revert ISTags to previous values that are ignored by the ProxySG. To force the ProxySG to recognize the old value, use the Sense Settings option as described in "Creating an ICAP Service" on page 325.

Persistent Connections

New ICAP connections are created dynamically as ICAP requests are received (up to the defined maximum connection limit). The connection remains open to receive further requests. If a connection error occurs, the connection closes to prevent further errors.

About Content Scanning

The ProxySG ICAP scanning solution prevents the spread of viruses and other malicious code by serving content that has been scanned by a supported ICAP server.

Determining Which Files to Scan

In determining which files to scan, this integrated solution uses the content scanning server's filtering in addition to ProxySG capabilities. Table 10.1 describes the supported content types and protocols.

Table 10.1: Content Types Scanned By ICAP Server and the ProxySG

ICAP Server supported content types	ProxySG supported protocols	Unsupported content protocols
All or specified file types, based on file extension, as configured on the server. Examples: .exe (executable programs), .bat (batch files), .doc and .rtf (document files), and .zip (archive files), or with specific MIME types.	<ul style="list-style-type: none"> • HTTP objects • FTP objects (uploads and downloads) • Transparent FTP responses <p>HTTPS connections terminated at a ProxySG.</p>	<ul style="list-style-type: none"> • Streaming content (for example, RTSP and MMS) • Live HTTP streams (for example, HTTP radio streams) <p>HTTPS connections tunneled through a Blue Coat client-side ProxySG.</p>

After the ProxySG retrieves a requested Web object from the origin server, it uses content scanning policies to determine whether the object should be sent to the ICAP server for scanning. If cached objects are not scanned or are scanned before a new pattern file was updated, the ProxySG rescans those objects upon:

- the next request for that object, or

Section A: ICAP

- the object is refreshed.

With the ProxySG, you can define flexible, enterprise-specific content scanning policies. Consider the following example. A business wants to scan software downloaded by employees from popular shareware Web sites. To do this, the business defines an appliance policy that includes a custom *scanshareware* action for the purpose. This rule includes URL domains related to the relevant shareware Web sites.

Before continuing, plan the types of policies you want to use. For more information, see "Creating ICAP Policy" on page 335.

Performing Response Modification

The ProxySG sends the first part (a preview) of the object to the ICAP server that supports response modification. The object preview includes the HTTP request and response headers, and the first few bytes of the object. After checking those bytes, the ICAP server either continues with the transaction (that is, asks the ProxySG to send the remainder of the object for scanning) or sends a notification to the appliance that the object is clean and opts out of the transaction.

The ICAP server features and configuration determine how scanning works, including the following:

- Handling of certain objects, including those that are infected and cannot be repaired.
- Whether to attempt to repair infected files.
- Whether to delete infected files that cannot be repaired from the ICAP server's archive.

Performing Request Modification

The ProxySG sends the client request to a ICAP server that supports request modification. The server might then return an HTTP response to the client (for example, sports not allowed); or the client request might be modified, such as stripping a referer header, before continuing to the origin content server.

Note: Some ICAP servers do not support virus scanning for request modification, only content filtering.

Returning the Object to the ProxySG

This object may be the original unchanged object, a repaired version of the original object minus a virus, or an error message indicating that the object contained a virus. Each of these responses is configured on the ICAP server, independent of the appliance and the ICAP protocol. If the appliance receives the error message, it forwards the error message to the client and does not save the infected file.

Section A: ICAP

Caching and Serving the Object

Once an object is determined cacheable, the ProxySG saves it and serves it for the subsequent content requests. When the ProxySG detects that the cached content has changed on the origin server, it fetches a fresh version and forwards it to the ICAP server for scanning. If a pattern file change occurs on the virus scanning server while content is still fresh, the already-cached object is rescanned. However, this only occurs for objects marked as clean by a previous ICAP scan.

When a virus is detected during an ICAP scan, the ICAP server might return a transformed (cleaned) object or an error page reporting that the virus was detected. This object is cached by the ProxySG, just as it would cache the original content, and is served until either the original content is updated on the origin server or the pattern file is updated on the ICAP server. When that occurs, the ProxySG *always* refetches content from the origin server before rescanning it. Already-cached objects are never rescanned.

ProxySG policies related to ICAP response scanning are created in the <Cache> layer. These policies apply to content fetches by clients, content distribute commands, refreshes, and pipeline fetches. For more information on policies, see "Creating ICAP Policy" on page 335. For more information on the <Cache> layer, refer to the *Blue Coat Content Policy Language Guide*.

Installing the ICAP Server

Follow the manufacturer instructions for installing the ICAP server, including any configuration necessary to work with the Blue Coat ProxySG. Based on your network environment, you might use the ProxySG with multiple ICAP servers or multiple scanning services on the same server. Configure options as needed, including the error message displayed to end users in the event the requested object was modified or blocked.

Creating an ICAP Service

An ICAP service on the ProxySG is specific to the ICAP server and includes the server IP address or hostname, as well as the supported number of connections. If you are using the ProxySG with multiple ICAP servers or multiple scanning services on the same server, add an ICAP service for each server or scanning service.

To Create and Configure an ICAP Service through the Management Console:

1. Select Configuration>External Services>ICAP Services.
2. Click New; the Add List Item dialog appears.
3. In the ICAP service name field, enter an alphanumeric name; click OK.
4. Highlight the new ICAP service name and click Edit; the Edit ICAP Service dialog appears.

Section A: ICAP

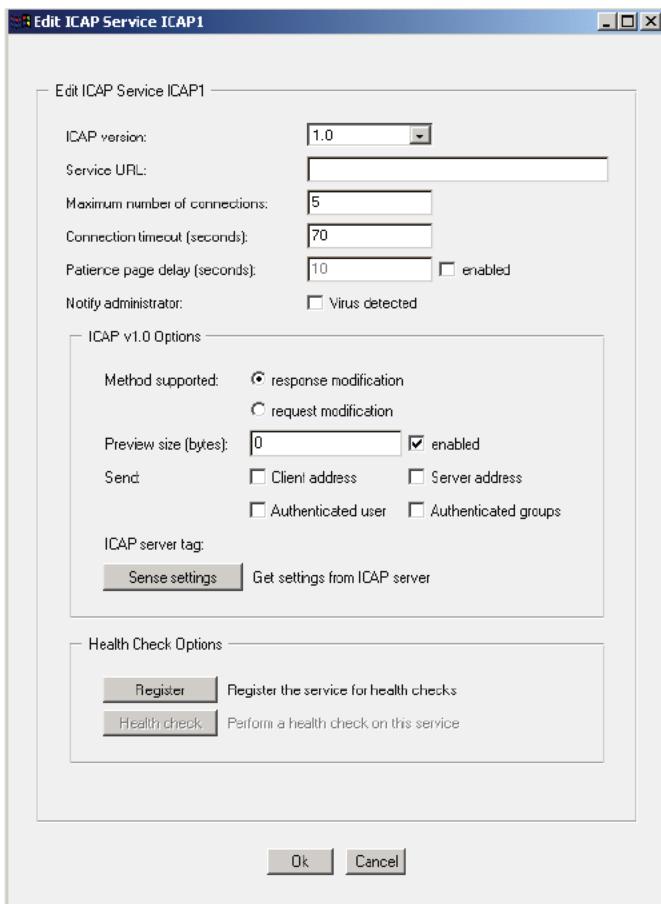


Figure 10-1: ICAP Service Dialog

The default ICAP version is 1.0 and cannot be changed.

5. Enter or select the following information:

- The service URL, which includes the URL schema, ICAP server hostname or IP address, and the ICAP port number. For example:

`icap://10.x.x.x/`

The default port number is 1344, which can be changed; for example:
`icap://10.x.x.x:99`. You can also give an HTTP URL, but you must define a port number.

Note: An ICAP service pointing to a WebWasher server must use `icap` as the protocol in the URL. Blue Coat also recommends that you review your specific ICAP server documentation, as each vendor might require additional URL information.

Section A: ICAP

- b. The maximum number of connections possible at any given time between the ProxySG and the ICAP server. The range is a number from 1 to 65535. The default is 5. The number of recommended connections is dependent on the capabilities of the ICAP server. Refer to the vendor's product information.
- c. The number of seconds the ProxySG waits for replies from the ICAP server. The range is 60 to 65536. The default timeout is 70 seconds.
- d. Optional: You can enable the ProxySG to display a default patience page when an ICAP server is processing a relatively large object. The page informs users that a content scan is in process. If enabled, the patience page is displayed after the designated time value is reached for scanned objects. Patience pages might not be displayed for truncated objects; Blue Coat recommends increasing the maximum cacheable object size (up to 1 GB) to reduce the amount of truncated objects.

Note: Patience pages display regardless of any pop-up blocking policy that is in effect.

To enable the patience page, in the Patience page delay field, enter the number of seconds the ProxySG waits before displaying the page. The range is 5 to 65535. Select Enable.

- e. Select Notify administrator: Virus detected to send an email to the administrator if the ICAP scan detects a virus. The notification is also sent to the Event Log and the Event Log email list.
- 6. The following steps configure ICAP v1.0 features:
 - a. Select the ICAP method: response modification or request modification.

Note: An ICAP server might have separate URLs for response modification and request modification services.

- b. Enter the preview size (in bytes) and select preview size enable. The ICAP server reads the object up to the specified byte total. The ICAP server either continues with the transaction (that is, receives the remainder of the object for scanning) or opts out of the transaction.

The default is 0. Only response headers are sent to the ICAP server; more object data is only sent if requested by the ICAP server.

Note: Trend Micro does not support previews for request modification mode.

- c. (Optional) Click Send: Client address or Server address to specify what is sent to the ICAP server: Send: Client address, Server address, Authenticated user, or Authenticated groups.
- d. (Optional) Clicking Sense Settings automatically configures the ICAP service using the ICAP server parameters. If you use the sense settings feature, no further steps are required; the ICAP service is configured. Otherwise, proceed with the manual configuration.
- 7. Click OK; click Apply.

Section A: ICAP

To Register a Newly Created ICAP Service for Health Checking:

For convenience, the Edit ICAP Service dialog allows you to register a newly-created ICAP service for health checking (this duplicates the functionality on the Configuration>Health Checks>General tab). Registering for health checking requires that a valid ICAP server URL was entered.

- Click Register; a dialog prompts confirmation; click OK.
- You can also click Health check to perform an immediate health check on this service.

To Monitor ICAP Health Checks:

In a browser, enter one of the following URLs to list health check information.

- To list all health check entries and their configuration parameters, enter:

`http://ProxySG_IP_address:8081/health_check/view`

- To list the statistics for all currently active entries, enter:

`http://ProxySG_IP_address:8081/health_check/statistics`

For more information about health checks, see Chapter 11: “Health Checks” on page 355.

Note: When a health check determines that a server is not healthy, the ProxySG no longer attempts to contact this server to perform ICAP actions. Any ICAP actions that refer to this server results in the return of the ICAP *server unavailable* error code. When an ICAP action references a service group, *server unavailable* is only returned when all the servers in this service group are determined to not be healthy.

To Create and Configure an ICAP Service through the CLI:

1. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) external-services  
SGOS#(config external-services) create icap service_name
```

Specify a unique alphanumeric name for each service.

2. To configure the service, enter the following commands:

```
SGOS#(config external-services) edit service_name  
SGOS#(config icap service_name) url icap://url
```

where `url` specifies the URL schema, ICAP server hostname or IP address, and the ICAP port number. The default port number is 1344.

Note: While `http://url:1344` is valid, an ICAP service pointing to a WebWasher server *must* use `icap` as the protocol in the URL.

```
SGOS#(config icap service_name) max-conn number
```

where `number` is the maximum number, from 1 to 65535, of connections the ICAP service uses to connect to the ICAP server. The default is 5. Blue Coat recommends that the setting not exceed 200.

```
SGOS#(config icap service_name) timeout timeout_seconds
```

Section A: ICAP

where *timeout_seconds* is the number of seconds, from 60 to 65535, the ProxySG waits for replies from the ICAP server. The default timeout is 70 seconds.

```
SGOS#(config icap service_name) notify virus-detected
```

Sends an email to the administrator if the ICAP scan detects a virus. The notification is also sent to the Event Log and the Event Log email list.

3. The following commands configure ICAP v1.0 features:

```
SGOS#(config icap service_name) methods {REQMOD | RESPMOD}
```

Specifies the ICAP service type: request modification or response modification.

Note: On most ICAP servers, one URL is designated for response modification and one for request modification.

```
SGOS#(config icap service_name) preview-size bytes
```

where *number* is the preview size in bytes. If specified, the ICAP server reads the object up to the specified byte total. The ICAP server either continues with the transaction (that is, receives the remainder of the object for scanning) or opts out of the transaction.

The default is 0. Only response headers are sent to the ICAP server; more object data is only sent if requested by the ICAP server.

Optional:

```
SGOS#(config icap service_name) send {client-address | server-address}
```

Specifies to send the client IP address or the server IP address to the ICAP server.

```
SGOS#(config icap service_name) send {authenticated-user | authenticated-groups}
```

Specifies to send authenticated user and group information to the ICAP server.

4. Optional: If the ICAP server is a version 1.0 server, you can use the **sense-settings** command to automatically configure the ICAP service using ICAP server parameters. Otherwise, proceed with the manual configuration in Step 3. To use the ICAP server parameters, enter the following command:

```
SGOS#(config icap services service_name) sense-settings
```

The ICAP service is now configured. No further steps are required.

5. Optional: You can enable the ProxySG to display a default patience page when an ICAP server is processing a relatively large object. The page informs users that a content scan is in process. If enabled, the patience page is displayed after the designated time value is reached for scanned objects. Patience pages might not be displayed for truncated objects; Blue Coat recommends increasing the maximum cacheable object size (up to 1 GB) to reduce the amount of truncated objects. To customize patience pages, see "Customizing ICAP Patience Text" on page 330.

```
SGOS#(config icap services service_name) patience-page seconds
```

where *seconds* is the duration before the patience page is displayed. The range is 5 to 65535. The default is disabled.

Section A: ICAP

Note: Patience pages display regardless of any pop-up blocking policy that is in effect.

Deleting an ICAP Service

The following steps describe how to delete an ICAP service.

Note: You cannot delete an ICAP service used in a ProxySG policy (that is, if a policy rule uses the ICAP service name) or that belongs to a service group.

To Delete an ICAP Service through the Management Console:

1. Select Configuration>External Services>ICAP.
2. Select the service to be deleted.
3. Click Delete; click OK to confirm.
4. Click Apply.

To Delete an ICAP Service through the CLI:

At the (config) prompt, enter the following commands:

```
SGOS# (config) external-services
SGOS# (config external-service) delete service_name
```

Customizing ICAP Patience Text

This section describes how to customize text displayed during ICAP scanning.

HTTP Patience Text

The ProxySG allows you to customize the patience pages that are displayed when HTTP clients experience delays as Web content is scanned. You can customize the following patience page components:

- Header—Contains HTML tags that define what appears in the dialog title bar. This component also contains the `<meta http-equiv>` tag, which is used to specify a non-English character set.

Section A: ICAP

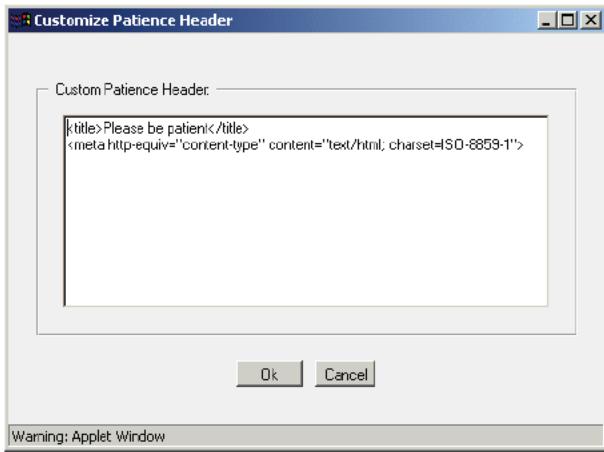


Figure 10-2: Customizing the Header Component

- **Summary**—HTML and text that informs users that a content scan is occurring.

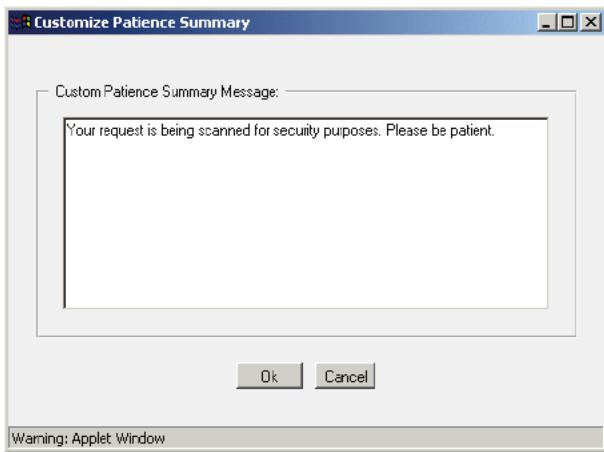


Figure 10-3: Customizing the Summary Component

- **Details**—Uses data to indicate scanning progress. The information includes the URL currently being scanned, the number of bytes processed, and the elapsed time of the scan

Section A: ICAP

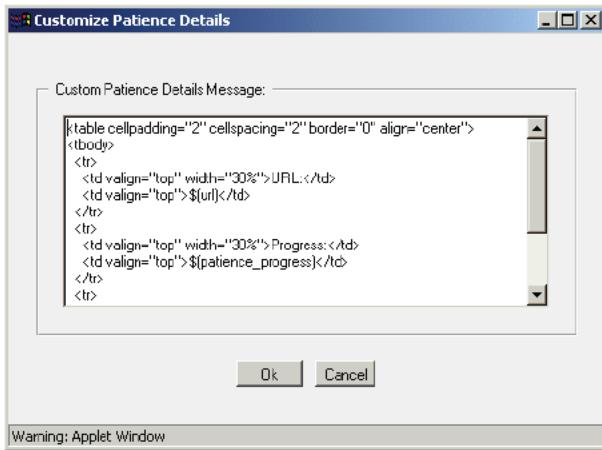


Figure 10-4: Customizing the Details Component

- **Help**—Displays instructions for users should they experience a problem with the patience page.

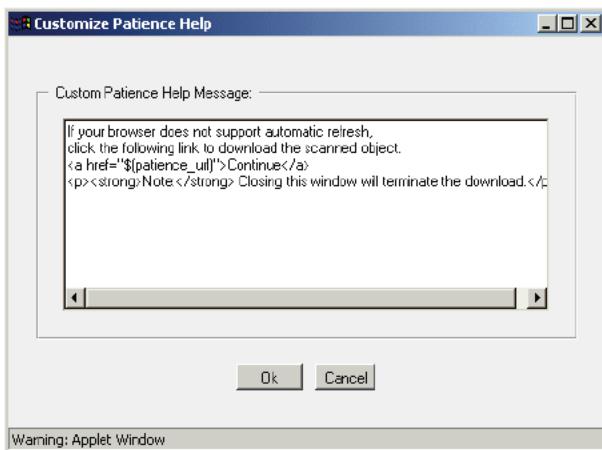


Figure 10-5: Customizing the Help Component

All of these components are displayed on the patience page.

To Customize ICAP Patience Text through the Management Console:

1. Select Configuration>External Services>ICAP>ICAP Patience Page.
2. In the HTTP Patience Page Customization field, click Header, Summary, Details, or Help; the appropriate customize dialog appears. Customize the FTP client patience text.
3. Click OK; click Apply.

Example

The following example demonstrates customizing the message summary.

Section A: ICAP

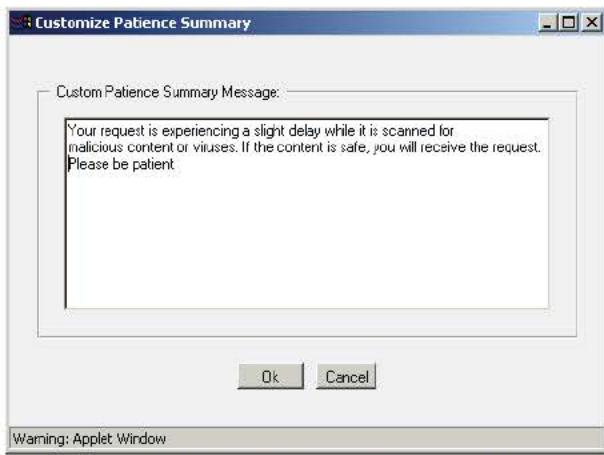


Figure 10-6: Entering a Custom Summary Message

To Customize ICAP Patience Text through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) external-services
SGOS#(config external-services) inline http icap-patience-{details | header | help | summary} eof
```

where:

eof	Specifies the end-of-file marker. After entering customized text, enter the end-of-file marker to end the customizing process.
details	The string that displays the progress of the content scanning.
header	The title of the page. Appears in the dialog title bar. The default is: <i>Please be patient</i>
help	Clients with browsers that do not support automatic refresh must click a link to load the content after scanning is complete. The default is: <i>If your browser does not support automatic refresh, click the following link to download the scanned object. Continue.</i> <i>Note: Closing this window terminates the download.</i>
summary	The text message informing users that a content scan is occurring. The default is: <i>Your request is being scanned for security purposes. Please be patient.</i>

Section A: ICAP

Example:

```
SGOS# (config) external-services
SGOS# (config external-services) inline http icap-patience-summary eof
Your request is experiencing a slight delay while it is scanned for malicious
content or viruses. If the content is safe, you will receive the request. Please
be patient. eof
ok
SGOS# (config external-services)
```

Windows XP, Service Pack 2 Behavior

With Windows XP, Microsoft is continually updating the security measures, which impacts how the ProxySG manages patience pages.

- Browsers running on Windows XP, Service Pack 2 (XP SP2), experience slightly different patience page behavior when pop-up blocking is enabled.
 - If pop-up blocking is not enabled, patience page behavior should be normal.
 - If pop-up blocking is enabled (the default), the ProxySG attempts to display the patience page in the root window.
 - If the download triggers an invisible Javascript window, the user can track the scanning progress with the progress bar at the bottom of the window; however, if other policy blocks Javascript active content, this bar is also not visible.
- If Internet Explorer blocks all downloads initiated by Javascript, the user must click the yellow alert bar to download the scanned object.
- Users experience two patience page responses for non-cacheable objects.

Interactivity and Limitations

- When ICAP scanning is enabled and a patience page is triggered, a unique URL is dynamically generated and sent to the browser to access the patience page. This unique URL might contain a modified version of the original URL. This is expected behavior.
- Patience pages and exceptions can only be triggered by left-clicking a link. If a user right-clicks a link and attempt to save it, it is not possible to display patience pages. If this action causes a problem, the user might see browser-specific errors (for example, an Internet site not found); however, ICAP policy is still in effect.
- A patience page is not displayed if a client object request results in an HTTP 302 response and the ProxySG pipelines the object in the `Location` header. Once the ProxySG receives the client request for the object, the client enters a waiting state because a server-side retrieval of the object is already in progress. The wait status of the client request prevents the patience page from displaying. To prevent the ProxySG from pipelining these requests (which decreases performance) and retain the ability to provide a patience page, configure HTTP:

```
#ProxySG (config) http no pipeline client redirects
```

- The status bar update does not work if it is disabled or if the Javascript does not have sufficient rights to update it.

Section A: ICAP

- Looping: Certain conditions cause browsers to re-spawn patience pages. For example, a site states it will begin a download in 10 seconds, initiates a pop-up download window, and returns to the root window. If the download window allows pop-ups, the patience page is displayed in another window. The automatic return to the root window initiates the download sequence again, spawning another patience page. If unnoticed, this loop could cause a system hang. The same behavior occurs if the user clicks the back button to return to the root window. For known and used download sites, you can create policy that redirects the page so that it doesn't return to the root window after a download starts.

FTP Patience Text

The patience text displayed to FTP clients during an ICAP scan can be modified.

To Customize ICAP Patience Text through the Management Console:

1. Select Configuration>External Services>ICAP>ICAP Patience Page.
2. In the FTP Patience Page Customization field, click Summary; the Customize FTP Patience Text dialog appears. Customize the FTP client patience text.
3. Click OK; click Apply.

To Customize ICAP Patience Text through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) external-services
SGOS# (config external-services) inline ftp icap-patience-text eof
```

Creating ICAP Policy

Defined ICAP policy dictates the anti-virus behavior for your enterprise. You can either use the Visual Policy Manager (VPM) or you can manually edit policy files. For more information on the VPM and defining policies, see "The Visual Policy Manager" on page 377.

Use the `request.icap_service()` (request modification) or `response.icap_service()` (response modification) properties to manage the ProxySG ICAP services.

VPM Objects

The VPM contains the following objects specific to AV scanning (linked to their descriptions in the VPM chapter).

Table 10.1: VPM ICAP Objects

Object	Layer>Column
"Virus Detected"	Web Access>Service
"ICAP Error Code"	Web Access>Service
"Return ICAP Patience Page"	Web Access>Action
"Set ICAP Request Service"	Web Access>Action
"Set ICAP Request Service"	Web Content>Action

Section A: ICAP

Table 10.1: VPM ICAP Objects

Object	Layer>Column
"Set ICAP Response Service"	Web Content>Action

Note: For CPL policy, refer to the *Blue Coat Systems ProxySG Content Policy Language Guide*.

Example ICAP Policy

The following VPM example demonstrates the implementation of an ICAP policy that performs virus scanning on both client uploads (to prevent propagating a virus) and responses (to prevent the introduction of viruses).

For this example:

- The ProxySG has configured ICAP services. The response service is corporateav1 and the request service is corporateav2.
- The ProxyAV is the virus scanner and is configured to serve password-protected files.
- A group named IT is configured on the ProxySG.
- The IT group wants to be allowed to download password protected files, but deny everyone else.

Procedure—To perform virus scanning, protecting both the server side and client side:

1. In the VPM, select Policy>Web Content Layer. Name the layer RequestAV.
2. Right-click the Action column; select Set. The Set Action Object dialog appears.
 - a. Select Set ICAP Request Service; the Add ICAP Request Service Object dialog appears.
 - b. From the Use ICAP request service drop-down list, select corporateav2.
 - c. Select Deny the client request. This prevents a client from propagating a threat. If a virus is found, the content is not uploaded. For example, a user attempts to post a document that has a virus.

Section A: ICAP

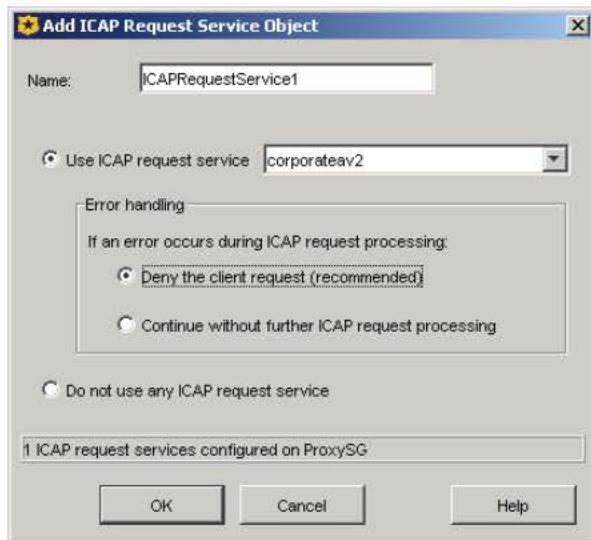


Figure 10-7: Specifying an ICAP Request Service Object.

- d. Click OK; click OK again to add the object to the rule.

RequestAV							
No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	Any	Any	Any	ICAPRequestService1	None	

Figure 10-8: The Web Content Layer policy.

3. In the VPM, select Policy>Web Access Rule. Name the rule ResponseAV.
4. Right-click the Action column; select Set. The Set Action Object dialog appears.
 - a. Select Set ICAP Response Service; the Add ICAP Response Service Object dialog appears.
 - b. From the Use ICAP response service drop-down list, select corporateav1.
5. Select Deny the client request. This scans the responses for viruses before the object is delivered to the client. If a virus is found, the content is not served.

Procedure—To log a detected virus:

1. In the VPM, select Policy>Web Access Layer. Name the layer AVErrors.
2. Right-click the Service column; select Set. The Set Service Object dialog appears.
 - a. Select Virus Detected (static object).
 - b. Click OK to add the object to the rule.
3. Right-click the Action column. Select Delete.
4. Right-click the Track column. Select Set; the Set Track Object dialog appears.

Section A: ICAP

- a. Click New; select Event Log. The Event Log dialog appears.
- b. In the Name field, enter VirusLog1.
- c. From the scroll-list, select icap_virus_details, localtime, and client-address. Click Insert.
- d. Click OK; click OK again to add the object to the rule.

AVErrors							
No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	Any	Virus Detected	Any	None	<input type="checkbox"/>	VirusLog1

Figure 10-9: The AVErrors rule.

Procedure—Create an exception for IT group:

1. In the VPM, select Policy>Add Web Access Layer. Name the rule AVExceptions.
2. Add the IT group object to the Source column.
3. Right-click the Service column; select Set. The Set Service Object dialog appears.
 - a. Click New; select ICAP Error Code. The Add ICAP Error Code Object appears.
 - b. Name the object password_protected.
 - c. Select Selected Errors.
 - d. From the list of errors, select Password Protected Archive; click Add.

Section A: ICAP

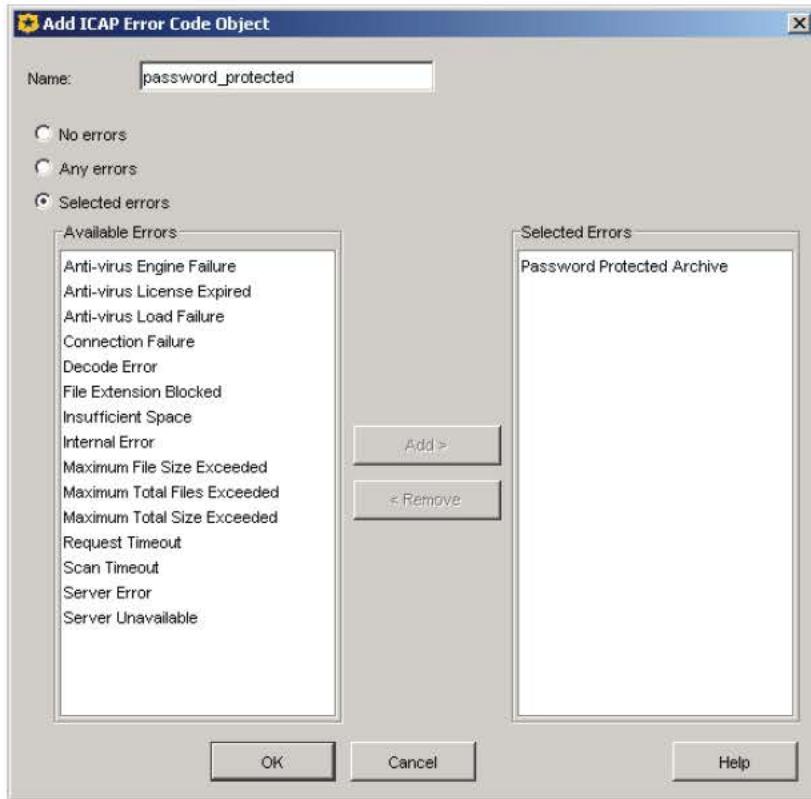


Figure 10-10: Specifying an ICAP Error Code object.

- e. Click OK; click OK again to add the object to the rule.
4. Right-click the Action column and select Allow.
5. Click Add Rule.
6. In the Service column, add the password_protected object.
7. Right-click the Action column; select Deny.

AVException							
No.	Source	Destination	Service	Time	Action	Track	Comment
1	IT	Any	password_protected	Any	Allow	None	
2	Any	Any	password_protected	Any	Deny	None	

Figure 10-11: The AVException layer.

Once this policy is installed:

- Virus scanning is performed for client attempts to upload content and content responses to client requests.

Section A: ICAP

- If a virus is detected and there were no scanning process errors, a log entry occurs.
- As the ProxyAV is configured to serve password-protected objects, only the IT group can download such files; everyone else is denied.

Exempting HTTP Live Streams From Response Modification

The following CPL examples demonstrate how to exempt HTTP live streams from response modification, as they are not supported by ICAP. The CPL designates user agents that are bypassed.

```
<proxy>
  url.scheme=http request.header.User-Agent="RealPlayer G2"
    response.icap_service(no)
  url.scheme=http request.header.User-Agent="(RMA)" response.icap_service(no)
  url.scheme=http request.header.User-Agent="(Winamp)" response.icap_service(no)
  url.scheme=http request.header.User-Agent="(NSPlayer)"
    response.icap_service(no)
  url.scheme=http request.header.User-Agent="(Windows-Media-Player)"
    response.icap_service(no)
  url.scheme=http request.header.User-Agent="QuickTime"
    response.icap_service(no)
  url.scheme=http request.header.User-Agent="(RealMedia Player)"
    response.icap_service(no)
```

Streaming Media Request Modification Limitation

Some HTTP progressive download streaming media transactions are complex enough to disrupt ICAP request modification services. If such behavior is noticed (most common with RealPlayer), implement the following workaround policy to bypass the ICAP request modification service for HTTP progressive downloads:

```
<proxy>
  url.scheme=http request_header.User-Agent="user_agent"
    request.icap_service(no)
  url.scheme=http request_header.User-Agent="user_agent"
    request.icap_service(no)

  where user_agent specifies a media player attribute that is disrupting service. For example:

<proxy>
  url.scheme=http request_header.User-Agent="(RealMedia Player)"
    request.icap_service(no)
  url.scheme=http request_header.User-Agent="RMA" request.icap_service(no)
```

CPL Notes

- If policy specifies that an ICAP service is to be used, but the service is not available, the default behavior is to fail closed—that is, deny the request or response. The following CPL allows objects to be served without ICAP processing if the server is down.

```
request.icap_service(service_name, fail_open)
response.icap_service(service_name, fail_open)
```

Section A: ICAP

Note: Blue Coat recommends this CPL to be used for internal sites; use with caution.

- To provide an exception to a general rule, the following CPL negates ICAP processing:

```
request.icap_service(no)  
response.icap_service(no)
```

Managing Virus Scanning

You might need to perform additional ProxySG maintenance concerning virus scanning, particularly for updates to the virus definition on the ICAP virus scanning server.

Advanced Configurations

This section summarizes more-advanced configurations between the ProxySG and multiple ICAP servers. These brief examples provide objectives and suggest ways of supporting the configuration.

Using Object-Specific Scan Levels

You can specify different scanning levels for different types of objects, or for objects from different sources.

This requires a service group of ICAP servers, with each server configured to provide the same level of scanning. For more information, see "Creating a Service Group" on page 348.

Improving Virus Scanning Performance

You can overcome request-handling limitations of ICAP servers. Generally, ProxySGs can handle many times the volume of simultaneous user requests that ICAP servers can handle.

This requires multiple ICAP servers to obtain a reasonable performance gain. On the ProxySG, define policy rules that partition requests among the servers. If you are going to direct requests to individual servers based on rules, configure in rule conditions that only use the URL. Note that you can increase the scale by using a service group, rather than use rules to partition requests among servers. For more information on using multiple ICAP servers, see "Creating a Service Group" on page 348. For more information on defining policies, see Chapter 12: "Managing Policy Files" on page 363, as well as the *Blue Coat Content Policy Language Guide*.

When the virus definitions are updated, the ProxySG stores a signature. This signature consists of the server name plus a virus definition version. If either of these changes, the ProxySG checks to see if the object is up to date, and then rescans it. If two requests for the same object are directed to different servers, then the scanning signature changes and the object is rescanned.

Updating the ICAP Server

If there is a problem with the integration between the ProxySG and a supported ICAP server after a version update of the server, you may need to configure the preview size the appliance uses. For information, see "Creating an ICAP Service" on page 325.

Section A: ICAP

Replacing the ICAP Server

If you replace an ICAP server with another supported ICAP server, reconfigure the ICAP service on the ProxySG:

```
SGOS#(config) external-services
SGOS#(config external-service) edit service_name
SGOS#(config service_name) url url
```

For information about these commands, see "Creating an ICAP Service" on page 325.

Access Logging

The ProxySG provides access log support for Symantec, Trend Micro, and Finjan ICAP 1.0 server actions (Management>Access Logging). The following sections describe access logging behavior for the various supported ICAP servers.

Symantec AntiVirus Scan Engine 4.0

When this Symantec server performs a scan, identifies a problem (for example, a virus), and performs a content transformation, the action is logged. For example:

```
"virus-id: Type=number; Resolution=[0 | 1 | 2]; Threat=name;"
```

where:

Type=number	Specifies the numeric code for the virus.
Resolution=	Specifies an integer value that indicates what action was taken to fix the file. Zero (0) defines the file is unrepairable, one (1) specifies that the file was repaired, and two (2) specifies that the file was deleted.
Threat=	Specifies the name of the virus.

Trend Micro Interscan WebProtect v 1.5

When of these Trend Micro ICAP servers performs a scan, identifies a problem (for example, a virus), and performs a content transformation, the action is logged. For example:

```
"virus-id: name"
```

where *name* specifies the name of the virus.

Important: The ivscan.ini ISWP configuration file on the Trend Micro server must contain the following entry:

```
'yes': security_gateway_virus_log=yes.
```

Finjan SurfinGate 7.0

When this Finjan ICAP server performs a scan, identifies a problem (for example, a virus), and performs a content transformation, the action is logged. For example:

```
"virus-id: name, response-info: Blocked, response-desc: virus_name was detected"
```

Section A: ICAP

Finjan ICAP servers also log occurrences of malicious mobile code.

Note: The access log string cannot exceed 256 characters. If the header name or value extends the length over the limit, then that string does not get logged. For example, if the `x-virus-id` header value is 260 characters, the access log displays `x-virus-id:` with no value because the value is too long to display. Furthermore, if the access log string is already 250 characters and the ProxySG attempts to append a `Malicious-Mobile-Type:` string, the string is not appended.

Access log entries might vary depending upon the type of ICAP scan performed and the custom log formats. For information about Access Logging, see Chapter 19: “Access Logging” on page 641.

References

The following are selected references for this feature.

Note: As with any Web site, addresses are subject to change or deletion at any time.

- **Symantec**—A provider of Internet security technology, including content and network security software and appliance solutions.
<http://www.symantec.com/>
<http://enterprisesecurity.symantec.com/products/>
- **Trend Micro**—A provider of network anti-virus and Internet content security software and services.
<http://www.trendmicro.com/>
- **Finjan**—A provider of proactive active content defense, virus protection, and Web and email content filtering solutions.
<http://www.finjan.com/>
- **ICAP Forum**—A resource on Internet Content Adaptation Protocol (ICAP), an evolving Web architecture. ICAP effectively adapts content for user needs.
<http://www.i-cap.org/>

Section B: Websense

Section B: Websense

This section describes how to create and manage Websense off-box services on the ProxySG. The ProxySG supports Websense off-box server versions 4.3 and higher.

For more information about Websense and content filtering, see Chapter 17: “Content Filtering” on page 545.

Creating a Websense Service

To Configure a Websense Off-box Service through the Management Console:

1. Select Configuration>External Services>Websense.
2. Click New; the Add List Item dialog appears.
3. In the Add Websense Service field, enter an alphanumeric name; click OK.
4. Highlight the new Websense service name and click Edit; the Edit Websense Service Name dialog appears.

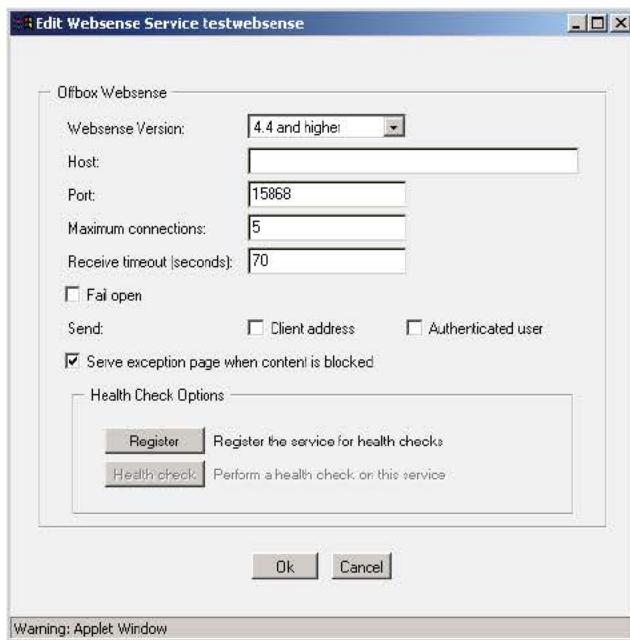


Figure 10-12: The Edit Websense Service Dialog

5. Enter following information:
 - a. Select the Websense server version: 4.3 or 4.4 and higher.
 - b. In the Host field, enter the hostname or IP address of the remote Websense server.
 - c. In the Port field, enter the port number of the Websense server; or leave as is to accept the default (15868).

Section B: Websense

- d. In the Maximum connections field, enter the maximum number of connections. The range is a number from 1 to 65535. The default is 5. Blue Coat recommends that the setting not exceed 200.
- e. In the Receive Timeout field, enter the number of seconds the ProxySG waits for replies from the Websense server. The range is 60 to 65535. The default timeout is 70 seconds.
6. Select the following options, as required:
 - a. Fail open—If a default Websense service is selected (from the External Services>Websense tab), a connection error with the Websense server results in requests and responses proceeding, as the default Websense service is subjected to policy.
 - b. Send client address—Sends the client IP address to the Websense server.
 - c. Send Authenticated user—Sends user information to the Websense server.
 - d. Serve exception page when content is blocked—If the requested content is defined by Websense as inappropriate, the client receives a page with information stating the content is blocked. When this option is selected, the exception page originates from the ProxySG; if not selected, the Websense server provides the exception page.
7. Click OK.
8. Optional: You can designate a default Websense service. On the Configuration>External Services>Websense tab, select a service from the Default service to use drop-down list.

To Register a Newly Created Websense Service for Health Checking:

For convenience, the Edit Websense Service dialog allows you to register a newly-created Websense service for health checking (this duplicates the functionality on the Configuration>Health Checks>General tab). Registering for health checking requires that a valid Websense server URL was entered.

- Click Register; a dialog prompts confirmation; click OK.
- You can also click Health check to perform an immediate health check on this service.

For more information about health checks, see Chapter 11: “Health Checks” on page 355.

To Configure a Websense Service through the CLI:

1. At the `(config)` command prompt, enter the following commands:

```
SGOS# (config) external-services
SGOS# (config external-services) create websense service_name
```

Specify a unique alphanumeric name for each service.

2. To configure the service, enter the following commands:

```
SGOS# (config external-services) edit service_name
SGOS# (config websense service_name) version {4.3 | 4.4}
```

where *version* specifies 4.3 or 4.4 and higher.

```
SGOS# (config websense service_name) host {hostname | IP_address}
```

where *hostname* or *IP_address* specifies the Websense server.

Section B: Websense

SGOS# (config websense service_name) **port** *port_number*

where *port_number* specifies the port number of the Websense server. The default port number is 15868.

SGOS# (config websense service_name) **max-conn** *number*

where *number* is the maximum number, from 1 to 65535, of connections the Websense service uses to connect to the Websense server. The default number is 5. Blue Coat recommends that the setting not exceed 200.

SGOS# (config websense service_name) **timeout** *timeout_seconds*

where *timeout_seconds* is the number of seconds, from 60 to 65535, the ProxySG waits for replies from the Websense server. The default timeout is 70 seconds.

SGOS# (config websense service_name) **send** {**client-address** | **authenticated-user**}

Specifies to send the client IP address or authenticated user information to the Websense server.

3. Optional: You can automatically detect the categories defined on the Websense server.

SGOS# (config websense service_name) **sense-categories**

4. Optional: You can designate a default Websense service.

SGOS# (config websense service_name) **apply-by-default**

This Websense service is now the default and is used if failover is enabled.

5. Optional: You can enable failover. If a default Websense service is selected (from the External Services>Websense tab), a connection error with the Websense server results in requests and responses proceeding, as the default Websense service is subjected to policy.

SGOS# (config websense service_name) **fail-open**

6. Optional: You can send a test URL to the Websense server to verify content filtering is active.

SGOS# (config websense service_name) **test-url** *url*

where *url* is a valid URL that points to a site determined categorized by Websense as inappropriate.

Deleting a Websense Service

The following steps describe how to delete an Websense service.

Note: You cannot delete a Websense service used in a ProxySG policy (that is, if a policy rule uses the Websense service name) or if the service belongs to a service group.

To Delete a Websense Service through the Management Console:

1. Select Configuration>External Service>Websense.
2. Select the service to be deleted.
3. Click Delete; click OK to confirm.

Section B: Websense

4. Click Apply.

To Delete an Websense Service through the CLI:

At the (config) prompt, enter the following commands:

```
SGOS#(config) external-services
SGOS#(config external-services) delete service_name
```

Section C: Service Groups

Section C: Service Groups

This section describes how to create and manage ICAP or Websense service groups. In high-traffic network environments, a service group accelerates response time by performing a higher volume of scanning.

Creating a Service Group

Create the service group and add the relevant ICAP or Websense services to the group. Services within group must be the same type (ICAP or Websense).

To Configure a Service Group through the Management Console:

1. Select Configuration>External Services>Service-Groups.
2. Click New; the Add List Item dialog appears.
3. In the Add Service Group field, enter an alphanumeric name; click OK.
4. Highlight the new service group name and click Edit; the Edit Service Group dialog appears.



Figure 10-13: The Edit Service Group Dialog

5. Click New to add a service to the service group; the Add Service Group Entry dialog appears.

Section C: Service Groups



Figure 10-14: The Add Service Group Entry Dialog

6. Select List ICAP services or List Websense services. The picklist displays the available configured services that are eligible for this service group.
7. Select a service; to select multiple services, use Ctrl-click. Click OK.
8. To assign a weight value to a service, select a service and click Edit; the Edit Service Group Entry weight dialog appears. In the Entry Weight field, assign a weight value. The valid range is 0-255. For detailed information about service weighting, see the next topic, "About Weighted Load Balancing" on page 350.
9. Click OK; click OK again to close the Edit Service Group Entry dialog
10. Click Apply.

To Configure a Service Group through the CLI:

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) external-services
SGOS#(config external-services) create service-group name
SGOS#(config service-group name) add service_name
```

Enter a unique alphanumeric name for each service; the ICAP or Websense service must already exist on the ProxySG.

2. Repeat the add service_name command for each service to be added.

The type of service group (ICAP or Websense) is determined by the first service added. For example, if the first added service is an ICAP service, the service group is automatically defined as an ICAP service group. If you attempt to add a Websense service, an error is displayed.

3. To assign weights to each service, enter the following commands:

```
SGOS#(config service-group name) edit service_name
SGOS#(config service-group name) weight value
```

where value is from 0 to 255. For information about weight values, see "About Weighted Load Balancing" on page 350.

Section C: Service Groups

Deleting a Service Group or Group Entry

You can delete the configuration for an entire service group from the ProxySG, or you can delete individual entries from a service group.

Note: A service or service group used in a ProxySG policy (that is, if a policy rule uses the entry) cannot be deleted; it must first be removed from the policy.

To Delete a Service Group through the Management Console:

1. Select Configuration>External Services>Service-Groups.
2. Select the service group to be deleted.
3. Click Delete; click OK to confirm.
4. Click Apply.

To Delete a Service Group through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) external-services
SGOS# (config external-services) delete service_group_name
```

To Delete a Service Group Entry through the Management Console:

1. Select Configuration>External Services>Service-Groups.
2. Select the service group to be modified.
3. Click Edit.
4. Select the service entry; click Delete.
5. Click OK; click Apply.

To Delete a Service Group Configuration through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) external-services
SGOS# (config external-services) edit service_group_name
SGOS# (config type name) remove entry_name
```

About Weighted Load Balancing

The ProxySG supports weighted load balancing in forwarding requests to service groups. By default, the ProxySG performs typical round-robin load balancing and evenly forwards requests sequentially to servers as defined within the service group. Manually assigning weights takes advantage of round-robin load balancing in service groups that are not homogeneous, or where the servers have different capacities.

Section C: Service Groups

Weighting determines what proportion of the load one server bears relative to the others. If all servers have either the default weight (1) or the same weight, each share an equal proportion of the load. If one server has weight 25 and all other servers have weight 50, the 25-weight server processes half as much as any other server.

Before configuring weights, consider the relative weights to assign to each server. Factors that could affect assigned weight of a ICAP server include the following:

- The processing capacity of the server hardware in relationship to other servers (for example, the number and performance of CPUs or the number of network interface cards)
- The maximum number of connections configured for the service. Note that the maximum connections setting pertains to how many simultaneous scans can be performed on the server, while weighting applies to throughput in the integration. While these settings are not directly related, consider both when configuring weighted load balancing. For more information on maximum connections, see "Creating an ICAP Service" on page 325 and "Creating a Websense Service" on page 344.

The table below provides an example of how weighting works with a service group of three ICAP servers, Server1, Server2, and Server3. Because Server3 is a higher-capacity server (including dual CPUs and multiple network interface cards (NICs)) compared to Server1 and Server2, it is assigned a heavier weight. Using the weights below, for every 100 requests forwarded to the service group, Server3 receives 60 requests, while Server1 and Server2 each receive 20 requests.

Table 10.1: Example of Weighted Load Balancing for an ICAP Service Group

ICAP server	Capacity	ICAP service / Maximum connections	Weight
Server1	Standard	Service1 / 10	1
Server2	Standard	Service2 / 10	1
Server3	High	Service3 / 25	3

Note: Setting the weight value to 0 (zero) disables weighted load balancing for the ICAP service. Therefore, if one ICAP server of a two-server group has a weight value of 1 and the second a weight value of 0, should the first server go down, a communication error results because the second server cannot process the request.

While you cannot specifically designate an ICAP server in a group as a backup, you can specify weight values that create a large differential between a server that is used continuously and one that is rarely used, thus simulating a backup server.

Section D: Displaying External Service and Group Information

Section D: Displaying External Service and Group Information

After configuring a service or service group, you can display information either for all or individual service groups.

To Display Information about all External Services and Groups through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) external-services
SGOS# (config external-services) view

; External Services
icap4
ICAP-Version:      1.0
URL:              icap://10.1.1.1
Max-conn:          5
Timeout (secs):   70
Health-checks:     no
Patience-page (secs): disabled
Notification:     never
Methods:           RESPMOD
Preview-size:      0
Send:              nothing
ISTag:

websense4
Version:          4.4
Host:              www.websense.com/list
Port:              15868
Max-conn:          5
Timeout (secs):   70
Send:              nothing
Fail-by-default:  closed
Apply-by-default: no
Serve-exception-page:yes

; External Service-Groups
CorpICAP
  total weight 5
entries:
  ICAP1
    weight 4
  ICAP2
    weight 1

BranchWebsense
  total weight  2
entries:
  Websense1
    weight    1
  Websense2
    weight    1
```

Section D: Displaying External Service and Group Information

To Display Information about an Individual Service or Service Group through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) external-services
SGOS#(config external-services) edit {service_name | service_group_name}
SGOS#(config type name) view
```


Chapter 11: Health Checks

This chapter discusses health checks for services and hosts and describes how to configure the ProxySG.

About General Health Checks

The ProxySG can perform health checks on a forwarding host or external server that is providing a service. The supported server types are HTTP, HTTPS, ICAP, Websense (off-box), and SOCKS gateways, Layer-3, and Layer 4 forwarding hosts.

Based on the health check type, the ProxySG periodically verifies the health status, and thus the availability, of the host. The time interval between checks is configurable. If the health check is successful, the ProxySG considers the host available. If the initial health check is not successful for a host, the ProxySG retries, using the number of attempts in the health check failure count. If the health check is not successful for every server in a domain, the ProxySG might not serve stale content from its object store, depending on the ProxySG configuration.

The following table describes the types of health checks.

Table 11.1: Types of Health Checks

Health check type	Description
HTTP	Use this type to confirm that the host can fulfill a content request over HTTP by the ProxySG. The ProxySG accepts only a 200 OK as a healthy response.
Criterion for success	The ProxySG fetches the object.
Criterion for failure	The ProxySG cannot fetch the object.
HTTPS	Use this type to confirm that the host can fulfill a content request over HTTPS by the ProxySG. The ProxySG accepts only a 200 OK as a healthy response.
Criterion for success	The ProxySG fetches the object.
Criterion for failure	The ProxySG cannot fetch the object.
Layer-3 health check	Use this type to confirm the basic connection between the ProxySG and the origin server. The server must recognize ICMP echoing. The ProxySG sends a ping (three Internet Control Message Protocol [ICMP] echo requests) to the host.
Criterion for success	The ProxySG receives at least one ICMP echo reply.
Criterion for failure	The ProxySG does not receive a single ICMP echo reply.
Layer-4 health check	Use this type to confirm that the ProxySG can connect to the host HTTP and FTP ports. The ProxySG attempts to establish a TCP connection to an HTTP port or FTP port on the host.

Table 11.1: Types of Health Checks (Continued)

Health check type	Description
Criterion for success	The ProxySG establishes the connection to the defined port (of any type), then closes it. For global forwarding checks, the first defined port in the forwarding host port list is used for the attempt (except for SOCKS gateways, in which the SOCKS port is used).
Criterion for failure	The ProxySG cannot establish the connection.
ICAP health check and Websense 4 off-box	Requests are not sent to <i>sick</i> services. If a health check determines the service is healthy, requests resume.

Configuring Service-Specific Health Checks

This section describes how to create a health check service for a specific host (for example, an ICAP server). A failed health check results in administrator notification; however, unlike global forwarding health checks, the ProxySG does not recognize the healthy or sick status of the host and thus alters where it sends transactions.

To Configure Health Checks through the Management Console:

Part 1: General Tasks

This part of the procedures is the same for all health check types.

1. Select Configuration>Health Checks>General.
2. Click New.
3. In the Add Health Check dialog, specify a name for the health check service; click OK.
4. In the Health Check list, select the newly created service and click Edit; the Edit Health Check dialog displays.

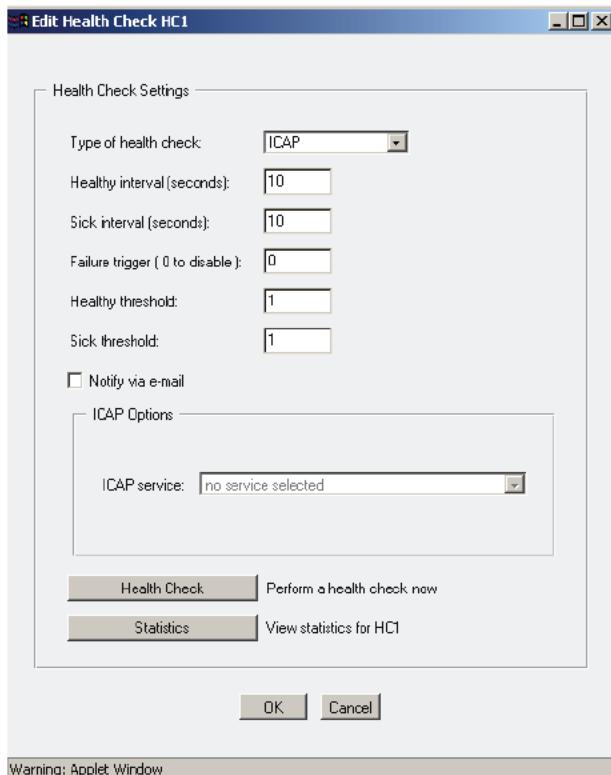


Figure 11-1: Edit Health Check Dialog

5. Select the health check type (HTTP, HTTPS, ICAP, Layer-3, Layer-4, or Websense off-box).
6. Specify the healthy interval, in seconds, between health checks to the server. The default is 10.
7. Specify the sick interval, in seconds, between health checks to the server that has been determined to be sick, or out of service. The default is 10.
8. Specify the failure trigger, or the number of failed connections to the server before a health check is triggered. Valid values are 0-65535, where 0 disables the trigger. The default is 0.
9. Specify the healthy threshold, or the number of successful health checks before an entry is considered healthy. Valid values are 1-65535. The default is 1.
10. Specify the sick threshold, or the number of failed health checks before an entry is considered sick. Valid values are 1-65535. The default is 1.
11. Optional: Select the Notify via email checkbox to send notification mail when the health of a service changes. Recipients are specified in Management>Event Logging>Mail.

Note: To enable health check notification, you must set the event logging level to **Informational** or **Verbose**. For more information about event logging, see "Event Logging and Notification" on page 698.

Part 2: Health Check Type Specific Tasks

This part of the procedure configures the health check based upon the type selected.

1. Upon selecting the health check type, the Options section of the dialog changes to display the appropriate configuration fields. Enter the required information:
 - HTTP and HTTPS: Enter the URL of the server to be checked.
 - ICAP: Select the ICAP service. The ICAP service must already be configured on the ProxySG (see Chapter 10: "External Services").
 - Layer-3 and Layer-4: Enter the host name; for Layer-4, also enter the port number.
 - Websense off-box: Select the Websense service. The Websense service must already be configured on the ProxySG (see Chapter 10: "External Services"). Enter the URL to be test-categorized, or click Use default.
2. Click OK to close the Edit Health Check dialog; Click Apply to apply the configuration to the ProxySG.

To Specify a Health Check through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) health-check
SGOS# (config health-check) create name
SGOS# (config health-check) edit name
SGOS# (config health-check name) type {layer-3 | layer-4 | http | https | icap | websense-offbox}
```

where *type* specifies the type of health check.

```
SGOS# (config health-check name) type parameter
```

where *type* is the type of health check and *parameter* is the required attribute:

```
layer-3 hostname host_name
layer-4 hostname host_name
layer-4 port port
{http | https} url url
```

icap servicename service_name—The ICAP service must already be configured on the ProxySG. See Chapter 10: "External Services".

websense-offbox servicename service_name—The Websense service must already be configured on the ProxySG. For more information, see Chapter 10: "External Services".

```
websense-offbox {url | default-url}
```

```
SGOS# (config health-check name) interval healthy seconds
```

where *seconds* specifies the interval between health checks to the server. The default is 10.

```
SGOS# (config health-check name) interval sick seconds
```

where *seconds* specifies the interval between health checks to the server that has been determined to be sick. The default is 10.

```
SGOS# (config health-check name) threshold healthy number
```

where *number* is the number of successful health checks before an entry is considered healthy. Valid values are 1-65535. The default is 1.

```
SGOS#(config health-check name) threshold sick number
```

where *number* is the number of failed health checks before an entry is considered sick. Valid values are 1-65535. The default is 1.

```
SGOS#(config health-check name) failure-trigger number
```

where *number* is the number of failed connections to the server before a health check is triggered. Valid values are 0-65535, where 0 disables the trigger. The default is 0.

Optional:

```
SGOS#(config) health-check name) notify
```

Sends e-mail notification when the health of a service changes. The recipients are specified in (config event-log) mail add *option*.

Note: To enable health check notification, you must set the event logging level to Informational or Verbose. For more information about event logging, see "Event Logging and Notification" on page 698

Perform an Instant Health Check

You can manually issue a health check request.

To Do a Health Check through the Management Console:

1. Select Health Checks>General.
2. Select a health check name.
3. Click Edit.
4. Click Health Check.

To Do a Health Check through the CLI:

At the (config) prompt, enter the following commands:

```
SGOS#(config) health-check
SGOS#(config) health-check) edit health_check_name
SGOS#(config) health-check name) perform-health-check
```

About Global Forwarding and SOCKS Gateway Health Checks

This section describes health checks that can be configured on the ProxySG that apply to all forwarding hosts and SOCKS gateway hosts.

When the ProxySG performs a health check on one or more hosts, it determines whether the host returns a response and is available to fill a content request. A positive health check indicates that there is an end-to-end connection and that the host is healthy and is able to return a response.

With multiple forwarding hosts, health checks are vital to ProxySG efficiency. When hosts respond positively to health checks, the ProxySG forwards requests to those hosts and not to unavailable hosts, which provides quicker content fill requests. With a single forwarding host, health checking is also important to determine whether the host is available.

Note: When a forwarding host or SOCKS gateway is created, it is automatically registered for health checks. Similarly, when a forwarding host or SOCKS gateway is deleted, it is removed from the health check registry.

Configuring Global Health Checks

This section describes how to configure the ProxySG to perform global health checks.

To Configure Global Forwarding Host or SOCKS Gateway Health Checks through the Management Console:

1. Select Configuration>Health Checks>Forwarding or SOCKS Gateway.

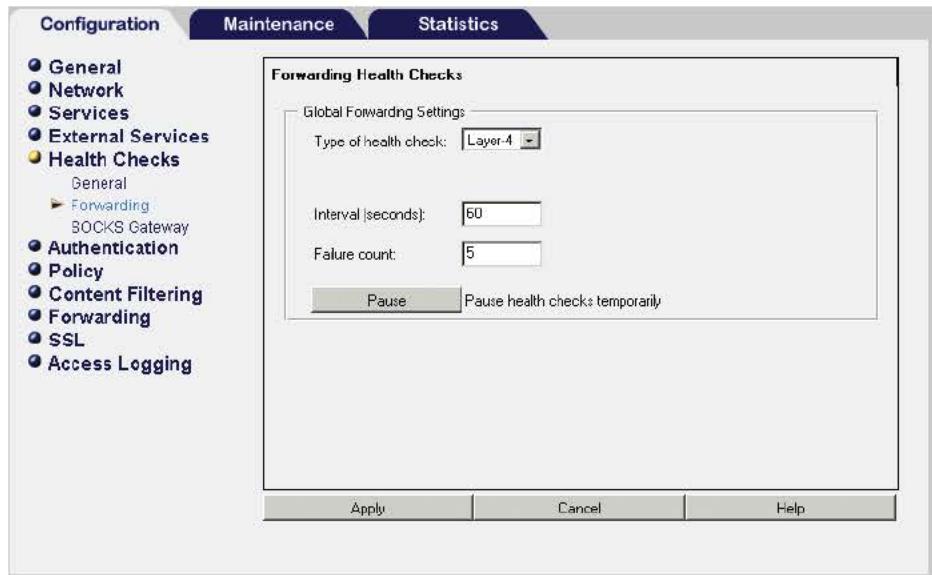


Figure 11-2: Global Forward Health Check Tab

2. Select the health check type:
 - Forwarding—HTTP, HTTPS, Layer-3, or Layer-4.
 - SOCKS Gateway—Layer-3 or Layer-4.
3. Specify the interval, in seconds, between health checks. The default is 60.
4. Specify the failure count, which specifies the number of sequential failures before the host is considered down. The default is 5.
5. Click Apply.

To Configure Global Forwarding Host Health Checks through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) health-check
SGOS# (config health-check) forwarding type {http | https | layer-3 | layer-4}
SGOS# (config health-check) forwarding interval seconds
```

where seconds specifies the time between health checks.

```
SGOS# (config health-check) forwarding failcount count
```

where count specifies the number of sequential failures before the host is considered down.

The default is 5.

To Configure Global SOCKS Gateways Health Checks through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) health-check
SGOS# (config health-check) socks-gateways type {layer-3 | layer-4}
SGOS# (config health-check) socks-gateways interval seconds
```

where seconds specifies the time between health checks.

```
SGOS# (config) health-check socks-gateways failcount count
```

where count specifies the number of sequential failures before the host is considered down.

The default is 5.

Pausing or Resuming Global Health Checking

You can temporarily halt global health checks and resume when ready. This is helpful if the ProxySG needs to be temporarily taken out of service.

Note: If the health check is paused, the state remains paused until the resume option is invoked. The paused state remains even after a reboot.

To Pause or Resume Health Checking through the Management Console:

1. Select Configuration>Health Checks>Forwarding or SOCKS Gateway.
2. Click Pause.
3. To resume health checks, click Resume.

To Pause or Resume Health Checking through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) health-check
SGOS# (config) health-check {forwarding | socks-gateways} {pause | resume}
```


Chapter 12: Managing Policy Files

Policy files contain the policies that manage every aspect of the ProxySG, from controlling user authentication and privileges to disabling access logging or determining the version of SOCKS.

The policy for a given system can contain several files with many layers and rules in each. Policies can be defined through the Visual Policy Manager (VPM) or composed in Content Policy Language (CPL). (Some advanced policy features are not available in VPM and can only be configured through CPL.)

Policies are managed through four files:

- Central policy file—Contains global settings to improve performance and behavior and filters for important and emerging viruses (such as Code Red and Nimda). This file is usually managed by Blue Coat, although you can point the ProxySG to a custom Central policy file instead.
- Forward policy file—Usually used to supplement any policy created in the other three policy files. The Forward policy file contains Forwarding rules when the system is upgraded from a previous version of SGOS (2.x) or CacheOS (4.x).
- Local policy file—A file you create yourself. When VPM is not the primary tool used to define policy, the Local file contains the majority of the policy rules for a system. If VPM is the primary tool, this file is either empty or includes rules for advanced policy features that are not available in VPM.
- Visual Policy Manager—The policy created by VPM can either supplement or override the policies created in the other policy files.

This chapter contains the following sections:

- "About Policy Files"
- "Creating and Editing Policy Files"
- "Managing the Central Policy File"
- "Viewing Policy Files"

To learn about writing policies, refer to the *Blue Coat Content Policy Language Guide*.

About Policy Files

When creating the files, keep in mind:

- The order in which the files are evaluated.
- The transaction default settings, which control whether you allow everything or deny everything by default.
- Whether or not to use VPM.

Policy File Evaluation

The order in which the ProxySG evaluates policy rules is important. Changes to the evaluation order can result in different effective policy, as the order of policy evaluation defines general rules and exceptions. While this order is configurable, the default and recommended order is:

VPM File—Local Policy File—Central Policy File—Forward File

This prevents policies in the Central file that block virus signatures from being inadvertently overridden by allow (access-granting) policy rules in the VPM and Local files.

When changing the policy file evaluation order, remember that final decisions can differ because decisions from files later in the order can override decisions from earlier files (the Forward policy file order cannot be changed).

For a new ProxySG, the default evaluation order is: VPM, Local, Central, and Forward.

For an upgraded ProxySG, the policy evaluation order is the order already existing on the appliance before the upgrade.

To Change Policy Order through the Management Console:

1. Select Configuration>Policy>Policy Options.

The Policy Options tab displays.

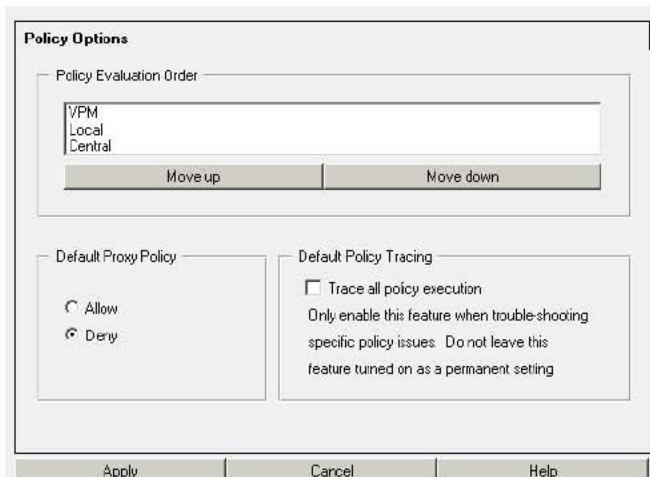


Figure 12-1: Policy Options Tab

2. To change the order, select the file to move and click the Move Up or Move Down button. Remember that the last file in the list overwrites decisions in files evaluated earlier.

To Change Policy Order through the CLI:

At the (config) command prompt, enter the command:

```
SGOS# (config) policy order v l c
```

where v (VPM), l (local), and c (central) specify the order of evaluation. These are case-insensitive, but you must enter all three in any order, including a space between each letter.

Note: Use the `show policy order` command to check the current settings.

Transaction Settings: Deny and Allow

The default <Proxy> transaction policy is *deny everything* or *allow everything*, depending on whether this is a new installation or an upgrade. You can change the default policy.

- A default <Proxy> transaction policy of Deny prohibits proxy-type access to the ProxySG: you must then create policies to explicitly grant access on a case-by-case basis. This is the default for those who are installing a new release of SGOS without an upgrade and for administrator transactions.
- A default <Proxy> transaction policy of Allow permits any and all proxy-types access to the ProxySG: you must then create policies to explicitly deny access on a case-by-case basis. This is the default for those upgrading from a previous version of CacheOS and for <Cache> transactions.

Changing the default <Proxy> transaction policy affects the basic environment in which the overall policy is evaluated. It is likely that you must revise policies to retain expected behavior after such a change.

Also consider:

- Changes to the evaluation order might result in different effective policy, because the order of policy evaluation defines general rules and exceptions.
- Changes made to <Proxy> transactions do not affect <Cache> transactions and <Admin> transactions.

To Configure Deny or Allow Default Policy through the Management Console:

1. Select Configuration>Policy>Policy Options.
2. Under Default Proxy Policy, select either Deny or Allow.
3. Click Apply.

To Configure the Deny or Allow <Proxy> Transaction Policy through the CLI:

At the (config) command prompt, enter the following command

```
SGOS# (config) policy proxy-default {allow | deny}
```

Policy Tracing

Tracing enabled with the Management Console or CLI is global; that is, it records every policy-related event in every layer. It should be used only while troubleshooting. For information on troubleshooting policy, refer to the *Blue Coat Content Policy Language Guide*. Turning on policy tracing of any kind is expensive in terms of system resource usage, and it will slow down the ProxySG's ability to handle traffic.

To Enable Policy Tracing through the Management Console:

1. Select Configuration>Policy>Policy Options.
2. Select Trace all policy execution.

3. Click Apply.

To Enable Policy Tracing through the CLI:

From the command prompt, enter the following command:

```
SGOS# policy trace {all | none}
```

Creating and Editing Policy Files

You can create and edit policy files two ways:

- Through the Management console (recommended).
- Through the CLI inline policy command (not recommended because the policies can grow large and using `inline policy` overwrites any existing policy on the ProxySG).

You can use VPM to create policy layers and rules in the VPM file. For information on managing the VPM file, see Chapter 13: “The Visual Policy Manager” on page 377.

To create or edit policy files, use CPL to define policy rules (refer to the *Blue Coat Content Policy Language Guide*). You can use the Management Console or CLI to create or edit policy files directly, or create a file that can be uploaded to the ProxySG through the Management Console or CLI.

Create and Edit Policy Files

You can install the policy files in the following ways.

- Using the ProxySG Text Editor, which allows you to enter directives (or copy and paste the contents of an already-created file) directly onto the ProxySG.
- Creating a local file on your local system; the ProxySG can browse to the file and install it.
- Using a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the ProxySG.
- Through the CLI `inline` command.

The ProxySG compiles the new policy from all source files and installs the policy, if the compilation is successful.

Important: If errors or warnings are produced when you load the policy file, a summary of the errors and/or warnings is displayed automatically. If errors are present, the policy file is not installed. If warnings are present, the policy file is installed, but the warnings should be examined.

To Define and Install Policy Files Directly through the Management Console:

1. Select Configuration>Policy>Policy Files>Policy Files.

The Policy Files tab displays.

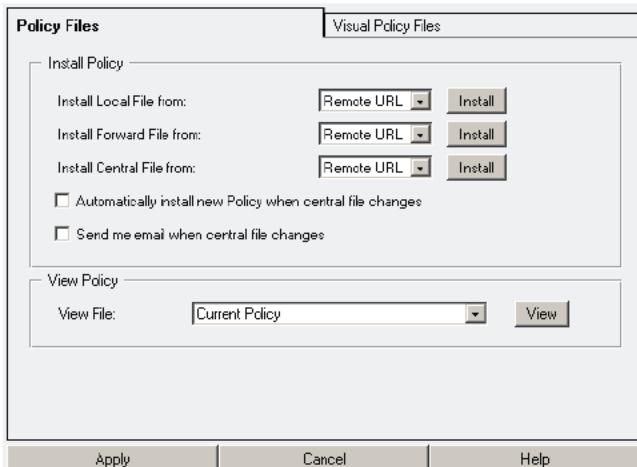


Figure 12-2: Policy Files Tab

2. From the appropriate Install Local/Forward/Central File from drop-down list, select the method you want to use to install the local, forward, or central policy configuration; click **Install** and complete one of the three procedures below:

- Installing a policy file using a Remote URL:**

In the Install Local/Forward/Central File dialog that appears, enter the fully-qualified URL, including the filename, where the policy configuration is located. To view the file before installing it, click **View**. Click **Install**. The Installation Status field summarizes the results; click the **Results** button to open the policy installation results window. Close the window when you are finished viewing the results; click **OK** in the Install Local/Forward/Central File dialog.

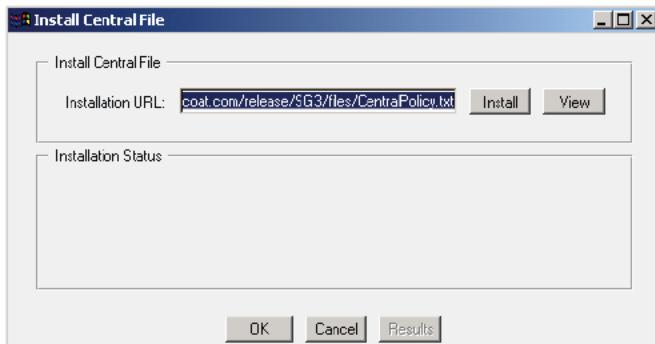


Figure 12-3: Policy Files Remote Installation Dialog

Note: If you use the default Blue Coat Central policy file, load it from:

<https://download.bluecoat.com/release/SG3/files/CentralPolicy.txt>

If you install a Central policy file, the default is already entered; change this field only if you want to create a custom Central policy file.

To load a Forward, Local, or a custom Central policy file, move it to an HTTP or FTP server, and then use that URL to download the file to the ProxySG.

Installing a policy file using a Local File:

In the Upload and Install File window that opens, either enter the path to the file into the **File to upload** field, or click **Browse** to display the Choose file dialog, locate the file on the local system, and open it. Click **Install**. When the installation is complete, the installation results display. View the results and close the window.

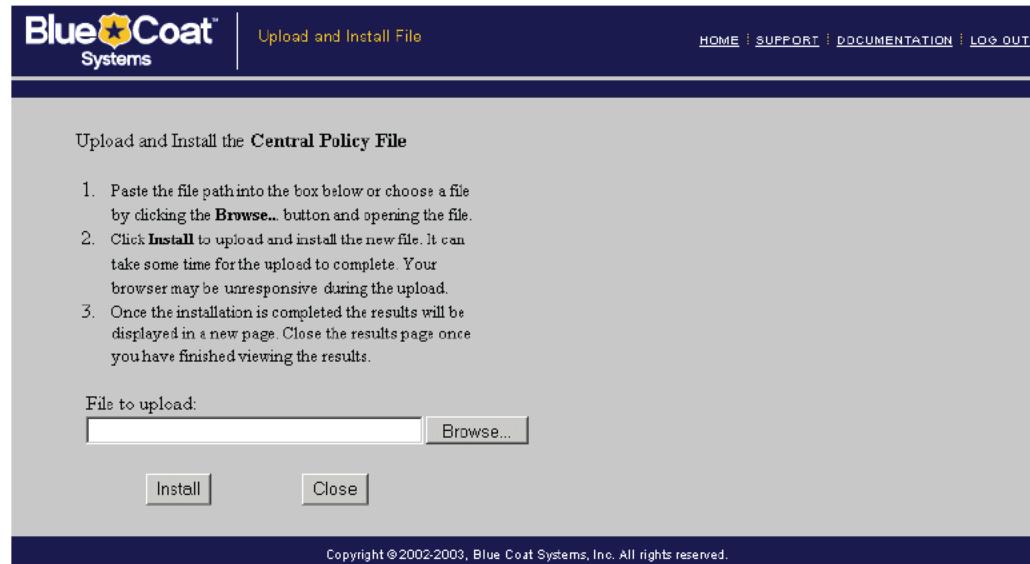


Figure 12-4: Specifying the Local Location of a Policy File

Installing a policy file using a Text Editor:

The current configuration is displayed in installable list format. Define the policy rules using CPL in the Edit and Install File window that opens (refer to the *Blue Coat Content Policy Language Guide*); click **Install**. When the installation is complete, a results window opens. View the results, close the results window and click **Close** in the Edit and Install File window.



Figure 12-5: Edit and Install File Window

Using the CLI Inline Command

To create policies using the CLI, you can use the `ProxySG inline` policy command. This command either creates a new policy file or, if the specified file already exists, overwrites an existing policy file. You cannot edit an existing policy file using this command.

Note: If you are not sure whether a policy file is already defined, check before using the `inline` policy command. For more information, see "Viewing Policy Source Files" on page 374.

To Create Policy Files through the CLI:

1. At the `(config)` command prompt, enter the following command:

`SGOS#(config) inline policy file end-of-input-marker`

where `file` specifies the type of policy you want to define: `Central` (Central policy file), `Forward` (Forward policy file), or `local` (local policy file).

Note: Do not use the `inline` policy command with files created using the VPM module.

`end-of-file-marker`—Specifies the string that marks the end of the current inline command input; `eof` usually works as a string. The CLI buffers all input until you enter the marker string.

2. Define the policy rules using CPL (refer to the *Blue Coat Content Policy Language Guide*).

Enter each line and press <Enter>. To correct mistakes on the current line, use <Backspace>. If a mistake has been made in a line that has already been terminated by <Enter>, exit the `inline policy` command by typing `Ctrlc` to prevent the file from being saved.

3. Enter the `eof` marker to save the policies and exit the `inline` mode.

For more information on the `inline` command, refer to the *Blue Coat Command Line Interface Reference*.

To Load Policy Files through the CLI:

At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) policy {forward-path | local-path | central-path} url  
SGOS#(config) load policy {forward | local | central}
```

The ProxySG compiles and installs the new policy. The ProxySG might display a warning if the new policy causes conflicts. If a syntax error is found, the appliance displays an error message. For information about these messages, refer to the *Blue Coat Content Policy Language Guide*. Correct the error, then reload the file.

Unloading Policy Files

To disable policies, do the following procedure to unload the compiled policy file from the ProxySG memory. These steps describe how to replace a current policy file with an empty policy file.

To keep a current policy file, either make a backup copy or rename the file before unloading it. By renaming the file, you can later reload the original policy file. If you use multiple policy files, back up or rename files as necessary. Alternatively, rather than use an empty policy file, you can delete the entire contents of the file, then reload it.

To unload policies defined using the VPM, you can either:

- Do the procedure below for unloading policies through the CLI.
- Use the VPM and individually delete all layers.

To Unload Policies through the Management Console:

1. Select Configuration>Policy>Policy Files>Policy Files.
2. Select Text Editor in the Install Local/Forward/Central File from drop-down list and click the appropriate Install button.
The Edit and Install the Local/Forward/Central Policy File window opens.
3. Delete the text and click Install.
4. View the results in the results page that opens; close the page.
5. Click Close.

To Unload Policies through the CLI:

1. At the `(config)` command prompt, enter the following command:

```
SGOS#(config) inline policy file end-of-input-marker
```

where:

<code>file</code>	Specifies the type of policy you want to define: <code>central</code> (central policy file), <code>local</code> (local policy file), <code>vpm-cpl</code> , or <code>vpm-xml</code> (VPM policy files, usually defined using the VPM).
<code>end-of-input-marker</code>	Specifies the string that marks the end of the current <code>inline</code> command input. The CLI buffers all input until you enter the marker string. <code>eof</code> is commonly used as the marker.

Note: If you use the CLI to unload VPM-generated policies, you must run the `inline` command twice; once for the CPL file and once for the XML file.

2. Enter an `end-of-input-marker` to save the policies and exit inline mode. Enter nothing else.
3. If you use multiple policy files, repeat step 1 and step 2 for each policy file used.

For more information on the `inline` policy command, refer to the *Blue Coat Command Line Interface Reference*.

Managing the Central Policy File

The Central policy file is updated when needed by Blue Coat. The file can be updated automatically or you can request email notification. You can also configure the path to point to your own custom Central policy file.

Configuring Automatic Installation

You can specify whether the ProxySG checks for a new version of the Central policy file. If a new version exists, the appliance can install it automatically.

Configuring the ProxySG for Automatic Installation

Do the following procedure to configure the ProxySG to check for and install a new version of the Central policy file.

To Configure Automatic Installation through the Management Console:

1. Select Configuration>Policy>Policy Files>Policy Files.
2. Select Automatically install new Policy when central file changes.
3. Click Apply.

To Configure Automatic Installation through the CLI:

At the `(config)` command prompt, enter the following command:

```
SGOS# (config) policy subscribe
```

Configuring a Custom Central Policy File for Automatic Installation

If you define your own Central policy file, you can configure the ProxySG to automatically install any subsequent updated version of the file. To use this capability, you must change the Central policy file's first line with each version update. With automatic installation, the ProxySG checks for a change to the first line of the file. In defining a custom Central policy file, add an item, such as a comment, to the first line of the Central policy file that changes with each update. The following is a sample first line, containing date information that is routinely updated with each version:

```
; Central policy file MonthDate, Year version
```

When you update and save the file in the original location, the ProxySG automatically loads the updated version.

Configuring Email Notification

You can specify whether the ProxySG sends email when the Central policy file changes. The email address used is the same as that used in diagnostic reporting; the event recipient for the custom heartbeat email. For information about diagnostic reporting, see "Diagnostic Reporting (Heartbeats)" on page 846.

To Configure Email Notification through the Management Console:

1. Select Configuration>Policy>Policy Files>Policy Files.
2. Select Send me email when central file changes.
3. Click Apply.

To Configure Email Notification through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) policy notify
```

Configuring the Update Interval

You can specify how frequently the ProxySG checks for a new version of the Central policy file. By default, the appliance checks for an updated Central policy file once every 24 hours (1440 minutes). You must use the CLI to configure the update interval. You cannot configure the update interval through the Management Console.

To Configure the Update Interval through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) policy poll-interval minutes
```

Checking for an Updated Central Policy File

You can manually check whether the Central policy file has changed. You must use the CLI. You cannot check for updates through the Management Console.

To Check for an Updated Central File through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) policy poll-now
```

The ProxySG displays a message indicating whether the Central file has changed.

Resetting the Policy Files

You can clear all the policy files automatically through the CLI.

To Clear all Policy Files through the CLI:

1. At the (config) command prompt, enter the following command:

```
SGOS# (config) policy reset
```

WARNING: This will clear local, central, forward and VPM policy. Are you sure you want to reset ALL policy files? (y or n)

The ProxySG displays a warning that you will be resetting all of your policy files.

2. Enter **y** to continue or **n** to cancel.

Note: This command does not change the default proxy policy settings.

Moving VPM Policy Files from One ProxySG to Another

VPM policy files are specific to the ProxySG where they were created. But just as you can use the same Central, Local, and Forward policy files on multiple ProxySG Appliances, you can use VPM policies created on one appliance on other appliances.

For detailed information on moving VPM policy files, see "Installing VPM-Created Policy Files" on page 456 in Chapter 13: "The Visual Policy Manager".

Viewing Policy Files

You can view either the compiled policy or the source policy files. Use these procedures to view policies defined in a single policy file (for example, using VPM) or in multiple policy files (for example, using the Blue Coat Central policy file and VPM).

Viewing the Installed Policy

Use the Management Console or a browser to display installed Central, Local, or Forward policy files.

Note: You can view VPM policy files through the Visual Policy Files tab.

To View Installed Policy through the Management Console:

1. Select Configuration>Policy>Policy Files>Policy Files.

2. In the View File drop-down list, select Current Policy to view the installed and running policy, as assembled from all policy source files. You can also select Results of Policy Load to view any warnings or errors resulting from the last attempt (successful or not) to install policy.
3. Click View.

The ProxySG opens a separate browser window and displays the installed policy file.

To View the Currently Installed Policy through a Browser:

1. Enter a URL in one of the following formats:

- If an HTTPS-Console is configured, use
`https://ip_address_of_ProxySG:HTTPS-Console_port/Policy/current` (the default port is 8082).
- If an HTTP-Console is configured, use
`http://ip_address_of_ProxySG:HTTP-Console_port/Policy/current` (the default port is 8081).

The ProxySG opens a separate browser window and displays the policy.

2. Review the policy, then close the browser.

To View the Currently Installed Policy through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) show policy
```

Viewing Policy Source Files

You can display source (uncompiled) policy files on the ProxySG.

To View Policy Source Files through the Management Console:

1. Select Configuration>Policy>Policy Files>Policy Files.
2. To view a policy source file, select the file you want to view (Local, Forward, or Central) from the View File drop-down list and click View.

The ProxySG opens a separate browser window and displays the appropriate source policy file.

To View Policy Source Files through the CLI:

At the (config) command prompt, enter one of the following commands:

```
SGOS# (config) show configuration
-or-
SGOS# (config) show sources policy {central | local | forward | vpm-cpl | vpm-xml}
```

The `show configuration` command displays general configuration information, followed by the policy source file contents. If the ProxySG is using multiple policy files, file source displays in this sequence: Central file, local file, VPM. The `show sources policy` command allows you to specify the policy files you want to view.

Note: You can use the `show configuration` command to save the output to a file for reference, in addition to displaying the current configuration. For more information, refer to the *Blue Coat Command Line Interface Reference*.

Viewing Policy Statistics

You can view policy statistics on all requests processed by the ProxySG. Use the Management Console or a browser. You cannot view policy statistics through the CLI.

To Review Policy Statistics through the Management Console:

1. Select Statistics>Advanced.
2. Click the Policy link.
3. Click the Show policy statistics link.
A separate browser window opens and displays the statistics.
4. Examine the statistics, then close the browser.

To Review Policy Statistics through a Browser:

1. Enter a URL in one of the following formats:
 - If an HTTPS-Console is configured, use
`https://ip_address_of_ProxySG:HTTPS-Console_port/Policy/statistics` (the default port is 8082).
 - If an HTTP-Console is configured, use
`http://ip_address_of_ProxySG:HTTP-Console_port/Policy/statistics` (the default port is 8081).

The ProxySG opens a separate browser window and displays the statistics.

2. Examine the statistics, then close the browser.

Chapter 13: The Visual Policy Manager

The Visual Policy Manager (VPM) is graphical policy editor included with the ProxySG. VPM allows you to define Web access and resource control policies without having an in-depth knowledge of Blue Coat Systems Content Policy Language (CPL) and without the need to manually edit policy files.

This chapter assumes that you are familiar with basic concepts of ProxySG policy functionality as described in Chapter 12: "Managing Policy Files".

While VPM creates only a subset of everything you can achieve by writing policies directly in CPL, it is sufficient for most purposes. If your needs require more advanced policies, consult the *Blue Coat Content Policy Language Guide*.

This chapter contains the following sections:

- "Section A: About the Visual Policy Manager"
- "Section B: Policy Layer and Rule Object Reference"
- "Section C: Detailed Object Column Reference"
- "Section D: Managing Policy Layers and Files"
- "Section E: Tutorials"

Related topics:

- *Blue Coat Content Policy Language Guide*
- Chapter 12: "Managing Policy Files"
- Chapter 17: "Content Filtering"

Section A: About the Visual Policy Manager

Section A: About the Visual Policy Manager

This section contains the following topics:

- "JRE Requirement" on page 379—Discusses the Java Runtime Environment component requirement.
- "Launching the Visual Policy Manager" on page 379—Describes how to start VPM from the Management Console.
- "About the Visual Policy Manager User Interface" on page 380—Describes VPM menu items, tool bars, and work areas.
- "About VPM Components" on page 383—Provides definitions of the policy layers and describes how rule objects comprise the layers.
- "The Set Object Dialog" on page 386—Describes the dialog used to select objects to be added or edited.
- "The Add/Edit Object Dialog" on page 387—Describes the dialog used to add and edit rule objects.

Section A: About the Visual Policy Manager

JRE Requirement

VPM requires the Java Runtime Environment Standard Edition (JRE) v.1.3.x or later from Sun Microsystems, Inc. If you have an earlier version, you must upgrade to at least JRE v. 1.3.x (except for JRE v. 1.4.0, which is *not* supported).

If an unsupported JRE version is installed when you attempt to start VPM for the first time, the ProxySG automatically connects to the Sun Microsystems download center to begin download and installation. Follow the instructions on-screen.

All browsers should use the default JRE that they ship with. VPM is completely independent from the Management Console. If the browser is configured properly with its default JRE, VPM uses the later JRE version it requires.

Note: If the JRE is v. 1.3.x, some VPM menus truncate if they exceed the visible screen. This does not occur with JRE v. 1.4.1.

Launching the Visual Policy Manager

To Launch VPM:

1. Select Configuration>Policy>Visual Policy Manager.

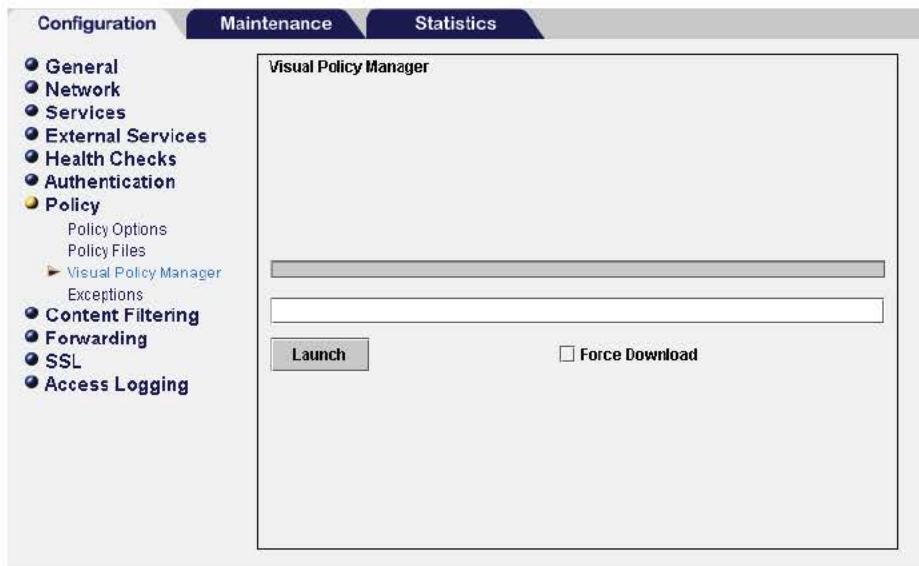


Figure 13-1: Launching VPM from the Management Console

2. Launch VPM. If this is the first time launching VPM following an OS upgrade, or to ensure you are launching the most current VPM version, click Force Download before clicking Launch.

If a valid JRE is already installed on your workstation, the ProxySG opens a separate browser window and starts VPM. The first time you start the policy editor, it displays an empty policy.

Section A: About the Visual Policy Manager

If a valid JRE is *not* installed on your workstation, a security warning dialog box appears. Click Yes to continue. Follow the instructions to install the JRE. After installation completes, a Launch VPM tab briefly displays before VPM starts.

Note: If using Internet Explorer: Depending on the browser version and settings, launching VPM from an HTTPS URL might display security warning messages (page contains secure and non-secure items). This is caused by the HTML link in the VPM launch page that links to the JRE download site at the Sun Web site. This message can be ignored. You can adjust the browser settings to display or not to display this message concerning secure and non-secure items.

About the Visual Policy Manager User Interface

The following figure labels VPM components.

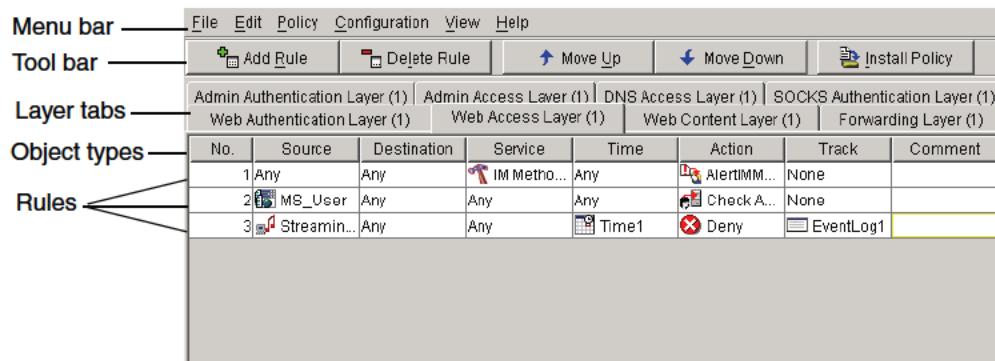


Figure 13-2: Visual Policy Manager

Section A: About the Visual Policy Manager

Menu Bar

The following table describes VPM Menu Bar items.

Table 13.1: VPM Menu Bar Items

File	Install Policy On ProxySG	Saves all new policy rules.
	Revert to existing Policy on ProxySG	Ignores changes and reloads installed policy rules.
	Exit	Exits the application.
Edit	Add Rule	Adds a new blank rule to the visible policy layer or removes a rule from the visible policy layer.
	Delete Rule	
	Cut Rule	Standard cut, copy, and paste operations.
	Copy Rule	
	Paste Rule	
	Move Rule Up	Moves rules up or down one position in a policy layer.
	Move Rule Down	
	Reorder Layers	Reorders the policy layers.
	Delete Layer	Deletes a specific policy layer.
Policy	Add Admin Authentication Layer	The Policy menu items add policy layers to be populated with policy rules.
	Add Admin Access Layer	
	Add DNS Access Layer	
	Add SOCKS Authentication Layer	
	Add Web Authentication Layer	
	Add Web Access Layer	
	Add Web Content Layer	
	Add Forwarding Layer	
Configuration	Set DNS Lookup Restrictions	Restricts DNS lookups during policy evaluation.
	Set Reverse DNS Lookup Restrictions	Restricts reverse DNS lookups during policy evaluation.
	Set Group Log Order	Configures the order in which the group information would be logged.
	Edit Categories	Edits content filtering categories.
View	Generated CPL	Displays the CPL generated by VPM.
	Current ProxySG VPM Policy Files	Displays the currently stored VPM policy files.
	Object Occurrences	Lists the user-created object(s) in the selected rule; lists use in other rules as well.
	Tool Tips	Toggles the tool-tip display on and off.
Help	Help Topics	Displays the online help.
	About	Displays copyright and version information.

Tool Bar

The VPM Tool Bar contains the following functions:

- Add Rule—Adds a blank rule to visible policy layer; all values for the rule are the defaults.
- Delete Rule—Deletes the selected rule from the visible policy layer.
- Move Up—Moves a rule up one position in the visible policy layer.

Section A: About the Visual Policy Manager

- **Move Down**—Moves a rule down one position in the visible policy layer.
- **Install Policy**—Converts the policies created in VPM into Blue Coat Content Policy Language (CPL) and installs them on the ProxySG.

Policy Layer Tabs

Every policy layer you create from the Policy>Add Layer menu is displayed as a tab. Click a tab and the rules included in that policy layer display below in the main body of the pane. Right-clicking a tab displays the options of renaming and deleting the policy layer.

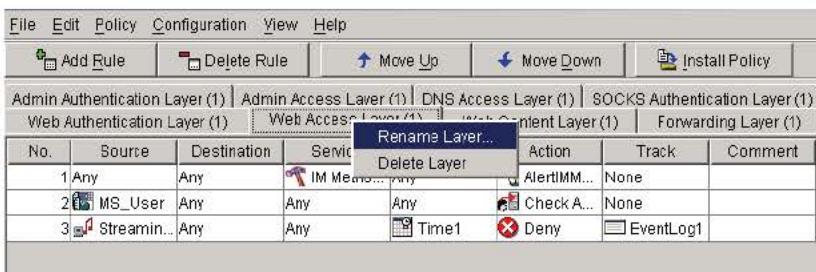


Figure 13-3: Right-click a Policy Tab to Rename or Delete a Policy Layer

Each VPM policy layer is described in later sections in this chapter.

Rules and Objects

A policy layer can contain multiple rules. Every rule is numbered and listed in a separate row. To create a new rule, click the Add Rule button; a new rule is added to the bottom of the list. If multiple rules exist within a policy layer, the ProxySG finds the first one that matches a given situation and ignores the remaining rules. Therefore, rule order is important. Use the Move buttons on the rule bar to reorder the rules in a policy.

Each rule is comprised of objects. The objects are the individual elements of a rule you specify. With the exception of No. (number), which indicates the order of the rule in the layer and is filled in automatically, all objects are configurable.

To specify or edit an object setting, position the mouse in the appropriate object cell within a rule and right-click to display the drop-down the menu.

Section A: About the Visual Policy Manager

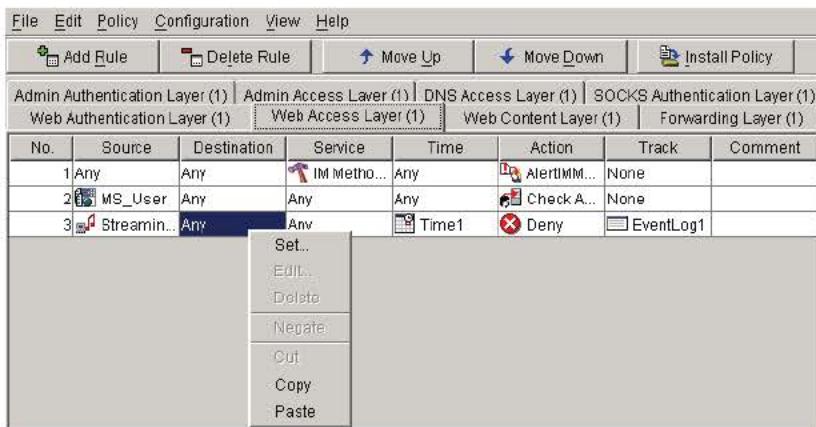


Figure 13-4: Right-click a Rule Cell to Set or Edit the Object Properties

Each object type is described in "Policy Layer and Rule Object Reference" on page 388.

About VPM Components

This section describes the specific policy layer types and rule objects.

Policy Layers

The layers are:

- Administration Authentication—Determines how administrators accessing ProxySG must authenticate.
- Administration Access—Determines who can access the ProxySG to perform administration tasks.
- DNS Access—Determines how the ProxySG processes DNS requests.
- SOCKS Authentication—Determines the method of authentication for that access the proxy through SOCKS.
- Web Authentication—Determines whether user clients that access the proxy or the Web must authenticate.
- Web Access—Determines what user clients accessing the proxy or the Web can access and any restrictions that apply.
- Web Content—Determines caching behavior, such as verification and ICAP redirection.
- Forwarding—Determines forwarding hosts and methods.

Section A: About the Visual Policy Manager

As you create policy layers, you will create many different layers of the same type. Often, an overall policy requires layers of different types designed to work together to perform a task. For example, Authentication and Access layers usually accompany each other; an Authentication layer determines if a user or client must authenticate, and an Access layer subsequently determines where that user or client can go (what ProxySG or Web sites they can access) once they are authenticated.

Each object type is described in "Policy Layer and Rule Object Reference" on page 388.

Rule Objects

Policy layers contain rule objects. Only the objects available for that policy layer type are displayed. There are two types of objects:

- Static Objects—A self-contained object that cannot be edited or removed. For example, if you write a rule that prohibits users from accessing a specific Web site, the Action object you select is Deny.
Static objects are part of the system and are always displayed.
- Configurable Objects—A configurable object requires parameters. For example, consider the rule mentioned in the previous item that prohibits users from accessing a specific Web site. In this case, the user is a Source object. That object can be a specific IP Address, user, group, user agent (such as a specific browser), and so on. Select one and then enter the required information (such as a verifiable user name or group name).

Configurable objects do not exist until you create them. A created object is listed along with all static objects in the list dialog, and you can reuse it in other applicable policy layers. For example, an IP address can be a Source or Destination object in many different policy-layer types.

Important: The orders of policy layers, and the order of rules within a layer are important. For more information, see "How Policy Layers, Rules, and Files Interact" on page 452.

While individual object-type menus occasionally contain entries specific to the object type, the basic menu options are:

- Allow—(Web Access Layer Action column only) Quick menu access; sets the policy to allow.
- Deny—(Web Access Layer Action column only) Quick menu access; sets the policy to deny.
- Set—Displays the Set Object dialog where you select an object or create a new one.
- Edit—Opens the Edit Object dialog where you edit an object or change to another.
- Delete—Removes the selected object from the current rule and restores the default.
- Negate—Defined as *not*. Negate provides flexibility in writing rules and designing the structure of policies. The following is a simple Web Access rule that states: "When any client tries to access a URL contained in an object of JobSearch, allow access."

Section A: About the Visual Policy Manager



The screenshot shows a software application window titled "File Edit Policy Configuration View Help". Below the menu bar is a toolbar with icons for "Add Rule", "Delete Rule", "Move Up", "Move Down", and "Install Policy". A navigation bar at the top lists several layers: Admin Authentication Layer (1), Admin Access Layer (1), DNS Access Layer (1), SOCKS Authentication Layer (1), Web Authentication Layer (1), Web Access Layer (1), Web Content Layer (1), and Forwarding Layer (1). The main area is a table with columns: No., Source, Destination, Service, Time, Action, Track, and Comment. A single row is present with values: 1, Any, JobSearch, Any, Any, Deny, None, and an empty comment field.

No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	JobSearch	Any	Any	Deny	None	

Figure 13-5: A Simple Web Access Policy Rule

Dragging the pointer to the Destination list, right-clicking to display the drop-down list, and clicking Negate invokes a red circle with a horizontal white line in the icon in the cell.



This screenshot is identical to Figure 13-5, except the "Destination" column for the single rule entry now contains a red icon with a white horizontal line through it, indicating a negation or "not" condition.

No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	JobSearch	Any	Any	Deny	None	

Figure 13-6: The Red Icon in the Cell Indicates Negation, or “Not”

The rule now specifies: “Allow access to everywhere but these JobSearch sites.”

- Cut, Copy, and Paste are the standard paste operations with the following restrictions: you can only paste anything cut or copied from the same column in the same table and the copy and paste functions do not work across multiple layers.

The following table describes the general function of each object type:

Object	Description
Source	Specifies the source attribute, such as an IP address, user, or group.
Destination	Specifies the destination attribute, such as a URL, IP address, and file extension.
Service	Specifies the service attribute, such as protocols, protocol methods, and IM file transfer limitations.
Time	Specifies day and time restrictions.
Action	Specifies what to do when the rule matches.
Track	Specifies tracking attributes, such as event log and E-mail triggers.
Comment	Optional. You can provide a comment regarding the rule.

Policy Layer/Object Matrix

The following table displays which object types are available in each policy layer

Policy Layer	Source	Destination	Service	Time	Action	Track	Comment
Admin Authentication	x				x	x	x
Admin Access	x				x	x	x
DNS Access	x	x		x	x	x	x
SOCKS Authentication	x				x	x	x

Section A: About the Visual Policy Manager

Policy Layer	Source	Destination	Service	Time	Action	Track	Comment
Web Authentication	x	x			x	x	x
Web Access	x	x	x	x	x	x	x
Web Content		x	x		x	x	x
Forwarding	x	x	x		x	x	x

The Set Object Dialog

This section discusses the Set Object dialog used to select objects for configuration.

The object rules in all policy layer types determine the conditions for a particular policy rule. Depending on the type of policy layer, an object can be anything from a user or group to an IP address or a URL and so forth.

To create a rule, right-click a cell in an object cell. The relevant Set Object dialog displays. In this dialog, select the objects for the rule or create new objects as necessary.

Objects have type-specific icons to provide a visual aid in distinguishing among different types in the list.

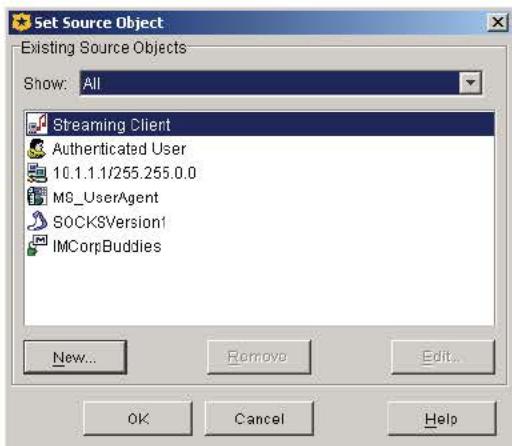


Figure 13-7: Set Destination Object Dialog with Selectable Objects

The Set Object dialog only displays or allows you to create the objects allowable in the specific option of the rule type you are creating. But if more than one policy-layer type uses the same object type (for example, IP address can be a source in rules for four of the five types of policies), then those existing objects display in all Set Object dialogs, regardless of policy-layer type.

Controlling the List of Objects in the Set Object Window

As you create more policies, it is likely that the lists of existing objects in the various Set Object dialogs expand. You can restrict the display of objects in the list to a specific type by selecting an object type from the Show drop-down list above the list. The following figure demonstrates the window displayed above with the list restricted to URL objects.

Section A: About the Visual Policy Manager

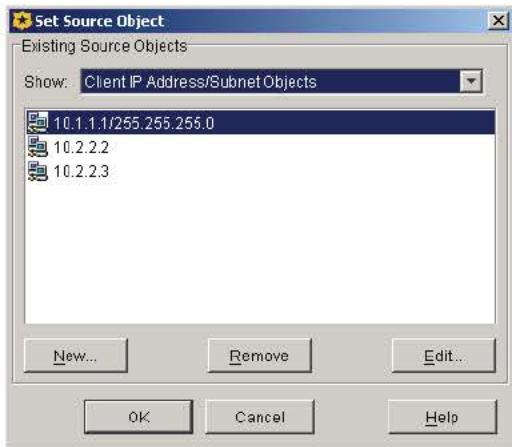


Figure 13-8: Limiting the Set Object Dialog View

The Add/Edit Object Dialog

From the Set Object dialog, the Add Object dialog is used to define configurable objects. Existing configurable options can be altered using the Edit Object dialog. In terms of functionality, the two dialogs are identical.

For the initial configuration of an object, click New on the Set Object dialog to display the Add Object dialog. Perform the tasks required to configure the object and click OK. The newly named and configured object appears in the list of selectable objects in the Set Object dialog and is ready to be selected for the rule.

To edit an existing object, select an object from the list and click Edit. The Edit Object dialog appears with the existing parameters on display. Edit as necessary and click OK.

To remove an existing object, select an object from the list and click Remove. A secondary prompt verifies your attempt to remove the object; click OK. The object is deleted.

Section B: Policy Layer and Rule Object Reference

Section B: Policy Layer and Rule Object Reference

This section contains the following topics:

- "About the Reference Tables" on page 389—Describes the table conventions used in this section.
- "Administration Authentication Policy Layer Reference" on page 389—Describes the objects available in this policy layer.
- "Administration Access Policy Layer Reference" on page 389—Describes the objects available in this policy layer.
- "DNS Access Policy Layer Reference" on page 389—Describes the objects available in this policy layer.
- "SOCKS Authentication Policy Layer Reference" on page 390—Describes the objects available in this policy layer.
- "Web Authentication Policy Layer Reference" on page 391—Describes the objects available in this policy layer.
- "Web Access Policy Layer Reference" on page 391—Describes the objects available in this policy layer.
- "Web Content Policy Layer Reference" on page 393—Describes the objects available in this policy layer.
- "Forwarding Policy Layer Reference" on page 393—Describes the objects available in this policy layer.

Section B: Policy Layer and Rule Object Reference

About the Reference Tables

The tables in this section list the static and configurable objects available for each policy layer.

Note: If viewing this document as a PDF, you can click an object name to jump to a description of that object (all objects are described in Section C). To jump back to a specific policy layer reference, click policy layer name in any object reference table that appears in the next section.

Administration Authentication Policy Layer Reference

The following table provides the objects available in the Administration Authentication policy layer.

Source Objects	Action Objects	Track Objects
Client IP Address/Subnet	Do Not Authenticate	Trace
Client Hostname	Deny	
Proxy IP Address/Port	Authenticate	
Combined Objects	Force Authenticate	

Administration Access Policy Layer Reference

The following table provides the objects available in the Administration Access policy layer.

Source Objects	Action Objects	Track Objects
Client IP Address/Subnet	Allow Read-Only Access	Event Log
Client Hostname	Allow Read-Write Access	Email
Proxy IP Address/Port	Deny	SNMP
User	Force Deny	Trace
Group		Combined Objects
Attribute		
Combined Objects		

DNS Access Policy Layer Reference

The following table provides the objects available in the DNS Access policy layer.

Source Objects	Destination Objects	Time Objects	Action Objects	Track Objects
Client IP Address/Subnet	DNS Response Contains No Data	Time	Bypass DNS Cache	Event Log
Proxy IP Address/Port	DNS Response IP Address/Subnet	Combined Objects	Do Not Bypass DNS Cache	Email
DNS Request Name	RDNS Response Host		Allow DNS From Upstream Server	SNMP
RDNS Request IP Address/Subnet	DNS Response CNAME		Serve DNS Only From Cache	Trace

Section B: Policy Layer and Rule Object Reference

Source Objects	Destination Objects	Time Objects	Action Objects	Track Objects
DNS Request Opcode	DNS Response Code		Enable/Disable DNS Imputing	Combined Objects
DNS Request Class	Category		Send DNS/RDNS Response Code	
DNS Request Type	Combined Objects		Send DNS Response	
DNS Client Transport Combined Objects			Send Reverse DNS Response Reflect IP Combined Objects	

SOCKS Authentication Policy Layer Reference

The following table provides the objects available in the SOCKS Authentication policy layer.

Source Objects	Action Objects	Track Objects
Client IP Address/Subnet	Do Not Authenticate	Trace
Client Hostname	Authenticate	
Proxy IP Address/Port	Force Authenticate	
SOCKS Version		
Combined Objects		

Section B: Policy Layer and Rule Object Reference

Web Authentication Policy Layer Reference

The following table provides the objects available in the Web Authentication policy layer.

Source Objects	Destination Objects	Action Objects	Track Objects
Client Hostname Unavailable	Destination IP Address/Subnet	Do Not Authenticate	Trace
Client IP Address/Subnet	Destination Host/Port	Deny	
Client Hostname	URL	Authenticate	
Proxy IP Address/Port	Category	Force Authenticate	
User Agent	Combined Objects		
Request Header			
Combined Objects			

Web Access Policy Layer Reference

The following table provides the objects available in the Web Access policy layer.

Web Access policy layers regulate, from a general to a granular level, who or what can access specific Web locations or content.

- Users, groups, individual IP addresses, and subnets, as well as object lists comprised of any combination of these, can be subject to rules.
- Rules can include access control for specific Web sites, specific content from any Web site, individual IP addresses, and subnets.
- Actions taken can range from allowing and denying access to more finely tuned changes or limitations.
- Rules can also be subject to day and time specifications and protocol, file type, and agent delimiters.

Source Objects	Destination Objects	Service Objects	Time Objects	Action Objects	Track Objects
Streaming Client	Destination IP Address/Subnet	Using HTTP Transparent Authentication	Time	Allow	Event Log
Client Hostname Unavailable	Destination Host/Port	Virus Detected	Combined Objects	Deny	Email
Authenticated User	URL	Client Protocol		Force Deny	SNMP
Client IP Address/Subnet	Category	Protocol Methods		Bypass Cache	Trace
Client Hostname	File Extensions	IM File Transfer		Do Not Bypass Cache	Combined Objects
Proxy IP Address/Port	HTTP MIME Types	IM Message Text		Check/Do Not Check Authorization	
User	Response Code	IM Message Reflection		Always Verify	

Section B: Policy Layer and Rule Object Reference

Source Objects	Destination Objects	Service Objects	Time Objects	Action Objects	Track Objects
Group	Response Header	Streaming Content Type ICAP Error Code		Use Default Verification Block/Do Not Block Pop-Up Ads	
Attribute	IM Buddy			Force/Do Not Force NTLM for Server Auth	
User Agent	IM Chat Room	Combined Objects		Reflect/Do Not Reflect IM Messages	
SOCKS Version				Block/Do Not Block IM Encryption	
Request Header				Return Exception Return Redirect	
IM User				Send IM Alert	
Client Negotiated Cipher				Modify Access Logging	
Client Negotiated Cipher Strength				Override Access Log Field	
Combined Objects				Rewrite Host Reflect IP Suppress Header Control Request Header/Control Response Header Strip Active Content Modify IM Message Return ICAP Patience Page Set External Filter Service Set ICAP Request Service Set FTP Connection Set SOCKS Acceleration Set Streaming Max Bitrate Combined Objects	

Section B: Policy Layer and Rule Object Reference

Web Content Policy Layer Reference

The following table provides the objects available in the Web Content policy layer.

The Web Content policy layer applies to requests independent of user identity.

Content scanning policy layers scan requested URLs and file types for viruses and other malicious code. You must have an ICAP service installed on the ProxySG to use this policy type.

Destination Objects	Action Objects	Track Objects
Destination IP Address/Subnet	Check/Do Not Check Authorization	Event Log
Destination Host/Port	Always Verify	
URL	Use Default Verification	Email
Category	Use Default Caching	SNMP
File Extensions	Do Not Cache	Trace
HTTP MIME Types	Force Cache	Combined Objects
Combined Objects	Mark/Do Not Mark As Advertisement Enable/Disable Pipelining Set External Filter Service Set ICAP Request Service Set ICAP Response Service Set TTL Modify Access Logging Override Access Log Field Combined Objects	

Forwarding Policy Layer Reference

The following table provides the objects available in the Forwarding policy layer.

Source Objects	Destination Objects	Service Objects	Action Objects	Track Objects
Streaming Client	Destination IP Address/Subnet	Client Protocol	Send Direct	Trace
Client IP Address/Subnet	Destination Host/Port	Combined Objects	Integrate/Do Not Integrate New Hosts	
Client Hostname	URL		Allow Content From Origin Server	
Proxy IP Address/Port	Combined Objects		Serve Content Only From Cache	
Combined Objects			Select SOCKS Gateway Select Forwarding Reflect IP Set IM Transport	

Section B: Policy Layer and Rule Object Reference

Source Objects	Destination Objects	Service Objects	Action Objects	Track Objects
			Set Streaming Transport Combined Objects	

Section C: Detailed Object Column Reference

Section C: Detailed Object Column Reference

This section contains the following topics:

- "Source Column Object Reference"
- "Destination Column Object Reference"
- "Service Column Object Reference"
- "Time Column Object Reference"
- "Action Column Object Reference"
- "Track Object Column Reference"
- "Comment Object Reference"
- "Using Combined Objects"
- "Creating Categories"

Section C: Detailed Object Column Reference

Source Column Object Reference

A *source* object specifies the communication or Web transaction origin that is evaluated by the policy. Not all policy layers contain the same source objects; once you understand each source object, however, you can configure as necessary in any layer of your policies.

Any

Applies to any source.

Streaming Client

This is a static object. This rule applies to any request from a streaming client.

Client Hostname Unavailable

This is a static object. This rule applies if the client IP address could not be looked up with a reverse DNS query.

Authenticated User

This is a static object. This rule applies to any authenticated user.

Client IP Address/Subnet

Specifies the IP address and, optionally, a subnet mask of a client. The policy defined in this rule applies only to this address or addresses on this subnet. This object is automatically named using the prefix Client; for example, Client: 1.2.0.0/255.255.0.0.

Client Hostname

Specifies a reverse DNS hostname resolved in the reverse lookup of a client IP address. Enter the host name and select matching criteria. This object is automatically named using the prefix Client; for example, Client: host.com. If you select a matching qualifier, that attribute is appended to the object in parentheses. For example, Client: host.com (RegEx).

Proxy IP Address/Port

Specifies the IP address and, optionally, a port on the ProxySG. The policy defined in this rule applies only to this address or addresses with this subnet.

User

Specifies an individual user in the form of a verifiable username or login name. Enter a user name and an authentication realm. The dialog then displays different information depending on the type of authentication realm specified. Select the appropriate realm from the drop-down list. Items in the list are taken from the realms configured by the administrator in the ProxySG.

Section C: Detailed Object Column Reference

LDAP

You can optionally select a User Base DN from a drop-down list. Entries in the User Base DN list come from those specified by the administrator in the ProxySG. You can also edit an entry selected in the list, or type a new one. Edited names and new names are retained in the list. Notice in the Full Name field that VPM takes the User Attribute type specified by the administrator in the ProxySG (cn= in the following illustration), and associates it with the user name and Base DN entered here.

Important: When you configure a realm, the ProxySG assumes a default primary user attribute (sAMAccountName for Active Directory; uid for Netscape/iPlanet Directory Server/SunOne; cn for Novel NDS). You can accept the default or change it. Whatever is entered there is what VPM uses here, entering it in the Full Name display field once a Base DN is selected.

If the primary user attribute specified in the ProxySG differs from the primary user attribute specified in the directory server, enter the latter in the User field with the appropriate value (in the format attribute=value). This replaces the entry in the Full Name field. Examine the following screenshot. Assume that the organization uses *phone* as the primary attribute in its LDAP directory:

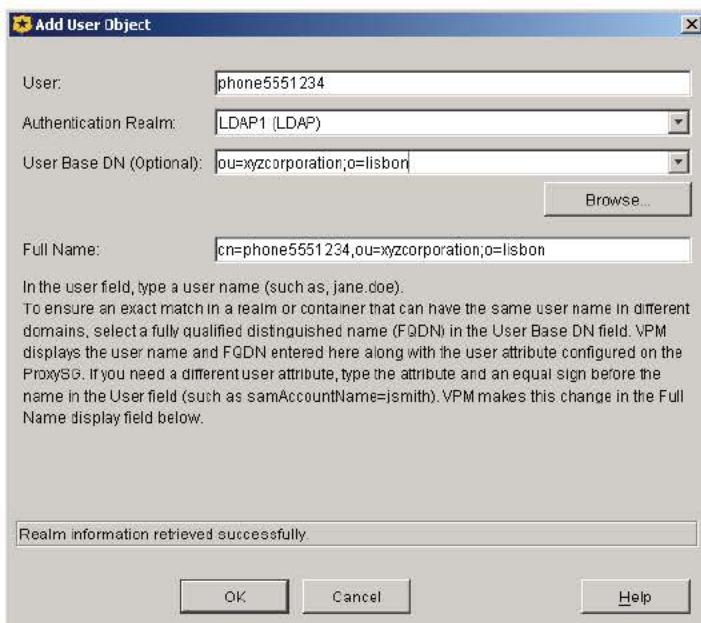


Figure 13-9: Specifying an LDAP Primary User Attribute

You can only enter a user attribute and equal sign in the User field if a User Base DN is selected.

NTLM

Entries in this list are not prepopulated. You must enter a name in the Domain Name field. An entered name is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays domain name and user name entered above.

Section C: Detailed Object Column Reference

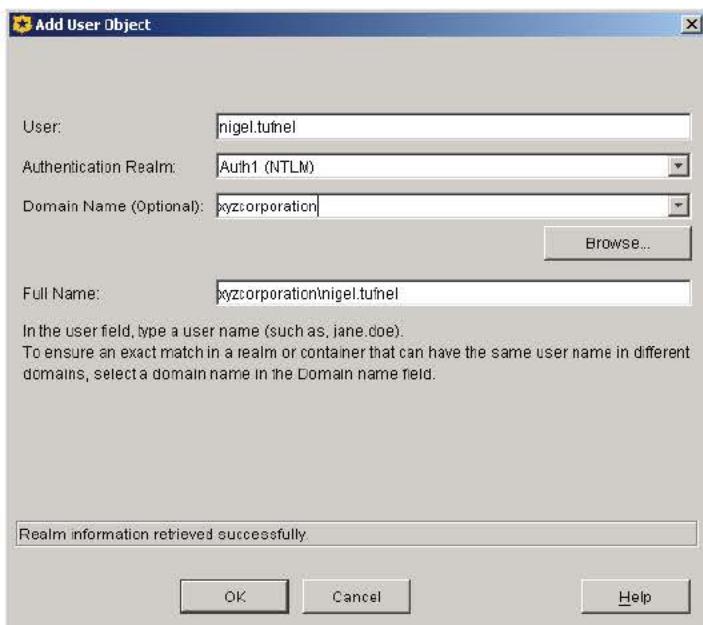


Figure 13-10: Adding an NTLM User with a FQDN or DN

RADIUS

Entries in this list are not prepopulated. You must enter a name in the User field. An entered name is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays domain name and user name entered above.

Local

Entries in this list are not prepopulated. You must enter a name in the User field. An entered name is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays domain name and user name entered above.

Certificate

If a Certificate realm is selected and that realm uses an LDAP realm as authentication realm, the Browse button is clickable. This option allows you to browse the LDAP database and select users, thus preventing typing errors possible from manually entering names in the fields. If the Certificate realm does not use an LDAP authentication realm, Browse is not displayed.

Group

Specifies a verifiable group name. Enter a user group and an authentication realm. The dialog then displays different information depending on the type of authentication realm specified.

- **Group field**—Replace the default with a verifiable group name.
- **Authentication Realm field**—Select the appropriate realm from the drop-down list. Items in the list are taken from the realms configured by the administrator in the ProxySG.

Section C: Detailed Object Column Reference

- LDAP—Entries in the Group Base DN list come from those specified by the administrator in the ProxySG. You can also edit an entry selected in the list, or type a new one. Edited names and new names are retained in the list. Notice in the Full Name field that VPM takes the User Attribute type specified by the administrator in the ProxySG (cn= in the following illustration), and conjoins it with the group name and Base DN entered here.

Important: When you create a group, the default attribute is cn= in the Full Name display field.

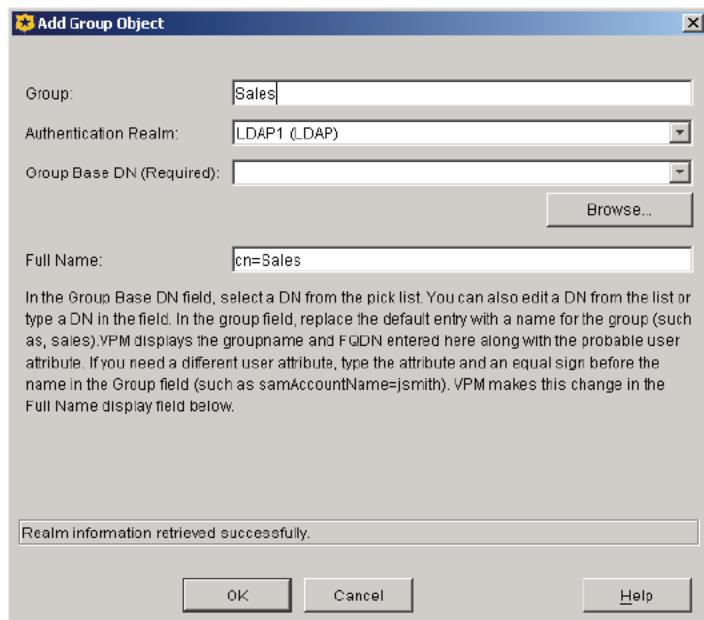


Figure 13-11: Creating an LDAP Group Object

If the primary user attribute specified in the ProxySG differs from the primary user attribute specified in the directory server, you need to enter the latter here. Do that by typing it in the Group field with the appropriate value (in the format attribute=value). Doing so replaces the entry in the Full Name field. Unlike the comparable situation when creating a user (described immediately above), when creating a group, the Group Base DN does not need to be selected in order to type the attribute=value pair in the Group field.

- NTLM—Entries in this list are not prepopulated. You must enter a name in the Domain Name field. A name typed in is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays the domain name and group name entered above.

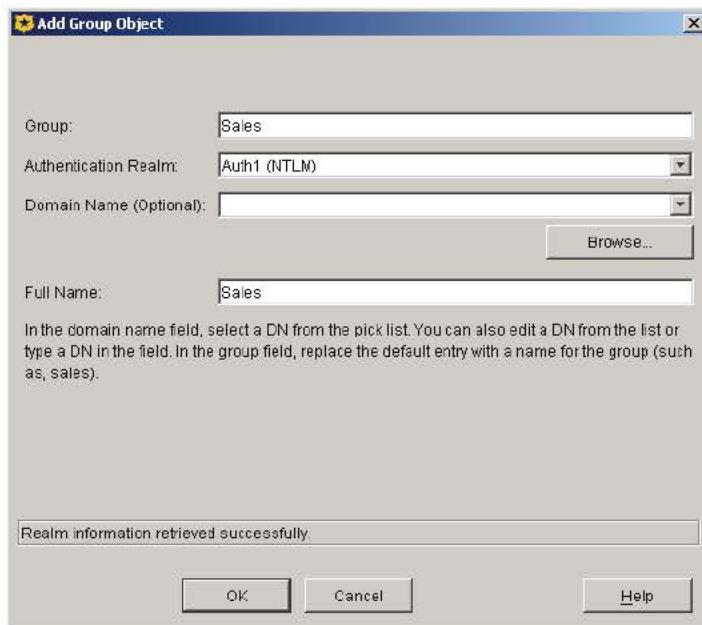
Section C: Detailed Object Column Reference

Figure 13-12: Creating an NTLM Group Object

- Local—Entries in this list are not prepopulated. You must enter a name in the Group field. A name typed in is retained and can subsequently be selected and edited. Notice in the Full Name field that VPM displays the group name entered above.
- Certificate—if a Certificate realm is selected and that realm uses an LDAP realm as authentication realm, the Browse button is clickable. This option allows you to browse the LDAP database and select users, thus preventing typing errors possible from manually entering names in the fields. If the Certificate realm does not use an LDAP authentication realm, Browse is not displayed.

Attribute

Specifies an LDAP or Radius realm attribute or service.

LDAP

Specifies a specific LDAP attribute (and optional value).

To Specify an LDAP Attribute:

1. In the Name field, enter a name for the object or leave as is to accept the default.
2. Select All LDAP or a specific realm.
3. Enter an Attribute Type.
4. Enter an Attribute Value, or leave blank to accept any value.

Section C: Detailed Object Column Reference

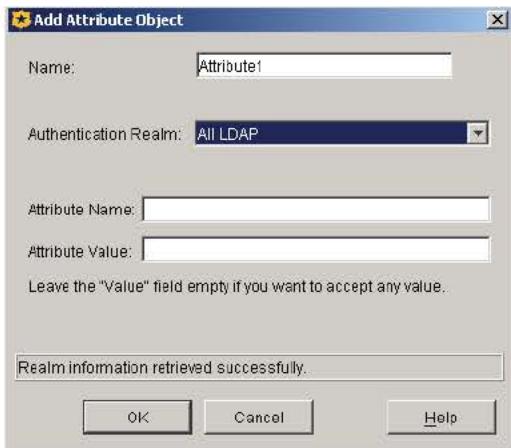


Figure 13-13: Specifying an LDAP Attribute

RADIUS

Specifies a RADIUS attribute.

To Specify a RADIUS Attribute:

Select from a drop-down list of available services.

1. In the Name field, enter a name for the object or leave as is to accept the default.
2. Select All RADIUS or a specific realm.
3. Select a RADIUS Attribute.

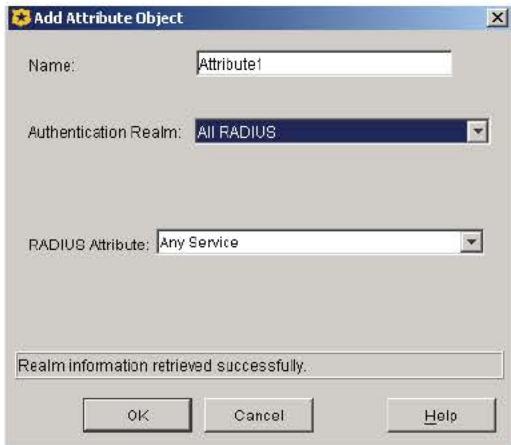


Figure 13-14: Specifying a RADIUS Attribute

Section C: Detailed Object Column Reference

DNS Request Name

Specifies a DNS request. Enter the host name and select matching criteria. This object is automatically named using the prefix DNS; for example, DNS: host.com. If you select a matching qualifier, that attribute is appended to the object in parentheses. For example, DNS: host.com (RegEx).

RDNS Request IP Address/Subnet

Specifies the reverse DNS IP address and, optionally, a subnet mask. The policy defined in this rule applies only to this address or addresses on this subnet. This object is automatically named using the prefix RDNS; for example, RDNS: 5.6.0.0/255.255.0.0.

DNS Request Opcode

Specifies OPCODEs to represent in the DNS header.

To Specify a DNS Request OPCODE Object:

1. In the Name field, enter a custom name or leave as is to accept the default.
2. Select one or more of the OPCODEs.
3. Click OK.

DNS Request Class

Specifies the DNS request class (QCLASS) properties.

To Specify a DNS Request Class Object:

1. In the Name field, enter a custom name or leave as is to accept the default.
2. Select one or more of the request classes.
3. Click OK.

DNS Request Type

Specifies the DNS request types (QTYPE) attributes.

To Specify a DNS Request Type Object:

1. In the Name field, enter a custom name or leave as is to accept the default.
2. Select one or more of the request types.
3. Click OK.

DNS Client Transport

Specifies the DNS client transport method, UDP or TCP.

Section C: Detailed Object Column Reference

To Specify a DNS Client Transport Object:

1. Select UDP Transport or TCP Transport. This object is automatically named using the prefix DNS; for example, DNS: Client Transport UDP.
2. Click OK.

SOCKS Version

Specifies the SOCKS version, 4 or 5. This object is automatically named as SOCKSVersion4 or SOCKSVersion5.

User Agent

Specifies one or more agents a client might use to request content. The choices include specific versions of: Microsoft Internet Explorer, Netscape Communicator, Microsoft Windows Media Player and NetShow, Real Media RealPlayer and RealDownload, Apple QuickTime, Opera, and Wget.

The policy defined in this rule applies to these selected agents. You can name this list and create other custom lists to use with other policy layer rules.

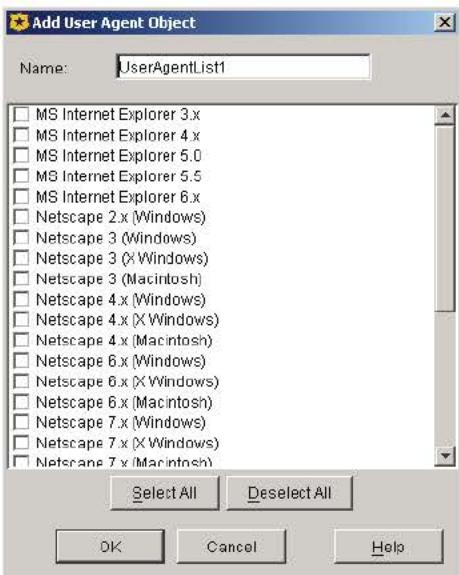


Figure 13-15: Selecting User Agents

Note: If you require a user agent not contained in this list, use the Request Header object, which can contain user agent specified as a header.

Request Header

Specifies the rule applies to requests containing a specific header. Blue Coat supplies a list of standard headers, but you can also select a custom header.

Section C: Detailed Object Column Reference

To Specify a Header:

1. In the Name field, enter a custom name or leave as is to accept the default.
2. From the Show drop-list select the viewing field from All to Standard or Custom, as desired. Standard displays only the default standard headers. Custom displays any admin-defined headers that exist.
3. From the Header Name drop-list, select a standard or custom header or enter a new custom header name.
4. In the Header Regex field, enter the header values to which this rule applies.

Example

An object named CorporateHeader with client IP address 10.1.1.1.



Figure 13-16: Specifying a Header

IM User

Specifies an IM user by their handle. IM traffic sent to or from this user is subject to this rule. You can enter a complete User ID, a string that is part of a User ID, or a string with a regular expression. Select the match type from the drop-down list to the right (Exact, Contains, or RegEx).

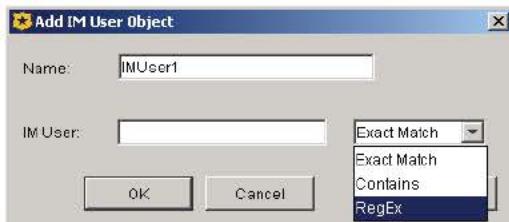


Figure 13-17: Specifying an IM User

Client Negotiated Cipher

Specifies a cipher code. Select a code from the drop-down list. This object is automatically named using the prefix Cipher; for example, Cipher: RC4-MD5.

Section C: Detailed Object Column Reference

Client Negotiated Cipher Strength

Specifies the cipher strength. Select Export, Low, Medium, or High from the drop-down list. This object is automatically named using the prefix Cipher Strength; for example, Cipher Strength: Medium.

Combined Source Object

Allows you to create an object that combines different source types. Refer to "Using Combined Objects" on page 444.

Source Column/Policy Layer Matrix

The following matrix lists all of the Source column objects and indicates which policy layer they apply to.

Object	Admin Auth	Admin Access	DNS Access	SOCKS Auth	Web Auth	Web Access	Web Content	Forwarding
Streaming Client						x		
Client Hostname Unavailable					x	x		
Authenticated User						x		
Client IP Address/Subnet	x	x	x	x	x	x		x
Client Hostname	x			x	x	x		x
Proxy IP Address/Port	x	x	x	x	x	x		x
User		x				x		
Group		x				x		
Attribute		x				x		
DNS Request Name			x					
RDNS Request IP Address/Subnet			x					
DNS Request Opcode			x					
DNS Request Class			x					
DNS Request Type			x					
DNS Client Transport			x					
SOCKS Version				x		x		
User Agent					x	x		
Request Header					x	x		
IM User						x		
Combined Objects	x	x	x	x	x	x		x

Section C: Detailed Object Column Reference

Destination Column Object Reference

A *destination* object specifies the communication or Web traffic destination that is evaluated by the policy. Not all policy layers contain the same destination objects; once you understand each destination object, however, you can configure as necessary in any layer of your policies.

Any

Applies to any destination.

DNS Response Contains No Data

This is a static object.

Destination IP Address/Subnet

Specifies the IP address and, optionally, a subnet mask of a destination server. The policy defined in this rule only applies to this address only or addresses within this subnet. This object is automatically named using the prefix Destination; for example, Destination: 1.2.0.0/255.255.0.0.

Destination Host/Port

Specifies the hostname or port of a destination server. The policy defined in this rule applies to this host on this port only. Enter the host name and port number, and select matching criteria. This object is automatically named using the prefix Destination; for example, Destination: company:80.

URL

Specifies a URL entered by a user.

To Specify a URL:

Select a radio button and enter the required information in the fields:

- Simple Match—Matches a partial URL. If a host name is specified, all hosts in that domain or subdomain match; if a path is specified, all paths with that path prefix match; if a scheme or port number is specified, only URLs with that scheme or port match. This object is automatically named using the prefix URL; therefore, the object is displayed as URL: host.com.
- Regular Expression Match—Specifies a regular expression. This object is automatically named using the prefix URL; therefore, the object is displayed as URL: host.com (RegEx).
- Advanced Match—Specifies a scheme (protocol), host, port range, and/or path. Enter a name at the top of the dialog to name the object. With host and path, you can select from the drop-down list to match exactly as entered or parts thereof: Exact Match, Contains, At Beginning, At End, or RegEx. If you select a matching qualifier, that attribute is appended to the object in parentheses. For example, URL: host.com (Contains).

Section C: Detailed Object Column Reference

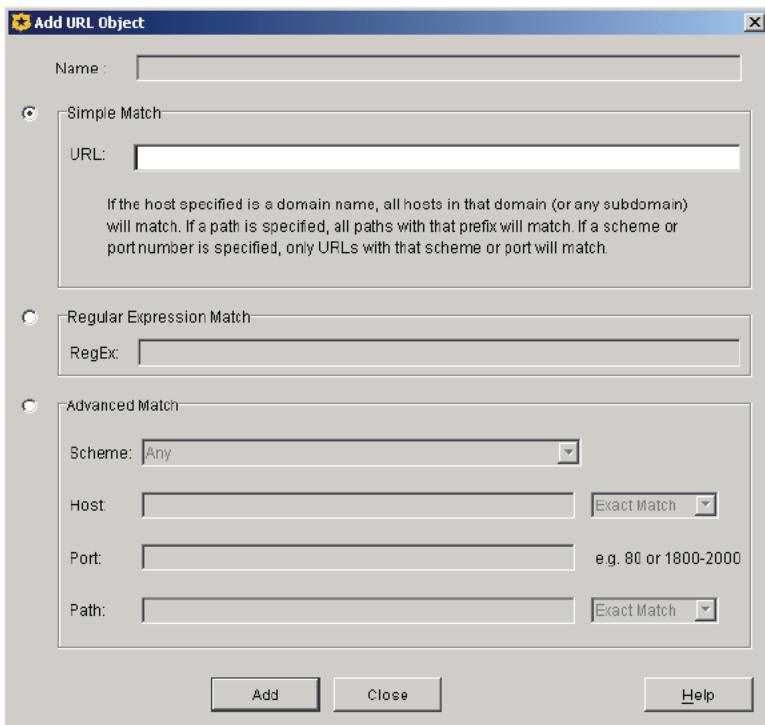


Figure 13-18: Specifying Destination URLs

Category

Displays a list of pre-defined URL categories. None and Unavailable always display. You can also create new categories from this dialog, which is the same dialog accessed through the VPM Menu Bar as described in "Creating Categories" on page 446.

Note: If one or more other administrators have access to the ProxySG through other workstations and are creating categories either through VPM or with inline commands, consider that newly-created or edited categories are not synchronized until the policy is installed. When the policy is installed with VPM, the categories are refreshed. If confusion occurs, select the File>Revert to Existing Policy on ProxySG Appliance option to restore the policy to the previous state and reconfigure categories.

File Extensions

Creates a list of file extensions. The rule is triggered for content with an extension matching any on the list. You can create multiple lists that contain various extensions to use in different rules. For example, create a list called Pictures, and select file extension types such as GIF, JPEG, BMP, XPM, and so on.

Section C: Detailed Object Column Reference

HTTP MIME Types

Creates a list of HTTP MIME content types. The rule is triggered for content matching any on the list. You can create multiple lists that contain various MIME types to use in different rules. For example, create a list called MicrosoftApps, and select MIME types application/vnd.ms-excel, application/vnd.ms-powerpoint, application/vnd.ms-project, and application/vnd.works.

Note: If you require a MIME type not contained in this list, use a URL object that uses the At End matching criteria.

Response Code

Specifies the rule applies to content responses containing a specific HTTP code. Select a code from the drop-down list. You can name the rule object or accept the default name.

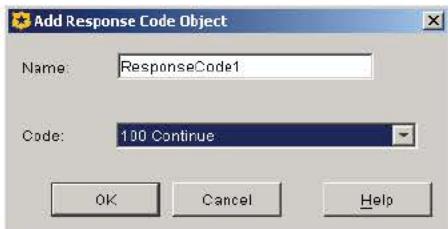


Figure 13-19: Specifying a Response Code

Response Header

Specifies the rule applies to content responses containing a specific header. Blue Coat supplies a list of standard headers, but you can also enter a custom header.

To Specify a Header:

1. In the Name field, enter a custom name or leave as is to accept the default.
2. From the Show drop-down list select the viewing field from All to Standard or Custom, as desired. Standard displays only the default standard headers. Custom displays any admin-defined headers that exist.
3. From the Header Name drop-down list, select a standard or custom header.
4. In the Header Regex field, enter the header string this rule applies to.

Section C: Detailed Object Column Reference

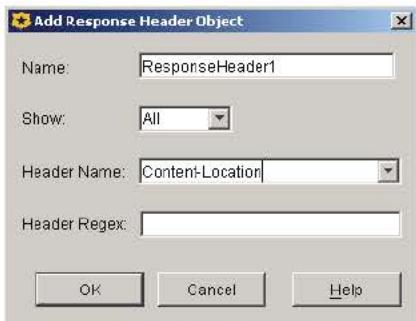


Figure 13-20: Specifying a Response Header

IM Buddy

Specifies an IM buddy by their handle. IM traffic sent to or from this buddy is subject to this rule. You can enter a complete buddy ID, a string that is part of a buddy ID, or a string with a regular expression. Select the match type from the drop-down list to the right (Exact, Contains, or RegEx).

IM Chat Room

Specifies an IM chat room by name or other triggers. IM traffic sent to this chat room is subject to this rule.

To Create a Chat Room Trigger:

1. In the Name field, enter a name for the object or leave as is to accept the default.
2. Select one or more of the following triggers:
 - Room ID—Specifies a specific IM chat room by its name. Enter a name and from the drop-down list select an option: Exact Match, Contains, or RegEx.
 - Type—Specifies the type of room. Select Private or Public.
 - Invite Only—Specifies to trigger if must be invited or not.
 - Voice Enabled—Specifies whether room supports voice chat or not.
 - Conference—Specifies whether room is a conference or not.
3. Click OK.

Example

An object named ChatRoom1 that triggers the rule if the room is private.

Section C: Detailed Object Column Reference

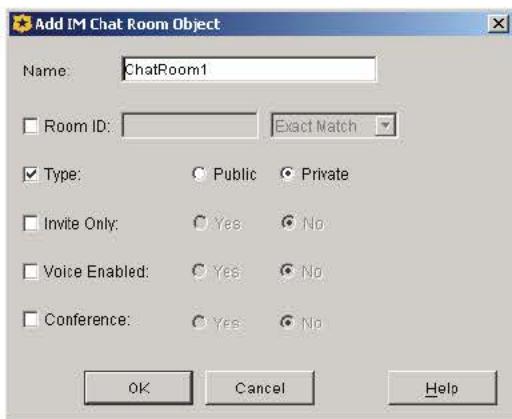


Figure 13-21: Chat Room Object

DNS Response IP Address/Subnet

Specifies the destination DNS IP address and, optionally, a subnet mask. The policy defined in this rule only applies to DNS responses containing this address or addresses within this subnet. This object is automatically named using the prefix DNS; for example, DNS: 1.2.3.4/255.255.0.0.

RDNS Response Host

Specifies a reverse DNS response hostname resolved in the reverse lookup of a client IP address. Enter the host name and select matching criteria. This object is automatically named using the prefix RDNS; for example, RDNS: host.com. If you select a matching qualifier, that attribute is appended to the object in parentheses. For example, RDNS: host.com (RegEx).

DNS Response CNAME

Specifies the rule applies to DNS CNAME responses matching a given hostname. Enter the host name and select matching criteria. This object is automatically named using the prefix DNS CNAME; therefore, the object is displayed as DNS CNAME: host.com.

DNS Response Code

Specifies the rule applies to DNS responses containing a specific DNS Response code. Select one or more codes from the list. You can name the rule object or accept the default name.

Combined Destination Objects

Allows you to create an object that combines different destination types. Refer to "Using Combined Objects" on page 444.

Section C: Detailed Object Column Reference

Destination Column/Policy Layer Matrix

The following matrix lists all of the Destination column objects and indicates which policy layer they apply to.

Object	Admin Auth	Admin Access	DNS Access	SOCKS Auth	Web Auth	Web Access	Web Content	Forwarding
Destination IP Address/Subnet					x	x	x	x
Destination Port					x	x	x	x
URL					x	x	x	x
Category			x			x	x	x
File Extensions						x	x	
HTTP MIME Types						x	x	
Response Header						x		
Response Code						x		
IM Buddy						x		
IM Chat Room						x		
DNS Response IP Address/Subnet			x					
RDNS Response Host			x					
DNS Response CNAME			x					
DNS Response Code			x					
Combined Objects			x		x	x	x	x

Service Column Object Reference

A *service* object specifies a service type, such as a protocol, that is evaluated by the policy. Not all policy layers contain the same service objects; once you understand each service object, however, you can configure as necessary in any layer of your policies.

Any

Applies to any service.

Using HTTP Transparent Authentication

This is a static object. The rule applies if the service is using HTTP transparent authentication.

Virus Detected

This is a static object. Based on a content scan, this object trigger is set as one of the following:

- yes—A virus was detected and there were no scanning process errors on either the ProxySG or the virus scanning server. Based on this, you can define an action. For example: to only allow to a specific person, such as the administrator, to see the object but deny to everyone else; begin a trace; and send to an access log.

Section C: Detailed Object Column Reference

Once the ProxySG caches a clean copy of the object (which might also be an exception page), the trigger is set to no and is not resent for content scanning on subsequent requests. This also prevents the repetitive logging of the same virus detection event in the logs, which allows for easier examination.

- no—No viruses were detected, nor were there any scanning process errors on either the ProxySG or the virus scanning server.

In all other cases, when the object was not able to be scanned and its state of clean or infected cannot be determined, the rule containing this trigger does not match. For example: the virus scanner is configured to block password-protected files; or the data is malformed and not scannable.

Client Protocol

Specifies the client protocol types. From the first drop-down list, select a type from the drop-down list: FTP, HTTP, HTTPS, Instant Messaging, SOCKS, Streaming, or TCP Tunneling. The second drop-down list allows you to select a protocol subset. For example, you can select the Streaming protocol and select Windows Media over HTTP.



Figure 13-22: Specifying Client Protocol Type

Protocol Methods

Specifies the protocol methods. Select a protocol from the drop-down list: FTP, HTTP, HTTPS, Instant Messaging, SOCKS. Next, select each specific method.

Section C: Detailed Object Column Reference

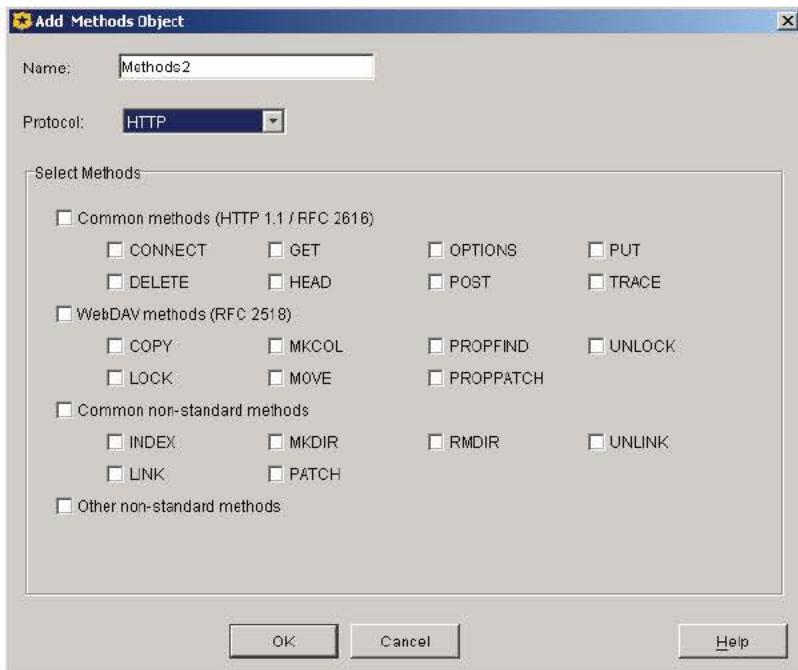


Figure 13-23: Specifying HTTP Protocol Methods

IM File Transfer

Specifies the rule is applied to IM file transfers, which can be triggered by matching the file name, file size, or both.

To Specify IM File Transfer Parameters:

1. In the Name field, enter a name for the object or accept the default.
2. To trigger by file name, select File. In the File field, specify a file name; from the drop-down list, select if file is matched exactly (Exact Match), if the file contains the name (Contains), or matched by regular expression (RegEx).
3. To trigger by message size, select Size. Enter a range; from the drop-down list, select the size attribute: bytes, kilobytes, megabytes, or gigabytes.

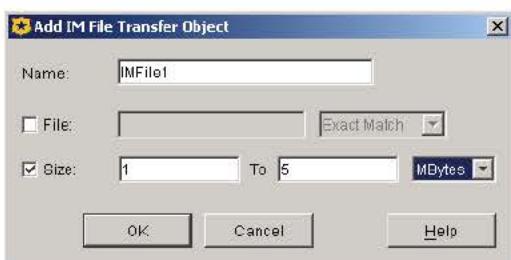


Figure 13-24: Limiting IM File Transfers

Section C: Detailed Object Column Reference**IM Message Text**

Specifies the rule is applied to IM message text, which can be triggered by any or all of the following: matching content keywords, message size, service type, and whether the content type is text or application.

To Specify IM Message Text Parameters:

1. In the Name field, enter a name for the object or accept the default.
2. To trigger by content keywords, select Text. In the Text field, specify a keyword; from the drop-down list, select if the file contains the text (Contains), or matched by regular expression (RegEx).
3. To trigger by message size, select Size. Enter a range; from the drop-down list, select the size attribute: bytes, kilobytes, megabytes, or gigabytes.
4. To specify the message route, select Route. From the drop-down list, select Service, Direct, or Chat.
5. To specify message type, select Text or Application.

Text specifies messages entered by a user; Application specifies messages sent by the client application, such as typing notifications.

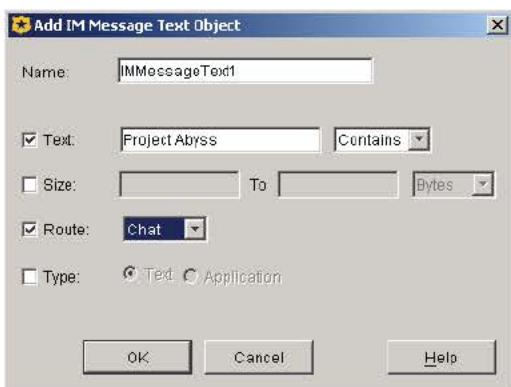


Figure 13-25: Triggering IM Rule with Text and Route Type

IM Message Reflection

Allows policy to test whether or not reflection is enabled for the current message and, if enabled, whether it is possible.

- Succeeded—IM reflection is enabled and is performed for this message.
- Failed—IM reflection is enabled, but not possible for this message because the recipient is not connected through this ProxySG.
- Disabled—IM reflection is not enabled for this message.

The objects are automatically named based on the selection and can be used in any rule.

Section C: Detailed Object Column Reference

Streaming Content Type

Defines streaming content by protocol.

To Specify Streaming Content Type:

1. In the Name field, enter a name for the object or accept the default.
2. Select All Streaming Content (all protocols become selected), or one or more streaming protocols.
3. Click OK.

ICAP Error Code

Defines an object that recognizes one or more ICAP error codes returned during an antivirus scan. The rule applies if the scan returns the specified errors.

To Specify ICAP Error Codes:

1. In the Name field, enter a name for the object or accept the default.
2. Select an option:
 - No errors—An ICAP scan was performed without scanning errors.
 - Any errors—An ICAP error code was returned during a scan.
 - Selected errors—An ICAP error code of a specific type or types.
In the Available Errors field, select one or more ICAP error codes (press and hold the Control key to select more than one type or the Shift key to select a block of types). Click Add.
3. Click OK.

Interactivity:

- Of the available Selected errors, only the following error codes are available for all virus scanning servers: Connection Failure, Internal Error, Request Timeout, Server Error, and Server Unavailable. The other errors are specific to the Blue Coat ProxyAV virus scanning server.
- If the ProxySG is configured to deny, this trigger *cannot* override that setting to allow; however, it can trigger an exception action to deny if the ProxySG is configured to allow (see "Return Exception" on page 423).

Combined Service Objects

Allows you to create an object that combines different service types. Refer to "Using Combined Objects" on page 444.

Service Column/Policy Layer Matrix

The following matrix lists all of the Service column objects and indicates to which policy layer they apply.

Section C: Detailed Object Column Reference

Object	Admin Auth	Admin Access	DNS Access	SOCKS Auth	Web Auth	Web Access	Web Content	Forwarding
Using HTTP Transparent Authentication						x		
Virus Detected						x		
Client Protocol						x	x	x
Protocol Methods						x	x	x
IM File Transfer						x		
IM Message Text						x		
IM Message Reflection						x		
Streaming Content Type						x		
ICAP Error Code						x		
Combined Objects						x	x	x

Time Column Object Reference

A *time* object specifies a block of time or time trigger that determines client access regarding other parameters in the rule (such Web sites and content types). Currently, the Time object is only applicable to the Web Access Layer.

Any

Applies anytime.

Time

Specifies the time restrictions.

To Configure Time Restrictions:

1. In the Name field, enter a name for the object or leave to accept the default.
2. Select Use Local Time Zone or Use UTC Time Zone.

Local time sets the rule to follow the ProxySG internal clock. UTC sets the rule to use the Universal Coordinated Time (also known as Greenwich Mean Time or GMT).

3. To specify a range for any given day, select Enable; in the Specify Time of Day Restriction (hh:mm) field, configure the times. The time style is military.

The range can be contained within one 24-hour calendar day, or overlap days. For example, configuring the time to range from 22:00 to 06:00 sets a limit from 10 at night to 6 the following morning.

4. To specify a day of the week restriction, select Enable; in the Specific Weekday Restriction field, select one or more days.

Section C: Detailed Object Column Reference

5. To specify a day of the month range restriction, select **Enable**; in the **Specify Day of Month Restriction** field, select the days, which are numbered from 01 to 31. To limit the range to specific day, configure the numbers to be the same. For example, selecting 22 and 22 specifies the rule to apply only the 22nd day of every month.
6. To specify a restriction that spans one or more months, select **Enable**; in the **Specify Annually-Recurring Date Restriction** field, select the month and day ranges. This calendar restriction applies every year unless the restriction is altered.
Overlapping months is allowed, similar to the behavior of day ranges in Step 3.
7. To specify a one-time only restriction, select **Enable**; in the **Specify Non-Recurring Date Restriction** field, select the year, month, and day ranges. This calendar restriction applies only during the time specified and will not repeat.

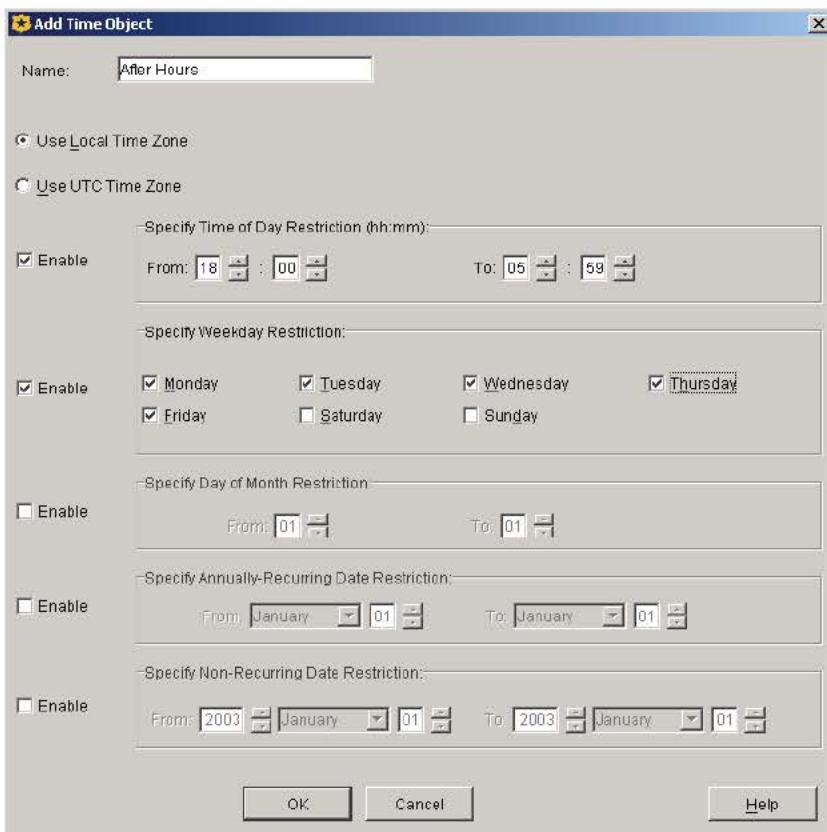


Figure 13-26: Configuring Time Limitations

Combined Time Object

Allows you to combine a time object that adheres to multiple time restrictions. See "Using Combined Objects" on page 444.

Section C: Detailed Object Column Reference

Time Column/Policy Layer Matrix

The following matrix lists all of the Time column objects and indicates which policy layer they apply to.

Object	Admin Auth	Admin Access	DNS Access	SOCKS Auth	Web Auth	Web Access	Web Content	Forwarding
Time			x			x		
Combined Objects			x			x		

Section C: Detailed Object Column Reference

Action Column Object Reference

An *action* object determines which action to take if other parameters, such as source, destination, service, and time requirements validate the rule. Not all policy layers contain the same action objects; once you understand each action object, however, you can configure as necessary in any layer of your policies.

Important: Because of character limitations required by the generated CPL, only alphanumeric, underscore, and dash characters can be used to define an action object name.

Allow

This is a static object. Selecting this overrides other related configurations and the specified user requests are allowed.

Deny

This is a static object. Selecting this overrides other related configurations and denies the specified user requests.

Force Deny

This is a static object. Forces a request to be denied, regardless if rules in subsequent layers would have allowed the request.

Allow Read-Only Access

This is a static object. Grants full access to view data on the appliance.

Allow Read-Write Access

This is a static object. Grants full access to view and manipulate data on the appliance.

Do Not Authenticate

This is a static object. Selecting this overrides other configurations and the specified users are not authenticated when requesting content.

Authenticate

Creates an authentication object to verify users. An authentication realm must exist on the ProxySG to be selected through VPM.

Note: In the SOCKS Authentication policy layer, the object is SOCKS Authenticate.

Section C: Detailed Object Column Reference

To Create an Authentication Object:

1. In the Name field, enter a name for the object or leave as is to accept the default.
2. From the Realm drop-down list, select an authentication realm, which must already exist on the ProxySG.
3. Optional (in the Web Authentication policy layer only): from the Mode drop-down list, select a mode. The mode determines the way the ProxySG interacts with the client for authentication specifying the challenge type and the accepted surrogate credential:
 - Auto—The default; the mode is automatically selected, based on the request. Selects among proxy, origin-IP, and origin-IP-redirect, depending on the type of connection (explicit or transparent) and the transparent authentication cookie settings.
 - Form Cookie—for forms-based authentication: cookies are used as surrogate credentials. The cookies are set on the OCS domain only, and the user is presented with the form for each new domain. This mode is most useful in reverse proxy scenarios where there are a limited number of domains.
 - Form Cookie Redirect—the user is redirected to the authentication virtual URL before the form is presented. The authentication cookie is set on both the virtual URL and the OCS domain. The user is only challenged when the credential cache entry expires.
 - Form IP—the user's IP address is used as a surrogate credential. The form is presented whenever the user's credential cache entry expires.
 - Form IP Redirect—This is similar to Form IP except that the user is redirected to the authentication virtual URL before the form is presented.
 - Proxy—for explicit forward proxies: the ProxySG uses an explicit proxy challenge. No surrogate credentials are used. This is the typical mode for an authenticating explicit proxy.
 - Proxy IP—the ProxySG uses an explicit proxy challenge and the client's IP address as a surrogate credential.
 - Origin—the ProxySG acts like an OCS and issues OCS challenges. The authenticated connection serves as the surrogate credential.
 - Origin IP—the ProxySG acts like an OCS and issues OCS challenges. The client IP address is used as a surrogate credential.
 - Origin Cookie—for transparent proxies: for clients that understand cookies but do not understand redirects; the ProxySG acts like an origin server and issues origin server challenges. The surrogate credential is used.
 - Origin Cookie Redirect—for transparent forward proxies: the client is redirected to a virtual URL to be authenticated, and cookies are used as the surrogate credential. The ProxySG does not support origin-redirects with the CONNECT method.
 - Origin IP Redirect—Significantly reduces security; only useful for reverse proxy and when clients have unique IP addresses and do not understand cookies (or you cannot set a cookie). Provides partial control of transparently intercepted HTTPS requests. The client is redirected to a virtual URL to be authenticated, and the client IP address is used as a surrogate credential. The ProxySG does not support origin-redirects with the CONNECT method.

Section C: Detailed Object Column Reference

- SG2—The mode is selected automatically, based on the request using the SGOS 2.x-defined rules.
4. (Optional) If you selected a Form mode in Step 3, the Form drop-down list becomes active. Select an authentication form that has already been created on the Authentication>Forms panel
 5. Click OK.

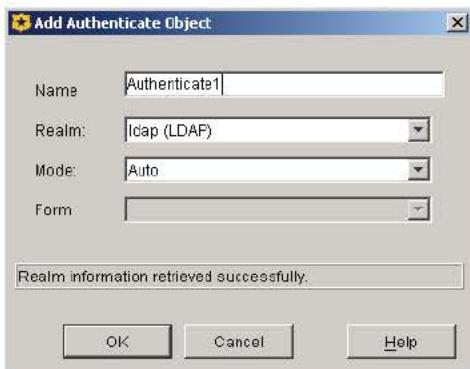


Figure 13-27: Specifying an Authentication Realm

Users are prompted to provide a valid user name and password.

Force Authenticate

Forces the user to authenticate even though the request is going to be denied for reasons that do not depend on authentication. This action is useful to identify a user before the denial so that the username is logged along with the denial.

Note: In the SOCKS Authentication policy layer, the object is Force SOCKS Authenticate.

Bypass Cache

This is a static object. Prevents the cache from being queried when serving a proxy request, and prevents the response from the origin server from being cached.

Do Not Bypass Cache

This is a static object. The ProxySG always checks if the destination is cached before going to the origin server; also, the content is cached if cacheable.

Bypass DNS Cache

This is a static object. Prevents the request from querying the DNS cache list of resolved lookup names or addresses.

Section C: Detailed Object Column Reference

Do Not Bypass DNS Cache

This is a static object. The ProxySG always queries the DNS cache list of resolved lookup names or addresses.

Allow DNS From Upstream Server

This is a static object. Allows the ProxySG to send requests for data not currently cached to DNS servers.

Serve DNS Only From Cache

This is a static object. Instructs the ProxySG to only serve a DNS request from content that is already cached.

Enable/Disable DNS Imputing

These are static objects. If DNS imputing is enabled, the ProxySG appends the suffixes in the DNS imputing list to hostnames looked up when the original name is not found.

Check/Do Not Check Authorization

These are static objects. These actions control whether or not the ProxySG forces a request to be sent to an upstream server every time to check authorization, even if the content is already cached. The check action is not usually required for upstream origin content servers performing authentication, as the ProxySG automatically tracks whether content required authentication in each case. However, it can be required when an upstream proxy is performing proxy authentication because of the way some proxies cache credential information, causing them not to reliably challenge every request. When requests are directed to an upstream proxy which operates in this manner, enabling Check Authorization ensures that all such requests are properly authorized by the upstream proxy before the content is served from the local cache.

Always Verify

This is a static object. Cached content is always verified for freshness for the sources, destinations, or service specified in the rule. For example, the CEO and Executive Staff always require content to be the most recent, but everyone else can be served from the cache.

Use Default Verification

This is a static object. Overrides the Always Verify action and instructs the ProxySG to use its default freshness verification.

Section C: Detailed Object Column Reference

Block/Do Not Block Pop-Up Ads

These are static objects. Blocks or allows pop-up windows. Blue Coat recommends creating separate Web Access policy layers that only contain pop-up blocking actions. Furthermore, many Web applications require pop-up windows. As it is unlikely that your intranet contains pages that pop-up unwanted advertising windows, Blue Coat recommends disabling pop-up blocking for your intranet. For example:

- Web Access rule 1: Specify the intranet IP address and subnet mask in the Destination column and select Do Not Block Popup Ads in the Action column.
- Web Access rule 2: Select Block Popup Ads in the Action column.

As you continue to modify policy, you can add more policy layers to block or allow specific IP addresses, but the policy layer as defined in the Web Access rule 2 above *must* always be positioned last, blocking pop-up ads is the default if a previous policy rule does not trigger.

For more concept information about pop-up windows, refer to "Blocking Pop-Up Windows" on page 473.

Force/Do Not Force NTLM for Server Auth

These are static objects. When configured for explicit proxy, Internet Explorer (IE) does not support an NTLM challenge from an origin server. If Force NTLM for Server Auth is applied, the ProxySG converts the 401-type server authentication challenge to a 407-type proxy authentication challenge, which IE supports. The ProxySG also converts the resulting Proxy-Authentication headers in client requests to standard server authorization headers, which allows an origin server NTLM authentication challenge to pass through when IE is explicitly proxied through the ProxySG.

Reflect/Do Not Reflect IM Messages

These are static objects. IM traffic can be contained and restricted to the network so that it never reaches the IM server. A hierarchy of ProxySG appliances manage the traffic and routes it depending on each ProxySG fail open and fail closed configurations. For detailed information about this deployment, refer to Chapter 16, Instant Messaging, of the *Blue Coat Configuration and Management Guide*.

Block/Do Not Block IM Encryption

These are static objects. AOL IM provides the option for clients to send encrypted messages through both standard messaging (through the IM service) and direct connection messaging. These objects allow you to block or not block the ability to send encrypted messages through AOL IM. For detailed information about security benefits of this feature, see Chapter 16, Instant Messaging, of the *Blue Coat Configuration and Management Guide*.

Return Exception

Allows you to select exception types and associate a custom message, if desired. Blue Coat provides a list of standard exceptions, but VPM also accepts user-defined values.

Section C: Detailed Object Column Reference

To Create a Return Exception Object:

1. In the Name field, enter a name for the object or leave as is to accept the default.
2. Perform one of the following:
 - Standard exception type: select one from the Built-in exception drop-down list.
 - Custom exception (which already must be defined on the ProxySG) type: select one from the User-defined exception drop-down list.
3. Optional: Select Force exception even if later policy would allow request to supersede other policy that applies to this request.
4. Optional: Select Allow re-authentication to allow the user to re-enter credentials should the first attempt fail.
5. Optional: in the Details field, enter a message that is displayed along with the summary and exception ID on the exception page displayed to the user when the exception is returned.

Example

An object named DNSException2 that upon a DNS server failure returns a message to the user instructing them to contact their support person.

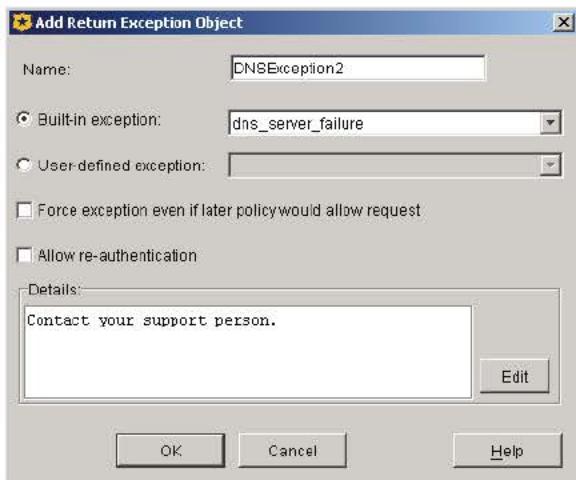


Figure 13-28: Return Exception Object

To create custom exceptions, see "Defining Exceptions" on page 477.

Return Redirect

Aborts the current transaction and forces a client request to redirect to a specified URL. For example, used to redirect clients to a changed URL; or redirecting a request to a generic page stating the Internet access policy. Applies only to HTTP transactions.

Section C: Detailed Object Column Reference

Note: Internet Explorer (IE) ignores redirect responses from FTP over HTTP requests, although Netscape Navigator obeys the redirect. To avoid problems with IE, do not use redirect when url.scheme=ftp.

If the URL that you are redirecting the browser to also triggers a redirect response from your policy, then you can put the browser into an infinite loop.

In the Name field, enter a name for the object (or leave as is to accept the default); in the URL field, enter the redirect destination URL.

Example

An object that redirects clients to an HTML policy statement page.

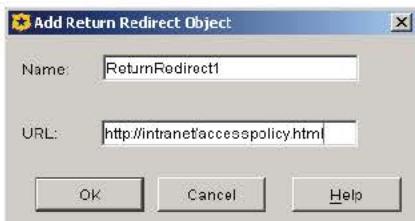


Figure 13-29: Return Redirect Object

Send IM Alert

Defines a message that is sent to an IM user by the ProxySG. The message is triggered by the IM parameters defined in the policy (for example, client login, sent or received messages, and buddy notification). Chapter 16: “Instant Messaging” on page 527 provides more information about regulating IM through the ProxySG, as well as VPM examples.

Example

A message that informs IM users their messaging is logged.

Section C: Detailed Object Column Reference



Figure 13-30: Send IM Alert Object

Modify Access Logging

Defines access logging behavior.

- Disable all access logging—No activity is logged for the requests matched by the rule.
- Reset to default logging—Resets to logging the request to the default log specified by the ProxySG configuration, if one exists.
- Enable logging to—Enables logging of requests matched by this rule to the specified log.
- Disable logging to—Disables logging of requests matched by this rule to the specified log.

Override Access Log Field

Allows you to manipulate access log entries. For any specific log value, you can suppress the value, encode the value in Base64, or rewrite the value.

To Override Access Log Fields:

1. In the Name field, enter a name for the object or leave as is to accept the default.
2. From the Log Name drop-down list, select a log (must already be configured on the ProxySG).
3. From the Field Name drop-down list, select an access log field.
4. Select one of the following:
 - Log original value—Records unmodified value in the access log.
 - Suppress value—Prevents value from appearing in the access log.
 - Base64 encode value—Records an encoded version of the value in the access log.
 - Rewrite value—in the field, enter a string that replaces the value.

Section C: Detailed Object Column Reference

- Edit—Clicking Edit calls the Select The Rewrite String dialog, which allows you to substitute the value with information defined by other field types.
5. Click OK.

Example

An object called CEOLogRewrite that suppresses log entries so persons, such as support personal, cannot view economically sensitive information to gain improper knowledge.



Figure 13-31: Overriding Access Log Fields

Rewrite Host

Rewrites host component of a URL, specifying either Windows Media, Real Media, or all protocols. Use this to redirect the request to a different host. For example, rewrite `www.foo.com` to `www.bar.com`. You can create and name multiple rewrites, but you can only specify one per rule.

To Specify a Rewrite:

1. In the Name field, enter a name or leave as is to accept to the default.
2. From the Scheme drop-down list, Windows Media, Real Media, or All to rewrite all URLs, regardless of protocol.
3. In the Pattern field, enter a host name (for example, `foo`).
4. In the Replacement field, enter the name the pattern is rewritten as (for example, `bar`).
5. Click OK.

Section C: Detailed Object Column Reference



Figure 13-32: Specifying a Host Rewrite

Reflect IP

Specifies which IP address is used when making connections to upstream hosts.

To Create a Reflect IP Object:

1. In the Name field, enter name for the object or leave as is to accept the default.
2. In the In outgoing client IP, reflect field, select one of the following:
 - Do not reflect IP—Disables reflecting IPs; the ProxySG uses the IP address of the interface that request is sent out on.
 - Incoming client IP [IP spoofing]—Reflects the client IP address.
 - Incoming proxy IP—Reflects the IP address of where the request arrived to.
 - Proxy IP—Specifies to reflect a specific IP of the ProxySG; enter the IP address in the field.
 - Use services configuration—Specifies whether to reflect IP in the configuration of the service which is used to process the request.
3. Click OK.

Example

This object reflects another IP address configured on the ProxySG.

Section C: Detailed Object Column Reference

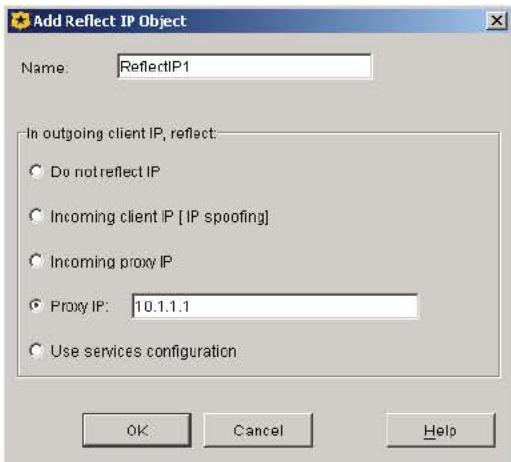


Figure 13-33: Reflect IP Object

Suppress Header

Specifies one or more standard headers that are suppressed (not transmitted) on the outbound request, the outbound response, or both.

To Create a Suppress Header Object:

1. In the Name field, enter name for the object or leave as is to accept the default.
2. Select Request, Response, or Both.
3. Select one or more header types from the list.
4. Click OK.

Example

An object called IntranetHeaders that suppresses headers so specified users can access economically sensitive information without people, such as support personal, being able to gain knowledge of sources.

Section C: Detailed Object Column Reference

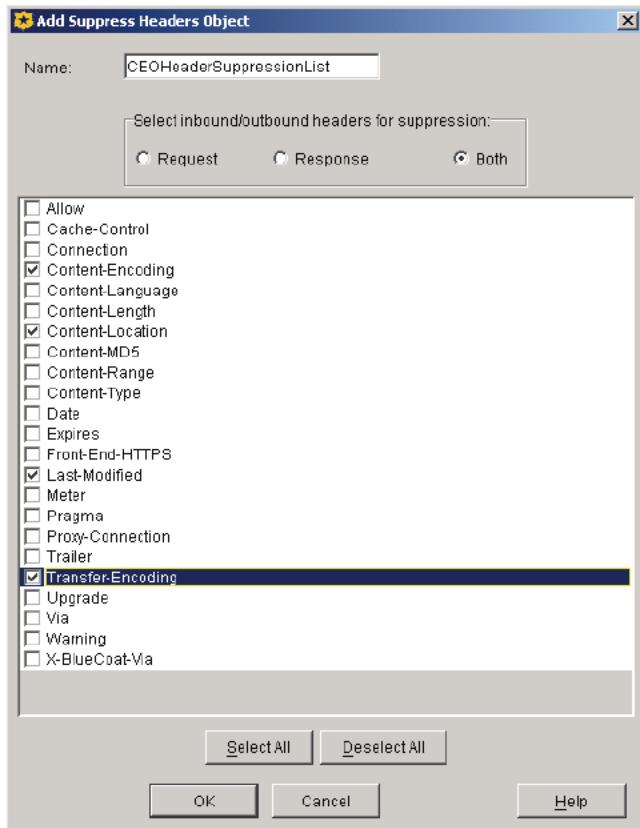


Figure 13-34: Creating a Suppressed Header List Object

"Modifying Headers" on page 476 provides more conceptual information about header modification.

Control Request Header/Control Response Header

For any request or response, specifies to:

- Insert a header with a specific value.
- Rewrite the value of a specific header.
- Suppress a specific header.

Section C: Detailed Object Column Reference



Figure 13-35: Rewriting the Request Header

Strip Active Content

Strips HTTP tags from specified active content HTML pages. For each item you select for removal, you can also create a customized message that is displayed to the user.

Note: Pages served over an HTTPS tunneled connection are encrypted, so the content cannot be modified.

"Stripping or Replacing Active Content" on page 474 provides detailed information about the different types of active content.

To Create a Strip Active Content Object:

1. In the Name field, enter name for the object or leave as is to accept the default.
2. Select the active content to be stripped.
3. The default message in the Replacement Text column is Active Content Removed. To replace the default message, double click the field and enter a message. For example, Java applets have been removed. To not display a message, delete the default and leave blank.

Section C: Detailed Object Column Reference

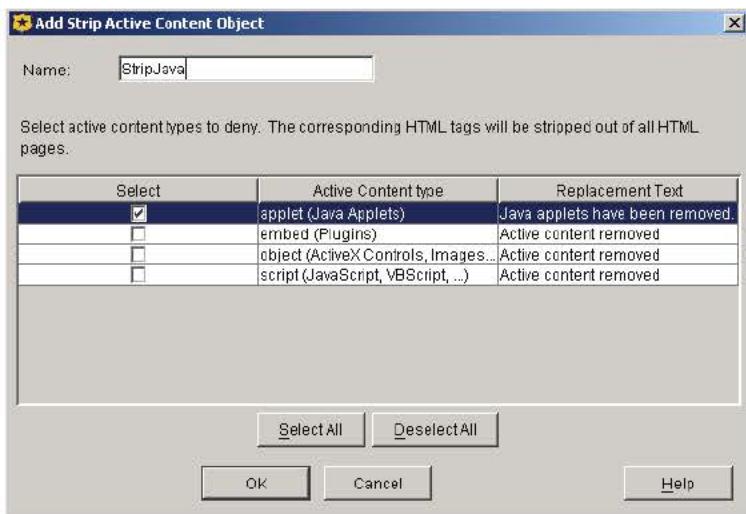


Figure 13-36: Creating a Strip Active Content Action Object

Exempting the ProxySG

Stripping active content might interfere with Web applications deployed on your intranet. For example, if you create a policy rule that removes Java applets, and the destination defined in the rule contains an IP address of a ProxySG functioning as a proxy, the policy rule actually disables the Management Console because the Console itself is comprised of Java applets.

To prevent this, for each ProxySG functioning as a proxy, create a rule that exempts the IP address of the ProxySG from the stripping action.

1. Click Add Rule.
2. Click Move Up; the rule to exempt the ProxySG must precede the rule that strips active content.
3. In the Destination field, enter the ProxySG IP address.
4. With the IP address entered, right-click it in the Destination field and select Negate from the drop-down list.
5. In the Action field, enter the Remove Active Contents, Java Apps action.

Web Authentication Layer (1) Admin Authentication Layer (1) Web Content Layer (1) Web Access Layer (1)							
No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	10.1.1.1	Any	Any	StripJava	None	

Figure 13-37: Exempting a ProxySG IP Address

Modify IM Message

In IM clients, replaces or appends the given text that is displayed to IM messages in clients that are logged in through the ProxySG. For example, inform users that their IM messaging activity is monitored.

Section C: Detailed Object Column Reference

1. In the Name field, enter a name for the object, or accept the default.
2. In the large, blank field, enter text to be displayed.
3. Select Set message text to replace the text displayed to the user. For example, Instant Messaging is not allowed during these hours. Alternatively, select Append to message text to add the text to the displayed message.

Chapter 16: “Instant Messaging” on page 527 provides more information about regulating IM through the ProxySG, as well as VPM examples.

Return ICAP Patience Page

Specifies to display an ICAP patience page after a determinable amount of time. Enter a time value (in seconds) that the ProxySG waits for content to be serviced from the origin content server before displaying the page that instructs users an ICAP scan is in progress.

Note: Patience pages display regardless of any pop-up blocking policy that is in effect.

Set External Filter Service

Specifies which installed content filtering service or service group a content request is subjected to or bypasses, and specifies what occurs if a communication error occurs between the ProxySG and the external service.

To Determine External Filter Service Request Behavior:

1. In the Name field, enter a name for the object or leave as is to accept the default.
2. To instruct all requests defined in the rule to route to a specific external filter service, select Use External Filter Service; from the drop-down list, select the external filter service or service group (which must already exist on the ProxySG).
3. Under Error Handling, select the action the ProxySG perform if an error occurs during a content scan:
 - Deny the client request (recommended)—The scan halts or does not begin, and the client does not receive any content. Blue Coat recommends this option for optimum security.
 - Continue without further external filter service processing—The scan halts or does not occur; however, the client receives the ProxySG-bypassed content. The security risk is increased, as malicious content can be brought into the network.

Section C: Detailed Object Column Reference

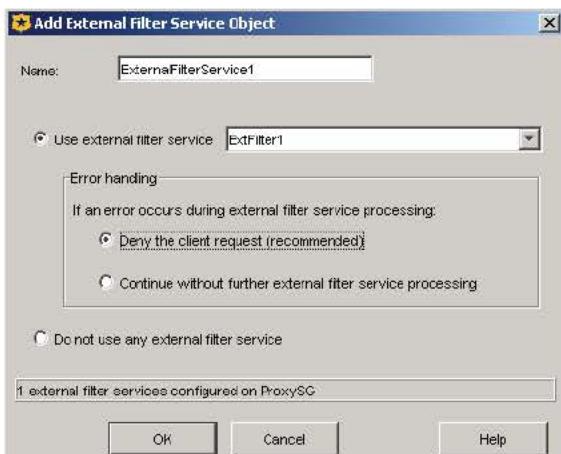


Figure 13-38: External Service Object

Set ICAP Request Service

Specifies which installed ICAP service or service group a content request routes to or bypasses, and specifies what occurs if a communication error occurs between the ProxySG and the ICAP server.

To Determine ICAP Request Behavior:

1. In the Name field, enter a name for the object or leave as is to accept the default.
2. To instruct all request or response types defined in the rule to route to a specific ICAP service, select Use ICAP Request Service; from the drop-down list, select the ICAP service or service group (which must already exist on the ProxySG).
3. Under Error Handling, select the action the ProxySG perform if an error occurs during an ICAP content scan:
 - Deny the client request (recommended)—The ICAP scan halts or does not begin, and the client does not receive any content. Blue Coat recommends this option for optimum security.
 - Continue without further ICAP request processing—The ICAP scan halts or does not occur; however, the client receives the ProxySG-bypassed content. The security risk is increased, as malicious content can be brought into the network.

The request is still subject to other content scanning policy, such as ICAP error codes, as well as the ProxySG allow/deny policy.

- If the ProxySG is set to fail-close and the virus scanner (a ProxyAV, for example) is configured to block, an ICAP exception action is generated without further policy evaluation.
- If the ProxySG is set to allow, further content scanning policy is allowed.

For related information, see "ICAP Error Code" on page 415.

Section C: Detailed Object Column Reference

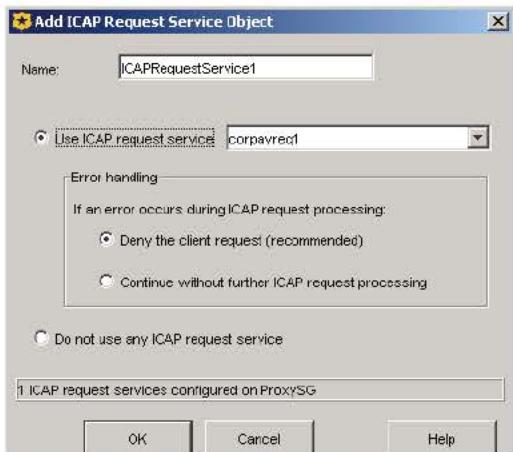


Figure 13-39: ICAP Service Object

Set ICAP Response Service

Identical to "Set ICAP Request Service", but applies to other protocol *responses*, such as HTTP and FTP.

Set FTP Connection

For an outgoing request over FTP, specifies whether the FTP connection should be made immediately or deferred, if possible. The benefit of deferring connections is that requests for previously cached content can be served without contacting the origin server, which reduces the FTP load on that server.

Set SOCKS Acceleration

Specifies whether or not accelerate SOCKS requests, and defines the transport method.

To Set SOCKS Acceleration:

1. In the Name field, enter a name for the object or leave as is to accept the default.

Section C: Detailed Object Column Reference

2. Select one of the following:
 - Automatically—Accelerates SOCKS requests automatically, based on the destination port receiving the connection.
 - Do Not Accelerate—Never accelerate SOCKS requests matched by this rule.
 - Accelerate via [HTTP | AOL IM | MSN IM | Yahoo IM]—Specifies the type of acceleration applied to requests matched by this rule.
3. Click OK.

Set Streaming Max Bitrate

Specifies the maximum bitrate, in kilobits per second, of requested streaming media. If a request exceeds this rule, the request is denied.

Send DNS/RDNS Response Code

Specifies to send out the default response code or a selectable error response code. Perform one of the following:

- Select Send Default DNS Response; optionally, enter a TTL value.
- Select Send Error Response Code and select a code from the drop-down list.

Send DNS Response

Specifies which IP address to return for a specified host.

To Set a DNS Response:

1. In the Host field, enter a host name that is returned.
2. To respond with the incoming IP address, select Respond with proxy IP.
3. To respond with one or more IP addresses:
 - a. Select Respond with listed IPs.
 - b. Click Add. The Add DNS Response IP dialog appears.
 - c. Enter an IP address and click Add.
 - d. Repeat as desired; click Close when finished.
4. (Optional) In the TTL field, enter a time-to-live value.
5. Click OK.

Send Reverse DNS Response

Specifies which host to return for a reverse DNS response. Optional: define a time-to-live value.

Section C: Detailed Object Column Reference

Do Not Cache

This is a static object. Specifies that objects requested by the defined source or served by the defined destination are never cached.

Force Cache

This is a static object. Specifies that objects are always cached; however, the object still must be a cacheable object. For example, RealMedia file types that are supported in pass-through mode only are not cached.

Use Default Caching

This is a static object. Overrides the Do Not Cache and Force Cache actions and instructs the ProxySG to use its default determination of whether or not to cache the content.

Mark/Do Not Mark As Advertisement

These are static objects. Specifies content to be identified as an advertisement. The ProxySG still fetches content from the cache (if present); however, just after serving to the client, the content is re-fetched from the ad server so that hit counters are updated.

Enable/Disable Pipelining

These are static objects. Enables or disables the ProxySG pipelining feature, which, when enabled, examines Web pages for embedded objects and requests them from the origin server in anticipation of a client request.

Set TTL

Specifies the time-to-live (TTL) an object is stored in the ProxySG. In the Name field, enter a name for the object (or leave as is to accept the default); in the TTL field, enter the amount of time in seconds.

Send Direct

This is a static object. Overrides forwarding host, SOCKS gateway, or ICP configurations and instructs the ProxySG to request the content directly from the origin server.

Integrate/Do Not Integrate New Hosts

This is a static object. Used in server accelerator deployments. When enabled, the corresponding host that is accessed is added to the list of hosts for which the ProxySG performs health checks. If that host name resolves to multiple IP addresses that correspond to different servers, the ProxySG fetches content from the available servers and ignores the servers that fail the health check.

Section C: Detailed Object Column Reference

Allow Content From Origin Server

This is a static object. Allows request to access content from an origin server if the content is not cached.

Serve Content Only From Cache

This is a static object. Requests to access content that is not cached are denied. If the content is cached, the content is served.

Select SOCKS Gateway

Specifies which SOCKS gateway, if any, to use; defines behavior if communication between the SOCKS gateway and the ProxySG is down.

- To instruct the rule to connect directly without routing through a SOCKS service, select Do not use SOCKS gateway.
- To instruct the rule to connect through a SOCKS gateway, select Use SOCKS Gateway and select an installed SOCKS service from the drop-down list.

In the If no SOCKS gateway is available field, select Deny the request or Connect directly, which allows requests to bypass the SOCKS service.

Select Forwarding

Specifies which forwarding host or group, if any, to use; defines behavior if communication between the forwarding and the ProxySG is down.

- To instruct the rule to connect directly without redirecting to a forwarding host or group, select Do not forward.
- To instruct the rule to redirect to a forwarding host, select Use Forwarding and select an installed forwarding host from the drop-down list.

In the If no forwarding is available field, select Deny the request (fail closed) or Connect directly (fail open), which allows requests to bypass the forwarding host.

- To instruct the rule to forward using the ICP configuration, select Forward using ICP.

Set IM Transport

Specifies the transport method used for IM traffic.

- Auto—Connects using the transport method used by the client.
- HTTP—Tunnels the IM requests over HTTP.
- Native—Connects using the native transport used by the service.

Section C: Detailed Object Column Reference

Set Streaming Transport

Specifies which streaming transport method the rule uses.

- Auto—Connects using the transport method used by the client.
- HTTP—Streaming over HTTP.
- TCP—Streaming over TCP.

Combined Action Objects

Allows you to combine an action object that invokes multiple actions. See "Using Combined Objects" on page 444.

Action Column/Policy Layer Matrix

The following matrix lists all of the Action column objects and indicates which policy layer they apply to.

Object	Admin Auth	Admin Access	DNS Access	SOCKS Auth	Web Auth	Web Access	Web Content	Forwarding
Allow						x		
Deny	x	x			x	x		
Allow Read-Only Access		x						
Allow Read-Write Access		x						
Do Not Authenticate	x			x	x			
Authenticate	x			x	x			
Force Authenticate	x			x	x			
Bypass Cache						x		
Do Not Bypass Cache						x		
Check Authorization						x	x	
Do Not Check Authorization						x	x	
Always Verify						x	x	
Use Default Verification						x	x	
Block Up Ads						x		
Do Not Block PopUp Ads						x		
Force NTLM For Server Auth						x		
Do Not Force NTLM For Server Auth						x		
Reflect IM Messages						x		
Do Not Reflect IM Messages						x		
Block IM Encryption						x		
Do Not Block IM Encryption						x		
Return Exception						x		
Return Redirect						x		

Section C: Detailed Object Column Reference

Object	Admin Auth	Admin Access	DNS Access	SOCKS Auth	Web Auth	Web Access	Web Content	Forwarding
Send IM Alert						x		
Modify Access Logging						x	x	
Override Access Log Field						x	x	
Rewrite Host						x		
Reflect IP			x			x		
Suppress Header						x		
Control Request Header						x		
Control Response Header						x		
Strip Active Content						x		
Modify IM Message						x		
Return ICAP Patience Page						x		
Set External Filter Service						x		
Set ICAP Request Service						x	x	
Set ICAP Response Service							x	
Use Default Caching							x	
Set FTP Connection						x		
Set SOCKS Acceleration						x		
Set Streaming Max Bitrate						x		
Send DNS/RDNS Response Code			x					
Send DNS Response			x					
Send Reverse DNS Response			x					
Do Not Cache							x	
Force Cache							x	
Mark As Advertisement							x	
Do Not Mark as Advertisement							x	
Enable Pipelining							x	
Disable Pipelining							x	
Set TTL							x	
Send Direct								x
Integrate New Hosts								x
Do Not Integrate New Hosts								x
Allow Content From Origin Server								x
Serve Content Only From Cache								x
Select SOCKS Gateway								x
Select Forwarding								x
Reflect IP								x
Set IM Transport								x

Section C: Detailed Object Column Reference

Object	Admin Auth	Admin Access	DNS Access	SOCKS Auth	Web Auth	Web Access	Web Content	Forwarding
Set Streaming Transport								x
Combined Objects			x			x	x	x

Track Object Column Reference

A *track* object defines the parameters for tracking and tracing traffic. All policy layers contain the same trace objects, but tracking parameters are layer-specific.

Note: Because of character limitations required by the generated CPL, only alphanumeric, underscore, and dash characters can be used to define an action object name.

Event Log, E-mail, and SNMP

You can customize the event log, E-mail notification, and SNMP with triggers. These triggers are the same for all three object types.

Customize an Event Log, E-mail, or SNMP Object:

1. Right-click the Tracking cell in a policy layer and select Set; the Set Track Object dialog appears.

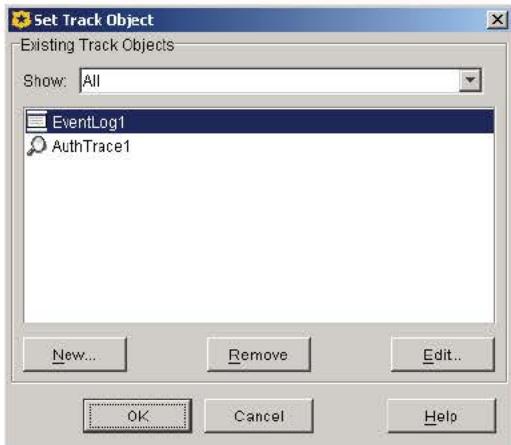


Figure 13-40: Add Track Object Dialog

2. Click New and select Event Log, Email, or SNMP; the appropriate add object dialog appears.
3. In the Name field, enter a name for this object or leave as is to accept the default.

Note: The E-mail object also contains a Subject field.

4. In the Message Text field, enter a customized message that appears with each entry.
5. Optional: In the Substitution Variables field, select a variable and click Insert. Repeat as required.

Section C: Detailed Object Column Reference

The substitution variables instruct the ProxySG to append specific information to the tracking object. The variables are categorized alphabetically, according to prefix.

Note: Some variables do not have prefixes.

Tracing Objects

This object specifies rule and Web traffic tracing.

Click Trace Level and select one of the following trace options:

- No Tracing—The default.
- Request Tracing—Generates trace output for the current request. The trace output contains request parameters (such as URL and client address), the final values of property settings, and descriptions of all actions taken.
- Rule and Request—Generates trace output that displays each rule that was executed
- Verbose Tracing—Generates the same output as Rule and Request, but also lists which rules were skipped because one or more of their conditions were false, and displays the specific condition in the rule that was false.

A trace destination can also be entered that specifies the destination for any trace produced by the current transaction. To specify a destination path, select Trace File and enter a path in the field. For example, abc.html.

If a trace destination is configured in multiple layers, the actual trace destination value displayed is the one specified in the last layer that had a rule evaluated (which has a destination property configured). Consider the following multiple Web Access Layer example, demonstrated by the generated CPL:

```
; ; Tab: [Web Access Layer (1)]
<Proxy>
    Deny trace.request(yes) trace.rules(no)trace.destination("abc.html"); Rule 1

; ; Tab: [Web Access Layer (2)]
<Proxy>
    Deny trace.request(yes) trace.rules(all) trace.destination("xyz.html"); Rule 1

; ; Tab: [Web Access Layer (3)]
<Proxy> Deny trace.request(yes) trace.rules(yes); Rule 1

; ; Tab: [Web Access Layer (4)]
<Proxy>
    Deny trace.request(yes) trace.rules(no) ; Rule 1
```

The resulting actions are:

- deny—from layer 4 rule 1
- trace.request(yes)—from layer 4 rule 1
- trace.rules(no)—from layer 4 rule 1

Section C: Detailed Object Column Reference

- `trace.destination("xyz.html")`—from layer 2 rule 1

The Trace File option can be used in conjunction with the Trace Level option or separately.

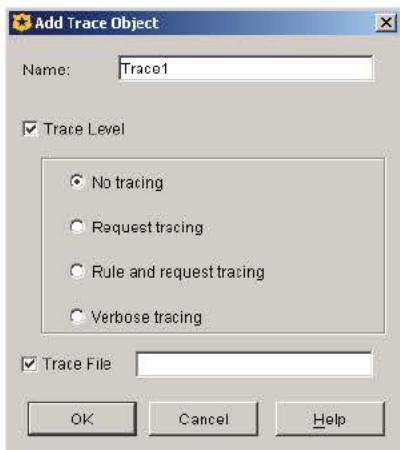


Figure 13-41: Creating a Trace Object

The default path of the trace file is accessible through one of the following URLs.

If the Management Console secure mode is enabled (the default on a new or upgraded system):

`https://SGOS_IP:8082/Policy/Trace/default_trace.html`

If the Management Console is operating in non-secure mode:

`http://SGOS_IP:8081/Policy/Trace/default_trace.html`

Combined Track Object

Allows you to combine track objects into one. See "Using Combined Objects"

Track Objects/Policy Layer Matrix

The following matrix lists all of the Track and column objects and indicates which policy layer they apply to.

Object	Admin Auth	Admin Access	DNS Access	SOCKS Auth	Web Auth	Web Access	Web Content	Forwarding
Event Log		x	x			x	x	
Email Log		x	x			x	x	
SNMP Objects		x	x			x	x	
Trace	x	x	x	x	x	x	x	x
Combined Objects		x	x			x	x	

Section C: Detailed Object Column Reference

Comment Object Reference

The Comment object allows you to write any text to aid in labeling the policy layer. The text in this field does not impact the performance of the rule.

Using Combined Objects

As previously discussed, you select one object for as many object types as required for a given rule. Most object types also have the option of using a combined object. This feature allows you to select multiple objects for a given type, thus creating more complex tools. There are two uses for combined conditions: lists and multiple object types. Also consider the Negate option, which exempts the objects in the list.

Example One

Consider the following example. You want a Web Content policy layer that as an action forces authorization *and* sends the response to an ICAP service for content scanning.



Figure 13-42: Set Action Object dialog

1. In the Set Action Object dialog, select New>Combined Action Object.

Section C: Detailed Object Column Reference

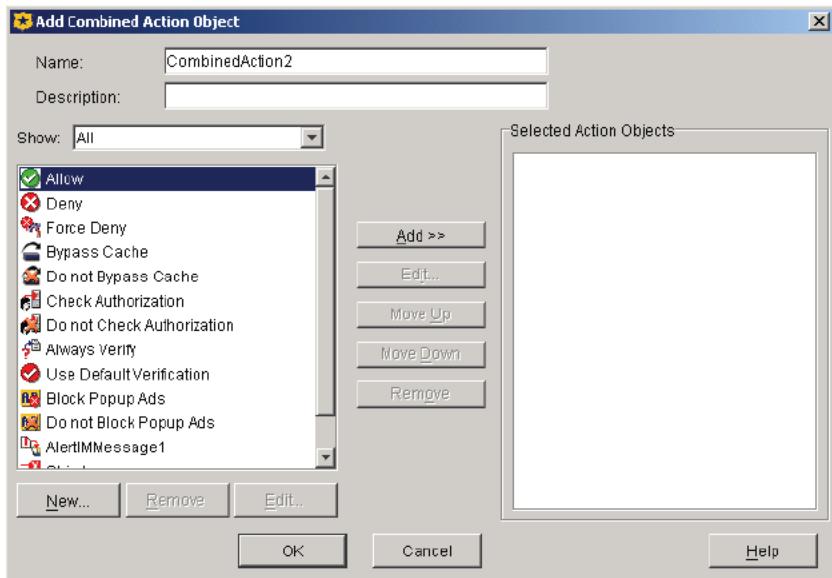


Figure 13-43: Add Combined Object Dialog

2. Select Check Authorization; click Add.
3. Select an existing ICAP service object. For this example, the object is named ICAPReqServ1. Click Add.

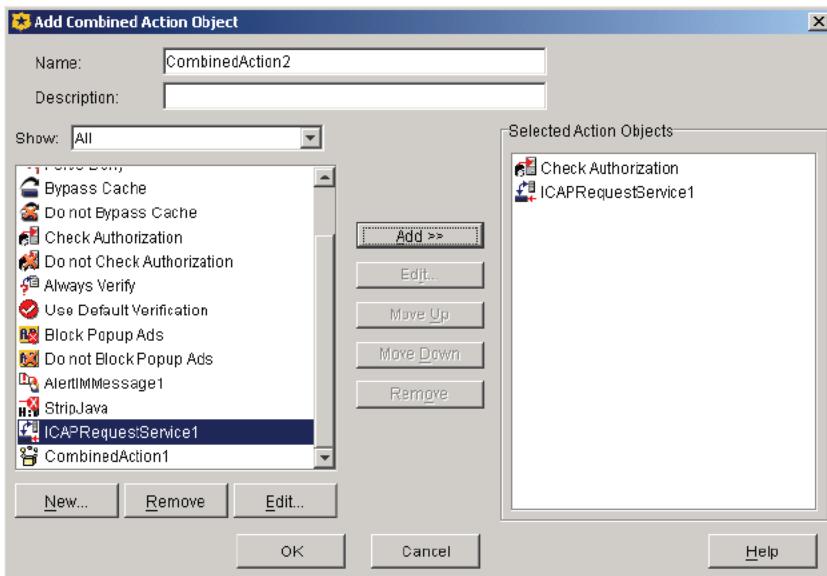


Figure 13-44: Creating a Combined Object

4. Click OK. The CombinedAction1 object appears as a separate, selectable object.

Section C: Detailed Object Column Reference

5. Select CombinedAction1; click OK. The object is now part of the rule.

Based on the other parameters specified in the rule, all requests are forced to an upstream server for authorization and the Web responses are subject to content scanning through the ICAP service.

Example Two

In the following example, the rule searches for one of the IP Address/Subnet objects and one of the streaming client user agents.

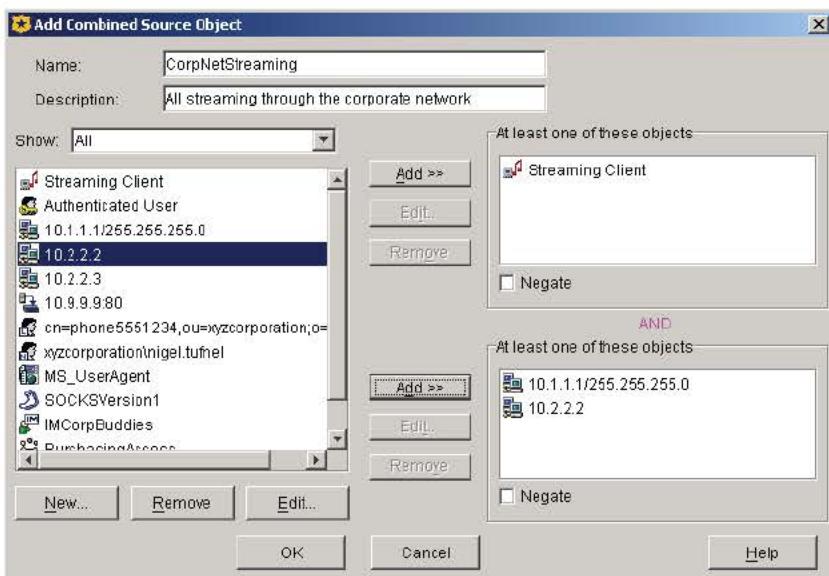


Figure 13-45: Combined Object with Multiple Object Types

Creating Categories

The Web Access, Web Content, and Forwarding policy layer Destination objects contain the Category object. This section describes how to create the content filter categories.

To Create a Category:

1. In VPM, select Configuration>Edit Categories.

The Edit Categories dialog appears.

Section C: Detailed Object Column Reference

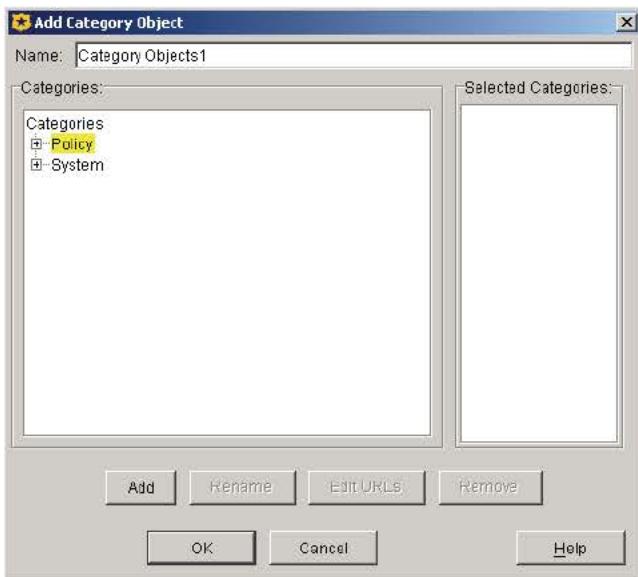


Figure 13-46: Edit Categories Dialog

2. Click Policy; click Add.
3. Drop the Policy list and select NewCategory1; click Edit. The Edit Locally Defined Category Object dialog appears.
4. Enter URLs appropriate for the content filter category you are creating; click OK.
5. Click Rename; in the dialog, enter a name for the object; click OK.
6. Click OK.

Note: If one or more other administrators have access to the ProxySG through other workstations and are creating categories either through VPM or with inline commands, consider that newly-created or edited categories are not synchronized until the policy is installed. When the policy is installed with VPM, the categories are refreshed. If too many categories are created at the same time and confusion occurs, select the File>Revert to Existing Policy on ProxySG Appliance option to restore the policy to the previous state and reconfigure categories.

Refreshing Policy

In between occurrences when either VPM is closed and reopened or Install Policies is invoked, VPM does not recognize changes to VPM-managed policy that were made on the ProxySG through another method. For example:

- Another administrator opens a separate VPM to make changes.
- Another administrator edits the local or central policy file through the serial console.
- Another administrator makes edits the local or central policy file through the Management Console.

Section C: Detailed Object Column Reference

- A new content filter database is downloaded automatically and the new update contains category changes.
- A new content filter database is downloaded manually by an administrator through the CLI or the Management Console.

Restricting DNS Lookups

This section discusses DNS lookup restrictions and describes how to create a list.

About DNS Lookup Restriction

The DNS lookup restriction list is a list of domain names that apply globally, regardless of policy layer definitions. Once a domain name is added to the list, DNS lookup requests do not occur for that domain name while policy is evaluated. For more detailed information about using DNS lookups, refer to the *Blue Coat Content Policy Language Guide*.

Creating the DNS Lookup Restriction List

The list is created from the VPM Menu bar.

To Create the DNS Lookup Restriction List:

1. Select Configuration>Set DNS Lookup Restrictions; the Set DNS lookup restrictions dialog appears.
The default is None; no domain names are restricted.
2. To restrict every domain name, select All.
3. To add specific domain names, perform the following steps.
 - a. Select Listed Host Patterns.
This enables the Host Patterns field.
 - b. Click Add; the Add Host Pattern dialog appears.
 - c. Enter a domain name; click OK.
 - d. Repeat to add other domain names.
 - e. Click OK.

Section C: Detailed Object Column Reference

Restricting Reverse DNS Lookups

This section discusses reverse DNS lookup restrictions and describes how to create a list.

About Reverse DNS Lookup Restriction

The Reverse DNS lookup restriction list is a list of subnets that apply globally, regardless of policy layer definitions. Once a subnet is added to the list, the ProxySG will not perform a reverse lookup of addresses on that subnet during policy evaluation. For more detailed information about using reverse DNS lookups, refer to the *Blue Coat Content Policy Language Guide*.

Creating the Reverse DNS Lookup Restriction List

The list is created from the VPM Menu bar. This prevents the ProxySG from performing reverse DNS lookups of addresses in the list while evaluating policy.

To Create the Reverse DNS Lookup Restriction List:

1. Select Configuration>Set Reverse DNS Lookup Restrictions; the Set Reverse DNS lookup restrictions dialog appears.
The default is None; no subnets are restricted.
2. To restrict every subnet, select All.
3. To add specific subnets, perform the following steps.
 - a. Select Listed Subnets.
This enables the Subnets field.
 - b. Click Add; the Add Subnet dialog appears.
 - c. Enter a subnet; click OK.
 - d. Repeat to add other subnets.
 - e. Click OK.

Setting the Group Log Order

This section discusses the group log order and describes how to create a list.

About the Group Log Order

The Group Log Order object allows you to establish the order group data appears in the access logs. For more detailed information about using group log ordering, refer to the *Blue Coat Content Policy Language Guide*.

Creating the Group Log Order List

The list is created from the VPM Menu bar.

Section C: Detailed Object Column Reference

To Create the Group Log Order List:

1. Select Configuration>Set Group Log Order; the Set Group Log Order dialog appears.
2. Click Add; the Add Group Object dialog appears.
3. In the Group Name field, enter the name of a group.
The group must be already configured on the ProxySG.
4. From the Authentication Realm drop-down list, select a realm.
5. Click OK.
6. Repeat as required to add more groups.
7. To order the list, select a group and click Move Up or Move Down until you achieve the desired order.
8. Click OK.

Section D: Managing Policy Layers and Files

Section D: Managing Policy Layers and Files

This section contains the following topics:

- "How Policy Layers, Rules, and Files Interact" on page 452—Describes the importance of rule order policy layer order.
- "Managing Policy Files" on page 455—Describes how to save and install policies on the ProxySG.
- "Installing VPM-Created Policy Files" on page 456—Describes how to propagate a policy file created on one ProxySG to another.
- "Viewing the Policy/Created CPL" on page 459—Describes how to view the underlying CPL that is created with VPM.

Section D: Managing Policy Layers and Files

How Policy Layers, Rules, and Files Interact

The following critical points discuss the behaviors and priorities of policy rules, layers, and files:

- Rules in different policy layers of the same type work together, and the order of policy layers is important.
- The order of policy layers of different types is important.
- The order of rules in a policy layer is important.
- Policy created in VPM is saved in a file on the ProxySG; the state of the VPM user interface is also stored as an XML file on the ProxySG.

Note: These files are stored *only* if the policy is installed without any errors.

- How the appliance evaluates those rules in relation to policy layers that exist in the central and local policy files is important. For more information, see Chapter 12: "Managing Policy Files".

How VPM Layers Relate to CPL Layers

VPM generates CPL in various layers, but the concept of layers presented in VPM is slightly different. VPM provides policy layers for special purposes. For example, Web Authentication and Web Authorization, which both generate CPL <Proxy> layers. This minimizes timing conflicts by restricting the choices of triggers and properties to those compatible timing requirements. The following table summarizes how to use VPM layers and which CPL layers result.

Table 13.2: VPM-Generated CPL Layers

Policy Purpose	VPM Layer	CPL Layer
Establish Administrator identities.	Admin Authentication	<Admin>
Control Administrator access.	Admin Authorization	<Admin>
Control DNS access.	DNS Access	<Proxy>
Establish SOCKS user identities.	SOCKS Authentication	<Proxy>
Establish user identities.	Web Authentication	<Proxy>
Control user access.	Web Access	<Proxy>
Control content independent of users.	Web Content	<Cache>
Control forwarding.	Forwarding	<Forward>

Note: VPM currently does not support the <Exception> layer.

Ordering Rules in a Policy Layer

The ProxySG evaluates the rules in the order in which they are listed in a policy layer. When it finds a rule that applies to the situation, it skips the remaining rules in the policy layer and goes on to the next policy layer.

Section D: Managing Policy Layers and Files

Consider the following simple example. Assume that a company has a policy that prohibits everyone from accessing the Web. This is a policy that is easy to create with a Web Access layer rule. Using source objects such as groups or subnets, you can create rules that deny access to any destination.

There are, however, likely to be exceptions to such a broad policy. For example, you want the manager of the purchasing department to be able to access the Web sites of suppliers. Members of the sales department need to access their customer Web sites. Creating Web Access rules for both these situations is also simple. But if you put all these rules in a single policy layer, then the rule prohibiting access to everyone must be ordered last, or the other two rules will not be applied.

The principle design of rules within policy layers is:
Always go from the specific to the general.

Using Policy Layers of the Same Type

Because the ProxySG skips the remaining rules in a policy layer as soon as it finds one that meets the condition, multiple policy layers and a combination of rules might be required to accomplish a task.

Consider the following example. A company does not want to prohibit its employees from accessing the Web, but it does not want them to abuse the privilege. To this end, the company wants employees who access the Web to authenticate when they do so; that is, enter a username and password. So the company creates a Web Authentication policy layer with a rule that says: "If anyone from anywhere in the company sends a request to a URL on the Web, authenticate the client before granting access."

The company also allows members of the group Sales to access various sports Web sites only during non-work hours. Given the Web Authentication rule above, these people must authenticate when they do this. But the company feels that it is not important for people going to these sites after hours to authenticate. So the company creates the following Web Access policy-layer rule:

- Grant Sales personnel access to sports Web sites from 5:00 PM to midnight.

But there are additional issues. Some members of the sales department spend a lot of time watching game highlights on video clips, and this takes up a lot of bandwidth. At the same time, a lot of customers access the company Web site in the evening (during non-work hours), so internal bandwidth should remain manageable. The company, therefore, limits the bandwidth available to the people in the Sales department with a Web Access layer rule that is identical to the one above in all respects except for the action:

- Grant Sales personnel access to sports Web sites from 5:00 PM to midnight, but limit the maximum streaming bitrate to 300 kilobits per second.

For both these rules to work, they need to be in separate policy layers. If they were in the same policy layer, the rule listed second would never be applied.

Section D: Managing Policy Layers and Files

Ordering Policy Layers

The order of policy layers is also important. The ProxySG evaluates policy layers in the order in which they are listed in VPM. When the ProxySG is going through policy layers, it does not execute a given rule as soon as it finds that it meets the specific situation. Rather, it compiles a list of all the rules that meet the condition; when it has gone through all the policy layers, it evaluates the list, resolves any apparent conflicts, and then executes the required actions. If there is a conflict between rules in different policy layers, the policy layer evaluated last takes precedence.

The principle design of policy layers is: Always go from the general to the specific; that is, establish a general rule in an early policy layer, and then write exception rules in later policy layers.

In the above example, there are two Web Access policy layers: one contains a rule stating that Sales personnel can access certain Web sites without authenticating, and the other states that when they do access these Web sites, limit the available bandwidth. The order of these policy layers is irrelevant. The order is irrelevant because there is no conflict between the rules in the layers.

The following is an example in which the order of policy layers does matter. Assume all URL requests from members of the purchasing department are directed to a single proxy server. To discourage employees from surfing the Web excessively during business hours, a company creates a Web Authentication Policy rule that says: "Whenever a client request comes in to the proxy server, prompt the client to authenticate."

Members of the purchasing department, however, need to access specific Web sites for business reasons, and the company does not want to require authentication every time they do this. So they create a Web Access policy rule that says: "If any member of the purchasing department sends a request to a specific URL contained in a combined-object list, allow access."

The policy layer with the first rule needs to come first in evaluation order; it is then overridden by the second rule in a subsequent policy layer.

Section D: Managing Policy Layers and Files

Managing Policy Files

This section describes how to use VPM to work with policy language rules.

Installing Policies

As you add policy layers and rules, your work is saved in a file on the ProxySG. However, policies only take effect when you install the policies. The ProxySG then compiles the policies into CPL format and saves the resulting policies in the `vpm.cpl` file. This overwrites any policies previously created using VPM. The appliance saves VPM-generated policies in a single file and loads it all at once. You do not need to load policies separately, as is the case with the local or central policy files.

To Use VPM to Install Policies:

- Select File>Install Policies, or
- Click **Install Policies** on the Rule bar.

If there is an error, VPM displays an error message and does not load the policy file. For information about error messages, see the *Blue Coat Content Policy Language Guide*. Correct the error, and then reload the file.

Notes:

The Category object and the DNS Lookup Restrictions, Reverse DNS Lookup Restrictions, and Group Log Order configuration objects generate CPL, regardless if they are or are not included in rules. These specific objects and features allow users to edit categories and lists that might or might not be used in current policies.

Refreshing Policy

In between occurrences when either VPM is closed and reopened or Install Policies is invoked, VPM does not recognize changes to VPM-managed policy that were made on the ProxySG through another method. For example:

- Another administrator opens a separate VPM to make changes.
- Another administrator edits the local or central policy file through the serial console.
- Another administrator makes edits the local or central policy file through the Management Console.
- A new content filter database is downloaded automatically and the new update contains category changes.
- A new content filter database is downloaded manually by an administrator through the CLI or the Management Console.

Reverting to a Previous Policy

If after creating new policies or editing an existing policy you decide to abandon the process and continue with the existing policy installed on the ProxySG, you can revert to that version. All current changes are deleted (VPM provides a verification prompt).

Section D: Managing Policy Layers and Files

To Revert to an Existing Installed Policy:

Select File>Revert to Existing Policy on ProxySG Appliance.

Changing Policies

You can change, edit, delete, add to, and otherwise manage policies created in VPM at any time by returning to VPM and working with policy layers and rules just as you did when creating them.

Disabling and Enabling Policy Rule

Occasionally, you may need to temporarily disable rules in a policy layer; for example, when troubleshooting compiles errors and warnings. This might help confirm that the ProxySG can successfully compile the remaining policy. After disabling a rule, you can edit the objects and re-enable the rule.

To Disable or Enable A Rule:

1. Click the appropriate policy layer tab.
2. Right-click in the No. column.
3. Click Disable Rule on the shortcut menu. The policy editor changes the rule text color to red. See the figure below.
4. To enable the rule, repeat steps 3 and 4. After you enable a disabled rule, the policy editor changes the rule text color to black.

Deleting a Policy Layer

To Delete a Policy Layer:

1. Right-click the tab of the policy layer to be deleted.
2. Select Delete Policy from the drop-down list.

You can also right-click the policy layer tab and select Edit>Delete Layer.

Installing VPM-Created Policy Files

Policies created with VPM are saved on the specific ProxySG on which they are created. SGOS automatically creates the following files when saving VPM-created policies:

```
config_policy_source.xml  
config_policy_source.txt
```

You can install VPM policies that were created on another ProxySG. This requires the following steps:

1. Copy the two VPM files that will be shared from the ProxySG on which they reside to a Web server.
2. Use the Management Console or CLI to load VPM files on another ProxySG.

Section D: Managing Policy Layers and Files

To Copy VPM Files from a ProxySG to a Web server:

1. Select Statistics>Advanced.
2. Scroll down and click Policy.

The page jumps down to the Policy files links.

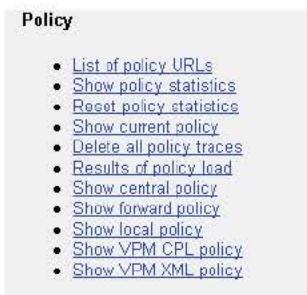


Figure 13-47: Policy Files in Custom URLs

3. Right-click the Show VPM CPL policy link.
4. In the Save As dialog, enter the full path to a directory on the Web server before the file name and click OK.

Important: The Save As dialog offers the appropriate default file name (`config_policy_source.xml` or `config_policy_source.txt`). You can change the names, including the extension. This can be helpful if an enterprise is using various sets of shared VPM files. You could rename files to indicate the ProxySG on which they were created, for example, or for a department that has a set of VPM-specific policies, used perhaps in multiple locations (`sales_vpm.cpl` and `sales_vpm.xml`).

5. Repeat the previous step for the second VPM file.

To Load VPM Files to a ProxySG through the Management Console:

1. Select Configuration>Policy>Policy Files>Visual Policy Files.

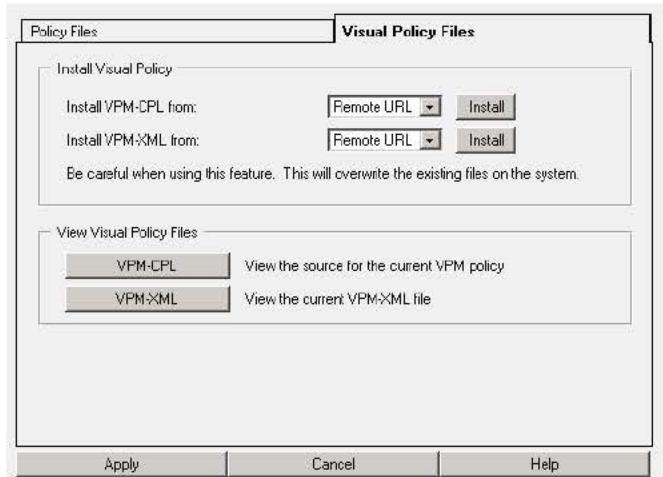
Section D: Managing Policy Layers and Files

Figure 13-48: Visual Policy Files Tab

2. In the VPM-CPL file field, type the URL to the first VPM file copied to the Web server (this is the file with the default .txt extension) and click **Install**.
3. In the VPM-XML file field, type the URL to the second VPM file copied to the Web server (this is the file with the default .xml extension) and click **Install**.
4. Click **Apply**.

Notes

- If VPM files already exist on the ProxySG, the URLs to those files display in the two file fields. To replace them, delete the URLs and type new ones. Installing new files overwrites any that are already present.
- To review VPM-generated policies before installing them, enter the URL to the CPL file on the Web server and click **View**.
- Regardless of whether you are installing new VPM files, you can review the CPL or XML files of the policies currently on the ProxySG. Click **VPM-CPL** and **VPM-XML** in the **View Visual Policy Files** box at the bottom of the dialog.
- Never edit either of the VPM files directly. Change the files only by working with the policies in VPM and saving changes there.

To Load VPM Files to a ProxySG through the CLI:

The two commands in the first step load one of the VPM policy files; the commands in the second step load the other policy file. In each case, *url* is the complete path, including file name, to the appropriate file on the Web server.

1. At the **config** command prompt, enter the following commands:

```
SGOS#(config) policy vpm-cpl-path url
SGOS#(config) load policy vpm-cpl
```

Section D: Managing Policy Layers and Files

2. At the config command prompt, enter the following commands:

```
SGOS# (config) policy vpm-xml-path url  
SGOS# (config) load policy vpm-xml
```

Viewing the Policy/Created CPL

View the CPL generated by installing VPM-created policy from VPM or the Management Console.

To View the Generated CPL through VPM:

Select View>Generated CPL.

To View the VPM Policy File:

Select View>Current ProxySG Appliance VPM Policy Files.

Important: Do *not* edit or alter VPM-generated files by opening the VPM policy file and working in the generated CPL. To edit, change, or add to VPM policies, edit the policy layers and re-install the policy.

Section E: Tutorials

Section E: Tutorials

This section contains the following topics:

- "Tutorial—Creating a Web Authentication Policy" on page 461
- "Tutorial—Creating a Web Access Policy" on page 465

Section E: Tutorials

Tutorial—Creating a Web Authentication Policy

This section is a tutorial that demonstrates how to create policies and rules for Web authentication.

Use Web Authentication policies to specify whether the individual making a request is prompted to authenticate by entering a username and password. In this example, a company uses a PAC file to configure most employee browsers to connect to a specific IP address on the ProxySG. It wants these users to authenticate when their browsers send a request to the proxy.

Create a Policy Layer

1. Start VPM from the Management Console, Configuration>Policy>Visual Policy Manager.
2. Select Policy>Add Web Authentication Layer.

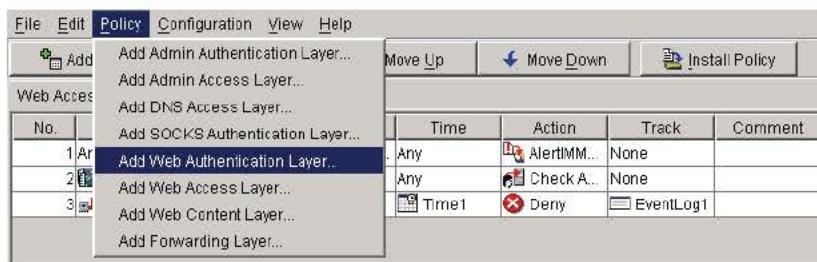


Figure 13-49: Creating a Policy Layer

3. A dialog displays offering a default name for the layer, consisting of the layer type and a number. Rename the layer or accept the default and click OK.



Figure 13-50: Add New Policy Table Dialog

4. VPM creates the new layer tab and adds a blank rule.

Example 1: Create an Authentication Rule

1. By default, the unmodified rule applies to everyone whose browsers connect to a specific IP address.

Web Access Layer (1) [Web Authentication Layer (1)]					
No.	Source	Destination	Action	Track	Comment
1	Any	Any	None	None	

Figure 13-51: Creating a Web Authentication Rule

2. Right-click the Source cell to drop the menu.
3. Select Set to open the Set Source Object dialog.

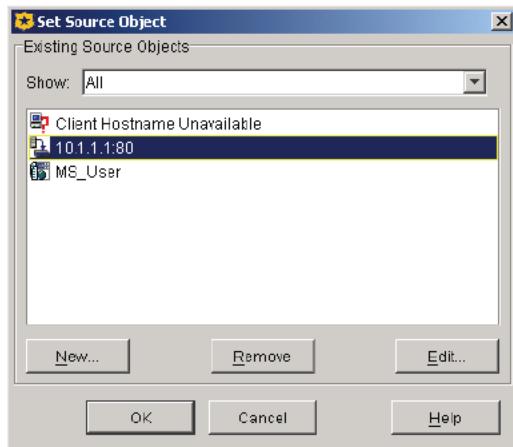
Section E: Tutorials

Figure 13-52: Selecting an IP Address Source Object

4. Select a proxy IP address or port; if necessary, click New to create a new one. This example selects IP address on the ProxySG where the PAC file sends most employee browsers.
5. Click OK to enter the IP address in the Source cell.

Web Access Layer (1) Web Authentication Layer (1)					
No.	Source	Destination	Action	Track	Comment
1	10.1.1.1:80	Any	None	None	

Figure 13-53: Completed Source Object

6. Create an authentication Action object. Right-click the Action cell to drop the menu and select Set; the Set Action Object dialog displays.
7. The only objects available are the pre-existing static objects, so you must create a new Authenticate object. Click New and select Authenticate.

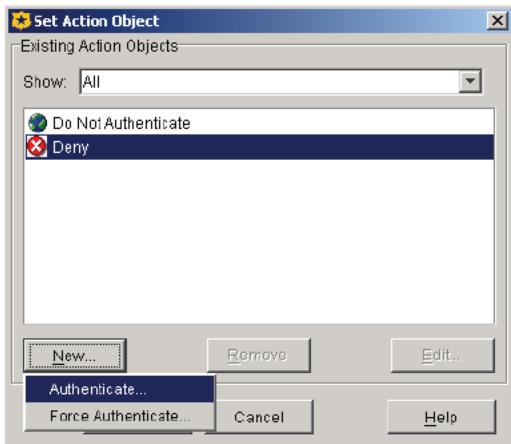


Figure 13-54: Selecting Authenticate

Section E: Tutorials

8. The Add Authenticate Object window displays. Note the following:
 - ❑ Name—Every configurable object has a name. The default name Authenticate1; change to Authenticate_XYZ_Corp, which is how it will be listed in the Add Object window.
 - ❑ Realm—Specifies the realm to be authenticated against from the drop-down list.
 - ❑ Mode—Specifies the authentication realm mode.



Figure 13-55: Specifying the Authentication Realm

9. Click OK to close the Add Action Object window, with the new Authenticate object in the list.

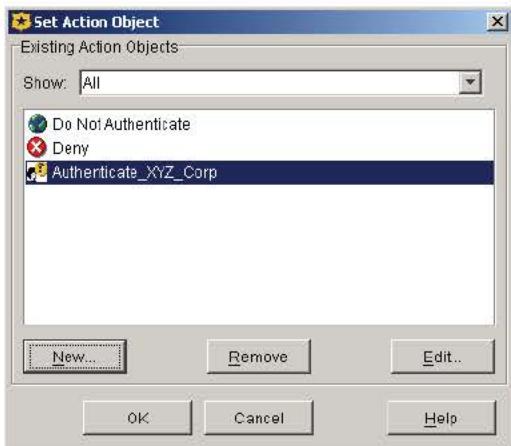


Figure 13-56: New Authentication Action Object

10. Click OK.

Web Authentication Layer (1)		Web ContentLayer (1)		Forwarding Layer (1)		Web Access Layer (2)	
No.	Source	Destination	Action	Track	Comment		
1	Any	Any	Authenticate_X... Authenticate_XYZ_Corp	None			

Figure 13-57: Completed Action Object

11. Create a Trace object to log all authentication activity. Right-click the Track cell to drop the menu and select Set; the Set Track Object dialog appears.

Section E: Tutorials

12. You must create a new Trace object. Click New and select Trace; the Add Trace Object appears.
13. In the Name field, enter AuthTrace.
14. Name the object AuthTrace1. Click Trace Level and Verbose to enable verbose tracing, which lists the rules that were skipped because one or more of their conditions were false and displays the specific condition in the rule that was false.



Figure 13-58: Creating a Trace Object

15. Click OK; click OK again to add the object. The rule is complete.

Web Access Layer (1) Web Authentication Layer (1)					
No.	Source	Destination	Action	Track	Comment
1	10.1.1.1:80	Any	Authenticate_X...	AuthTrace	

Figure 13-59: Completed Rule

Example 2: Exempt Specific Users from Authentication

Certain individuals and groups are exempt from the above restriction. Individuals in the purchasing department are allowed to the Web so they can order online from supplier Web sites. And the company does not want them to authenticate.

1. To create a new rule, click Add Rule.

Web Access Layer (1) Web Authentication Layer (1)					
No.	Source	Destination	Action	Track	Comment
1	10.1.1.1:80	Any	Authenticate_X...	AuthTrace	
2	Any	Any	None	None	

Figure 13-60: Adding a Second Web Authentication Policy Layer Rule

2. People in the purchasing group use the same PAC file and thus their browsers are directed to the same IP address. A Combined Source Object is needed that includes the purchasing group, who are their own subnet.

Section E: Tutorials

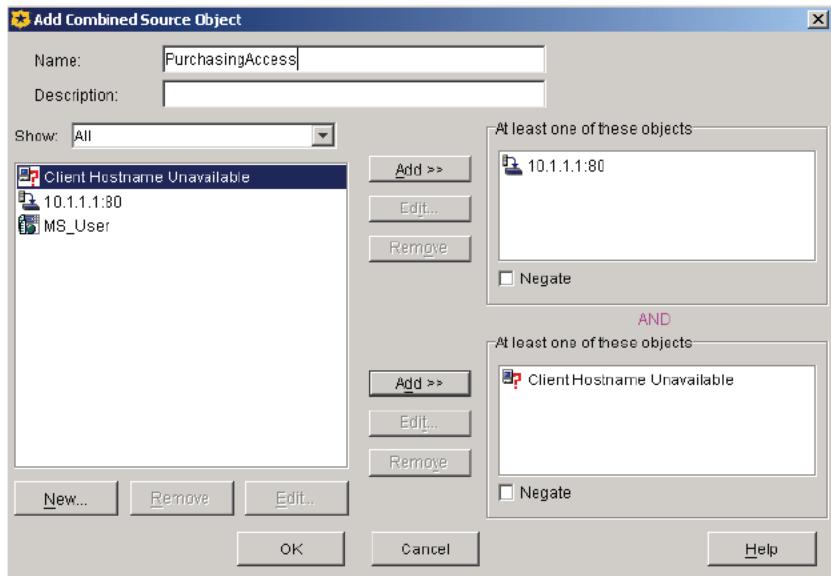


Figure 13-61: A Combined Object

The new rule in the policy layer accepts the default Action Object to not authenticate and does not require a Trace Object.

Web Access Layer (1) Web Authentication Layer (1)					
No.	Source	Destination	Action	Track	Comment
1	10.1.1.1:80	Any	Authenticate_X...	AuthTrace	
2	PurchasingAcc...	Any	None	None	

Figure 13-62: Updated Second Rule

However, a problem exists. The second rule cannot be evaluated because the first rule affects everyone who goes through the proxy. The rules need to be reversed.

3. Select the second rule and click Move Up to reorder the rules.

Web Access Layer (1) Web Authentication Layer (1)					
No.	Source	Destination	Action	Track	Comment
1	PurchasingAcc...	Any	None	None	
2	10.1.1.1:80	Any	Authenticate_X...	AuthTrace	

Figure 13-63: Reordered Rules

Tutorial—Creating a Web Access Policy

This section is a tutorial that demonstrates how to create policies and rules for Web access.

Use ProxySG policies to define end-user access to Web resources. For more information about Web access policies, see Chapter 17: "Content Filtering". This section provides examples.

Section E: Tutorials

Example 1: Restrict Specific Websites From Access

This example demonstrates a simple rule that denies everyone access to job searching Web sites. This rule requires you to configure only one rule option; it uses the defaults for all other options.

1. Start the policy editor and select Policy>Add Web Access Layer. VPM displays a tab with the name of the new policy; beneath that is a new rule-specific row. Notice that the default Action is Deny.

Web Access Layer (1) Web Authentication Layer (1)							
No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	Any	Any	Any	None	None	

Figure 13-64: Creating a New Policy Layer

2. Right-click Destination and select Set; the Set Destination Object dialog appears.

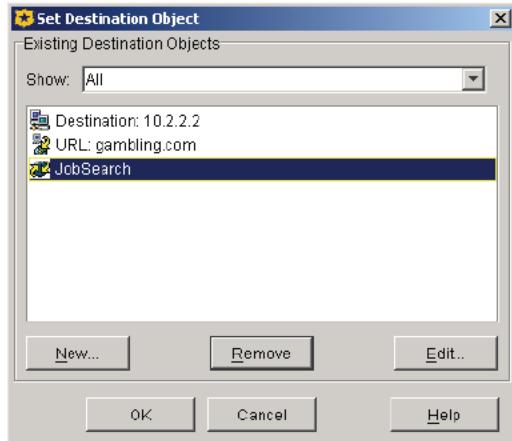


Figure 13-65: Set Destination Dialog

3. Click New; select URL. The Add URL Object dialog appears.

Section E: Tutorials

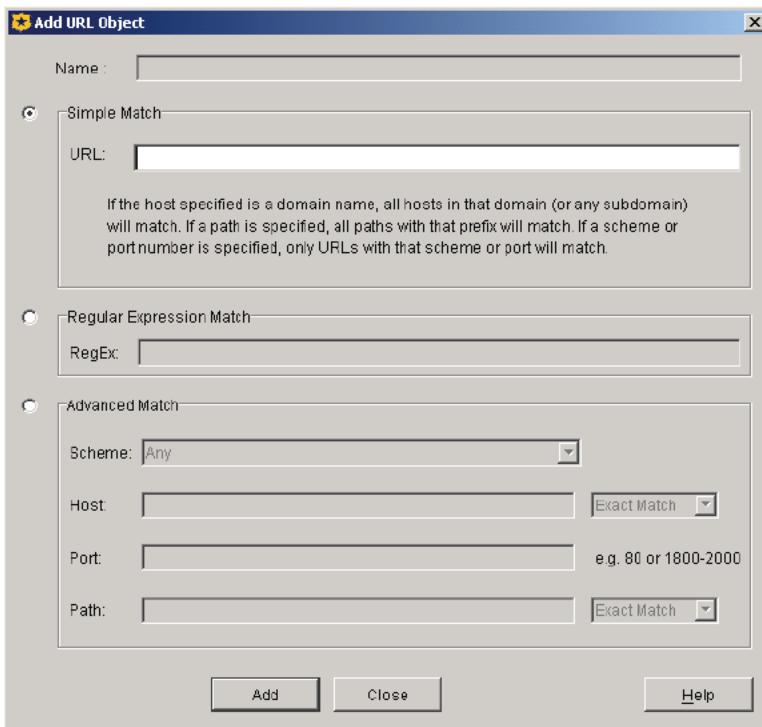


Figure 13-66: Add URL Object Dialog

4. Click Simple Match; in the URL field, enter hotjobs.com and click Add.
5. Repeat Step 4 twice, entering bajobs.com and monster.com.
6. Click Close; the entered URLs appear as selectable items.

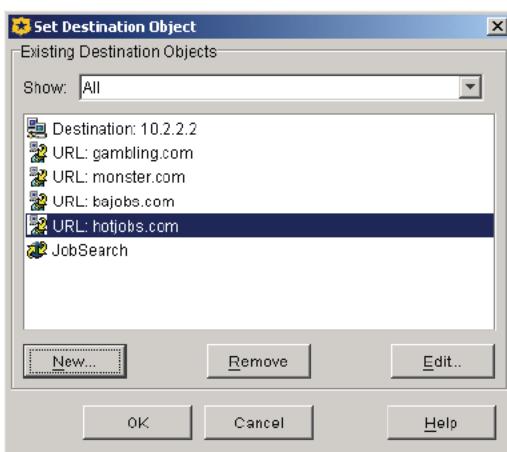


Figure 13-67: New URLs

7. Click New and select Combined Destination Object; the Add Combined Destination Object dialog appears.

Section E: Tutorials

8. Name the object JobSearchURLs. Select each newly added URL and click the first Add button.

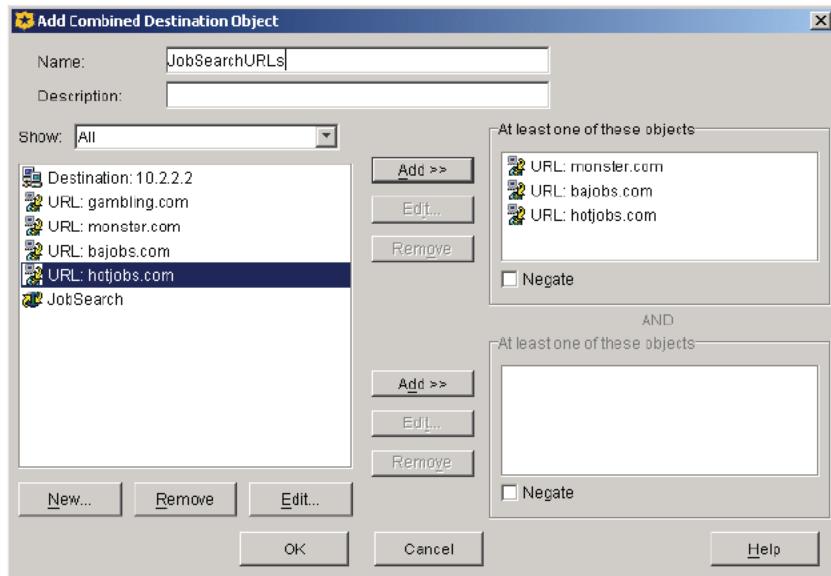


Figure 13-68: Creating a Combined Destination Object with URLs

9. Click OK; with the JobSearchURLs object highlighted, click OK. The object is now part of the rule.

Web Access Layer (2) Web Authentication Layer (1) Web Access Layer (1)							
No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	JobSearchU...	Any	Any	Deny	None	

Figure 13-69: Completed Rule

As the default Action is deny, the rule is complete. No one can access these Web sites.

10. To activate the rule, click Install Policies.

Example 2: Allow Specific Users to Access Specific Websites

The after-hours IT shift is comprised of part-time college interns who are on call to handle small problems, but are not involved in major projects. Therefore, you allow them to browse certain sports and entertainment Web sites when all is quiet; access is allowed from two workstations and you still want to track their browsing activity.

Configuring the Source Object

1. Add a new rule to the policy and position the pointer in the Source cell.

Section E: Tutorials

Web Access Layer (1) Web Authentication Layer (1)							
No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	JobSear...	Any	Any	None	None	
2	Any	Any	Any	Any	Deny	None	

Figure 13-70: Setting a Source Rule Option

2. Right-click the Source cell and select Set to display the Add Source Object dialog.
3. Click New and select Combined Source Object; the Add Combined Source Object appears.
4. Name the object IT_PM_Shift.
5. Under the selectable list of objects, click New and select Client IP Address/Subnet; the Add Client IP Address/Subnet Object dialog appears.
6. Enter the IP address of the first workstation and click Add; repeat for the second; click Close.
7. Select each IP address and click the first Add.

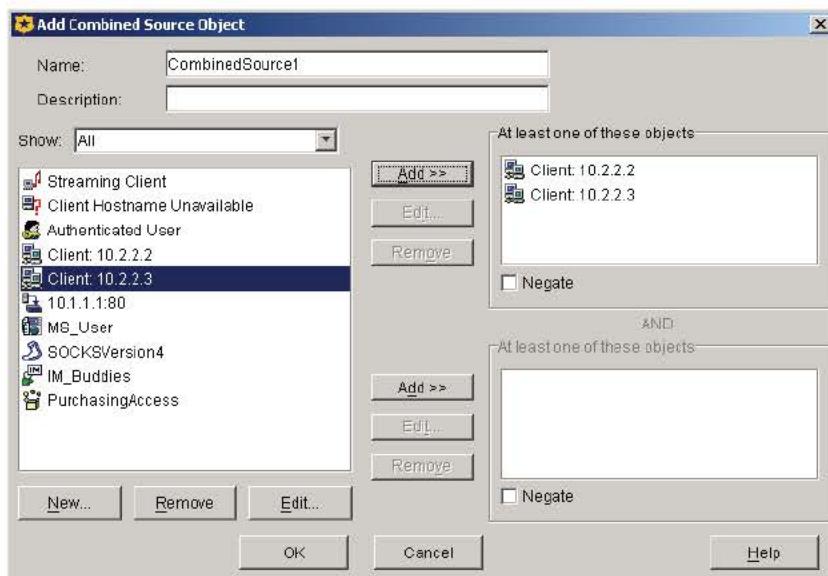


Figure 13-71: Combined IP Address Object

8. Click OK; click OK again to add the Source object to the rule.

Configuring the Destination Object

1. Right-click the Destination field and select Set; the Set Destination Object dialog appears.
2. Click New and select Category; the Add Category Object dialog appears.

Section E: Tutorials

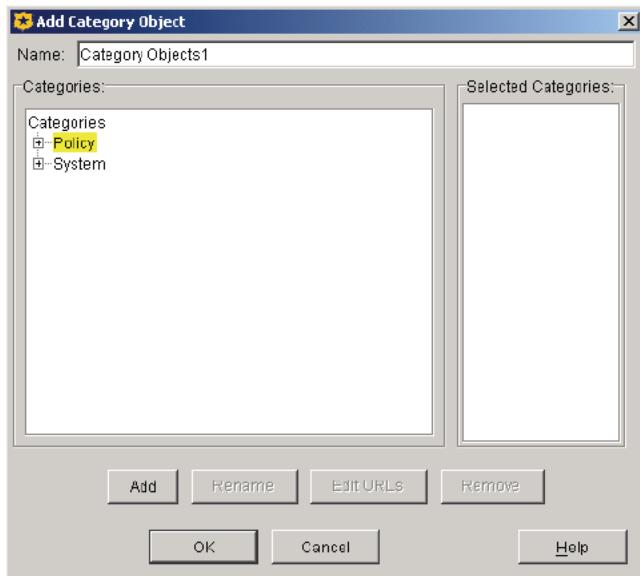


Figure 13-72: Category Dialog

3. Select Policy and click Add; the Enter Name for New Category dialog appears.
4. Name the object Sports URLs and click OK.
5. Select Sports URLs and click Edit URLs. The Edit Locally Defined Category Object dialog appears.
6. Enter the URLs for the allowable sports Web sites.

Section E: Tutorials

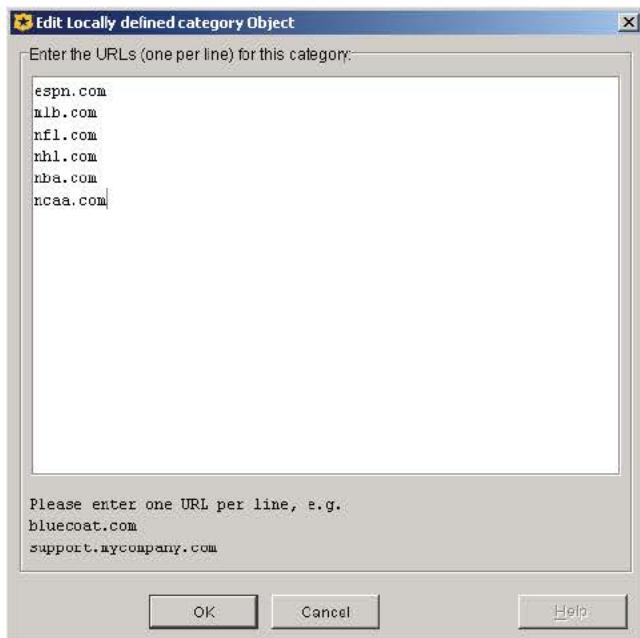


Figure 13-73: Sports URLs Category

7. Click OK; under Policy, select Sports URLs; click OK.
8. Repeat Steps 3 through 7, creating a category called Entertainment URLs with the URLs ew.com, rollingstone.com, and variety.com.
9. Create a Combined Object named Allowable PM IT Websites with the two Categories: Sports URLs and Entertainment URLs. Click OK twice to add the object to the rule.

Configuring the Time Object

This example allows the specified users to access the sports and entertainment Websites after business hours.

1. Right-click the Time field and select Set; the Set Time Object dialog appears.
2. Click New and select Time Object; the Add Time Object dialog appears.
3. Name the object After Hours.
4. Select Local Time. In the Specific Time of Day Restriction field, select Enable and set the time from 18:00 to 05:59.

This defines after hours as 6:00 PM to 6:00 AM.

5. In the Specific Weekday Restriction field, select Enable and select Monday, Tuesday, Wednesday, Thursday, and Friday.

This defines the days of the week to which this rule applies.

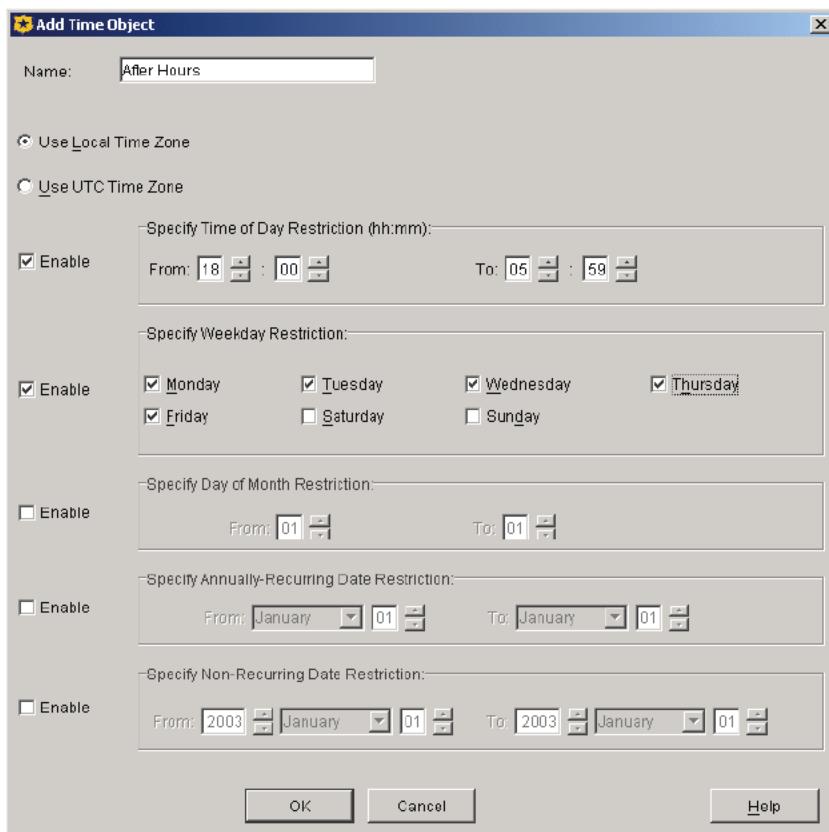
Section E: Tutorials

Figure 13-74: After Hours Time Object

- Click OK to add the Time Object to the rule.

Configuring the Action Option

- Right-click Action select Set; the Set Action Object dialog appears.
- Allow is a static object. Select Allow and click OK.

The rule is now complete.

Web Access Layer (1)		Web Authentication Layer (1)					
No.	Source	Destination	Service	Time	Action	Track	Comment
1	Any	JobSear...	Any	Any	None	None	
2	IT_PM_S...	Allowabl...	Any	After Hou...	Allow	None	

Figure 13-75: Completed Rule

Chapter 14: Advanced Policy

This chapter provides conceptual information about ProxySG advanced policy features. While many Blue Coat Systems features have a policy component, some features have no configuration component outside policy. Configuring advanced policy is done by defining rules in the Visual Policy Manager (VPM) or by composing Content Policy Language (CPL). While some examples are provided in this chapter, references to the relevant VPM chapter component are included in each section.

This chapter contains the following topics:

- "Blocking Pop-Up Windows"
- "Stripping or Replacing Active Content"
- "Modifying Headers"
- "Defining Exceptions"

Excluding exceptions, you *must* use policy to implement these capabilities. (For exceptions, you can create a list outside of policy to install on the system.)

Blocking Pop-Up Windows

The ProxySG allows you to block pop-up windows, which are usually in the form of unsolicited advertisements. Pop-up windows are blocked by inserting Javascript code into each HTML Web page. Every time the Web page tries to open a new window, the code attempts to determine if the window is a result of user click. The window is allowed to open if the ProxySG determines a user clicked a button or link; otherwise, the window does not open.

Limitations

Because of the dynamic nature of the Web, blocking pop-up windows is not a perfect solution. Keep in mind the following limitations before configuring this feature:

- Windows that contain desired or useful information cannot be distinguished from undesired content, such as advertisements.
- If the Web browser caches a page that spawns pop-up windows before the blocking policy was installed, pop-up ads continue to be served from that page regardless of current policy.
- Animated ads contained within Web pages are not blocked. Commonly seen in scrolling or drop-down form, these are not true pop-up windows but are contained within the page. Users who see these ads might believe that pop-up window blocking is not implemented.
- Pop-up windows that are delivered via HTTPS are not blocked.
- Although the Blue Coat request headers tell a Web server not to use compression, it is possible (though not likely) for a Web server to be configured to send compressed responses anyway. The pop-up blocking feature does not work on compressed HTML pages.

Recommendations

- To compensate for limiting factors, administrators and users can override pop-up blocking:
 - Administrators—Use VPM to create policy rules that exempt pop-up blocking for specific Web sites and IP address ranges. For example, Blue Coat recommends disabling pop-up blocking for your intranet, which commonly resides on a IP address range.
 - Users—When a pop-up window is blocked, a message is displayed in the status bar:
blocked popup window -- use CTRL Refresh to see all popups.
While pressing the Control key, click the Web browser Refresh button; the page is reloaded with pop-up blocking disabled for that action.
- Create a separate Web Access policy layer for pop-up blocking actions. This alleviates interference with Web applications deployed on your intranet that require pop-up windows.
- To prevent a cached Web page from spawning pop-up windows, clear the browser cache, then reload the page without holding down the CTRL key.

Blocking pop-up windows is accomplished through the Visual Policy Manager. See "Block/Do Not Block Pop-Up Ads" in Chapter 13: "The Visual Policy Manager" on page 377 for information about how to create blocking actions in a policy layers.

Stripping or Replacing Active Content

Scripts activated within Web pages can pose a security concern. The ProxySG policy can be configured to supplement standard virus scanning of Web content by detecting and removing the HTML tags that launch active content such as Java applets or scripts. In addition, the removed content can be replaced with predefined material, a process referred to as *active content transformation*.

When the ProxySG is configured to perform active content transformation, Web pages requested by a client are scanned before they are served and any specified tags and the content they define are either removed or replaced. Since the transformed content is not cached, the transformation process is based on a variety of conditions, including time of day, client identity, or URL.

Note: Pages served over an HTTPS tunneled connection are encrypted, so the content cannot be modified.

The following tags and related content can be removed or replaced:

- <APPLET>—Java applets, as defined by HTML <applet> elements.
- <EMBED>—Embedded multimedia objects displayed using Netscape Navigator plug-ins as defined by HTML <embed> elements.
- <OBJECT>—Embedded multimedia objects displayed using Internet Explorer Active-X controls and other multimedia elements, as defined by HTML <object> elements
- <SCRIPT>—Embedded Javascript and VBScript programs, whether these are represented as HTML <script> elements, Javascript entities, Javascript URLs, or event handler attributes. The <noscript> tag is *not* affected by this features.

Stripping active content is accomplished through the Visual Policy Manager or by composing CPL.

- See "Strip Active Content" in Chapter 13: "The Visual Policy Manager" on page 377 for information about how to create a strip active content object in a Web Access policy layer.
- Refer to the *Blue Coat Content Policy Language Guide*.

About Active Content Types

The following sections provide more detail about the types of active content that can be removed or replaced.

Script Tags

Scripts are generally placed between the start and end tags `<SCRIPT>` and `</SCRIPT>`. The type of script used is defined by the `LANGUAGE` attribute; for example, `<SCRIPT LANGUAGE="JavaScript 1.0">`). When the `LANGUAGE` attribute is undefined, the browser assumes JavaScript.

When `transform active_content` is configured to remove scripts, the basic operation is to remove all content between and including `<SCRIPT>` and `</SCRIPT>`, regardless of the language type, and substitute any defined replacement text. A notable exception occurs when a script is defined in the header portion of the HTML document (defined by the `<HEAD>` tag). In this case, the script is simply removed. This is because images, objects, and text are not allowed in the header of an HTML document. If the end script tag `</SCRIPT>` is missing from the document (the end of the document is defined as either up to the `</BODY>` or `</HTML>` tag, or the last character of the document), then all content from the start `<SCRIPT>` tag to the end of the document is removed.

JavaScript Entities

JavaScript entities have the following format: `&{javascript code}` and are found anywhere in the value part of an attribute (that is, `<IMG SRC=""&{images.logo};"`). You can define more than one entity in the value portion of the attribute. When `transform active_content` is configured to remove scripts, all JavaScript entities attribute/value pairs are removed. No replacement text is put in its place.

JavaScript Strings

JavaScript strings have the following format: `javascript: javascript code` and are found anywhere in the value part of an attribute, though usually only one of them can be defined in an attribute. Most modern browsers support JavaScript strings. When `transform active_content` is configured to remove scripts, all JavaScript string attribute/value pairs are removed. No replacement text is put in its place.

JavaScript Events

JavaScript events are attributes that start with the keyword `on`. For example, ``. The HTML 4.01 specification defines 21 different JavaScript events:

`onBlur, onChange, onClick, onDblClick, onDragDrop, onFocus, onKeyDown,
onKeyPress, onKeyUp, onLoad, onMouseDown, onMouseMove, onMouseOut, onMouseOver,
onMouseUp, onMove, onReset, OnResize, onSelect, onSubmit, onUnload`

Both Microsoft Internet Explorer and Netscape have defined variations on these events as well as many new events. To catch all JavaScript events, the active content transformer identifies any attribute beginning with the keyword `on`, not including `on` itself. For example, the attribute `onDonner` in the tag `` is removed even though `onDonner` does not exist as a valid JavaScript event in the browser. In this case, the transformed file would show ``.

Embed Tags

HTML `<EMBED>` tags are not required to have an `</EMBED>` end tag. Many Web browsers do, however, support the `<EMBED> </EMBED>` tag pair. The text between the tags is supposed to be rendered by the browsers when there is no support for the embed tag, or if the MIME-type of the embed object is not supported. Thus, when `transform active_content` is configured to transform embed tags, only the `<EMBED>` tag is removed and replaced with any replacement text. Any occurrence of the end tag `</EMBED>` is simply removed, leaving the text between the beginning and end tags intact.

Object Tags

Objects tags have a start `<OBJECT>` and end `</OBJECT>` tag pair, and the attributes `CODETYPE` and `TYPE` determine the type of object. The text between the tags is supposed to be rendered by the browsers when the object tag is not supported, so when `transform active_content` is configured to transform object tags, only the `<OBJECT>` and `</OBJECT>` tags are removed and replaced with any replacement text. The text between the tags remains. The `CODETYPE` or `TYPE` attributes do not affect the transformation. Also, if the end `</OBJECT>` tag is missing, the transformation will not be affected.

Modifying Headers

The request headers are sent when users access Web objects that contain a lot of information. This can raise a concern that such details compromise the privacy or security of the enterprise or user.

When a user clicks on a link, the Web browser sets the request's Referer header to the URL of the Web page that contained the link. (This header is not set if the URL was entered or selected from a favorites or bookmarks list.) If an internal Web page provides links to external Web sites, users clicking those links sends the URL of the internal pages, and are logged in the Web logs of those external sites. This is not usually an issue; however, if the external Web site is a competitor Web site or another site with interest in the internal details of your enterprise, this might be a concern.

For example, how you structure your intranet might suggest something about your company's current or future direction. Certain project names or codewords might show up in directory or file names. Exposing the structure of the intranet makes it easier for hackers to attack the network.

The broad solution of deleting Referer headers from all requests presents a problem because some Web sites will not serve images or other linked objects unless the Referer header is set to a referring page on that same Web site. The solution implemented by Blue Coat is to strip the Referer header only when the target Web page resides on the Internet and the referring page is on an internal host.

Suppressing headers is accomplished through the Visual Policy Manager or by composing CPL.

- See "Suppress Header" in Chapter 13: "The Visual Policy Manager" on page 377 for information about how to create a strip active content object in a Web Access policy layer.
- Refer to the *Blue Coat Content Policy Language Guide*.

Defining Exceptions

Exceptions (formerly called message or RMG pages) are sent in response to certain ProxySG client requests, such as denial by policy, failure to handle the request, and authentication failure. Exceptions are returned to users based on policy rules defined by the ProxySG administrator. For example, if a client sends a request for content that is not allowed, an exception HTML page (for HTTP connections) or an exceptions string (for non-HTTP connections) is returned, informing the client that access is denied.

Two types of exceptions are used: built-in and user-defined.

Built-in Exceptions

Built-in exceptions are a set of pre-defined exceptions contained on the ProxySG. Built-in exceptions send information back to the user under operational contexts that are known to occur, such as *policy_denied* or *invalid_request*.

Built-in exceptions are always available and can also have their contents customized; however, built-in exceptions cannot be deleted, and you cannot create new built-in exceptions.

The table below lists the built-in exceptions and the context under which they are issued.

Table 14.1: Built-in Exceptions

Exception Type	Issued When
authentication_failed	The transaction cannot be authenticated, usually because the credentials were incorrect. <code>authentication_failed</code> is a synonym for <code>deny.unauthorized</code> .
authentication_failed_password_expired	The authentication server reports that the credentials provided have expired, and a new password must be obtained.
authentication_redirect_from_virtual_host	Transparent redirect authentication is being used. This exception redirects the transaction from the virtual authentication host to the original request.
authentication_redirect_to_virtual_host	Transparent redirect authentication is being used. This exception redirects the transaction to the virtual authentication host.
authentication_success	Transparent redirect authentication with cookies is being used. This exception redirects the transaction to the original request, but removes the authentication cookie from the request URL.
authorization_failed	The <code>deny.unauthorized</code> policy action is matched. This exception notifies the user that their currently authenticated identity is not permitted to perform the requested operation, but they may have some other credentials that would allow their request through (for example, they get an opportunity to enter new credentials).

Table 14.1: Built-in Exceptions (Continued)

Exception Type	Issued When
configuration_error	A configuration error on the ProxySG was detected, and the requested operation could not be handled because of the configuration error. This exception is a likely indicator that the administrator of the ProxySG will have to intervene to resolve the problem.
connect_method_denied	A user attempted an CONNECT method to a non-standard port when explicitly proxied. Blue Coat does not allow CONNECT methods to non-standard ports by default because it is considered a security risk to do so.
content_filter_denied	A particular request is not permitted because of its content categorization.
content_filter_unavailable	An external content-filtering service could not be contacted, and the ProxySG is failing closed in such a situation.
dns_server_failure	The request could not be processed because the ProxySG was unable to communicate with the DNS server in order to resolve the destination address of the request.
dns_unresolved_hostname	The request could not be processed because the ProxySG was unable to resolve the hostname in the request with DNS.
dynamic_bypass_reload	The dynamic_bypass policy action is matched.
gateway_error	There was a network error while attempting to communicate with the upstream gateway.
icap_communication_error	A network error occurred while the ProxySG was attempting to communicate with an external ICAP server.
internal_error	The ProxySG encountered an unexpected error that resulted in the inability to handle the current transaction.
invalid_request	The request received by the ProxySG was unable to handle the request because it detected that there was something fundamentally wrong with the syntax of the request.
license_expired	The requested operation cannot proceed because it would require the usage of an unlicensed feature.
method_denied	The requested operation utilizes a method that has been explicitly denied because of the service properties associated with the request.
not_implemented	The protocol cannot handle the requested operation because it utilizes a feature that is not currently implemented.
policy_denied	policy_denied is a synonym for deny.
policy_redirect	A redirect action is matched in policy.
radius_splash_page	The RADIUS/TACACS splash generator feature is in use, and the user must be authorized by RADIUS/TACACS. (The RADIUS/TACACS secrets must be configured through the (config) splash-generator commands.)
refresh	A refresh (using the HTTP Refresh: header) is required. The refresh exception (by default) refreshes the originally requested URL (or in some cases, its post-imputed form).

Table 14.1: Built-in Exceptions (Continued)

Exception Type	Issued When
silent_denied	An exception (silent_denied) is matched in policy. This exception is pre-defined to have no body text, and is “silent” in that it results in only the status code being sent to the client.
ssl_domain_invalid	There was a failure contacting an upstream host through HTTPS because the certificate presented by the upstream host was either the incorrect one or invalid.
ssl_failed	A secure connection could not be established to an upstream host. This is typically because the upstream host is not configured to accept SSL connections.
tcp_error	A network error occurred attempting to communicate with an upstream host.
unsupported_protocol	The protocol used in the request is not understood.

Most of the above exceptions can be initiated directly through the policy exception property. However, some require additional state that makes initiating them either problematic or out of context. The following are exceptions that cannot be initiated through the exception property:

- authentication_failed
- authentication_failed_password_expired
- authentication_redirect_from_virtual_host
- authentication_redirect_to_virtual_host
- authentication_success
- dynamic_bypass_reload
- license_expired
- radius_splash_page
- ssl_domain_invalid
- ssl_failed

To view the content of a built-in exception, enter the following commands at the (config) prompt:

```
SGOS#(config) exceptions
SGOS#(config exceptions) show exceptions configuration_error
configuration_error exception:
all protocols:
summary text:
    ProxySG configuration error
details text:
    Your request could not be processed because of a configuration error:
$(exception.last_error)
help text:
    The problem is most likely because of a configuration error,
$(exception.contact) and provide them with any pertinent information from this
message.
http protocol:
    code: 403
```

User-Defined Exceptions

User-defined exceptions are created and deleted by the administrator. If a user-defined exception is referenced by policy, it cannot be deleted. The default HTTP response code for user-defined exceptions is 403.

Note: For users who are explicitly proxied and use Internet Explorer to request an HTTPS URL, an exception body longer than 900 characters might be truncated. The workaround is to shorten the exception body.

Note also that an exception body less than 512 characters might cause a *page does not exist* 404 error. If this occurs, use the `exception.autopad(yes|no)` property to pad the body to more than 513 characters. For more information on the `exception.autopad` property, refer to the *Blue Coat Content Policy Language Guide*.

About Exception Definitions

Each exception definition (whether built-in or user-defined) contains the following elements:

- Identifier—Identifies the type of exception. Table 14.1 on page 477 lists the built-in exception types. For user-defined exceptions, the identifier is the name specified upon creation.
- Format—Defines the appearance of the exception. For an HTTP exception response, the format is an HTML file. For other protocols, where the user agents are not able to render HTML, the format is commonly a single line.
- Summary—A short description of the exception that labels the exception cause. For example, the default `policy_denied` exception summary is “Access Denied”.
- Details—The default text that describes reason for displaying the exception. For example, the default `policy_denied` exception (for the HTTP protocol) detail is: Your request has been denied by system policy.
- Help—An informative description of common possible causes and potential solutions for users to take. For example, if you want the categorization of a URL reviewed, you can append the `$(exception.category_review_url)` and `$(exception.category_review_message)` substitutions to the `$(exception.help)` definition. Note that you must first enable this capability through content filtering configuration. For information on enabling review categorization, see “Selecting Category Providers” on page 546.
- Contact—Used to configure site-specific contact information that can be substituted in all exceptions. Although it is possible to customize contact information on a per-exception basis, customizing the top-level contact information, which is used for all exceptions, is sufficient in most environments.
- HTTP-Code—The HTTP response code to use when the exception is issued. For example, the `policy_denied` exception by default returns the 403 Forbidden HTTP response code.

Important: Fields other than Format must be less than 8000 characters. If they are greater than this, they will not be displayed.

When defining the above fields, you can use substitution variables that are particular to the given request. Some of the above fields are also available as substitutions:

- `$(exception.id)`
- `$(exception.summary)`
- `$(exception.details)`
- `$(exception.help)`
- `$(exception.contact)`

Additionally, the `Format`, `Summary`, `Details`, `Help` and `Contact` fields can be configured specifically for HTTP, or configured commonly for all protocols.

The `Format` field, the body of the exception, is not available as a substitution. However, the `Format` field usually includes other substitutions. For example, the following is a simple HTML format:

```
<html>
<title>$ (exception.id): $ (exception.summary)</title>
<body><pre>
Request: $ (method) $ (url)
Details: $ (exception.details)
Help: $ (exception.help)
Contact: $ (exception.contact)
</pre></body></html>
```

Some additionally useful substitutions related to exceptions are:

- `$(exception.last_error)`—For certain requests, the ProxySG determines additional details on why the exception was issued. This substitution includes that extra information.
- `$(exception.reason)`—This substitution is determined internally by the ProxySG when it terminates a transaction and indicates the reason that the transaction was terminated. For example, a transaction that matches a DENY rule in policy has its `$(exception.reason)` set to "Either 'deny' or 'exception' was matched in policy".

About the Exceptions Hierarchy

Unlike the error pages in previous SGOS releases, exceptions are not required to have its entire contents defined. Exceptions are stored in a hierarchical model, and *parent* exceptions can provide default values for *child* exceptions. There are two parent exceptions from which other exceptions are derived: `exception.all` and `exception.user-defined.all`.

Each built-in and user-defined exception derives its default values from the `all` exception. For example, by default the built-in exceptions do not define the `format` field. Instead, they depend on the `all` exception's `format` field definition. To change the `format` text for all built-in and user-defined exceptions, customize the `format` field for the `all` exception.

The `user-defined.all` exception is the parent of all user-defined exceptions, but it is also a child of the `all` exception. Configuring `exception.user-defined.all` is only necessary if you want certain fields to be common for all user-defined exceptions, but not common for built-in exceptions.

The following example demonstrates using the exception inline command to configure the \$(exception.contact) substitution for every HTTP exception:

```
#(config exceptions) inline http contact EOF
For assistance, contact <a href="mailto:sysadmin@example.com">sysadmin</a>EOF
```

The following example configures a different \$(exception.contact) substitution for every HTTP exception:

```
#(config exceptions) user-defined inline http contact EOF
For assistance, contact <a
href="mailto:policyadmin@example.com">policyadmin</a>EOF
```

About the Exceptions Installable List

The Exceptions Installable List uses the Structured Data Language (SDL) format. This format provides an effective method to express a hierarchy of key/value pairs. For example, the following is SDL file before customization:

```
(exception.all
  (format "This is an exception: $(exception.details)")
  (details "")
  (exception.policy_denied
    (format "")
    (details "your request has been denied by system policy")
  )
)
```

This SDL file defines an exception called `policy_denied` that defines the \$(exception.details) substitution as "Your request has been denied by system policy". Because the exception does not define the `format` field, it inherits the `format` field from its parent exception (`exception.all`). When the `policy_denied` exception is issued, the resulting text is: This is an exception: your request has been denied by system policy.

Suppose you want to customize the \$(exception.contact) substitution for every HTTP exception. Edit the `exception.all` component.

Note: The default HTTP format and built-in exception definitions have been removed for example purposes.

```
(exception.all
  (contact "For assistance, contact your network support team.")
  (details "")
  (format "$(exception.id) : $(exception.details)")
  (help "")
  (summary "")
  (http
    (code "200")
    (contact "")
    (details "")
    (format <<EOF
<format removed>
```

```

EOF
)
(help "")
(summary "")
)
<built-in exceptions removed>
)

```

To add the `$(exception.contact)` information, modify the `contact` substitution under the `http` node:

```

(exception.all
(contact "For assistance, contact your network support team.")
(details "")
(format "$(exception.id) : $(exception.details)")
(help "")
(summary "")
(http
(code "200")
(contact "For assistance, contact <a
href="mailto:sysadmin@example.com">sysadmin</a>") EOF
(details "")
(format <<EOF
<format removed>

EOF
)
(help "")
(summary ""))
)
<built-in exceptions removed>
)
)

```

Keep in mind the following conditions when modifying exception installable lists:

- Every exception installable list must begin with a definition for `exception.all`.
- In the exceptions' installable list, all definitions must be enclosed by `exception.all` and its accompanying closing parenthesis; that is,

```
(exception.all
(exception.policy_denied)
)
```
- Keep the definition strings under the enclosed parentheses short, no longer than one line if possible.
- Blue Coat strongly recommends downloading the existing exceptions installable list, then modifying it.

Creating or Editing Exceptions

You can create or edit an exception with the CLI or with installable lists on the Management Console.

Note: You cannot create user-defined exceptions for Patience Pages.

To Create or Edit an Exception through the CLI:

1. At the (config) prompt, enter the following commands:

```
SGOS#(config) exceptions
SGOS#(config exceptions) create definition_name
SGOS#(config exceptions) edit definition_name
SGOS#(config exceptions user-defined.definition_name) http-code numeric HTTP
response code
SGOS#(config exceptions user-defined.definition_name) inline ?
contact Set the $(exceptions.contact) substitution
details Set the $(exceptions.details) substitution
format Set the format for this exception
help Set the $(exceptions.help) substitution
http Configure substitution fields for just HTTP exceptions
summary Set the $(exception.summary) substitution
SGOS#(config exceptions user-defined.definition_name) inline contact eof
string eof
SGOS#(config exceptions user-defined.definition_name) inline details eof
string eof
SGOS#(config exceptions user-defined.definition_name) inline format eof
string eof
SGOS#(config exceptions user-defined.definition_name) inline help eof
string eof
SGOS#(config exceptions user-defined.definition_name) inline summary eof
string eof
```

2. (Optional) View the results.

```
SGOS#(config exceptions user-defined.test) show exceptions user-defined.test
$(exception.id):
    test
$(exception.summary):
    Connection failed
$(exception.details):
    Connection failed with stack error
$(exception.contact):
    Tech Support
```

To Delete a User-Defined Exception:

- From the (config) prompt, enter the following commands:

```
SGOS#(config) exceptions
SGOS#(config exceptions) delete exception_name
ok
```

Note: You cannot delete a user-defined exception that is referenced by policy. You must remove the reference to the exception from the policy before deleting the exception.

Using the Management Console to Create and Install an Exceptions List

The Management Console allows you to create and install exceptions with the following methods:

- Using the ProxySG Text Editor, which allows you to customize the existing exceptions file.

- Creating a local file on your local system; the ProxySG can browse to the already-created file and install it.
- Using a remote URL, where you place an already-created exceptions list on an FTP or HTTP server to be downloaded to the ProxySG.

When the Exceptions file is customized, it updates the existing exceptions already on the ProxySG. The configuration remains in effect until it is overwritten by another update; it can be modified or overwritten using CLI commands.

To Install an Exceptions Definition through the Management Console:

1. Select Configuration>Policy>Exceptions.

The Exceptions tab displays.

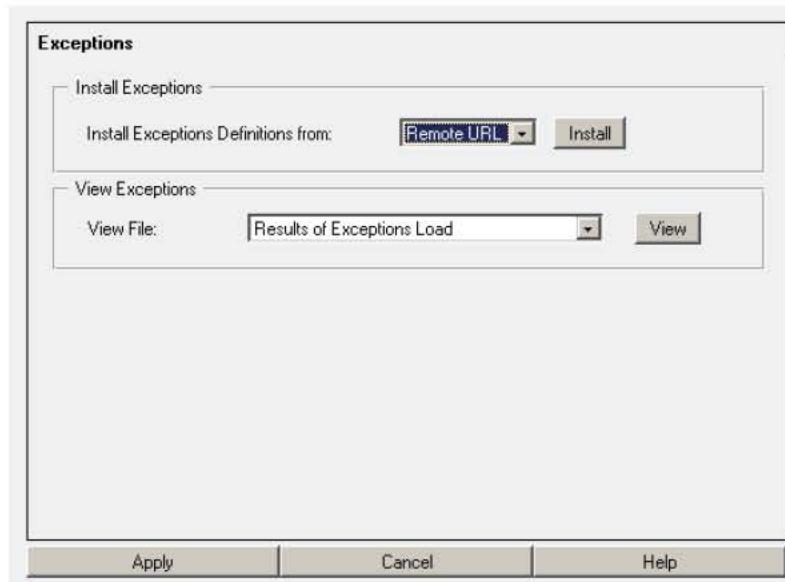


Figure 14-1: Selecting the Exceptions Definitions Download Method

Note: Click View to examine the existing definitions: Current Exceptions, Default Exceptions Source, Exceptions Configuration, and Results of Exception Load.

2. From the Install Exceptions Definitions From drop-down list, select the method used to install the exceptions configuration; click Install.

Remote URL:

Enter the fully-qualified URL, including the filename, where the configuration is located. To view the file before installing it, click View. Click Install. View the installation status; click OK.

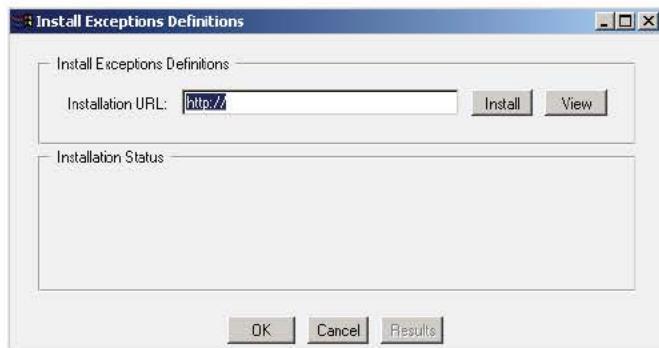


Figure 14-2: Specifying the Remote Location of an Exceptions Configuration

Local File:

Click **Browse** to bring up the Local File Browse window. Browse for the file on the local system. Open it and click **Install**. When the installation is complete, a results window opens. View the results, close the window, and click **Close**.



Figure 14-3: Specifying the Local Location of a Exception Definition

Viewing Exceptions

You can view the exceptions defined on the ProxySG, including how the defined HTML appears to users. The following are the viewable defined exception components:

- **Current Exceptions**—Displays all of the exceptions as they are currently defined.
- **Default Exceptions Source**—Displays the default ProxySG exceptions.
- **Exceptions Configuration**—Displays a page from which you can click links to view how exceptions appear in HTML to users.
- **Results of Exception Load**—Displays the results of the last installable list load, including any errors and warning to be fixed.

To View Exceptions through the Management Console:

1. Select Configuration>Policy>Exceptions.

The Exceptions tab displays.

2. From the View Exceptions Definitions From drop-down list, select the page to view; click View.

Text Editor:

The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click Install. When the installation is complete, a results window opens. View the results, close the window, and click Close.

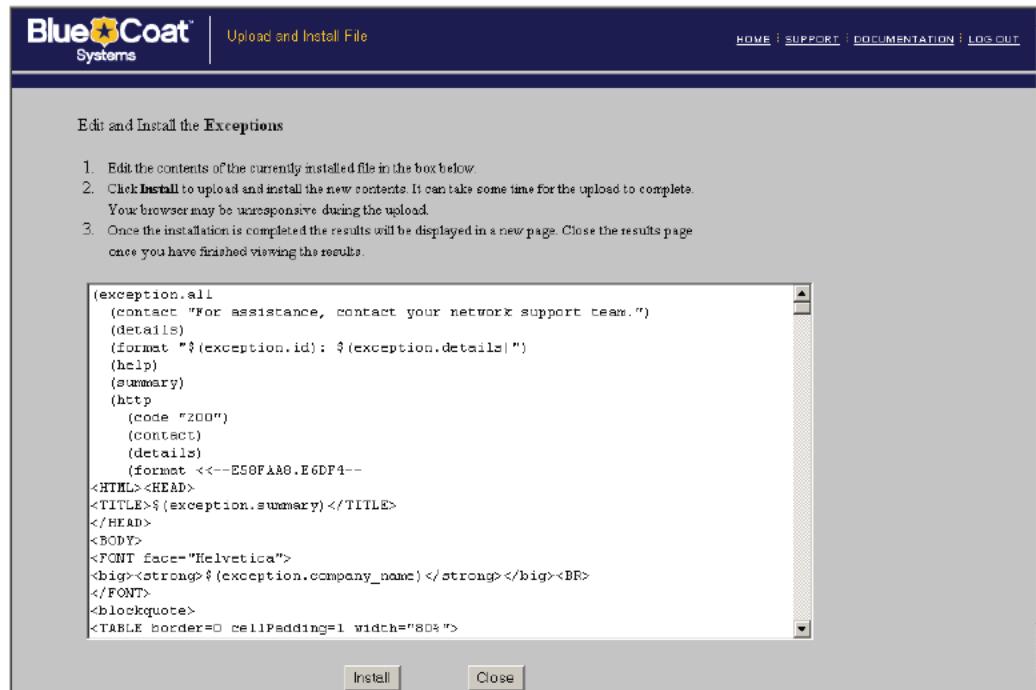


Figure 14-4: Using the ProxySG Text Editor

3. Click **Apply**.

Chapter 15: Streaming Media

This chapter contains the following sections:

- "Section A: About Streaming Media"—Provides streaming media terminology, general concepts, and information, such as player limitations and supported formats.
- "Section B: Configuring Streaming Media"—Provides feature-related concepts and procedures for configuring the ProxySG to manage streaming media applications and bandwidth.
- "Section C: Windows Media Player"—Describes how to configure the Windows Media client and describes associated limitations and access log conventions.
- "Section D: RealPlayer"—Describes how to configure the Real Media client and describes associated limitations and access log conventions.
- "Section E: QuickTime Player"—Describes how to configure the QuickTime client and describes associated limitations and access log conventions.

Related Topics:

- Chapter 5: "Managing Port Services" on page 113
- Chapter 6: "Configuring Proxies" on page 137
- Chapter 21: "Statistics" on page 711

Section A: About Streaming Media

This section contains the following topics:

- "Streaming Media Overview"
- "Streaming Media Protocols"
- "Streaming Media Player Support"
- "Streaming Media Authentication"
- "Streaming Media Caching Behavior"

Streaming Media Overview

Streaming is a method of content delivery. With media streaming, video and audio are delivered over the Internet rather than the user having to wait for an entire file to be downloaded before it can be played.

Streaming media support on the ProxySG provides the following features:

- Streaming media files can be live as well as prerecorded.
- Employs flexible delivery methods: unicast, multicast, HTTP, TCP, and UDP.
- Ability to seek, fast-forward, reverse, and pause.
- Ability to play entire file and control media playback, even before it is downloaded.
- Adjust media delivery to available bandwidth, including multi-bit-rate and thinning support.

Important: The ProxySG streaming media components require valid licenses. For more information, see Chapter 2: "Licensing" on page 31.

Supported Streaming Media Clients

The ProxySG supports Microsoft Windows Media, RealNetworks RealPlayer, and Apple QuickTime clients. The specific protocols are discussed in "Streaming Media Protocols" on page 491.

Real Media Upgrade/Downgrade Support

As SGOS 3.x employs a new Real Media proxy implementation, the RealProxy configurations from previous releases are not supported. For more information, refer to the *Blue Coat SGOS 3.x Upgrade Guide*.

Delivery Method

The ProxySG supports the following streaming delivery methods:

Section A: About Streaming Media

- Unicast—A one-to-one transmission, where each client connects individually to the source, and a separate copy of data is delivered from the source to each client that requests it. Unicast supports both TCP- and UDP-based protocols. The majority of streaming media traffic on the Internet is unicast.
- Multicast—Allows efficient delivery of streaming content to a large number of users. Multicast enables hundreds or thousands of clients to play a single stream, thus minimizing bandwidth use.

The ProxySG provides caching, splitting, and multicast functionality.

Serving Content

Using the ProxySG for streaming delivery minimizes bandwidth use by allowing the ProxySG to handle the broadcast and allows for policy enforcement over streaming use. The delivery method depends on if the content is live or video-on-demand.

Live Unicast Content

A ProxySG can serve many clients through one unicast connection by receiving the content from the origin server and then splitting that stream to the clients that request it. This method saves server-side bandwidth and reduces the server load. You cannot pause or rewind live broadcasts. A live broadcast can be of prerecorded content. A common example is a company president making a speech to all employees.

Video-on-Demand Unicast Content

A ProxySG can store frequently requested data and distribute it upon client requests. Since the ProxySG is closer to the client than the origin server, the data is served locally, which saves firewall bandwidth and increases quality of service by reducing pauses or buffering during playback. The ProxySG provides higher quality streams (also dependent on the client connection rate) than the origin server because of its closer proximity to the end user. VOD content can be paused, rewound, and played back. Common examples include training videos or news broadcasts.

Multicast Content

The ProxySG can take a unicast stream from the origin media server and deliver it as a multicast broadcast. This enables the ProxySG to take a one-to-one stream and split it into a one-to-many stream, saving bandwidth and reducing the server load. It also produces a higher quality broadcast.

For Windows Media multicast, an NSC file is downloaded through HTTP to acquire the control information required to set up content delivery.

For Real Media and QuickTime (through RTSP), multicasting maintains a TCP control (accounting) channel between the client and media server. The multicast data stream is broadcast using UDP from the ProxySG to streaming clients, who join the multicast.

Streaming Media Protocols

This section describes the vendor-specific streaming protocols supported by the ProxySG.

Section A: About Streaming Media

Windows Media Protocols

The ProxySG supports the following protocols:

- MMS-UDP (Microsoft Media Streaming—User Data Protocol)
- MMS-TCP (Microsoft Media Streaming—Transmission Control Protocol)
- HTTP streaming.
- All protocols between the client and the ProxySG for video-on-demand and live unicast content.
- MMS-TCP and HTTP streaming between the ProxySG and origin server for video-on-demand and live unicast content.
- Multicast-UDP is the only delivery protocol supported for multicast. No TCP control connection exists for multicast delivery.

The following briefly describes each of the supported delivery protocols:

- MMS-UDP—UDP provides the most efficient network throughput from server to client. The disadvantage to UDP is that many network administrators close their firewalls to UDP traffic, limiting the potential audience for Multicast-UDP-based streams.

The Windows Media Player attempts to connect in the following order:

- Multicast session. Multicast-UDP uses a TCP connection for control messages and UDP for streaming data. TCP provides packet receipt acknowledgement back to the sender. This insures control message delivery.
- MMS-TCP session. If an MMS-UDP session cannot be established, the client falls back to MMS-TCP automatically.

The ProxySG then establishes a connection to the origin server running the Microsoft Windows Media service.

- MMS-TCP—TCP provides a reliable protocol for delivering streaming media content from a server to a client. At the expense of less efficiency compared to MMS-UDP data transfer, MMS-TCP provides a reliable method for streaming content from the origin server to the ProxySG.

Note: The MMS protocol is usually referred to as either MMS-TCP or MMS-UDP depending on whether TCP or UDP is used as the transport layer for sending streaming data packets. MMS-UDP uses a TCP connection for sending and receiving media control messages, and a UDP connection for streaming the actual media data. MMS-TCP uses TCP connections to send both control and data messages.

- HTTP Streaming—The Windows Media server also supports HTTP-based media control commands along with TCP-based streaming data delivery. This combination has the benefit of working with all firewalls that let only Web traffic through (port 80).

Depending on the configuration, if MMS-UDP is used between the ProxySG and the client, the appliance can use MMS-TCP, HTTP, or multicast-UDP as the connection to the media server. No protocol relationship exists between the ProxySG and the media server, or between the ProxySG and the client.

Section A: About Streaming Media

Real Media Protocols

The ProxySG supports the following Real Media protocols:

Client-side

- RDT over unicast UDP (RTSP over TCP, RDT over unicast UDP)
- Interleaved RTSP (RTSP over TCP, RDT over TCP on the same connection)
- RDT over multicast UDP (RTSP over TCP, RDT over multicast UDP; for live content only)
- HTTP streaming (RTSP and RDT over TCP tunneled through HTTP)—HTTP streaming is supported through a handoff process from HTTP to RTSP. HTTP accepts the connection and, based on the headers, hands off to RTSP. The headers identify an RTSP URL.

Server-side

- Interleaved RTSP
- HTTP streaming

Unsupported Protocols

The following Real Media protocols are not supported in this version of SGOS:

- PNA.
- Server-side RDT/UDP (both unicast and multicast).

QuickTime Protocols

The ProxySG supports the following protocols:

- RTP over unicast UDP (RTSP over TCP, RDT over unicast UDP)
- Interleaved RTSP (RTSP over TCP, RDT over TCP on the same connection)
- HTTP streaming (RTSP and RDT over TCP tunneled through HTTP)—HTTP streaming is supported through a handoff process from HTTP to RTSP. HTTP accepts the connection and, based on the headers, hands off to RTSP. The headers identify an RTSP URL.

Server-side

- Interleaved RTSP
- HTTP streaming

Unsupported Protocols

The following QuickTime protocols are not supported in this version of SGOS:

- Server-side RTP/UDP, both unicast and multicast, is not supported.
- Client-side multicast is not supported.

Section A: About Streaming Media

Streaming Media Player Support

This section describes which media player and server versions the ProxySG supports. It also provides the supported streaming content formats.

Consider that the various players might experience limitations dependent upon certain SGOS configurations and features. Feature sections list such limitations, as necessary.

Supported Windows Media Players and Servers

The ProxySG supports the following versions and formats:

- Windows Media Player 6.4, 7, and 9
- Windows Media Server 4.1
- Windows Media Server 9

Supported Real Media Players and Servers

The ProxySG supports the following versions:

- RealOne Player, version 2
- RealPlayer 8
- RealServer 8
- Helix Universal Server

Note: Blue Coat recommends that you not deploy a Helix proxy in between the ProxySG and a Helix server where the Helix proxy is the parent to the ProxySG. This causes errors with the Helix server. The reverse is acceptable (using a Helix proxy as a child to the ProxySG).

Supported QuickTime Players and Servers

The ProxySG supports the following versions, but in pass-through mode only:

- QuickTime Players 6.x and 5.x
- Darwin Streaming Server 4.1.x and 3.x.
- Helix Universal Server

Streaming Media Authentication

The following sections discuss authentication between streaming media clients and ProxySG appliances and between ProxySG appliances and origin content servers (OCS).

Section A: About Streaming Media

Windows Media Server-Side Authentication

Windows Media server authentication for HTTP and MMS supports the following authentication types:

- HTTP—BASIC Authentication and Membership Service Account
- HTTP—BASIC Authentication and Microsoft Windows NT LAN Manager (NTLM) Account Database
- NTLM Authentication and NTLM Account Database

The ProxySG supports the caching and live-splitting of server-authenticated data. The functionality is also integrated with partial caching functionality so that multiple security challenges are not issued to the Windows Media Player when it accesses different portions of the same media file.

When Windows Media content on the server is accessed for the first time, the ProxySG caches the content along with the authentication type enabled on the server. The cached authentication type remains until the appliance learns that the server has changed the enabled authentication type, either through cache coherency (checking to be sure the cached contents reflect the original source) or until the ProxySG connects to the origin server (to verify access credentials).

Authentication type on the server refers to the authentication type enabled on the origin server at the time when the client sends a request for the content.

Windows Media Proxy Authentication

If proxy authentication is configured, Windows Media clients are authenticated based on the policy settings. The proxy (the ProxySG) evaluates the request from the client and verifies the accessibility against the set policies. The Windows Media player then prompts the client for the proper password. If the client is accepted, the Windows Media server might also require the client to provide a password for authentication. If a previously accepted client attempts to access the same Windows Media content again, the ProxySG verifies the user credentials using its own credential cache. If successful, the client request is forwarded to the Windows Media server for authentication.

Windows Media Player Authentication Limitations

Consider the following proxy authentication limitations with the Windows Media player (except when specified, these do not apply to HTTP streaming):

- For Windows Media Player 6.4 only: if the media server is configured for NTLM authentication, Windows Media Player 6.4 uses the credentials of the logged-on user to satisfy the challenged request. If the media server or proxy authentication type is NTLM, configure the Windows Media server to accept logged-on user credentials.
- For Windows Media Player 6.4 only: if proxy authentication is not configured and the media server is configured as BASIC and the user fails to provide a valid username and password, the user fails to receive another dialog box. Instead, the request fails to open the stream.
- If the proxy authentication type is configured as BASIC and the server authentication type is configured as NTLM, the default is denial of service.

Section A: About Streaming Media

- If proxy authentication is configured as NTLM and the server authentication is configured as BASIC, the proxy authentication type defaults to BASIC.
- The ProxySG does not support authentication based on `url_path` or `url_path_regex` conditions when using `mms` as the `url_scheme`.
- Transparent style HTTP proxy authentication fails to work with Windows Media players when the credential cache lifetime is set to 0 (independent of whether server-side authentication is involved).
- If proxy authentication is configured, a request for a stream through HTTP prompts the user to enter access credentials twice: once for the proxy authentication and once for the media server authentication.
- Additional scenarios involving HTTP streaming exist that do not work when the TTL is set to zero (0), even though only proxy authentication (with no server authentication) is involved. The ProxySG returning a 401-style proxy authentication challenge to the Windows Media Player 6.0 does not work because the Player cannot resolve inconsistencies between the authentication response code and the server type returned from the ProxySG. This results in an infinite loop of requests and challenges. Example scenarios include transparent authentication—resulting from either transparent request from player or hard-coded service specified in the ProxySG—and request of cache-local (ASX-rewritten or unicast alias) URLs.

Real Media Proxy Authentication

If proxy authentication is configured, Real Media clients are authenticated based on the policy settings. The proxy (the ProxySG) evaluates the request from the client and verifies the accessibility against the set policies. Next, RealPlayer prompts the client for the proper password. If the client is accepted, the Real Media server may also require the client to provide a password for authentication. If a previously accepted client attempts to access the same Real Media content again, the ProxySG verifies the user credentials using its own credential cache. If successful, the client request is forwarded to the Real Media server for authentication.

Real Media Player Authentication Limitation

Using RealPlayer 8.0 in transparent mode with both proxy and Real Media server authentication configured to BASIC, RealPlayer 8.0 always sends the same proxy credentials to the media server. This is regardless of whether a user enters in credentials for the media server. Therefore, the user is never authenticated and the content is not served.

QuickTime Proxy Authentication

BASIC is the only proxy authentication mode supported for QuickTime clients. If an NTLM challenge is issued, the mode automatically downgrades to BASIC.

Streaming Media Caching Behavior

The following sections describe how the ProxySG and SGOS process and store streaming media requests. Discussed are caching, video on demand (VOD), live splitting, bit rate support, and pre-populating content.

Section A: About Streaming Media

Streaming Media Caching Behavior

Windows Media

The ProxySG caches Windows Media-encoded video and audio files. The standard extensions for these file types are: .wm, .wma, and .asf.

Real Media

The ProxySG caches Real Media-encoded files, such as RealVideo and RealAudio. The standard extensions for these file types are: .rm, .ra, and .rv.

QuickTime

The ProxySG does not cache QuickTime content (.mov files). All QuickTime content is served in *pass-through* mode only.

Miscellaneous

The ProxySG supports all other files pass-through mode only; such files are not cacheable. Examples of these types of files are: MPEG (including .mp3), .rt, .rp, .swf, .gif, .smil, .jpg, and .jpeg.

Video On Demand (VOD)

The ProxySG supports the caching of files for VOD streaming. First, the client connects to the ProxySG, which in turn connects to the origin server and pulls the content, storing it locally. Subsequent requests are served from the ProxySG. This provides bandwidth savings, as every *hit* to the ProxySG means less network traffic. Blue Coat also supports partial caching of streams.

Note: On-demand files must be unicast.

Live Splitting

The ProxySG supports splitting of live content, but behavior varies depending upon the media type.

For live streams, the ProxySG can split streams for clients that request the same stream. First, the client connects to the ProxySG, which then connects to the origin server and requests the live stream. Subsequent requests are split from the appliance.

Two streams are considered identical by the ProxySG if they share the following characteristics:

- The stream is a live or broadcast stream.
- The URL of the stream requested by client is identical.
- MMS, MMSU, MMST, and HTTP are considered as identical.

Section A: About Streaming Media

Note: If the origin server is made up of multiple servers, stream splitting sometimes does not occur because Windows Media player 6.4 does not send domain information to the ProxySG; the appliance can only split streams based on the host IP address. In addition, if the URL is composed of hostnames instead of IP addresses, splitting does not occur across WMP 6.4 and WMP 7.0 clients.

Splitting of live unicast streams provides bandwidth savings, since subsequent requests do not increase network traffic.

Multiple Bit Rate Support

The ProxySG supports multiple bit rate (MBR), which is the capability of a single stream to deliver multiple bit rates to clients requesting content from caches from within varying levels of network conditions (such as different connecting bandwidths and traffic). This allows the ProxySG and the client to negotiate the optimal stream quality for the available bandwidth even when the network conditions are bad. MBR increases client-side streaming quality, especially when the requested content is not cached.

Only the requested bitrate is cached. Therefore, a media client that requests a 50Kbps stream receives that stream, and the Blue Coat ProxySG caches only the 50Kbps bitrate content.

Bitrate Thinning

Thinning support is closely related to MBR, but different in that thinning allows for data rate optimizations even for single data-rate media files. If the media client detects that there is network congestion, it requests a subset of the single data rate stream. For example, depending on how congested the network is, the client requests only the *key video frames* or audio-only instead of the complete video stream.

Pre-Populating Content

The ProxySG supports pre-population of streaming files (QuickTime content is *not* supported) from HTTP servers and origin content servers. Downloading streaming files from HTTP servers reduces the time required to pre-populate the file. With previous SGOS versions, pre-population was accomplished through streaming from the media server. The required download time was equivalent to the file length; for example, a two-hour movie required two hours to download. With the pre-population content management feature, if the media file is hosted on a HTTP server, the download time occurs at normal transfer speeds of an HTTP object, and is independent of the *play length* of the media file.

Note: Content must be hosted on a HTTP server in addition to the media server.

Using the `content pull` CLI command, content is downloaded from the HTTP server and renamed with a given URL argument. A client requesting the content perceives that the file originated from a media server. If the file on the origin media server experiences changes (such as naming convention), SGOS bypasses the cached mirrored version and fetches the updated version.

Section B: Configuring Streaming Media

Section B: Configuring Streaming Media

This section contains the following topics:

- "Limiting Bandwidth"
- "Configuring the Refresh Rate"
- "Configuring HTTP Handoff"
- "Forwarding Client Logs to the Media Server"
- "Configuring Media Server Authentication Type (Windows Media)"
- "About Multicast Streaming"
- "Managing Multicast Streaming for Windows Media"
- "Managing Multicast Streaming for Real Media"
- "Managing Simulated Live Content (Windows Media)"
- "ASX Rewriting (Windows Media)"
- "About Fast Streaming (Windows Media)"

Related Topics

You must also configure the network service (Configuration>Network>Services) to assign port numbers and modes (transparent or proxy). For more information, see Chapter 6: "Configuring Proxies" on page 137.

Limits Bandwidth

The following sections describe bandwidth limitation and how to configure the ProxySG to limit global and protocol-specific media bandwidth.

About Bandwidth Limitation

Streaming media bandwidth management is achieved by configuring the ProxySG to restrict the total number of bits per second the appliance receives from the origin media servers and delivers to clients. The configuration options are flexible to allow you to configure streaming bandwidth limitations for the ProxySG, as well as for each streaming protocol (Windows Media, Real Media, and QuickTime).

Note: Bandwidth claimed by HTTP, non-streaming protocols, and network infrastructure is not constrained by this limit. Transient bursts that occur on the network can exceed the hard limits established by the bandwidth limit options.

Once configured, the ProxySG limits streaming access to the specified threshold. If a client tries to make a request after a limit has been reached, the client receives an error message.

Section B: Configuring Streaming Media

Note: If a maximum bandwidth limitation has been specified for the ProxySG, the following condition may occur. If a Real Media client, followed by a Windows Media client, requests streams through the same ProxySG and total bandwidth exceeds the maximum allowance, the Real Media client enters the rebuffering state. The Windows Media client continues to stream.

Consider the following features when planning to limit streaming media bandwidth:

- ProxySG to server (all protocols)—The total kilobits per second allowed between the appliance and any origin content server or upstream proxy for all streaming protocols. Setting this option to 0 effectively prevents the ProxySG from initiating any connections to the media server. The ProxySG supports partial caching in that no bandwidth is consumed if portions of the media content are stored in the ProxySG.
- Client to ProxySG (all protocols)—The total kilobits per second allowed between streaming clients and the ProxySG. Setting this option to 0 effectively prevents any streaming clients from initiating connections through the ProxySG.
- ProxySG to server—The total kilobits per second allowed between the Appliance and the media server. Setting this option to 0 effectively prevents the ProxySG from accepting media content.

Limiting ProxySG bandwidth restricts the following streaming media-related functions:

- Live and video-on-demand media, the sum of all bitrates
 - Limits the ability to fetch new data for an object that is partially cached
 - Reception of multicast streams
 - Client to ProxySG—The total kilobits per second allowed between Windows Media streaming media clients and the ProxySG. Setting this option to 0 effectively prevents streaming clients from making connections to the ProxySG.
- Limiting server bandwidth restricts the following streaming media-related functions:
- MBR is supported; the ProxySG assumes the client is using the maximum bit rate
 - Limits the transmission of multicast streams
 - Client connections—The total number of clients that can connect concurrently. Once this limit is reached, clients attempting to connect receive an error message and are not allowed to connect until other clients disconnect. Setting this variable to 0 effectively prevents any streaming media clients from connecting.

Configuring Bandwidth Limitation—Global

This section describes how to limit all bandwidth use through the ProxySG.

To Specify the Bandwidth Limit for all Streaming Protocols through the Management Console:

1. Select Configuration>Services>Streaming Proxies>General.

The General tab displays.

Section B: Configuring Streaming Media

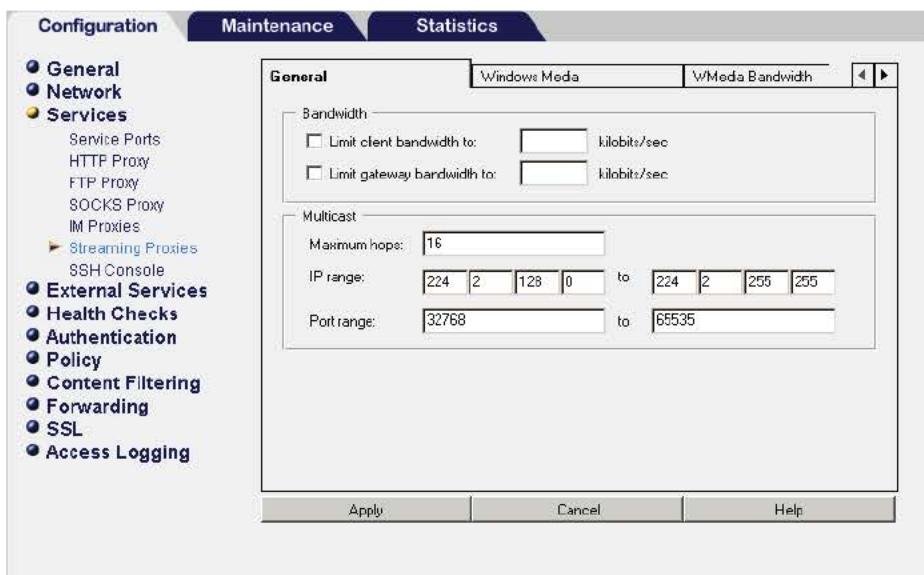


Figure 15-1: Streaming Media General Tab

2. To limit the client connection bandwidth:
 - a. In the Bandwidth field, select Limit client bandwidth to.
 - b. In the Kbits/sec field, enter the total number of kilobits to specify the maximum number of kilobits per second that the ProxySG allows for all streaming client connections.
3. To limit the ProxySG (origin server/upstream connection) bandwidth:
 - a. In the Bandwidth field, select Limit gateway bandwidth to.
 - b. In the Kbits/sec field, enter the total number of kilobits to specify the maximum number of kilobits per second that the ProxySG allows for all streaming connections to origin media servers.

To Specify Bandwidth Limit for all Streaming Protocols through the CLI:

To limit the client connection bandwidth, at the `(config)` command prompt, enter the following command:

```
SGOS#(config) streaming max-client-bandwidth kbits_second
```

To limit the ProxySG (origin server/upstream connection) bandwidth, at the `(config)` command prompt, enter the following command:

```
SGOS#(config) streaming max-gateway-bandwidth kbits_second
```

Note: To allow maximum client bandwidth, use the `streaming windows-media no max-client-bandwidth` or the `streaming windows-media no max-gateway-bandwidth` command.

Section B: Configuring Streaming Media

Configuring Bandwidth Limitation—Protocol-Specific

This section describes how to limit bandwidth use per-protocol (Windows Media and Real Media) through the ProxySG.

To Specify the Bandwidth Limit for Windows Media, Real Media, or QuickTime through the Management Console:

1. Select Configuration>Services>Streaming Proxies>WMedia Bandwidth or RMedia Bandwidth or QuickTime Bandwidth.
2. To limit the bandwidth for client connections to the ProxySG:
 - a. Select Limit client bandwidth to.
 - b. In the Kbits/sec field, enter the number of kilobits to specify the maximum number of kilobits per second that the ProxySG allows for all streaming client connections.
3. To limit the bandwidth for connections from the ProxySG to origin content servers:
 - a. Select Limit gateway bandwidth to.
 - b. In the Kbits/sec field, enter the number of kilobits to specify the maximum number of kilobits per second that the ProxySG allows for all streaming connections to origin media servers.

To Specify the Bandwidth Limit for Windows Media, Real Media, or QuickTime through the CLI:

To limit the client connection bandwidth, at the `(config)` prompt, enter the following command:

```
SGOS#(config) streaming {windows-media | real-media | quicktime}  
max-client-bandwidth kbits_second
```

To limit the ProxySG (origin server/upstream connection) bandwidth, at the `(config)` command prompt, enter the following command:

```
SGOS#(config) streaming {windows-media | real-media | quicktime}  
max-gateway-bandwidth kbits_second
```

Note: To allow maximum client bandwidth, use the `streaming windows-media no max-client-bandwidth` or the `streaming windows-media no max-gateway-bandwidth` command.

Configuring Bandwidth Limitation—Fast Start (Window Media)

Note: This section applies to Windows Media only.

This section describes how to configure the maximum bandwidth (in kilobytes per second) each Windows Media Player can start with. Upon connection to the ProxySG, streaming media clients will not consume more bandwidth (in kilobits per second) than the defined value.

Section B: Configuring Streaming Media

To specify the maximum starting bandwidth through the CLI:

At the (config) prompt, enter the following command:

```
SGOS# (config) streaming windows-media max-fast-bandwidth kbps
```

Maximum Connections

This section describes how to configure the maximum number of streaming clients, on a per-protocol basis, that can connect to the ProxySG.

To Specify the Maximum Number of Client Connections through the Management Console:

1. Select Configuration>Services>Streaming Proxies>WMedia Bandwidth or Real Media Bandwidth or QuickTime Bandwidth.
2. To limit the bandwidth for connections from the ProxySG to Windows Media origin servers:
 - a. Select Limit maximum connections.
 - b. In the clients field, enter the total number of clients that can connect concurrently.

To Specify the Maximum Number of Client Connections through the CLI:

At the (config) prompt, enter the following command:

```
SGOS# (config) streaming {windows-media | real-media | quicktime} max-connections  
number
```

Note: To allow maximum number of connections, invoke the **streaming {windows-media | real-media | quicktime} no max-connection** command.

Configuring the Refresh Rate

The refresh feature specifies the length of time before cached streaming content is checked for freshness.

The default is never refresh. Blue Coat recommends that you change this setting.

To Set the Refresh Rate through the Management Console:

1. Select Configuration>Services>Streaming Proxies>Windows Media or Real Media.
2. Perform one of the following:
 - a. In the Check freshness every n.nn hours field, enter the length of time before the cached streaming content is checked for freshness.
 - b. To force the ProxySG to check every time for freshness, select Check freshness every access.
3. Click Apply.

Section B: Configuring Streaming Media

To Set the Refresh Rate through the CLI:

At the (config) prompt, enter the following commands:

```
SGOS# (config) streaming {windows-media | real-media} refresh-interval  
number.number
```

where *number.number* is the length of time before the cached streaming content should be checked for freshness.

Note: A value of 0 requires the streaming content to always be checked for freshness.

To disable freshness checking, enter the following command:

```
SGOS# (config) streaming {windows-media | real-media} no refresh-interval
```

Configuring HTTP Handoff

HTTP handoff is enabled by default. This section describes HTTP handoff and how to disable the feature.

About HTTP Handoff

When a Windows Media, Real Media, or QuickTime client requests a stream from the ProxySG over port 80, which in common deployments is the only port allowing traffic through a firewall, the HTTP module passes control to the streaming module so HTTP streaming can be supported through the HTTP proxy port.

The ProxySG supports HTTP streaming. It does not support HTTP downloading of media files from HTTP servers and their subsequent caching and serving as streaming files. An HTTP connection is established through port 80 that allows you to send streaming data from the origin server to the clients through the ProxySG.

Note: The default setting for HTTP Handoff is enabled. If you do not want HTTP streams to be cached or split, change this setting to disabled.

Disabling HTTP Handoff

To Disable HTTP Port Handoff through the Management Console:

1. Select Configuration>Services>Streaming Proxies>Windows Media or Real Media or QuickTime.
2. Deselect Enable HTTP handoff.
3. Click Apply.

To Disable the HTTP Port Handoff through the CLI:

At the (config) prompt, enter the following command:

```
SGOS# (config) streaming {windows-media | real-media | quicktime} http-handoff  
disable
```

Section B: Configuring Streaming Media

Forwarding Client Logs to the Media Server

This section describes media server compatibility and how to forward client logs.

About Forwarding Client Logs

The ProxySG logs information, such as client IP address, the date, and the time, to the origin server for Windows Media and Real Media content.

Note: For Real Media, the log is only forwarded before a streaming session is halted; QuickTime log forwarding is not supported.

Both HTTP streaming and MMS-TCP support logging to the origin server. Logging information is generated for both the server-side connection and the client-side connection that the ProxySG makes to the server. (For more information on what is logged to the origin server, see Chapter 19: “Access Logging” on page 641).

Logging messages are embedded in a log message sent to the content server when:

- The ProxySG receives an end-of-file notification.
- The ProxySG-server connection is closed.
- A user stops the stream. The *connection* is not stopped; the same connection to the OCS remains and is used to send client information. This prevents starting another connection to the OCS.
- A user opens a new file without closing or stopping the current one.

Windows Media only:

- A user seeks to a new position or uses fast forward or reverse.
- A file is looped in a live scenario. Logging occurs whenever playing of a file ends before going on to play another. (Windows Media Player 6.4 does not log this instance.)

When the ProxySG receives a log record from the client, the ProxySG records the log in the access log and then it forwards the log to the origin content server. As necessary, the ProxySG sends log records to the origin media server for whatever content the appliance fetched to populate itself.

Configuring the ProxySG to Forward Client Logs

To Enable Forwarding Client-generated Logging to the Origin Media Server through the Management Console:

1. Select Configuration>Services>Streaming Proxies>Windows Media or Real Media.
2. Select Forward client-generated logs to origin media server.
3. Click Apply.

To Enable or Disable Forwarding Client-generated Logging through the CLI:

At the (config) command prompt, enter the following command:

Section B: Configuring Streaming Media

```
SGOS# (config) streaming {windows-media | real-media} log-forwarding {enable | disable}
```

Configuring Media Server Authentication Type (Windows Media)

Note: This section applies to Windows Media streaming only.

Configure the ProxySG to recognize the type of authentication the origin content server is using: BASIC or NTLM.

To Configure the Media Server Authentication Type through the CLI:

At the (config) prompt, enter the following command:

```
SGOS# (config) streaming windows-media server-auth-type {basic | ntlm}
```

About Multicast Streaming

This section describes multicast streaming and how to configure the ProxySG to manage multicast broadcasts.

About Serving Multicast Content

- How multicast content is handled through the ProxySG depends on whether the ProxySG is delivering Windows Media or Real Media multicast broadcasts (QuickTime is not supported). For Windows Media, the ProxySG takes a multicast stream from the origin server and delivers it as a unicast stream. This avoids the main disadvantage of multicasting—that all of the routers on the network must be multicast-enabled to accept a multicast stream. Unicast-to-multicast, multicast-to-multicast, and broadcast alias-(scheduled live from stored content)-to-multicast are also supported.
- For Real Media, the ProxySG takes a unicast stream from the origin RealServer and delivers it as a multicast stream. This enables the ProxySG to take a one-to-one stream and split it into a one-to-many stream, saving bandwidth and reducing the server load.

Multicast to Unicast Live Conversion at the ProxySG

The ProxySG supports converting multicast streams from an origin content server to unicast streams. The stream at the ProxySG is given the appropriate unicast headers to allow the appliance to direct one copy of the content to each user on the network.

Multicast streaming only uses UDP protocol and does not know about the control channel, which transfers essential file information. The .nsc file (a file created off-line that contains this essential information) is retrieved at the beginning of a multicast session from an HTTP server. The `multicast-alias` command specifies an alias to the URL to receive this .nsc file.

The converted unicast stream can use any of the protocols supported by Windows Media and Real Media, including HTTP streaming.

Section B: Configuring Streaming Media

When a client requests the alias content, the ProxySG uses the URL specified in the `multicast-alias` command to fetch the `.nsc` file from the HTTP server. The `.nsc` file contains all of the multicast-related information, such as addresses and `.asf` file header information that is normally exchanged through the control connection for unicast-delivered content.

Configuring the ProxySG Multicast Network

This section describes how to configure the ProxySG multicast service. Additional steps are required to configure the ProxySG to serve multicast broadcasts to streaming clients (Windows Media and Real Media). Those procedures are provided in subsequent sections.

To Configure the Multicast Service through the Management Console:

1. Select Configuration>Services>Streaming Proxies>General.
2. In the Maximum Hops field, enter a time-to-live (TTL) value.
3. In the IP Range fields, enter the IP address range.
4. In the Port Range fields, enter the port range.
5. Enable Windows and Real Media multicast; see the next section, "Managing Multicast Streaming for Windows Media" and "Managing Multicast Streaming for Real Media" on page 511.

Managing Multicast Streaming for Windows Media

This section describes multicast station and `.nsc` files, and describes how to configure the ProxySG to send multicast broadcasts to Windows Media clients.

About Multicast Stations

A multicast station is a defined location from where the Windows Media player retrieves live streams. This defined location allows `.asf` streams to be delivered to many clients using only the bandwidth of a single stream. Without a multicast station, streams must be delivered to clients through unicast.

A multicast station contains all of the information needed to deliver `.asf` content to a Windows Media player or to another ProxySG, including:

- IP address
- Port
- Stream format
- TTL value (time-to-live, expressed hops)

The information is stored in an `.nsc` file, which the Window Media Player must be able to access to locate the IP address.

Section B: Configuring Streaming Media

If Windows Media Player fails to find proper streaming packets on the network for multicast, the player can roll over to a unicast URL. Reasons for this include lack of a multicast-enabled router on the network or if the player is outside the multicast station's TTL. If the player fails to receive streaming data packets, it uses the unicast URL specified in the .nsc file that is created from the multicast station configuration. All .nsc files contain a unicast URL to allow rollover.

Unicast to Multicast

Unicast to multicast streaming requires converting a unicast stream on the server-side connection to a multicast station on the ProxySG. The unicast stream must contain live content before the multicast station works properly. If the unicast stream is a video-on-demand file, the multicast station is created but will not be able to send packets to the network. For video-on-demand files, use the broadcast-alias command, discussed below.

Multicast to Multicast

Use the `multicast-alias` command to get the source stream for the multicast station.

About Broadcast Aliases

A broadcast alias defines a playlist, specify a starting time, date, and the number of times the content will be repeated.

Creating a Multicast Station

To create a multicast station, you must perform the following:

- Define a name for the multicast station.
- Define the source of the multicast stream.
- The port range to be used.
- Define the address range of the multicast stream.
- Define the TTL value.
- Create the multicast alias, unicast alias, and broadcast alias commands to enable the functionality.

Note: You must configure multicast stations through the CLI.

Syntax

```
multicast-station name {alias | url} [address | port | ttl]
```

where

- `name` specifies the name of the multicast station, such as `station1`
- `{alias | url}` defines the source of the multicast stream. The source can be a URL or it can be a multicast alias, a unicast alias, or simulated live. (The source commands must be set up before the functionality is enabled within the multicast station.)

Section B: Configuring Streaming Media

- [address | port | ttl] are optional commands that you can use to override the default ranges of these values. (Defaults and permissible values are discussed below.)

Example 1: Create a Multicast Station

This example:

- Creates a multicast station, named *station1*, on ProxySG 10.25.36.47.
- Defines the source as mms://10.25.36.47/tenchi.
- Accepts the address, port, and TTL default values.

```
SGOS# (config) streaming windows-media multicast-station station1
mms://10.25.36.47/tenchi.
```

To delete multicast *station1*:

```
SGOS# (config) streaming no multicast-station station1
```

Example 2: Create a Broadcast Alias and Direct a Multicast Station to use It

This example:

- To allow unicast clients to connect through multicast, creates a broadcast alias named *array1*; defines the source as mms://10.25.36.48/tenchi2.
- Instructs the multicast station from Example 1, *station1*, to use the broadcast alias, *array1*, as the source.

```
SGOS# (config) streaming windows-media broadcast-alias array1
mms://10.25.36.48/tenchi2 0 today noon
SGOS# (config) streaming windows-media multicast-station station1 array1
```

Changing Address, Port, and TTL Values

Specific commands allow you to change the address range, the port range, and the default TTL value. To leave the defaults as they are for most multicast stations and change it only for specified station definitions, use the *multicast-station* command.

The *multicast-station* command randomly creates an IP address and port from the specified ranges.

- **Address-range:** the default ranges from 224.2.128.0 to 224.2.255.255; the permissible range is 224.0.0.2 and 239.255.255.255.
- **Port-range:** the default ranges from 32768 to 65535; the permissible range is between 1 and 65535.
- **TTL value:** the default is 5 hops; the permissible range is from 1 to 255.

Syntax, with defaults set

```
multicast address-range <224.2.128.0>-<224.2.255.255>
multicast port-range <32768>-<65535>
multicast ttl <5>
```

Section B: Configuring Streaming Media

Getting the .nsc File

The .nsc file is created from the multicast station definition and saved through the browser as a text file encoded in a Microsoft proprietary format.

Without an .nsc file, the multicast station definition does not work.

To get an .nsc file from newly created *station1*, open the file by navigating through the browser to the multicast station's location (where it was created) and save the file as *station1.nsc*.

The file location, based on the streaming configuration above:

- `http://10.25.36.47/MMS/nsc/station1.nsc`

Save the file as *station1.nsc*.

Note: You can also enter the URL in the Windows Media Player to start the stream.

The newly created file is not editable; the settings come from streaming configuration file. In that file, you have already defined the following pertinent information for the file:

- ❑ The address, which includes TTL, IP Address, IP Port, Unicast URL, and the NSC URL. All created .nsc files contain a unicast URL for rollover in case the Windows Media Player cannot find the streaming packets.
- ❑ The description, which references the MMS URL that you defined.
- ❑ The format, which contains important ASF header information. All streams delivered by the multicast station definition have their ASF headers defined here.

Monitoring the Multicast Station

You can determine the multicast station definitions by viewing the streaming windows configuration. To determine the current client connections and current ProxySG connections, use the `show streaming windows-media statistics` command.

To View the Multicast Station Setup through the CLI:

```
SGOS#(config) show streaming windows config
; Windows Media Configuration
license: 1XXXXXXXXX-XXXXXXX-XXXXXX
logging: enable
logging enable
http-handoff: enable
live-retransmit: enable
transparent-port (1755): enable
explicit proxy: 0
refresh-interval: no refresh interval (Never check freshness)
max connections: no max-connections (Allow maximum connections)
max-bandwidth: no max-bandwidth (Allow maximum bandwidth)
max-gateway-bandwidth: no max-gateway-bandwidth (Allow maximum bandwidth)
multicast address: 224.2.128.0 - 224.2.255.255
multicast port: 32768 - 65535
multicast TTL: 5
```

Section B: Configuring Streaming Media

```

asx-rewrite:          No rules
multicast-alias:      No rules
unicast-alias:        No rules
broadcast-alias:      No rules
multicast-station:    station1 mms://10.25.36.47/tenchi 224.2.207.0 40465 5
(playing)

```

Note: *Playing* at the end of the multicast station definition indicates that the station is currently sending packets onto the network. The IP address and port ranges have been randomly assigned from among the default ranges allowed.

To View the Multicast Station Statistics through the CLI:

```

SGOS# (config) show streaming windows stat
;Windows Media Statistics
Current client connections:
  by transport:0 UDP, 0 TCP, 0 HTTP, 1 multicast
  by type: 1 live, 0 on-demand
Current gateway connections:
  by transport: 0 UDP, 1 TCP, 0 HTTP, 0 multicast
  by type:1 live, 0 on-demand

```

Managing Multicast Streaming for Real Media

This section describes how to configure Real Media multicast streaming.

About Real Media Multicast Broadcasts

The ProxySG receives a unicast stream from the origin RealServer and serves it as a multicast broadcast. This allows the ProxySG to take a one-to-one stream and split it into a one-to-many stream, saving bandwidth and reducing the server load. It also produces a higher quality broadcast.

Multicasting maintains a TCP control (accounting) channel between the client and RealServer. The multicast data stream is broadcast using UDP from the ProxySG to RealPlayers, who join the multicast. The ProxySG support for Real Media uses UDP port 554 (RTSP) for multicasting. This port number can be changed to any valid UDP port number.

Enabling Real Media Multicast

To Enable Multicast through the Management Console:

1. Select Configuration>Services>Streaming Proxies>RMedia Bandwidth.
2. Select Enable multicast.
3. Click Apply.

Section B: Configuring Streaming Media

To Set the Refresh Rate through the CLI:

At the (config) prompt, enter the following commands:

```
SGOS# (config) streaming real-media multicast enable
```

Managing Simulated Live Content (Windows Media)

This section describes simulated live content and how to configure the ProxySG to manage and serve simulated live content.

Note: This section applies only to Windows Media.

About Simulated Live Content

The simulated live content feature defines playback of one or more video-on-demand files as a scheduled live event, which begins at a specified time. The content can be looped multiple times, or scheduled to start at multiple start times throughout the day. If used in conjunction with the `multicast-alias` command, the live content is multicast; otherwise, live content is accessible as live-splitting sources. The feature does *not* require the content to be cached.

Once a starting date and time for the simulated live content have been set, the broadcast of the content starts when there is at least one client requesting the file. Clients requesting the simulated live content before the scheduled time are put into wait mode. Clients requesting the content after all of the contents have played receive an error message. Video-on-demand content does not need to be on the ProxySG before the scheduled start time, but prepopulating the content on the Appliance provides better streaming quality.

Before configuring simulated live, consider the following:

- The simulated live content name must be unique. Aliases are not case sensitive.
- The name cannot be used for both a unicast and a multicast alias name.
- Once simulated live content is referenced by one or more multicast stations, the simulated live content cannot be deleted until all multicast stations referencing the simulated live content are first deleted.

The multicast station appears as another client of simulated live content, just like a Windows Media Player.

Note: This note applies to HTTP only. If a client opens Windows Media player and requests an alias before the starting time specified in the `broadcast-alias` option, the HTTP connection closes after a short time period. When the specified time arrives, the player fails to reconnect to the stream and remains in waiting mode.

Three scenarios can occur when a client requests the simulated live content:

- Clients connect before the scheduled start time of the simulated live content: clients are put into *wait* mode.

Section B: Configuring Streaming Media

- Clients connect during the scheduled playback time of the simulated live content: clients receive cached content for playback.
- Clients connect after the scheduled playback time of the simulated live: the client receives an error message.

The ProxySG computes the starting playtime of the broadcast stream based on the time difference between the client request time and the simulated live starting time.

Creating a Broadcast Alias for Simulated Live Content

Syntax

```
streaming windows-media broadcast-alias alias url loops date time
```

where:

- ❑ *alias* is the name of the simulated live content.
- ❑ *url* is the URL for the video-on-demand stream. Up to 128 URLs can be specified for simulated live content.
- ❑ *loops* is the number of times you want the content to be played back. Set to 0 (zero) to allow the content to be viewed an indefinite number of times.
- ❑ *date* is the simulated live content starting date. Valid date strings are in the format *yyyy-mm-dd* or *today*. You can specify up to seven start dates by using the comma as a separator (no spaces).
- ❑ *time* is the simulated live content starting time. Valid time strings are in the format *hh:mm* (on a 24-hour clock) or one of the following strings:
 - *midnight*, *noon*
 - *1am*, *2am*, ...
 - *1pm*, *2pm*, ...

Specify up to 24 different start times within a single date by using the comma as a separator (no spaces).

Example 1

This example creates a playlist for simulated live content. The order of playback is dependent on the order you enter the URLs. Up to 128 URLs can be added.

```
SGOS# (config) streaming windows-media broadcast-alias alias url
```

Example 2

This example demonstrates the following:

- creates a simulated live file called *bca*
- plays back *mms://ocs.bca.com/bca1.asf* and *mms://ocs.bca.com/bca2.asf*
- configures the ProxySG to play back the content twice
- sets a starting date and time of today at 4 p.m., 6 p.m., and 8 p.m.

Section B: Configuring Streaming Media

```
SGOS# (config) streaming windows-media broadcast-alias bca  
mms://ocs.bca.com/bca1.asf 2 today 4pm,6pm,8pm  
SGOS# (config) streaming windows-media broadcast-alias bca  
mms://ocs.bca.com/bca2.asf
```

To Delete Simulated Live Content:

```
SGOS# (config) streaming windows-media no broadcast-alias alias
```

ASX Rewriting (Windows Media)

This section describes ASX rewriting and applies to Windows Media only.

About ASX Rewrite

The ProxySG provides proxy support for Windows Media Player 6.4, although the player itself does not support the specification of explicit proxies using the MMS protocol.

If your environment does not use a Layer 4 switch or the Cisco Web Cache Control Protocol (WCCP), the ProxySG can operate as a proxy for Windows Media Player 6.4 clients by rewriting the Windows Media metafile (which contains entries with URL links to the actual location of the streaming content) to point to the appliance rather than the Windows Media server. The metadata files can have .asx, .wvx, or .wax extensions, but are commonly referred to as .asx files. The .asx file refers to the actual media files (with .ASF, .WMV, and .WMA extensions). An .asx file can refer to other .asx files, although this is not a recommended practice. If the file does not have one of the metafile extensions and the Web server that is serving the metadata file does not set the correct MIME type, it will not be processed by the Windows Media module. Also note that the .asx file with the appropriate syntax must be located on an HTTP (not Windows Media) server.

The ASX rewrite module is triggered by either the appropriate file extension or the returned MIME type from the server (x-video-asf).

Note: If an .asx file syntax does not follow the standard <ASX> tag-based syntax, the ASX rewrite module is not triggered.

For the ProxySG to operate as a proxy for Windows Media Player 6.4 requires the following:

- The client is explicitly proxied for HTTP content to the ProxySG that will rewrite the .asx metafile.
- The streaming media ProxySG is configurable.

Note: Windows Media Player automatically tries to roll over to different protocols according to its Windows Media property settings before trying the rollover URLs in the .asx metafile.

With the `asx-rewrite` command, you can implement redirection of the streaming media to a ProxySG by specifying the rewrite protocol, the rewrite IP address, and the rewrite port.

The protocol specified in the ASX rewrite rule is the protocol the client uses to reach the ProxySG. You can use forwarding and policy to change the default protocol specified in the original .asx file that connects to the origin media server.

Section B: Configuring Streaming Media

When creating ASX rewrite rules, you need to determine the number priority. It is likely you will create multiple ASX rewrite rules that affect the .asx file; for example, rule 100 could redirect the IP address from 10.25.36.01 to 10.25.36.47, while rule 300 could redirect the IP address from 10.25.36.01 to 10.25.36.58. In this case, you are saying that the original IP address should be redirected to the IP address in rule 100. If that IP address is not available, the ProxySG looks for another rule matching the incoming IP address.

Notes and Limitations

Before creating rules, consider the following.

- Each rule you create must be checked for a match; therefore, performance might be affected if you create large amounts of rules.
- Lower numbers have a higher priority than high numbers.

Note: Rules can only be created through the CLI.

- ASX rewrite rules configured for multiple ProxySGs configured in an HTTP proxy-chaining configuration can produce unexpected URL entries in access logs for the *downstream* ProxySG (the ProxySG that the client proxies to). The combination of proxy-chained ProxySGs in the HTTP path coupled with ASX rewrite configured for multiple ProxySGs in the chain can create a rewritten URL requested by the client in the example form of:

```
protocol1://downstream_SecApp/redirect?protocol2://<upstream_SecApp>/redirect?protocol3://origin_host/origin_path
```

In this scenario, the URL used by the downstream ProxySG for caching and access logging may be different than what is expected. Specifically, the downstream ProxySG creates an access log entry with protocol2://upstream_SecApp/redirect as the requested URL. Content is also cached using this truncated URL. Blue Coat recommends that the ASX rewrite rule be configured for only the downstream ProxySG, along with a proxy route rule that can forward the Windows Media streaming requests from the downstream to upstream ProxySGs.

Syntax for the asx-rewrite command:

```
asx-rewrite rule # in-addr cache-proto cache-addr [cache-port]
```

where:

- *in-addr*—Specifies the hostname or IP address delivering the content
- *cache-proto*—Specifies the rewrite protocol on the ProxySG. Acceptable values for the rewrite protocol are:
 - mmsu specifies Microsoft Media Streaming UDP
 - mmst specifies Microsoft Media Streaming TCP
 - http specifies HTTP
 - mms specifies either MMS-UDP or MMS-TCP
 - * specifies the same protocol as in the .asx file

Section B: Configuring Streaming Media

If the .asx file is referred from within another .asx file (not a recommended practice), use a * for the *cache-proto* value. This specifies that the protocol specified in the original URL will be used. As a conservative, alternative approach, you could use HTTP for the *cache-proto* value.

- *cache-addr*—Specifies the rewrite address on the ProxySG.
- *cache-port*—Specifies the port on the ProxySG. This value is optional.

To set up the .asx rewrite rules through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) streaming windows-media asx-rewrite number in-addr cache-proto  
cache-addr cache-port
```

Note: To delete a specific rule, enter `streaming windows-media no asx-rewrite number`.

To ensure that an ASX rewrite rule has been modified immediately, clear the local browser cache.

Example

This example:

- Sets the priority rule to 200
- Sets the protocol to be whatever protocol was originally specified in the URL and directs the data stream to the appropriate default port.
- Provides the rewrite IP address of 10.9.44.53, the ProxySG.

```
SGOS#(config) streaming windows-media asx-rewrite 200 * * 10.9.44.53
```

Note: ASX files must be fetched from HTTP servers. If you are not sure of the network topology or the content being served on the network, use the asterisks to assure the protocol set is that specified in the URL.

ASX Rewrite Incompatibility With Server-side NTLM Authentication

Server-side authentication (MMS only, not HTTP) is supported if the origin media server authentication type is BASIC or No Auth. However, if you know that a Windows Media server is configured for NTLM authentication, the following procedure allows you to designate any virtual IP addresses to the NTLM authentication type. If you know that all of the activity through the ProxySG requires NTLM authentication, you can use the IP address of the appliance.

To Designate an IP Address to an Authentication Type through the CLI:

1. If necessary, create a virtual IP address that will be used to contact the Windows Media server.
2. At the (config) prompt, enter the following command:

```
SGOS#(config) streaming windows-media server-auth-type ntlm ip_address
```
3. Configure the ASX rewrite rule to use the IP address.

Section B: Configuring Streaming Media

- a. To remove the authentication type designation:

```
SGOS#(config) streaming windows-media no server-auth-type ip_address
```

- b. To return the authentication type to BASIC:

```
SGOS#(config) streaming windows-media server-auth-type basic ip_address
```

About Fast Streaming (Windows Media)

Note: This feature applies to Windows Media only.

Windows Media Server version 9 contains a feature called Fast Streaming that allows clients to provide streams with extremely low buffering time.

SGOS 3.2.x supports the following functionality for both cached and uncached content:

- Fast Start
- Fast Cache

Fast Recovery and Fast Reconnect are currently not supported.

Section C: Windows Media Player

Section C: Windows Media Player

This section describes how to configure the Windows Media Player client and describes associated limitations and access log conventions.

Configuring Windows Media Player

To apply the ProxySG Windows Media streaming services, Windows Media Player 6.4 or higher must be installed and configured to use explicit proxy.

Note: If using Windows Media Player 6.4, you must define the HTTP explicit proxy.

MMS explicit proxy is defined with the `asx-rewrite` command (discussed earlier in this chapter) or with CPL (`url_host_rewrite`).

Note: The example below uses Windows Media Player 9.0. Installation and setup varies with different versions of Windows Media Player.

To Configure Windows Media Player:

1. Start Windows Media Player.
2. Select Tools>Options>Network.

The Network tab displays.

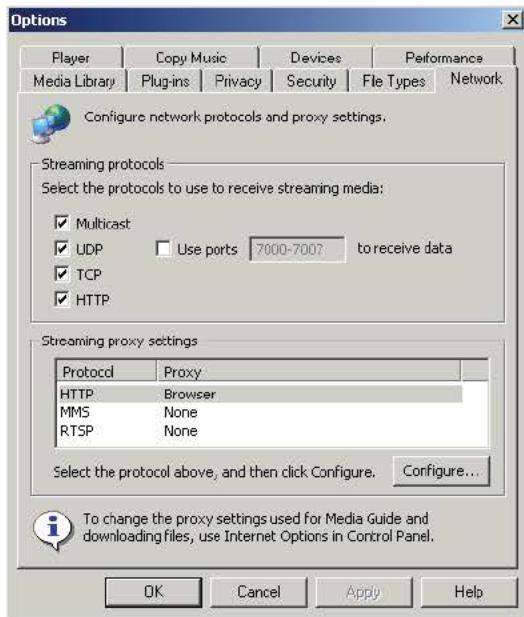


Figure 15-2: Configuring Windows Media Player Proxy

Section C: Windows Media Player

3. In the Streaming proxy settings section, select MMS and click Configure. The Configure Protocol window displays for the selected protocol.
4. Select Use the following proxy server and enter the ProxySG IP address and the port number used for the explicit proxy (the default MMS port is 1755).
5. Click OK; click OK again to close the Options dialog.

Limitations

This section describes Windows Media Player limitations that might affect performance.

Striding Limitations

When you use the Windows Media Player, consider the following limitations in regard to using fast forward and reverse (referred to as *striding*):

- If you request a cached file and repeatedly attempt play and fast forward, the file freezes.
- If you attempt a fast reverse of a cached file that is just about to play, you receive an error message, depending on whether you have a proxy:
 - Without a proxy: A device attached to the system is not functioning.
 - With a proxy: The request is invalid in the current state.
- If Windows Media Player is in pause mode for more than ten minutes and you press fast reverse or fast forward, an error message displays: The network connection has failed.

Other Limitations

- Applies to Version 6.4 only: for ASX rewriting to occur, the player must be configured to use the ProxySG as the HTTP proxy. Configuring the browser only as the HTTP proxy is not sufficient.
- Applies to Versions 6.4 and 9: if a `url_host_rewrite` rule is configured to rewrite a host name that is a domain name instead of an IP address, a request through the MMS protocol fails and the host is not rewritten. As the connect message sent by the player at the initial connection does not contain the host name, a rewrite cannot occur. HTTP requests are not affected by this limitation.
- If explicit proxy is configured and the access policy on the ProxySG is set to `deny`, a requested stream using HTTP from Windows Media Player 9 serves the stream directly from the origin server even after the request is denied. The player sends a request to the OCS and plays the stream from there.

Blue Coat recommends the following policy:

```
<proxy>
  streaming.content=yes deny
-or-
<proxy>
  streaming.content=windows_media deny
```

Section C: Windows Media Player

The above rules force the HTTP module to hand-off HTTP requests to the MMS module. MMS returns the error properly to the player, and does not go directly to the origin server to try to server the content.

- If you request an un-cached file using the HTTP protocol, the file is likely to stop playing if the authentication type is set to BASIC or NTLM and you initiate rapid seeks before the buffering begins for a previous seek. The Windows Media Player, however, displays that the file is still playing.
- If a stream is scheduled to be accessible at a future time (using a simulated live rule), and the stream is requested before that time, the Windows Media Player enters a waiting stage. This is normal. However, if HTTP is used as the protocol, after a minute or two the Windows Media Player closes the HTTP connection, but remains in the waiting stage, even when the stream is broadcasting.

Note: For authentication-specific limitations, see "Windows Media Player Authentication Limitations".

Windows Media Access Log Formats

See Appendix B: "Access Log Formats" on page 751.

Section D: RealPlayer

Section D: RealPlayer

This section describes how to configure Real Player and describes associated limitations and access log formats.

Configuring RealPlayer

To use the ProxySG Real Media streaming services with an explicit proxy configuration, the client machine must have RealPlayer installed and configured to use RTSP streams. If you use transparent proxy, no changes need to be made to the RealPlayer.

To Configure RealPlayer:

Note: This procedure features RealOne Basic, version 2.0. Installation and setup menus vary with different versions of RealPlayer. Refer to the RealPlayer documentation to configure earlier versions of RealPlayer.

1. Start RealPlayer.
2. Select Tools>Preferences.

The Preferences dialog appears.

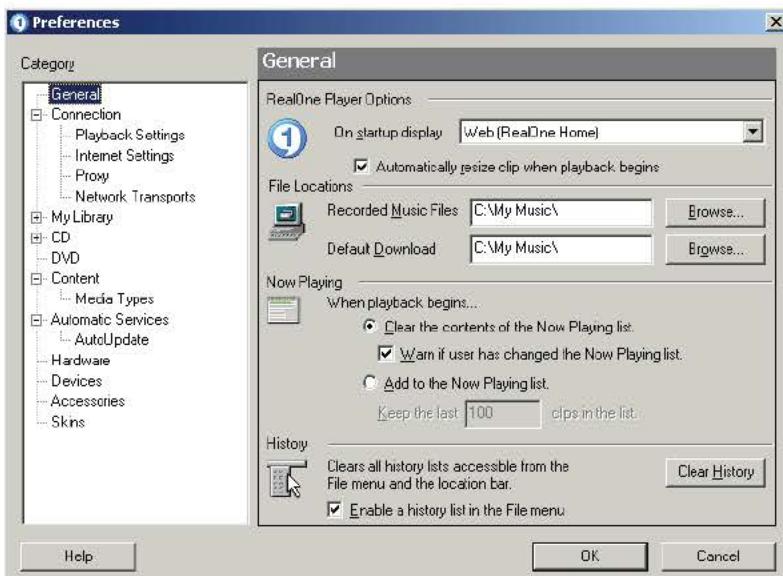


Figure 15-3: RealOne Preferences Dialog

3. Click Proxy. In the Streaming Setting section, click Change Settings; the Streaming Proxy Settings dialog appears.
4. In the PNA and RTSP proxies: field, click Use Proxies and in the RTSP field enter the IP address of the proxy ProxySG. Also enter the RTSP port number (the default is 554).

Section D: RealPlayer

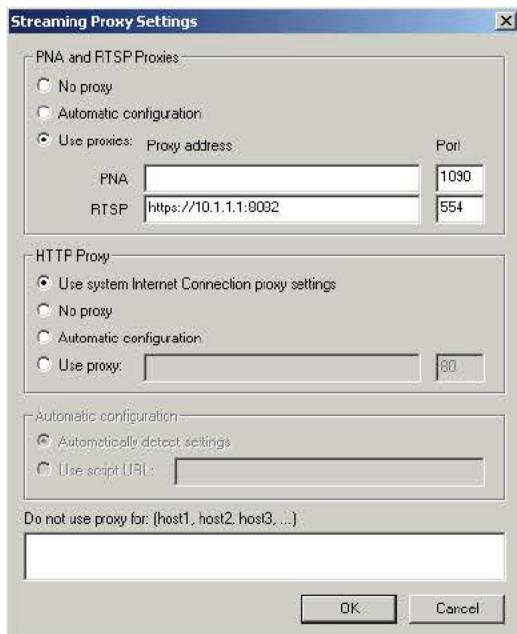


Figure 15-4: Configuring the RealPlayer to Proxy through the ProxySG

These settings must match the settings configured in the ProxySG. If you change the ProxySG explicit proxy configuration, you must also reconfigure the RealPlayer.

5. For HTTP Proxy, if you have an HTTP proxy already configured in your browser, select Use system Internet Connection proxy settings.

Note: If using transparent proxy, RTSP port 554 is set by default and cannot be changed.

6. In the Do not use proxy for: section, you can enter specific hosts and bypass the ProxySG.

Note: This can also be accomplished with policy, which is the recommended method.

7. Click OK to close the Streaming Proxy Settings dialog.
8. To configure RealPlayer transport settings, select Network Transports.
9. Click RTSP Settings.

The RTSP Transport Settings dialog appears.

Section D: RealPlayer

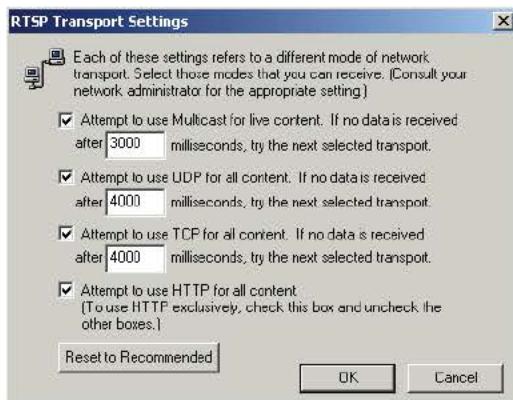


Figure 15-5: Configuring RealPlayer RTSP Transport Settings

10. Click the appropriate boxes based on your network configuration. For example, if your firewall does not accept UDP, select Attempt to use TCP for all content. Blue Coat recommends using the default settings.
11. Click OK.
12. To allow the creation of access log entries, RealPlayer must be instructed to communicate with the RealServer. Perform one of the following or both as necessary:
 - RealPlayer 8—Select View>Preferences>Support; click Send connection-quality data to RealServers; click OK.
 - RealOne Player—Select Tools>Preferences>Internet Settings; in the Internet Settings field, click Send connection-quality data to RealServers; click OK.

Real Media Access Log Formats

See Appendix B: "Access Log Formats" on page 751.

Limitations and Known Issues

For authentication-specific limitations, see "Real Media Player Authentication Limitation" on page 496.

Section E: QuickTime Player

Section E: QuickTime Player

This section describes how to configure the QuickTime client and describes associated limitations and access log formats.

Configuring QuickTime Player

This section describes how to configure the QuickTime player for explicit proxy to the ProxySG.

To Configure QuickTime:

1. Select **Edit>Preferences>QuickTime Preferences**.

The QuickTime Settings dialog appears.



Figure 15-6: Configuring the QuickTime Client Proxy

2. Deselect **Use System Settings**.
3. Select **RTSP proxy server**; enter the IP address of the ProxySG to connect to and the port number (554 is the default).
These settings must match the settings configured in the ProxySG. If you change the ProxySG explicit proxy settings, set similar settings in RealPlayer.
4. Close the dialog.

QuickTime Access Log Formats

See Appendix B: "Access Log Formats" on page 751.

Limitations

For authentication-specific limitations, see "QuickTime Proxy Authentication" on page 496.

Section E: QuickTime Player

Access Log Format

See Appendix B: “Access Log Formats” on page 751.

Section E: QuickTime Player

Chapter 16: Instant Messaging

This chapter discusses how to control Instant Messaging (IM) activity through the ProxySG.

About Securing Instant Messaging

Instant Messaging usage in an enterprise environment creates security concerns because regardless of how network security is configured, IM connections can be made from any established protocol, such as HTTP or SOCKS, on any open port. Because it is common for coworkers to use IM to communicate, especially in remote offices, classified company information can be exposed outside the network. Viruses and other malicious code can also be introduced into the network from file sharing through IM clients.

The ProxySG serves as an IM proxy. You can control IM actions by allowing or denying IM communications and file sharing based on users (both employee identities and IM handles), groups, file types and names, and other triggers. All IM communications can be logged and archived for review.

The ProxySG supports the AOL, MSN, and Yahoo IM protocols.

Recommended Deployments

For large networks with unimpeded Internet access, Blue Coat Systems recommends transparently redirecting the IM protocols to the ProxySG, which requires the ProxySG bridging feature or an L4 switch or WCCP.

For networks that do not allow outbound access, Blue Coat recommends using the SOCKS proxy and configuring policy and content filtering denials for HTTP requests to IM servers.

About the Instant Messaging Protocol Services

The ProxySG accepts connections for the supported IM protocols on ports specified in services. The following are the default service ports (transparent, but disabled):

- AOL-IM: 5190
- MSN-IM: 1863 and 6891
- Yahoo-IM: 5050 and 5101

These ports are disabled by default.

MSN port 1863 and Yahoo port 5050 are the default client login ports. MSN port 6891 and Yahoo port 5101 are the default for client-to-client direct connections and file transfers. If these ports are not enabled:

- Client-to-client direct connections do not occur.
- After a file transfer request is allowed by the ProxySG, the resulting data is sent directly from one client to another without passing through the ProxySG:

- For MSN: The above bullet point only applies to MSN version previous to and including 6.0. Post-6.0 versions use a dynamic port for file transfers; therefore, port 6891 is not required for the ProxySG to intercept file transfers.
- For Yahoo: The above bullet only applies to standard file transfer requests. Port 5101 must be enabled to allow file list requests.

Note: All file transfers for AOL clients are handled through the default (5190) or specified client login port.

To enable a default IM port or configure additional IM services, see Chapter 5: “Managing Port Services” on page 113.

About HTTP Proxy Support

SGOS 3.2 supports instant messaging through HTTP proxy. IM clients can be configured to connect to IM services through HTTP, which allows IM activity from behind restrictive firewalls.

Before SGOS 3.2, HTTP IM communications were passed through the ProxySG. The ProxySG now supports HTTP proxy for Yahoo, MSN, and AOL IM clients, including application of policies and IM activity logging. This is accomplished by the HTTP proxy handing off IM communications to the IM proxy.

Limitations

- Certain IM clients can experience reduced functionality when using HTTP proxy. For example, AOL IM disables direct IM and file transfers when connecting through an HTTP proxy.

Note: Configuring HTTP proxy in the client configuration does not guarantee IM clients use HTTP proxy. An MSN client always attempts to connect to the service using its native protocol. If this fails, it fails over to use the configured HTTP proxy. AOL and Yahoo, however, always use their configured proxy regardless if the native proxy is available.

- AOL—Direct connections, file transfers, and files sharing are not available. AOL and Yahoo, however, always use their configured proxy regardless if the native proxy is available.
- Yahoo—Client cannot create a chat room.

About Instant Messaging Reflection

IM reflection allows you to contain IM traffic within the enterprise network, which further reduces the risk of exposing company-confidential information through public IM networks. Normally, an IM sent from one buddy to another is sent to and from an IM service. With IM reflection, IM traffic between buddies, including chat messaging, on the same network never has to travel beyond the ProxySG. This includes IM users who login to two different ProxySG appliances configured in a hierarchy (proxy chaining).

IM Reflection Diagrams

The following diagrams depict how the ProxySG manages IM reflection.

IM Reflection with Fail Open

The following diagram demonstrates IM reflection deployment with fail open on a ProxySG that is configured to attempt to reflect all IM activity. IM clients 1 and 2 logged into the same ProxySG, while client 3 is outside the network. IM activity between clients 1 and 2 are reflected by the ProxySG; IM activity between clients 1 and 3 are forwarded to the IM service provider for normal delivery.

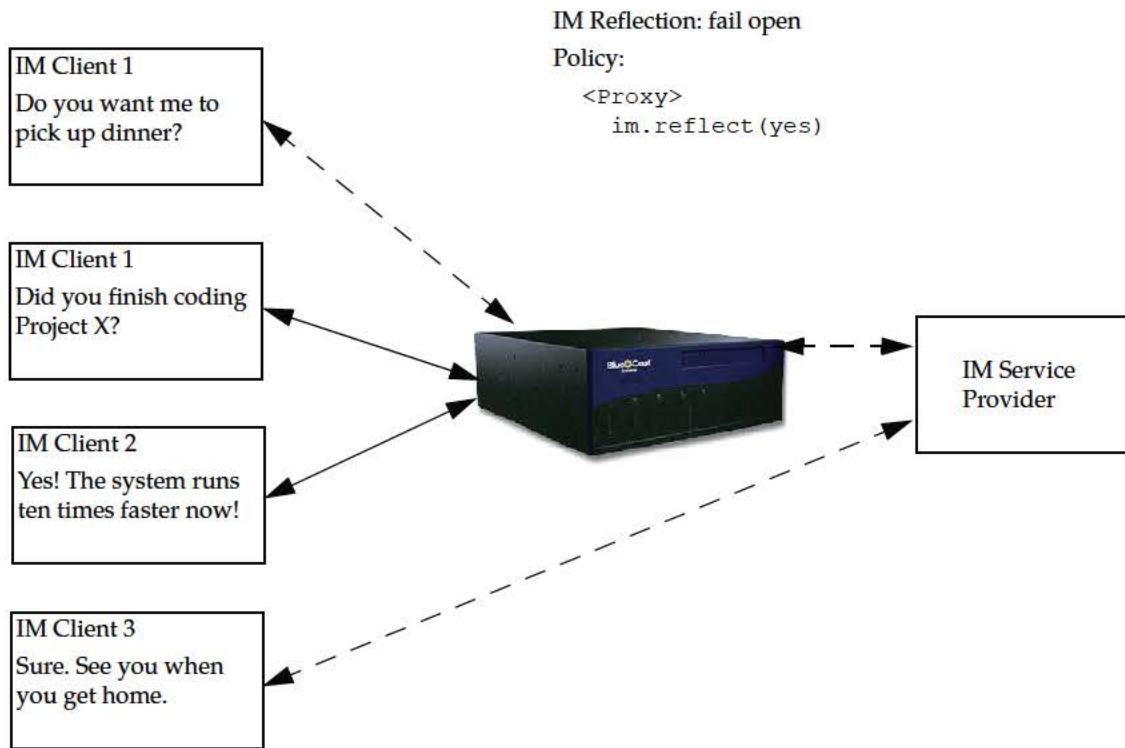


Figure 16-1: IM Reflection with Fail Open

IM Reflection With Fail Closed

By adding a policy rule to deny IM service to clients not logged into the ProxySG, client 1 receives a denial of service message when trying to message client 3.

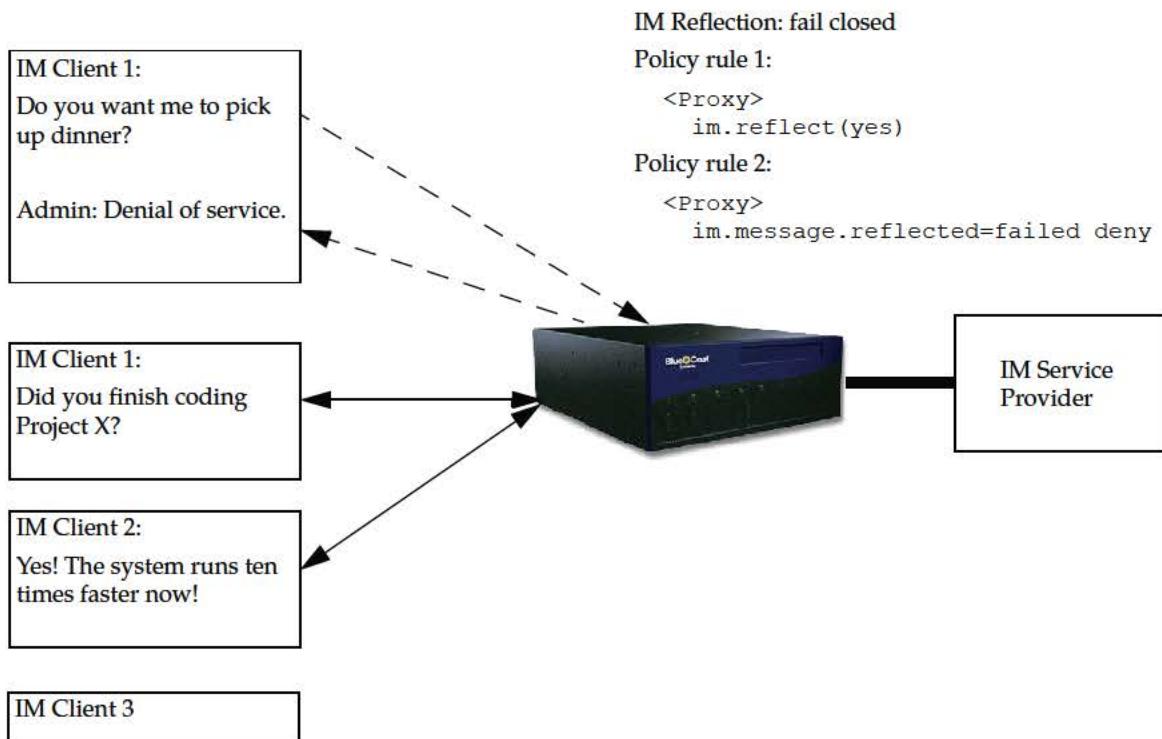


Figure 16-2: IM Reflection with Fail Closed

IM Reflection With A Hierarchy Of Proxies

Larger enterprise networks have users logging in through different primary ProxySG appliances. IM reflection is still possible by using SOCKS and HTTP forwarding, policy, and a ProxySG hierarchy.

Consider the following deployment. IM Clients 1 and 2 are located on the same main campus, but log into different primary ProxySG appliances, PSG 1 and PSG 2, which proxy to the intermediate ProxySG, PSG 3. IM Client 3 is an employee in a remote location and logs into PSG 4. PSG 5 is the corporate root appliance. IM Client 4 is a buddy of IM Client 2, but is not on the employee network.

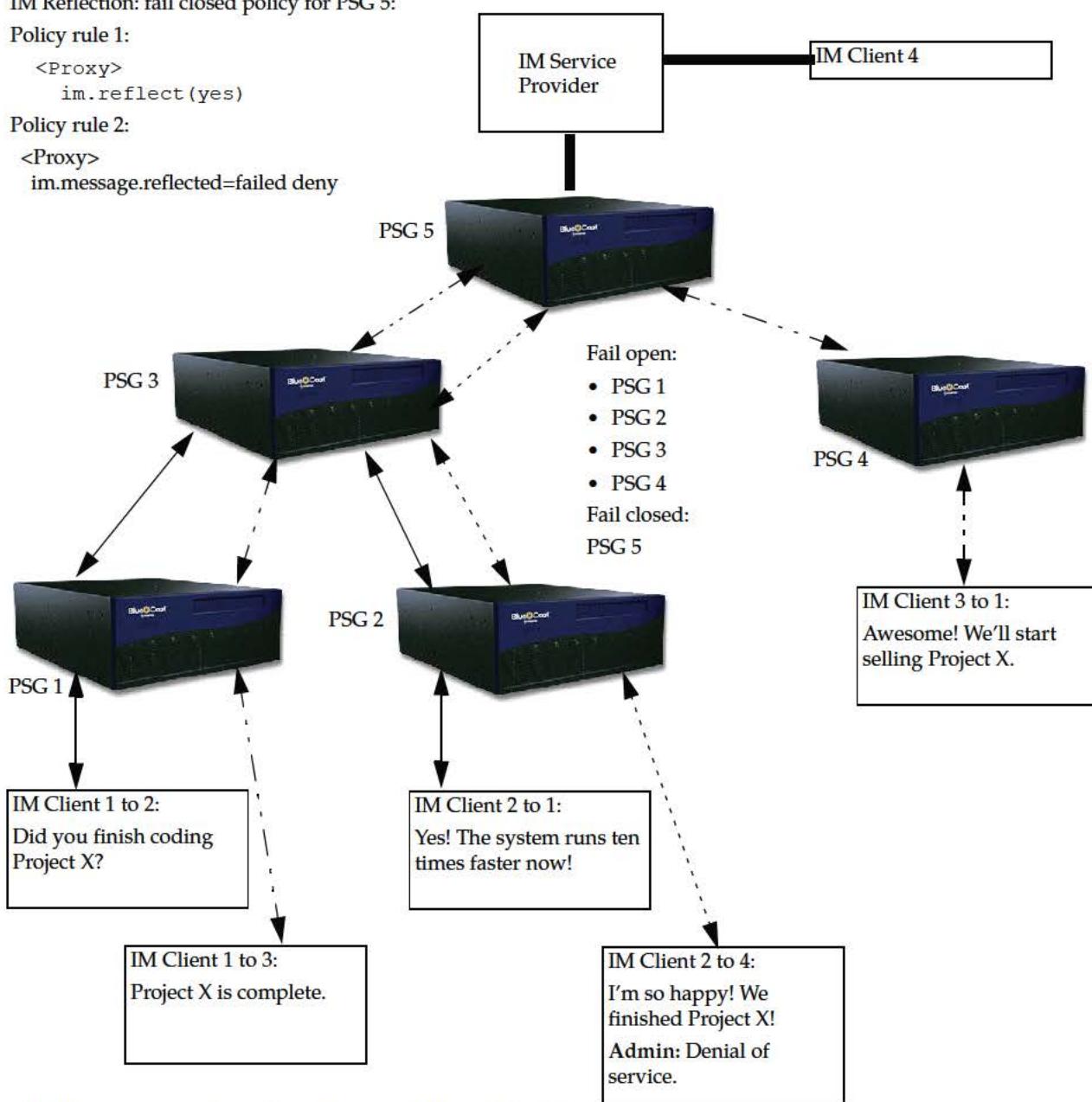
IM Reflection: fail closed policy for PSG 5:

Policy rule 1:

```
<Proxy>
im.reflect(yes)
```

Policy rule 2:

```
<Proxy>
im.message.reflected=failed deny
```



IM Reflection: proxy hierarchy, fail closed policy for PSG 1-4:

```
define condition "IM protocols" client.protocol=(aol-im,msn-im,yahoo-im) end
condition "IM protocols"
```

```
<Forward>
condition="IM protocols" socks_gateway(gateway_1) socks_gateway.fail_open(no)
```

Figure 16-3: IM Reflection with SOCKS Forwarding in a Proxy Hierarchy

Each primary and intermediate ProxySG (PSGs 1, 2, 3, and 4) forward IM traffic that is not reflectable (policy to fail open) to the next ProxySG in the chain. If the next ProxySG services the appropriate IM client, the message is reflected and delivered. The root ProxySG, PSG 5, has a policy to fail closed. Therefore, all IM traffic forwarded to it that cannot be reflected, such as IM Client 2's attempt to contact IM Client 4, is denied access to the public IM service.

Further policy fine-tuning can allow or disallow IM forwarding based on other triggers. For example, the group Corp-Market can send messages to anyone inside or outside the network, but all other groups are prohibited from sending messages to the outside.

About Instant Messaging Proxy Authentication

The ProxySG supports explicit proxy authentication if explicit SOCKS V5 proxy is specified in the IM client configuration.

Because the IM protocols do not support proxy authentication natively, authentication for transparently redirected clients is not supported because policies requiring authentication would deny transparently redirected clients.

HTTP Proxy Limitations

The following proxy authentication limitations apply to IM clients using HTTP proxy:

- AOL IM—Proxy authentication is supported.
- MSN IM (5.0 and above)—While the MSN IM client does support user credentials, it cannot respond to HTTP proxy authentication requests from the ProxySG and the MSN passport service login fails. You can, however, add policy to pass-through the traffic to the MSN passport.com site without requiring authentication.
- Yahoo IM—Yahoo IM clients do not have proxy authentication configuration abilities.

Securing AOL Encryption Capability

This section describes AOL encryption capabilities and how to manage them with ProxySG policy.

About AOL Encryption

AOL IM provides the option for clients to send encrypted messages through both standard messaging (through a service) and direct connection messaging. While this encryption benefits IM users, it provides a security risk for corporate network administrators implementing a communication policy through a proxy. Encryption-capable AOL IM buddies can enable encryption and communicate. Because the ProxySG cannot decrypt these communications, policy cannot be applied and sensitive material can be transferred between buddies without a denial of service or access logging for key-word matching. The ProxySG also cannot replace or append encrypted text, rendering that IM proxy feature useless.

To allow unabated proxy control of IM traffic, SGOS 3.2 can strip the encryption capabilities from AOL and Trillian IM clients. While this might appear counter-intuitive to securing communications, greater security and control are gained from the ability to apply policy to message content and to log communications. Determine the need to strip encryption based on your enterprise proxy requirements.

Note: If encryption is blocked, the service does not recognize the logged-in IM client as capable of encryption. If a proxied client attempts to create a chatroom with encryption on, the client receives a create error. This behavior is expected.

Policy for Stripping AOL Encryption

The policy property is only applicable to the im.method=login trigger; other properties are not affected. Once encryption stripping is enabled, any existing encryption capabilities and certificates are stripped when a client logs in, and the IM service recognizes the clients as not able to send encrypted messages.

VPM

In a Web Access Layer, select Block IM Encryption in the Action column.

CPL

Add the following property to the policy file:

```
<Proxy>
    im.block_encryption(yes)
```

Instant Message Proxies

This section discusses the IM proxy behavior and configurations on the ProxySG.

Configuring Instant Message DNS Redirection

The ProxySG can be configured as an IM proxy that performs a DNS redirection for client requests. This provides greater control because it prevents IM clients from making outside connections.

The IM clients provide the DNS lookup to the IM server, which the ProxySG DNS module uses to connect to the IM server. To the client, the ProxySG appears to be the IM server. A virtual IP address used only for IM must be configured, as it is used to represent the IM server address for all IM protocols.

To Configure Instant Message DNS Redirection through the Management Console:

1. Create a virtual IP address to be used for IM DNS redirection through the ProxySG. Navigate to Configuration>Network>Advanced>VIPs.
2. Select Configuration>Services>IM Proxies>IM Proxy Settings.
3. In the General Settings field, select the configured VIP from the Explicit Proxy Virtual IP drop-down list.
4. In the Protocol Settings field, select an IM protocol to define: AOL, MSN, or Yahoo. Once selected, the appropriate host fields display below. Each field contains the default hosts used by clients to connect to the IM service.
 - AOL: Native IM Host, HTTP IM Host, and Direct IM Proxy Host.
 - MSN: Native IM Host and HTTP IM Host.

- Yahoo: Native IM Host, HTTP IM Host, HTTP Chat Host, Upload Host, and Download Host.

Important: Only edit these hosts if the client experiences a change in its hardcoded value.

To Configure Instant Message DNS Redirection through the CLI:

At the `(config)` prompt, enter the following commands:

```
SGOS#(config) virtual-ip address  
SGOS#(config) im explicit-proxy-vip address
```

where `address` is the same VIP defined with the previous command.

```
SGOS#(config) im host
```

where `host` is:

```
aol-direct-proxy-host host  
aol-http-host host  
aol-native-host host  
msn-http-host host  
msn-native-host host  
yahoo-download-host host  
yahoo-http-host host  
yahoo-http-chat-host host  
yahoo-native-host host  
yahoo-upload-host host
```

To view the current default or configured hosts, enter the `show im` command.

Configuring Instant Message Alert Settings

This section describes how to configure the IM proxy settings on the ProxySG. You can assign an administrator buddy name for each client type, and determine how exception messages are sent.

An administrator buddy name can be a registered name user handle or a fictitious handle. The benefit of using a registered name is that users can send IM messages to the administrator directly to report any issues, and that communication can be logged for tracking and record-keeping.

To Configure the IM Proxy Setting through the Management Console:

1. Select Configuration>Services>IM Proxies>IM Alert Settings.

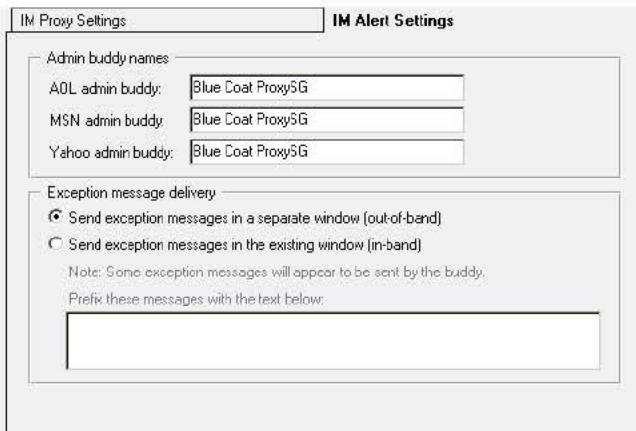


Figure 16-4: The IM Proxy Screen

2. In the Admin buddy names field, enter the handle or handles for the administrator.
3. In the Exception message delivery field, select the method that exception messages are delivered to IM users.
 - Send exception messages in a separate window (out-of-band)—if an exception occurs, the user receives the message in a separate IM window.
 - Send exception messages in the existing window (in-band)—If an exception occurs, the message appears in the same IM window.

If in-band is selected, the message appears to be sent by the buddy on the other end, with the exception that when in a chat room, the message always appears to be sent by the configured Admin buddy name. You can enter a prefix message that appears in the client window before the message. For example: "From the Company Administrator: Inappropriate IM use. Refer to Employee Conduct Handbook concerning Internet usage."

Note: Regardless of the IM exception delivery configuration, IM alert messages triggered by policy based on certain protocol methods are always sent out-of-band because a specific buddy is not associated.

4. Click Apply.

To Configure the IM Proxy Setting through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) im [aol | msn | yahoo]-admin-buddy admin_handle
```

Specifies the handle or handles for the administrator; configure for each IM client type.

```
SGOS#(config) im exceptions [in-band | out-of-band]
```

Specifies the method the exception messages are delivered to IM users. If in-band is selected, enter the following command to specify a prefix message:

```
SGOS# (config) im buddy-spoof-message text
```

Configuring Instant Messaging HTTP Handoff

IM Handoff allows the Blue Coat HTTP proxy to handle requests from supported IM protocols. If IM HTTP handoff is disabled, requests are passed through, and IM-specific policies are not applied.

Handoff should be enabled (the default) if you write IM policy.

If you want to allow a specific IM client to connect through HTTP through the ProxySG and that IM protocol has not been licensed, disable IM HTTP handoff to allow the traffic to be treated as plain HTTP traffic and to avoid an error in the licensing check done by the IM module. This might be also be necessary to temporarily pass through traffic from new versions of IM clients that are not yet supported by Blue Coat.

To Disable Instant Messaging HTTP Handoff through the Management Console:

1. Select Configuration>Services>IM Proxies>IM Proxy Settings.
2. Deselect Enable HTTP Handoff.

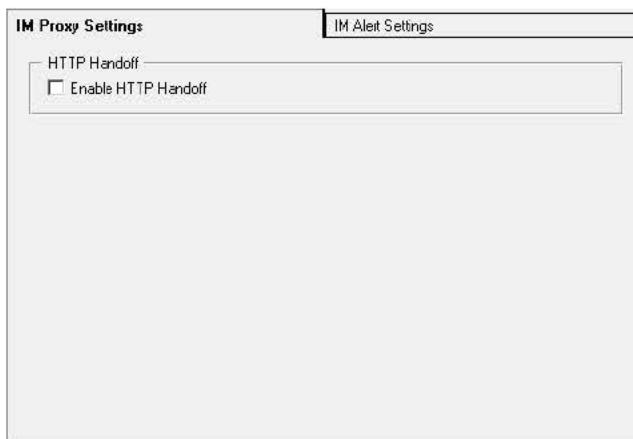


Figure 16-5: Disabling IM HTTP Handoff

To Disable Instant Messaging HTTP Handoff through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) im http-handoff disable
```

Configuring Instant Messenger Clients

This section describes how to configure the IM clients to send traffic through the ProxySG.

General Configuration

As each IM client has different menu structures, the procedures to configure them differ. This section provides the generic tasks that need to be completed.

Explicit Proxy

Perform the following tasks on the IM client:

1. Navigate to the Connection Preferences dialog.
2. Select Use Proxies.
3. Select proxy type as SOCKS V5.
4. Enter the ProxySG IP address.
5. Enter the SOCKS port number; the default is 1080.
6. Enter authentication information, if required.

Transparent Proxy

IM clients do not require any configuration changes for transparent proxy. An L4 switch or inline ProxySG routes the traffic.

Yahoo Messenger Client Explicit Proxy Configuration Screen

The following example configures a Yahoo Messenger client for explicit proxy.

1. Select Login>Preferences>Connection.
2. Click Connection.
3. Select Use proxies.
4. Select Enable SOCKS proxy; select Ver 5.
5. Enter the server name.
6. Enter the port number (the default is 1080).
7. If authentication is required on the ProxySG, enter the authentication user name and password.

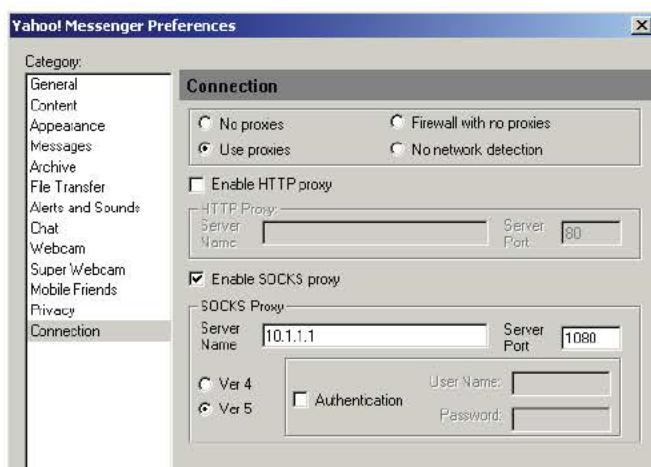


Figure 16-6: Yahoo IM Client Explicit Proxy Configuration

Notes

If Yahoo Messenger is configured for explicit proxy (SOCKS) through the ProxySG, the IM voice chat feature is disabled. Any client attempting a voice chat with a client behind the ProxySG firewall receives an error message. The voice data stream is carried by default on port 5001; therefore, you can create and open this port and configure Yahoo IM to use transparent proxy. However, the ProxySG only supports the voice data in pass-through mode.

AOL Messenger Client Explicit Proxy Configuration Screen

The following example configures an AOL Messenger client for explicit proxy.

1. Select My AIM>Edit Options>Edit Preferences>Sign On/Off.
2. Click Connection.
3. Select Connect using proxy.
4. Select SOCKS 5.
5. Enter the server name.
6. Enter the port number (the default is 1080).
7. If authentication is required on the ProxySG, enter the authentication user name and password.

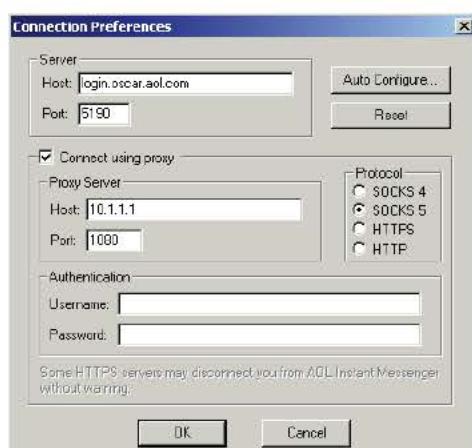


Figure 16-7: AOL IM Client Explicit Proxy Configuration

MSN Messenger Client Explicit Proxy Configuration Screen

The following example configures an MSN Messenger client for explicit proxy.

1. Select Tools>Options.
2. Click Connection.
3. Select I use a proxy server.
4. Select SOCKS Version 5.
5. Enter the server name.

6. Enter the port number (the default is 1080).
7. If authentication is required on the ProxySG, enter the authentication user name and password.

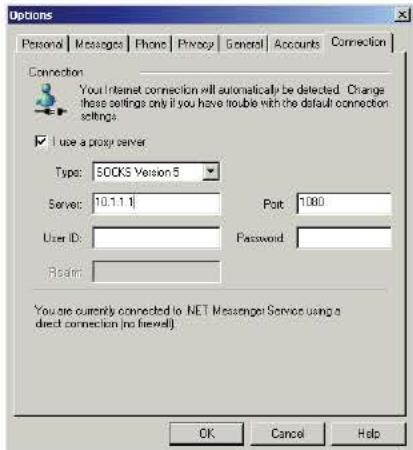


Figure 16-8: MSN IM Client Explicit Proxy Configuration

VPM Examples

Once the IM clients are configured to send traffic through the ProxySG, you can control and limit IM activity. The Visual Policy Manager (VPM) allows you to create rules that control and track IM communications, including IM activities based on users and groups, IM handle, chat room handle, file name, and other triggers.

To learn about the VPM, see Chapter 13: "The Visual Policy Manager".

Example 1: File Transfer

The following example demonstrates an IM rule created with the VPM that IM handle Nigel1 can perform a file transfer at any time, but the file must be between 1 and 5 MB in size, and the handle, the file path, and file size are logged:

1. In the VPM, select Policy>Add Web Access Layer; name it IM_FileTransfer.
2. Right-click the Source field; select Set. The Set Source Object dialog appears.
3. Click New; select IM User. The Add IM User Object dialog appears.
4. In the IM User field, enter Nigel1; click OK in each dialog.
5. Right-click the Service field; select Set. The Set Service Object dialog appears.
6. Click New; select IM File Transfer. The Add IM File Transfer dialog appears.
7. Select Size and enter a range 1 and 5; select MBytes from the drop-down list; click OK in each dialog.
8. Right-click the Track field; select Set. The Add Track Object dialog appears.
9. Click New; select Event Log. The Add Event Log Object dialog appears.

10. From the Substitution Variables list, select x-im-buddy-name and click insert. Repeat for x-im-file-path and x-im-file-size. Click OK in each dialog.
11. Click Install Policy.

Example 2: Send an IM Alert Message

The following example demonstrates a rule created with the VPM that informs all IM users when they login that their IM activity is tracked and logged.

1. In the VPM, select Policy>Add Web Access Layer; name it IM_NotifyMessage.
2. Right-click the Service field; select Set. The Set Service Object dialog appears.
3. Click New; select Protocol Methods. The Add Methods Object dialog appears.
4. From the Protocol drop-down list, select Instant Messaging.
5. Click Login/Logout; LOGIN; click OK to close the dialog; click OK to insert the object in the rule.
6. Right-click the Service field; select Set. The Set Service Object dialog appears.
7. Click New; select Send IM Alert. The Add Send IM Alert Object dialog appears.
8. In the Alert Text field, enter a message that appears to users. For example, Notice: Your Instant Messaging message activity is tracked and logged.
9. Click OK to close the dialog; click OK to insert the object in the rule.

Statistics

The IM statistics allow you to track IM connections, file transfers, and messages that are currently in use and in total, or have been allowed and denied. The information can be displayed for each IM client type or combined.

IM Connection Data Tab

The following IM Connection Data statistics indicate current and overall connection data since the last statistics clear:

- Native Clients—The number of native IM clients connected.
- HTTP Clients—The number of HTTP IM clients connected.
- Chat Sessions—The number of IM chats occurring.
- Direct IM Sessions—The number of chats using direct connections.
- File Transfers—The number of file transfers sent through IM clients.

To View the Connection Data Statistics:

1. Select Statistics>IM History>IM Connection Data.

The IM Connection Data tab displays.

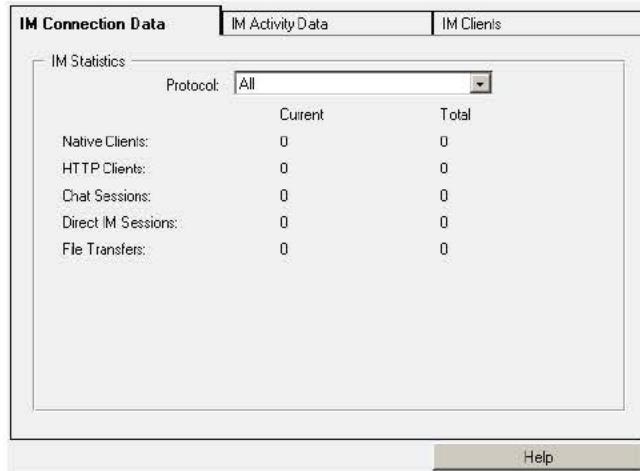


Figure 16-9: IM Connection Statistics Data Tab

2. The default protocol is All. To select a specific protocol, select AOL, MSN, or Yahoo from the drop-down list.

IM Activity Data Tab

The following IM Activity Data statistics indicate allowed and denied connections since the last statistics clear:

- Logins—The number of times IM clients have logged in.
- Messages—The number of IM messages.
- File Transfers—The number of file transfers sent through IM clients.
- Voice Chats—The number of voice conversations through IM clients.
- Messages—The number of IM messages reflected or not reflected (if IM Reflection policy is enabled).

To View the Activity Data Statistics:

1. Select Statistics>IM History>IM Activity Data.

The IM Activity Data tab displays.

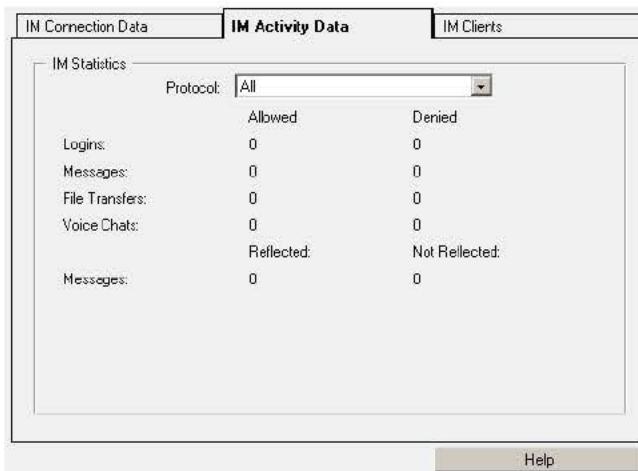


Figure 16-10: IM Connection Statistics Data Tab

2. The default protocol is All. To select a specific protocol, select AOL, MSN, or Yahoo from the drop-down list.

IM Clients Tab

The IM Clients tab displays dynamic graphical statistics for connections over 60 minutes, 24 hours and 30 days. The page can display all values in the graph or clip a percentage of peak values. When peak values are clipped by a percentage, that percentage is allowed to fall off the top of the scale.

For example, if you clip 25% of the peaks, the top 25% of the values are allowed to exceed the scale for the graph, showing greater detail for the remaining 75% of the values.

Move the cursor over the graphs to dynamically display the color-coded AOL, MSN, Yahoo, and total statistics.

To View the Client Connection Statistics:

1. Select Statistics>IM History>IM Clients.

The IM Clients tab displays.

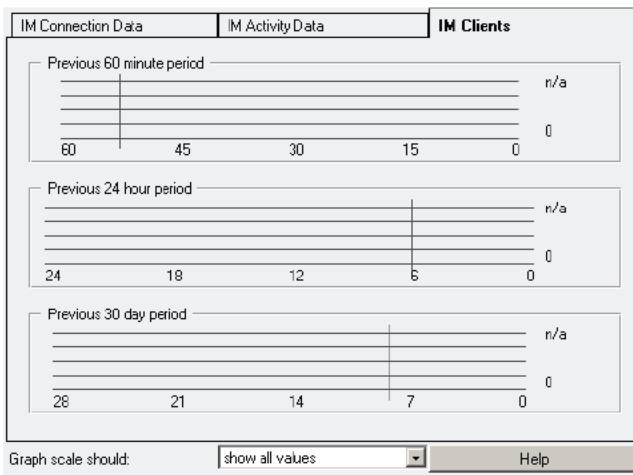


Figure 16-11: IM Client Data Statistics

2. To change the graph scale, select a clip value from the drop-down list.

Related Material

Refer to the following Blue Coat documentation for related IM information:

- Chapter 13: “The Visual Policy Manager” on page 377
- *Blue Coat Content Policy Language Guide*

Chapter 17: Content Filtering

The ProxySG allows the use of *content filtering* to control the type of content retrieved by the ProxySG and to filter requests made by clients. You can use a local content-filtering database and/or content-filtering policy to reduce the infinite number of URLs to a small number of categories and then manage those categories. Categories can be used anywhere you would use a URL-based trigger.

You can also combine the ProxySG local database and policies with a content-filtering vendor to provide a cohesive approach to managing access to the Web.

This chapter contains the following topics:

- "Overview"
- "Selecting Category Providers"
- "Configuring a Local Database"
- "Configuring Blue Coat Web Filter"
- "Configuring InterSafe"
- "Configuring Proventia Web Filter"
- "Configuring SmartFilter"
- "Configuring SurfControl"
- "Configuring Websense"
- "How to Apply Policy to Categorized URLs"
- "Using Content-Filtering Vendors with ProxySG Policies"

Overview

Content filtering allows you to categorize Web sites (such as sports and gambling). Once the Web sites and content are categorized, access to that content can be controlled through policy.

The ProxySG content filtering feature (which requires a license—see Chapter 2: “Licensing” on page 31) allows you to integrate subscription-based filtering lists that are automatically updated and categorized as the Web changes.

Content filtering allows you to block sites based on what you believe to be in them. You can either filter URLs yourself, allowing or denying permission to them using your own local content-filtering database, or you can use a third-party content-filtering vendor to provide the categories and assign the categories to URLs. Consider that, based on the ever-changing nature of the Web, manually maintaining a local content filter database is an overwhelming task.

Categories and their meanings are defined by the specific category providers. For third-party databases, the most up-to-date information on how categories are assigned to URLs can be obtained from the provider's Web site. Examples in this document are believed to be correct at the time of publication, but could be affected by subsequent changes in third-party databases.

Once the content is categorized, you can control access to the categories (using policy) by username, department, time of day, and other criteria.

To use a third-party vendor for content filtering, contact the vendor for license and authorization information. Continue with the appropriate section to configure the properties.

- "Selecting Category Providers" on page 546
- "Configuring a Local Database" on page 549
- "Configuring Blue Coat Web Filter" on page 554
- "Configuring InterSafe" on page 561
- "Configuring Proventia Web Filter" on page 566
- "Configuring SmartFilter" on page 571
- "Configuring SurfControl" on page 579
- "Configuring Websense" on page 583

To use policy to create and manage categories, see "How to Apply Policy to Categorized URLs" on page 588. To use policy to refine third-party vendor content filtering, see "Using Content-Filtering Vendors with ProxySG Policies" on page 591.

Selecting Category Providers

You can select a local database or a third-party vendor database for content filtering, view the filtering categories available, and test a URL through either the Management Console or the CLI.

To Select a Local Database or Third-Party Vendor Database through the Management Console:

1. Select Configuration>Content Filtering>General.

The General tab displays.

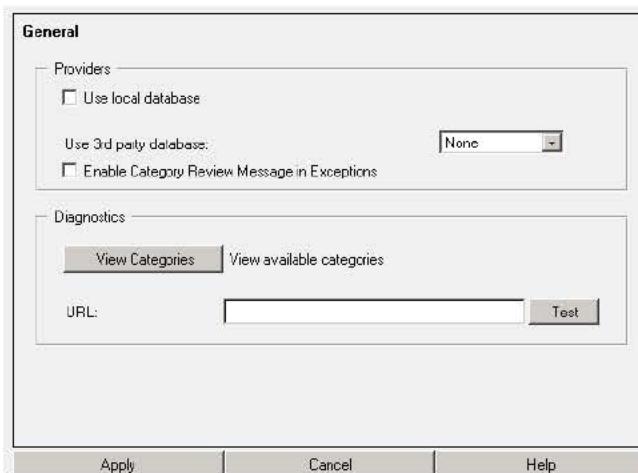


Figure 17-1: Content Filtering, General Tab

2. (Optional) To use a local database for content filtering, select the Use local database checkbox.

3. (Optional) If you have a licensed third-party vendor that you want to use (either instead of or in addition to a local database), select the vendor from the Use 3rd party database drop-down list. Select None to stop using a vendor.
4. (Optional) If you are using a provider that supports it, you can select the Enable Category Review Message in Exceptions. In conjunction with two substitutions—`$(exception.category_review_url)` and `$(exception.category_review_message)`—you can request that specific URLs be reviewed for correct categorization.

If you enable the Category Review Message, the two substitutions are automatically appended to the “help” element of all exception definitions. For information on using the `$(exception.help)` element, see “About Exception Definitions” on page 480.

Note: The substitution values are empty if the selected content filter provider does not support review messages, or if the provider was not consulted for categorization, or if the categorization process failed due to an error.

5. Click Apply.
6. (Optional) To see all categories available for use in policy, click View Categories. Note that categories will not be displayed for a vendor or local database if no database has been downloaded.
7. To see what categories a Web site is assigned by your current configuration, enter the URL into the URL field and click Test.

To Select a Local or Third-Party Vendor Database through the CLI:

1. At the `(config)` command prompt, enter the following command to enter content-filter mode:

```
SGOS# (config) content-filter
```

2. (Optional) To use a local database for content filtering, enter the following command:

```
SGOS# (config content-filter) use-local-database
```

3. (Optional) To stop using a local database for content filtering, enter the following command:

```
SGOS# (config content-filter) no use-local-database
```

4. (Optional) If you have a licensed third-party vendor that you want to use (either instead of or in addition to a local database), enter the following command to select a vendor:

```
SGOS# (config content-filter) select-provider {bluecoat | intersafe | proventia | smartfilter | surfcontrol | websense}
```

5. (Optional) You can request that specific URLs be reviewed for correct categorization.

```
SGOS# (config content-filter) review-message | no review-message
```

If you enable the Category Review Message, two substitutions—

`$(exception.category_review_url)` and `$(exception.category_review_message)`—are automatically appended to the `help` element of all exception definitions. For information on using the `$(exception.help)` element, see “About Exception Definitions” on page 480.

Note: The substitution values are empty if the selected content filter provider does not support review messages, or if the provider was not consulted for categorization, or if the categorization process failed due to an error.

6. (Optional) To stop using any third-party vendor, enter the following command:

```
SGOS#(config content-filter) select-provider none
```

7. (Optional) To identify the categories assigned by the current configuration to a particular URL, enter the following command:

```
SGOS#(config content-filter) test-url url
```

where *url* specifies the URL for which you want to identify categories.

8. (Optional) To view all available categories, which may include those created by policy, a local database if enabled, a selected vendor, and the system, enter the following command:

```
SGOS#(config content-filter) categories
```

Categories defined by Policy:

```
Sports URLs  
Entertainment
```

Categories defined by Local:

```
cat1  
cat2  
cat3  
cat4
```

Categories defined by SurfControl:

```
Web-based Email  
Motor Vehicles
```

```
.
```

```
.
```

```
Chat
```

(Long list truncated)

Categories defined by System:

```
none  
unavailable  
unlicensed
```

9. (Optional) View the content-filtering configuration.

```
SGOS#(config content-filter) view  
Provider Local  
Status: Ready  
  
Download URL: ftp://10.25.36.47/list-1000000-cat.t  
Download Username: anonymous  
Automatic download: Enabled  
Download time of day (UTC): 0  
Download on: sun, mon, tue, wed, thu, fri, sat  
Download log:  
Local database download at: Wed, 28 Jan 2004 00:19:48 UTC  
Downloading from ftp://10.25.36.47/list-1000000-cat.txt
```

```

Download size:      16274465
Database date:     Wed, 28 Jan 2004 00:22:04 UTC
Total URL patterns: 1000000
Total categories:   10
Provider:           Websense
Status:              Ready
Download License key: TUVW67XYZ89ABC0
Download Server:     download.websense.com
Email contact:
Automatic download: Enabled
Download time of day (UTC): 0
Download on:          sun, mon, tue, wed, thu, fri, sat
Use regular expression filters: No
Config Server:        Disabled
Config Server listening port: 15870
Download log:
  Websense download at: Wed, 28 Jan 2004 22:11:37 UTC
  Downloading from download.websense.com
  Download size:      63642227
  Database version:   71617
  Database date:      2004-01-28
  License expires:    Sun, 28 Nov 2004 08:00:00 UTC
  License max users: 25
  Licenses in use:   1

```

Configuring a Local Database

You can create your own local database file and download it to the ProxySG. This file is created in the same way that policy files are created, except that only *define category* statements are allowed in the local database. Refer to the *Blue Coat Content Policy Language Guide* for information on define category statements, or see "Defining Custom Categories in Policy" on page 592.

Note: You might find it convenient to put your local database on the same server as any policy files you are using.

Two main reasons to use a local database instead of a policy file for defining categories are:

- A local database is more efficient than policy if you have a large number of URLs.
- A local database separates administration of categories from policy. This separation is useful for three reasons:
 - It allows different individuals or groups to be responsible for administrating the local database and policy.
 - It keeps the policy file from getting cluttered.
 - It allows the local database to share categories across multiple boxes that have different policy.

However, some restrictions apply to a local database that do not apply to policy definitions:

- No more than 200 separate categories are allowed.
- Category names must be 32 characters or less.

- A given URL pattern can appear in no more than four category definitions.

You can choose to use any combination of the local database, policy files, or VPM to manage your category definitions. See "How to Apply Policy to Categorized URLs" on page 588 for more information. You can also use both a local database and a third-party vendor for your content filtering needs.

Use the ProxySG Management Console or the CLI to configure local database content filtering and to schedule automatic downloads. For information about scheduling automatic downloads, see "Scheduling Automatic Downloads for a Local Database" on page 553.

To Configure Local Database Content Filtering through the Management Console:

1. Select Configuration>Content Filtering>Local Database.

The Local Database tab displays.

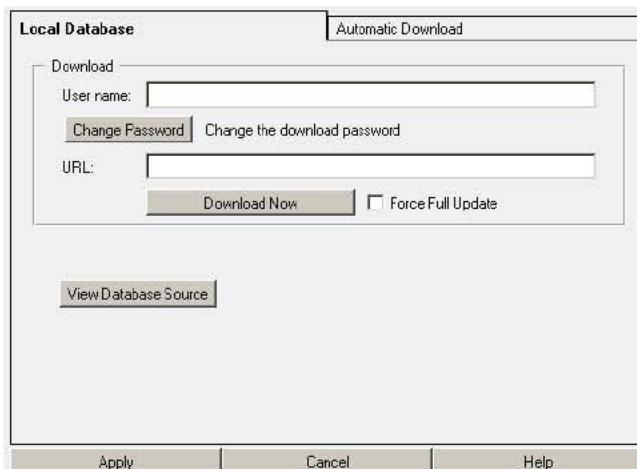


Figure 17-2: Local Database Configuration Tab

2. (Optional) If you need a password to access the download site, click **Change Password**, enter the password in the Change Password dialog, and click **OK**.
3. Enter the database download URL in the URL field.
4. (Optional) To see a display of the currently installed text file, click **View Database Source**; close the display when you are finished.
5. Click **Apply**.
6. (Optional) To download the local database right away, complete the following steps.

Note: You can return here at any time to download a database on demand (remember that the automatic download feature, if configured, keeps you up-to-date—see "Scheduling Automatic Downloads for a Local Database" on page 553).

Ordinarily, the ProxySG will check to see if the database has changed before initiating a download. If the database is up to date, then no download is necessary and none is performed. You can override this check and force a download by selecting the Force Full Update checkbox; this option is not needed under normal circumstances.

-
- a. Click Download Now (if you want to download a full database, first select the Force Full Update checkbox—this option is unnecessary under normal circumstances).

The Local Installation status dialog displays with the message Local download in progress.

When the operation is complete, the dialog message changes to The new Local filter was successfully downloaded and installed. Use the "Results" button to view full details.

- b. Click Results to see the completion message:

```
Download log:  
Local database download at: Thu, 08 Jan 2004 01:10:44 UTC  
Downloading from ftp://10.25.36.47/list-1000000-cat.txt  
Download size: 16274465  
Database date: Thu, 08 Jan 2004 01:12:56 UTC  
Total URL patterns: 1000000  
Total categories: 10
```

To Configure Local Database Content Filtering through the CLI:

The following commands allow you to enter the username, specify the URL from which the database is to be downloaded, and do an immediate download of the local database.

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) content-filter  
SGOS#(config content-filter) local  
  
SGOS#(config local) download username username  
SGOS#(config local) download password password  
-or-  
SGOS#(config local) download encrypted-password encrypted_password  
SGOS#(config local) download url url  
SGOS#(config local) clear
```

where:

username	<i>username</i>	Identifies the username needed to access the download site, if any.
encrypted-password	<i>encrypted_password</i>	Allows you to take a password previously encrypted by the ProxySG and cut and paste the encrypted password on the same appliance (or another appliance if it shares the same password-display keyring). The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted.
password	<i>password</i>	Identifies the password needed to access the download site, if any.
download url	<i>url</i>	The local URL.
clear		Clears the database from the system.

2. (Optional) To download the database now, enter one of the following commands:

```
SGOS#(config local) download get-now  
-or-  
SGOS#(config local) download full-get-now
```

where:

download get-now	Initiates an immediate database download. If the database is already up-to-date, no download will be initiated.
download full-get-now	Initiates an immediate database download, forcing a download whether or not an update is necessary. This option is unnecessary under most circumstances.

3. (Optional) To view the local database source file, enter the following command:

```
SGOS#(config local) source
```

4. (Optional) To view the configuration, enter the following command:

```
SGOS#(config local) view  
Status: Ready  
Download URL: ftp://10.25.36.47/list-1000000-cat.txt  
Download Username: user1  
Automatic download: Enabled  
Download time of day (UTC): 0  
Download on: sun, mon, tue, wed, thu, fri, sat  
Download log:  
Local database download at: Fri, 02 Jul 2004 18:40:11 UTC  
Downloading from ftp://10.25.36.47/list-1000000-cat.txt  
Download size: 612  
Database date: Fri, 02 Jul 2004 18:38:57 UTC  
Total URL patterns: 8  
Total categories: 5
```

Scheduling Automatic Downloads for a Local Database

Note: By default, the automatic download setting is enabled (for every day at midnight, UTC) and does not need to be configured unless you want to change the schedule or disable auto-download.

To download the local database without creating a schedule, see "Configuring a Local Database" on page 549.

The Automatic Download tab allows you to set the times the local database will be downloaded. You can specify an automatic download on the day and time you prefer. Because sites become stale quickly, Blue Coat recommends downloading on an automatic schedule frequently.

When the database is downloaded, a log is available that includes the information about how the database was updated, but in a more detailed form. You can view the download log through the Management Console (Statistics>Advanced>Content Filter Service) or the CLI (SGOS# (config) show content-filter status).

Setting Local Database Automatic Download Times through the Management Console:

1. Select Configuration>Content Filtering>Local Database>Automatic Download.

The Automatic Download tab displays.

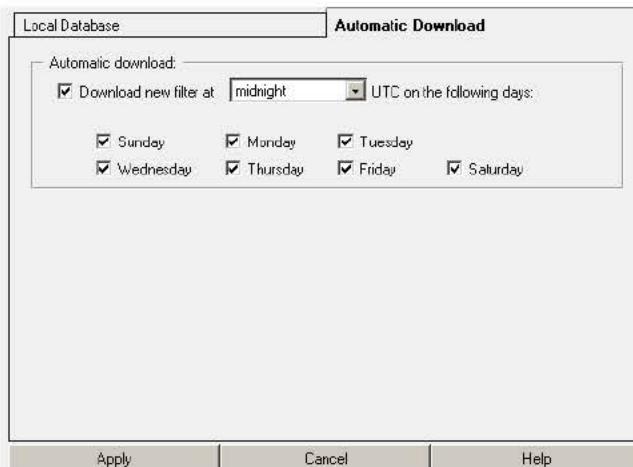


Figure 17-3: Local Database Automatic Download Tab

2. To set up a schedule for local database downloads, select the Download new filter at checkbox and select the time of day from the drop-down list. The default is Midnight.
3. All days are selected by default. Deselect days as needed.
4. Click Apply when finished.

Setting Local Database Automatic Download Times through the CLI:

1. At the `(config)` command prompt, enter the following commands to enable or disable automatic downloading of the local database.

```
SGOS#(config) content-filter
SGOS#(config content-filter) local
SGOS#(config local) download auto
-or-
SGOS#(config local) no download auto
```

2. At the `(config local)` command prompt, enter the following command to select the day(s) to automatically download the local database.

```
SGOS#(config local) download day-of-week {all | none | sun | mon | tue | wed | thu | fri | sat}
-or-
SGOS#(config local) no download day-of-week {sun | mon | tue | wed | thu | fri | sat}
```

where `all` selects all days of the week, and `none` clears all days of the week from the schedule. All days are selected by default; to deselect days, enter `none` and enter specific days. You can only select one day each time, but it is appended to the list. You can also use the `no download day-of-week` command to clear specific days from the schedule.

3. Enter the following command to specify the hour (UTC) of the selected days during which the download should be performed.

```
SGOS#(config local) download time-of-day 0-23
```

4. (Optional) To download the local database now, enter the following command:

```
SGOS#(config local) download get-now
```

Note: Downloading the database now does not affect the automatic database download schedule.

Configuring Blue Coat Web Filter

Blue Coat Web Filter (BCWF) is a highly effective content filter that can quickly learn and adapt to the working set of its users. Also, BCWF provides a network service that can dynamically examine and categorize Web pages as they are requested. This dynamic real-time categorization enhances both the accuracy and freshness of the BCWF filtering solution.

Note: If you selected Blue Coat Web Filter on the General tab, a small database that contains the category list was downloaded immediately, while the full BCWF database loaded in the background. All filtering was done by the BCWF dynamic categorization service while the full database downloaded.

No username or password is required during the trial period (60 days).

For information on configuring dynamic categorization, see "Configuring Dynamic Categorization for Blue Coat Web Filter" on page 559.

Use the ProxySG Management Console or the CLI to configure BCWF.

To Configure Blue Coat Web Filter through the Management Console

1. Select Configuration>Content Filtering>Blue Coat Web Filter.

Figure 17-4: Blue Coat Web Filter Configuration Tab

2. When you subscribed to the BCWF Service, you received a username and password for access to download updates. Enter your username into the Username field and click the Change Password button to enter or change your password. (If you are in the trial period, no username or password is required.)
3. The default database download location is displayed in the URL field. If you have been instructed to use a different URL, enter it here. You can restore the default at any time by clicking Set to default.
4. (Optional) To download the Blue Coat Web Filter database immediately, complete the following steps.

Note: You can return here at any time to download a database on demand (remember that the automatic download feature, if configured, keeps you up to date—see "Scheduling Automatic Downloads for Blue Coat Web Filter" on page 558).

Ordinarily, the ProxySG checks to see if the database has changed before initiating a download. If the database is up to date, no download is necessary and none is performed. If an incremental update is available on the server, then it is downloaded (an incremental update contains only the changes between the current installed version and the latest published version of the database, and is much smaller than a full copy of the database). You can override this process and force a download of the full database by selecting Force Full Update; this option is not needed under normal circumstances.

- a. Click Download Now (to download a full database, select Force Full Update—this option is unnecessary under normal circumstances).

The Blue Coat Web Filter Installation status dialog box displays with the message Blue Coat Web Filter download in progress.

When the operation is complete, the dialog changes to indicate installation status.

Figure 17-5: Blue Coat Web Filter Database Successfully Downloaded

- b. Click Results to see the Blue Coat Web Filter download log:

```
Download log:  
Blue Coat download at: Thu, 10 Feb 2005 00:04:06 UTC  
Downloading from https://list.bluecoat.com/bcwf/activity/download/bcwf.db  
Requesting differential update  
Differential update applied successfully  
Download size: 84103448  
Database date: Wed, 09 Feb 2005 08:11:51 UTC  
Database expires: Fri, 11 Mar 2005 08:11:51 UTC  
Database version: 2005040
```

To Configure Blue Coat Web Filter Content Filtering through the CLI

The following commands allow you to enter the Blue Coat Web Filter username and password and define the default URL and the default URL location.

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) content-filter  
SGOS#(config content-filter) bluecoat  
SGOS#(config bluecoat) download username username  
SGOS#(config bluecoat) download password password  
-or-  
SGOS#(config bluecoat) download encrypted-password encrypted-password  
SGOS#(config bluecoat) download url {default | url}
```

where:

download username	username	Specifies the username assigned to you for database download. If you are in the trial period, no username is required.
-------------------	----------	--

download encrypted-password	<i>encrypted_password</i>	Allows you to take a password previously encrypted by the ProxySG and cut and paste the encrypted password on the same appliance (or another appliance if it shares the same password-display keyring). The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted. If you are in the trial period, no password is required.
download password	<i>password</i>	Specifies the password assigned to you for database download. If you are in the trial period, no password is required.
download url	default	Specifies the use of the default download URL.
	<i>url</i>	The URL is the Blue Coat Web Filter URL. You can change it if directed to do so.

2. (Optional) To download the database now, enter one of the following commands:

```
SGOS#(config bluecoat) download get-now
-or-
SGOS#(config bluecoat) download full-get-now
```

where:

download get-now	Initiates an immediate database download. An incremental update is requested.
download full-get-now	Initiates an immediate full-size database download. This option is unnecessary under most circumstances.

3. (Optional) View the configuration.

```
SGOS#(config bluecoat) view
Status: Ready
Download URL: https://list.bluecoat.com/bcwf/activity/download/bcwf.db
Download Username:
Automatic download: Enabled
Download time of day (UTC): 0
Download on: sun, mon, tue, wed, thu, fri, sat
Download log:
Download log:
Blue Coat download at: Thu, 10 Feb 2005 00:04:06 UTC
Downloading from
    https://list.bluecoat.com/bcwf/activity/download/bcwf.db
Requesting differential update
Differential update applied successfully
Download size: 84103448
Database date: Wed, 09 Feb 2005 08:11:51 UTC
Database expires: Fri, 11 Mar 2005 08:11:51 UTC
Database version: 2005040
```

Scheduling Automatic Downloads for Blue Coat Web Filter

Note: By default, the automatic download setting is enabled (for every day at midnight, UTC) and does not need to be configured unless you want to change the schedule or disable auto-download.

To download the Blue Coat Web Filter database without creating a schedule, see "Configuring Blue Coat Web Filter" on page 554.

The Automatic Download tab allows you to set the times at which the Blue Coat Web Filter database is downloaded. You can specify an automatic download on the day and time you prefer. Because sites become stale quickly, Blue Coat recommends downloading on an automatic schedule frequently.

When the database is downloaded, a log is available that includes the information about how the database was updated, but in a more detailed form. You can view the download log through the Management Console (Statistics>Advanced>Content Filter Service) or the CLI (SGOS#(config) `show content-filter status`).

Setting Blue Coat Web Filter Automatic Download Times through the Management Console

1. Select Configuration>Content Filtering>Blue Coat Web Filter>Automatic Download.

Figure 17-6: Blue Coat Web Filter Automatic Download Tab

2. To set up a schedule for Blue Coat Web Filter database downloads, select Download new filter at and select the time of day from the drop-down list. The default is Midnight.
3. All days are selected by default. Clear checkboxes as needed.
4. Click Apply when finished.

Setting Blue Coat Web Filter Automatic Download Times through the CLI

1. At the `(config)` command prompt, enter the following commands to enable or disable automatic downloading of the Blue Coat Web Filter database.

```
SGOS# (config) content-filter  
SGOS# (config content-filter) bluecoat
```

```
SGOS# (config bluecoat) download auto
-or-
SGOS# (config bluecoat) no download auto
```

2. At the (config bluecoat) command prompt, enter the following commands to select or deselect the day(s) to automatically download the local database.

```
SGOS# (config bluecoat) download day-of-week {all | none | sun | mon | tue | wed | thu | fri | sat}
-or-
SGOS# (config bluecoat) no download day-of-week {sun | mon | tue | wed | thu | fri | sat}
```

where **all** selects all days of the week, and **none** clears all days of the week from the schedule.

All days are selected by default; to deselect days, enter **none** and enter specific days. You can only select one day each time, but it is appended to the list. You can also use the **no download day-of-week** command to clear specific days from the schedule.

3. Enter the following command to specify the hour (UTC) of the selected days during which the download should be performed.

```
SGOS# (config bluecoat) download time-of-day 0-23
```

4. (Optional) To download the Blue Coat Web Filter database now, enter the following command:

```
SGOS# (config bluecoat) download get-now
```

Downloading the database now does not affect the automatic database download schedule.

Configuring Dynamic Categorization for Blue Coat Web Filter

The Dynamic Categorization tab allows you to enable or disable dynamic categorization and its various forms of behavior on the ProxySG. By default, dynamic categorization is enabled.

Note: The dynamic service is consulted only when the installed BCWF database does not contain complete categorization for an object. This dispatch mechanism is independent of results from other categorization services.

Dynamic analysis of content is done on a remote network service, and not locally on the ProxySG. If the category returned by this service is blocked by policy, the offending material never enters the network in any form.

Administrators might need to process certain URL requests in real time while other requests can be done in the background. Some requests might avoid dynamic categorization entirely as circumstances dictate. Therefore, the choice of real-time, background mode, or no dynamic categorization for each URL categorization can be made on a per-transaction basis using Blue Coat policy. The configuration establishes a default mode; Blue Coat policy can override that default. For more information, see Chapter 13: "The Visual Policy Manager" or refer to the *Blue Coat Content Policy Language Guide*.

Dynamic categorization has two types of cost:

- Bandwidth: Represents the round trip request/response from the ProxySG to the service. Because the dynamic categorization protocol is compact, this cost is minimal.

- Latency: Represents the time spent waiting for the dynamic categorization service to provide a result.

These costs are only incurred when a URL cannot be categorized by a database lookup on the ProxySG. SGOS 4.x offers three modes of operation to compensate for some of this cost:

- Real-time mode (default). Real-time mode incurs both bandwidth and latency costs. The advantage of real-time mode dynamic categorization is that Blue Coat policy has access to the results of dynamic categorization, which means that policy decisions are made immediately upon receiving all available information.
- Background mode. Background mode incurs only the bandwidth cost. In background mode once a call is made to the dynamic categorization service, the URL request immediately proceeds without waiting for the external service to respond. The system category *pending* is assigned to the request, indicating that the policy was evaluated with potentially incomplete category information.

Once received, the results of dynamic categorization are entered into a categorization cache (as are the results of real-time requests). This cache ensures that any subsequent requests for the same or similar URLs can be categorized quickly, without needing to query the external service again.

- Do not categorize. Dynamic categorization is not done (unless explicitly requested by policy). This mode is distinct from disabling the service. When *Do not categorize* is set as the default, dynamic categorization (in either real time or background mode) can be explicitly invoked by policy. When the service is disabled, no dynamic categorization is done, regardless of policy, and the ProxySG does not make any contact with the dynamic categorization service.

To Configure Dynamic Categorization through the Management Console

1. Select Configuration>Content Filtering>Blue Coat>Dynamic Categorization.

Figure 17-7: Blue Coat Web Filter Dynamic Categorization

Dynamic Categorization is enabled by default. To disable it, clear the checkbox. If dynamic categorization is disabled, then the ProxySG does not contact the dynamic categorization service, even when no category is found for a URL in the database, and any dynamic categorization properties specified in policy are ignored. If dynamic categorization is enabled, it is only invoked while BCWF is in use.

2. To change the Dynamic Categorization Settings, select one of the following:

- Do not categorize dynamically. The loaded database is consulted for category information. URLs not found in the database show up as category *none*.
- Categorize dynamically in the background. Objects not categorized by the database are dynamically categorized when time permits.
- Categorize dynamically in real-time, the default. Objects not categorized by the database are dynamically categorized.

To Configure Dynamic Categorization through the CLI

The following commands allow you to analyze and manage requested Web pages in real time. You can also configure dynamic categorization settings and specify behavior when doing dynamic categorization.

At the (config) command prompt, enter the following commands:

```
SGOS# (config) content-filter
SGOS# (config content-filter) bluecoat
SGOS# (config bluecoat) service enable | disable
SGOS# (config bluecoat) service mode {background | realtime | none}
```

where:

service	enable disable	Enable or disable dynamic categorization. Dynamic categorization is enabled by default.
service mode	background realtime none	Do dynamic categorization one of three ways: <ul style="list-style-type: none"> • background: Objects not categorized by the database are dynamically categorized when time permits. • realtime: The default. Objects not categorized by the database are dynamically categorized. • none: The loaded database is consulted for category information. URLs not in the database show up as category <i>none</i>.

Configuring InterSafe

Use the ProxySG Management Console or the CLI to configure InterSafe content filtering.

To Configure InterSafe Content Filtering through the Management Console:

1. Select Configuration>Content Filtering>InterSafe.

The InterSafe tab displays.

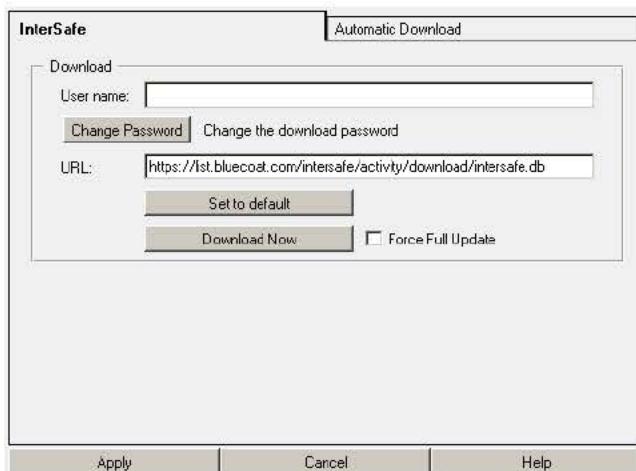


Figure 17-8: InterSafe Configuration Tab

2. Enter the username and password assigned to you for downloading the InterSafe database: enter your username into the Username field and click the Change Password button to enter or change your password.
3. The default database download location is displayed in the URL field. If you have been instructed to use a different URL, enter it here. You can restore the default at any time by clicking Set to default.
4. (Optional) To download the InterSafe database right away, complete the following steps.

Note: You can return here at any time to download a database on demand (remember that the automatic download feature, if configured, keeps you up-to-date—see "Scheduling Automatic Downloads for InterSafe" on page 565).

Ordinarily, the ProxySG will check to see if the database has changed before initiating a download. If the database is up to date, then no download is necessary and none is performed. If an incremental update is available on the server, then it is downloaded (an incremental update contains only the changes between the current installed version and the latest published version of the database, and is much smaller than a full copy of the database). You can override this process and force a download of the full database by selecting the Force Full Update checkbox; this option is not needed under normal circumstances.

- a. Click Download Now (if you want to download a full database, first select the Force Full Update checkbox—this option is unnecessary under normal circumstances).

The InterSafe Installation status dialog box displays with the message **InterSafe download in progress**.

When the operation is complete, the dialog changes to:

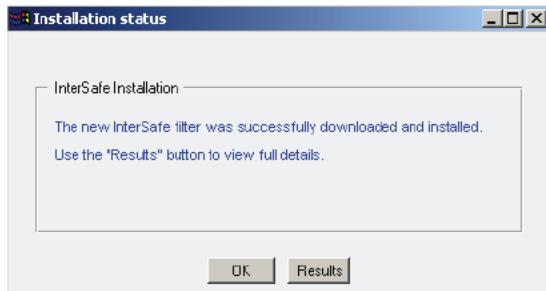


Figure 17-9: InterSafe Database Successfully Downloaded

- b. Click Results to see the InterSafe download log:

```
Download log:  
InterSafe download at: Tue, 28 Sep 2004 20:16:16 UTC  
Downloading from https://list.bluecoat.com/.../download/intersafe.db  
Warning: Unable to determine current database version; requesting full  
update  
Download size: 8106572  
Database date: Fri, 10 Sep 2004 07:02:08 UTC  
Database expires: Sun, 10 Oct 2004 07:02:08 UTC  
Database version: 3
```

To Configure InterSafe Content Filtering through the CLI:

The following commands allow you to enter the InterSafe username and password and define the default URL and the default URL location.

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) content-filter  
SGOS#(config content-filter) intersafe  
  
SGOS#(config intersafe) download username username  
SGOS#(config intersafe) download password password  
-or-  
SGOS#(config intersafe) download encrypted-password encrypted-password  
SGOS#(config intersafe) download url {default | url}
```

where:

download username	<i>username</i>	Specifies the username assigned to you for database download.
download encrypted- password	<i>encrypted_password</i>	Allows you to take a password previously encrypted by the ProxySG and cut and paste the encrypted password on the same appliance (or another appliance if it shares the same password-display keyring). The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted.
download password	<i>password</i>	Specifies the password assigned to you for database download.
download url	default <i>url</i>	Specifies the use of the default download URL. The URL is the InterSafe URL. You can change it if directed to do so.

2. (Optional) To download the database now, enter one of the following commands:

```
SGOS# (config intersafe) download get-now  
-or-  
SGOS# (config intersafe) download full-get-now
```

where:

download get-now	Initiates an immediate database download. An incremental update will be requested.
download full-get-now	Initiates an immediate full-size database download. This option is unnecessary under most circumstances.

3. (Optional) View the configuration.

```
SGOS# (config intersafe) view  
Status: Ready  
Download URL: https://list.bluecoat.com/.../download/intersafe.db  
Download Username: admin  
Automatic download: Enabled  
Download time of day (UTC): 0  
Download on: sun, mon, tue, wed, thu, fri, sat  
Download log:  
InterSafe download at: Tue, 28 Sep 2004 20:23:16 UTC  
Downloading from https://list.bluecoat.com/.../download/intersafe.db  
Warning: Unable to determine current database version; requesting full update  
Download size: 8106572  
Database date: Fri, 10 Sep 2004 07:02:08 UTC  
Database expires: Sun, 10 Oct 2004 07:02:08 UTC  
Database version: 3
```

Scheduling Automatic Downloads for InterSafe

Note: By default, the automatic download setting is enabled (for every day at midnight, UTC) and does not need to be configured unless you want to change the schedule or disable auto-download.

To download the InterSafe database without creating a schedule, see "Configuring InterSafe" on page 561.

The Automatic Download tab allows you to set the times at which the InterSafe database is downloaded. You can specify an automatic download on the day and time you prefer. Because sites become stale quickly, Blue Coat recommends downloading on an automatic schedule frequently.

When the database is downloaded, a log is available that includes the information about how the database was updated, but in a more detailed form. You can view the download log through the Management Console (Statistics>Advanced>Content Filter Service) or the CLI (SGOS# (config) show content-filter status).

Setting InterSafe Automatic Download Times through the Management Console:

1. Select Configuration>Content Filtering>InterSafe>Automatic Download.

The Automatic Download tab displays.

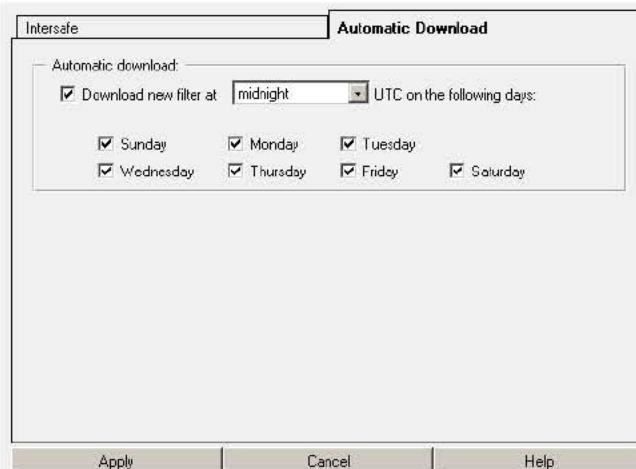


Figure 17-10: InterSafe Automatic Download Tab

2. To set up a schedule for InterSafe database downloads, select the Download new filter at checkbox and select the time of day from the drop-down list. The default is Midnight.
3. All days are selected by default. Deselect days as desired.
4. Click Apply when finished.

Setting InterSafe Automatic Download Times through the CLI:

1. At the `(config)` command prompt, enter the following commands to enable or disable automatic downloading of the InterSafe database.

```
SGOS#(config) content-filter
SGOS#(config content-filter) intersafe

SGOS#(config intersafe) download auto
-or-
SGOS#(config intersafe) no download auto
```

2. At the `(config intersafe)` command prompt, enter the following commands to select or deselect the day(s) to automatically download the local database.

```
SGOS#(config intersafe) download day-of-week {all | none | sun | mon | tue | wed
| thu | fri | sat}
-or-
SGOS#(config intersafe) no download day-of-week {sun | mon | tue | wed | thu |
fri | sat}
```

where `all` selects all days of the week, and `none` clears all days of the week from the schedule. All days are selected by default; to deselect days, enter `none` and enter specific days. You can only select one day each time, but it is appended to the list. You can also use the `no download day-of-week` command to clear specific days from the schedule.

3. Enter the following command to specify the hour (UTC) of the selected days during which the download should be performed.

```
SGOS#(config intersafe) download time-of-day 0-23
```

4. (Optional) To download the InterSafe database now, enter the following command:

```
SGOS#(config intersafe) download get-now
```

Downloading the database now does not affect the automatic database download schedule.

Configuring Proventia Web Filter

Use the ProxySG Management Console or the CLI to configure Proventia Web Filter content filtering.

To Configure Proventia Web Filter Content Filtering through the Management Console:

1. Select Configuration>Content Filtering>Proventia Web Filter.

The Proventia Web Filter tab displays.

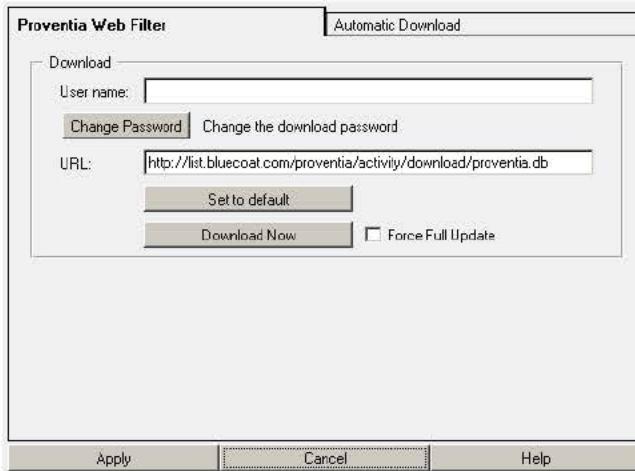


Figure 17-11: Proventia Web Filter Configuration Tab

2. Enter the Proventia Web Filter username and password: enter your username into the Username field and click the Change Password button to enter or change your password.
3. The default database download location is displayed in the URL field. If you have been instructed to use a different URL, enter it here. You can restore the default at any time by clicking Set to default.
4. (Optional) To download the Proventia Web Filter database right away, complete the following steps.

Note: You can return here at any time to download a database on demand (remember that the automatic download feature, if configured, keeps you up-to-date—see "Scheduling Automatic Downloads for Proventia Web Filter" on page 569).

Ordinarily, the ProxySG will check to see if the database has changed before initiating a download. If the database is up to date, then no download is necessary and none is performed. If an incremental update is available on the server, then it is downloaded (an incremental update contains only the changes between the current installed version and the latest published version of the database, and is much smaller than a full copy of the database). You can override this process and force a download of the full database by selecting the Force Full Update checkbox; this option is not needed under normal circumstances.

- a. Click Download Now (if you want to download a full database, first select the Force Full Update checkbox—this option is unnecessary under normal circumstances).

The Proventia Installation status dialog box displays with the message Proventia download in progress.

When the operation is complete, the dialog message changes to The new Proventia filter was successfully downloaded and installed. Use the "Results" button to view full details.

- b. Click Results to see the Proventia Web Filter download log:

```
Download log:  
  Proventia download at: Sat, 10 Jul 2004 18:54:43 UTC  
  Downloading from http://list.bluecoat.com/proventia/activity/download/proventia.db  
  Requesting differential update  
  Download size:      144913364  
  Database date:     Wed, 16 Jun 2004 09:40:34 UTC  
  Database expires:   Sat, 06 Feb 2106 06:28:16 UTC  
  Database version:  16777216
```

To Configure Proventia Web Filter Content Filtering through the CLI:

The following commands allow you to enter the Proventia Web Filter username and password and define the default URL and the default URL location.

1. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) content-filter  
SGOS#(config content-filter) proventia  
  
SGOS#(config proventia) download username username  
SGOS#(config proventia) download password password  
-or-  
SGOS#(config proventia) download encrypted-password encrypted-password  
SGOS#(config proventia) download url {default | url}
```

where:

<code>download username</code>	<code>username</code>	Specifies the username assigned to you for database download.
<code>download encrypted- password</code>	<code>encrypted_password</code>	Allows you to take a password previously encrypted by the ProxySG and cut and paste the encrypted password on the same appliance (or another appliance if it shares the same password-display keyring).
<code>download password</code>	<code>password</code>	The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted.
<code>download url</code>	<code>default</code>	Specifies the password assigned to you for database download.
	<code>url</code>	Specifies the use of the default download URL. The URL is the Proventia Web Filter URL. You can change it if directed to do so.

2. (Optional) To download the database now, enter one of the following commands:

```
SGOS#(config proventia) download get-now  
-or-  
SGOS#(config proventia) download full-get-now
```

where:

download get-now	Initiates an immediate database download. An incremental update will be requested.
download full-get-now	Initiates an immediate full-size database download. This option is unnecessary under most circumstances.

3. (Optional) View the configuration.

```
SGOS# (config proventia) view
Status: Ready
Download URL: http://list.bluecoat.com/proventia/activity/download/proventia.db
Download Username:
Automatic download: Enabled
Download time of day (UTC): 0
Download on: sun, mon, tue, wed, thu, fri, sat
Download log:
Proventia download at: Sat, 10 Jul 2004 19:21:51 UTC
Downloading from http://list.bluecoat.com/proventia/activity/download/proventia.db
Requesting differential update
Download size: 144913364
Database date: Wed, 16 Jun 2004 09:40:34 UTC
Database expires: Sat, 06 Feb 2106 06:28:16 UTC
Database version: 16777216
```

Scheduling Automatic Downloads for Proventia Web Filter

Note: By default, the automatic download setting is enabled (for every day at midnight, UTC) and does not need to be configured unless you want to change the schedule or disable auto-download.

To download the Proventia Web Filter database without creating a schedule, see "Configuring Proventia Web Filter" on page 566.

The Automatic Download tab allows you to set the times at which the Proventia Web Filter database is downloaded. You can specify an automatic download on the day and time you prefer. Because sites become stale quickly, Blue Coat recommends downloading on an automatic schedule frequently.

When the database is downloaded, a log is available that includes the information about how the database was updated, but in a more detailed form. You can view the download log through the Management Console (Statistics>Advanced>Content Filter Service) or the CLI (SGOS# (config) show content-filter status).

Setting Proventia Web Filter Automatic Download Times through the Management Console:

1. Select Configuration>Content Filtering>Proventia Web Filter>Automatic Download.

The Automatic Download tab displays.

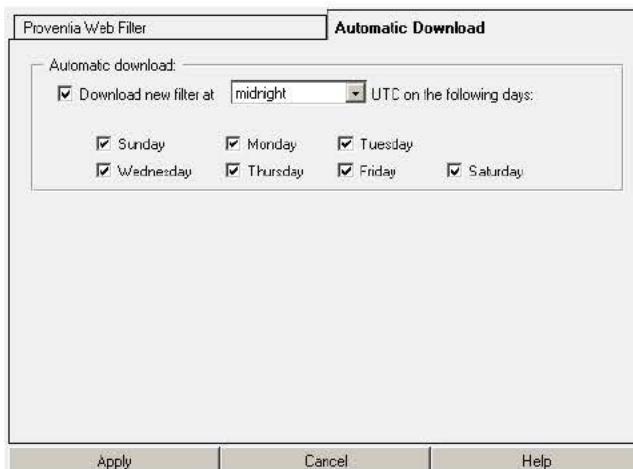


Figure 17-12: Proventia Web Filter Automatic Download Tab

2. To set up a schedule for Proventia Web Filter database downloads, select the Download new filter at checkbox and select the time of day from the drop-down list. The default is Midnight.
3. All days are selected by default. Deselect days as desired.
4. Click Apply when finished.

Setting Proventia Web Filter Automatic Download Times through the CLI:

1. At the `(config)` command prompt, enter the following commands to enable or disable automatic downloading of the Proventia Web Filter database.

```
SGOS#(config) content-filter
SGOS#(config content-filter) proventia
SGOS#(config proventia) download auto
-or-
SGOS#(config proventia) no download auto
```

2. At the `(config proventia)` command prompt, enter the following commands to select or deselect the day(s) to automatically download the local database.

```
SGOS#(config proventia) download day-of-week {all | none | sun | mon | tue | wed |
| thu | fri | sat}
-or-
SGOS#(config proventia) no download day-of-week {sun | mon | tue | wed | thu |
fri | sat}
```

where `all` selects all days of the week, and `none` clears all days of the week from the schedule. All days are selected by default; to deselect days, enter `none` and enter specific days. You can only select one day each time, but it is appended to the list. You can also use the `no download day-of-week` command to clear specific days from the schedule.

3. Enter the following command to specify the hour (UTC) of the selected days during which the download should be performed.

```
SGOS#(config proventia) download time-of-day 0-23
```

4. (Optional) To download the Proventia Web Filter database now, enter the following command:

```
SGOS# (config proventia) download get-now
```

Downloading the database now does not affect the automatic database download schedule.

Configuring SmartFilter

Use the ProxySG Management Console or the CLI to configure SmartFilter content filtering.

Differences Between SmartFilter Version 3 and Version 4

SmartFilter version 3 and version 4 have different category lists. Even when categories have similar names, they might have changed in meaning or cover different URLs. Before you switch from version 3 to version 4, you should consider how your policy will be affected, and take steps to avoid unwanted transitional behavior. Table 17.1 is a table of version equivalencies between categories. Where a version 3 category has an obvious version 4 equivalent, CPL will recognize the version 3 name as a deprecated synonym for the version 4 name. A CPL compilation warning will be generated for references to these categories. In two cases, there is no direct equivalent for the version 3 category ("Lifestyle" has been dropped as a category by SmartFilter, and "Mature" has been split into several sub-categories). These names will not be recognized, and you will need to update policy accordingly.

For example, the following policy was compiled using version 3:

```
<proxy>
    category=Sex exception(content_filter_denied)
    category=Nudity exception(content_filter_denied)
    category=Mature exception(content_filter_denied)
```

After configuring and downloading a version 4 list, the policy will still compile, but will generate the following warnings:

```
Warning: Obsolete category name: 'Sex' is now 'Pornography'
Warning: Unknown category: 'Mature'
```

While the first warning is just advising you of a name change (the content continues to be blocked), none of the content formerly categorized as `Mature` will be blocked. You may wish to modify policy to include some or all of the equivalent new subcategories:

```
<proxy>
    category=Pornography exception(content_filter_denied)
    category=Nudity exception(content_filter_denied)
    category=( "Sexual Material", Alcohol, Tobacco, Weapons, Profanity, \
    "Provocative Attire", Tasteless/Gross) exception(content_filter_denied)
```

The version 4 category names shown above are subject to change, because they are defined by the control list and can be updated by SmartFilter. See "Selecting Category Providers" on page 546 for instructions on how to view a list of all current category names.

Table 17.1: Category Names in Version 3 and Version 4

Version 3 Category Names	Version 4 Category Names
Art/Culture	Art/Culture/Heritage
Anonymizer/Translator	Anonymizers, Anonymizing Utilities
Chat	Chat, Instant Messaging, Forum/Bulletin Boards

Table 17.1: Category Names in Version 3 and Version 4 (Continued)

Crim. Skills	Criminal Skills, Malicious Sites
Cults/Occult	Religion and Ideology
Dating	Dating/Personals
Drugs	Drugs
Entertainment	Entertainment/Recreation/Hobbies
Extreme	Extreme, Violence, Profanity, Tasteless/Gross
Gambling	Gambling
Games	Games
Gen. News	General News
Hate Speech	Hate Speech
High Bandwidth	Media Downloads, Internet Radio/TV, Streaming Media, Shareware/Freeware
Humor	Humor
Investing	Stock Trading
Job Search	Job Search
<i>Lifestyle</i>	(deprecated)
<i>Mature</i>	<i>Alcohol, Provocative Attire, Profanity, Sexual Materials, Tobacco, Weapons</i>
Nudity	Nudity
Online Sales	Shopping/Merchandizing, Auction
Politics/Religion	Politics/Opinion, Religion and Ideology
Personal	Personal Pages
Portal Sites	Portal Sites
Self-Help/Health	Health
Sex	Pornography
Sports	Sports
Travel	Travel
Usenet News	Usenet News
Webmail	Web Mail

Note: The categories in italics are NOT translated from version 3 to version 4. When a version 3 category that IS translated has more than one version 4 category (for instance, “Politics/Religion”), the version 3 category is automatically translated to the first version 4 category that appears in the table (the version 3 example, “Politics/Religion,” would translate to the version 4 “Politics/Opinion”).

To Configure SmartFilter Content Filtering through the Management Console:

1. Select Configuration>Content Filtering>SmartFilter.
2. The SmartFilter tab displays.

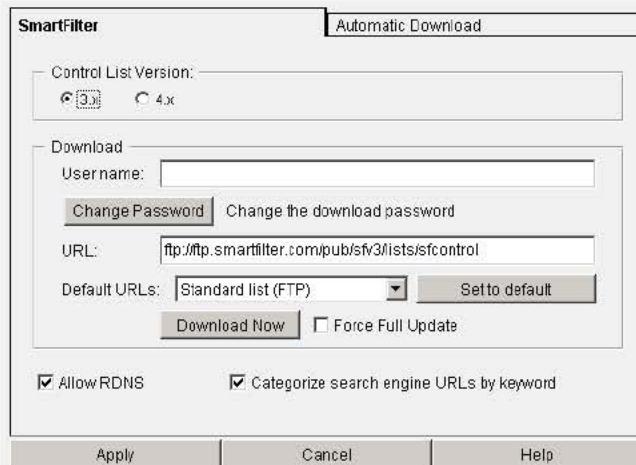


Figure 17-13: SmartFilter Configuration Tab

3. To change the version of the SmartFilter control list, select a version in the Control List Version field (3.x or 4.x) and click OK in the SmartFilter version changed dialog that appears. To complete the change, you must set the download URL as appropriate for the new version (step 5, below) and download the new version of the SmartFilter database (step 9, below). See "Differences Between SmartFilter Version 3 and Version 4" on page 571 for instructions about category differences that could affect your content-filtering policy.
4. Enter the username and password assigned to you for downloading the SmartFilter database: enter your username into the Username field and click the Change Password button to enter or change your password.
5. To set the download URL, complete one of the following two steps:
 - a. The default database download URL is displayed in the URL field. If you have been instructed to use a different URL, enter it in the URL field.
 - b. You can restore or change the default database download URL at any time. For version 4.x, click Set to default. For version 3.x, select the protocol (FTP or HTTP) and the type of control list (Standard or Premier) that you want to use to download the SmartFilter database by choosing one of the four options in the Default URLs drop-down list; click the Set to default button.

Note: If you have a low-RAM platform, such as the 400-0 model platform, use the Standard list rather than the Premier list to avoid performance degradation.

6. (Optional) SmartFilter lookups can require use of reverse DNS to properly categorize a Web site. To disable the use of reverse DNS by Smartfilter, uncheck the Allow RDNS checkbox.

Important: Disabling reverse DNS prevents SmartFilter from correctly classifying some sites and can increase the likelihood of the ProxySG serving inappropriate content.

7. (Optional) By default, SmartFilter categorizes search engines based on keywords in the URL query. To disable this setting, deselect Categorize search engine URLs based on keywords.

Note: Leaving keywords enabled can cause unexpected results. For example, the keyword *electoral college* falls into the educational category.

8. Click **Apply**.
9. (Optional) To download the SmartFilter database right away, complete the following steps.

Note: You can return here at any time to download a database on demand (remember that the automatic download feature, if configured, keeps you up-to-date—see "Scheduling Automatic Downloads for SmartFilter" on page 577).

Ordinarily, the ProxySG will check to see if the database has changed before initiating a download. If the database is up to date, then no download is necessary and none is performed. If an incremental update is available on the server, then it is downloaded (an incremental update contains only the changes between the current installed version and the latest published version of the database, and is much smaller than a full copy of the database). You can override this process and force a download of the full database by selecting the Force Full Update checkbox; this option is not needed under normal circumstances.

- a. Click **Download Now** (if you want to download a full database, first select the Force Full Update checkbox—this option is unnecessary under normal circumstances).

The SmartFilter Installation status dialog box displays with the message SmartFilter download in progress.

When the operation is complete, the dialog message changes to The new SmartFilter filter was successfully downloaded and installed. Use the "Results" button to view full details.

- b. Click **Results** to see the completion message:

```
Download log:  
SmartFilter download at: Tue, 06 Apr 2004 20:27:14 UTC  
Checking incremental update  
Warning: Unable to open input control list  
Warning: Unable to open installed control list  
Downloading full control file  
SmartFilter download at: Tue, 06 Apr 2004 20:27:14 UTC  
Downloading from http://example.com/...version=4.0  
Download size: 45854194  
Database version: 95  
Database date: Tue, 06 Apr 2004 07:05:01 UTC  
Database expires: Tue, 11 May 2004 07:05:01 UTC
```

Note: The first time you download a SmartFilter database, warnings appear in the results message under **Checking incremental update**. These are expected, and represent the normal process of checking to see if an incremental update is possible. The next time you download a SmartFilter database, the ProxySG will check the previously downloaded database, and download only what is necessary to keep the database current.

You can expect similar warnings the first time you attempt a download after changing SmartFilter versions from 3.x to 4.x (or vice versa). A full download will be necessary the first time the new version is downloaded; subsequent downloads should only need an incremental update.

To Configure SmartFilter Content Filtering through the CLI:

The following commands allow you to select a SmartFilter version, enter a username, specify a URL from which the database is to be downloaded, and do an immediate download of the SmartFilter database.

1. At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) content-filter
SGOS#(config content-filter) smartfilter
SGOS#(config smartfilter) list-version {3 | 4}
```

- a. If you chose list-version 3, enter the following commands:

```
SGOS#(config smartfilter) download username username
SGOS#(config smartfilter) download password password
-or-
SGOS#(config smartfilter) download encrypted-password encrypted_password
SGOS#(config smartfilter) download url url
-or-
SGOS#(config smartfilter) download url {standard-list | premier-list {http | ftp}}
SGOS#(config smartfilter) allow-rdns | no allow-rdns
```

- b. If you chose list-version 4, enter the following commands:

```
SGOS#(config smartfilter) allow-rdns | no allow-rdns
SGOS#(config smartfilter) use-search-keywords
```

where:

<code>list-version</code>	<code>3 4</code>	Specifies the version (3.x or 4.x) of the SmartFilter control list. See "Differences Between SmartFilter Version 3 and Version 4" on page 571 for instructions about category differences that could affect your content-filtering policy.
<code>download username</code>	<code>username</code>	Version 3.x only. Specifies the username assigned to you for database download.

download encrypted-password	<i>encrypted_password</i>	Version 3.x only. Allows you to take a password previously encrypted by the ProxySG and cut and paste the encrypted password on the same appliance (or another appliance if it shares the same password-display keyring). The primary use of the encrypted-password command is to allow the ProxySG to reload a password that it encrypted.
download password	<i>password</i>	Version 3.x only. Specifies the password assigned to you for database download.
download url	<i>url</i>	Version 3.x only. Specifies the URL of the downloaded database. The URL is the SmartFilter URL. You can change it if directed to do so.
	{standard-list {http ftp} premier-list {http ftp}}}	Version 3.x only. Select the type of control list (Standard or Premier) and the protocol (FTP or HTTP) that you want to use to download the SmartFilter database. If you have a low-RAM platform, such as the 400-0, select standard-list to avoid performance degradation.
allow-rdns	no	A toggle that enables or disables reverse DNS lookup.
use-search-keywords	no	Version 4.x only. Allows you to categorize search engines based on keywords in the URL query.

2. (Optional) To download the database now, enter one of the following commands:

```
SGOS#(config smartfilter) download get-now
-or-
SGOS#(config smartfilter) download full-get-now
```

where:

download get-now

Initiates an immediate database download. An incremental update will be requested.

download full-get-now

Initiates an immediate full-size database download. This option is unnecessary under most circumstances.

3. (Optional) View the configuration.

```

SGOS# (config smartfilter) view
Status: Ready
Use control list version: 3
Download URL: ftp://ftp.smartfilter.com/pub/sfv3/lists/...
Download Username: cf00100002
Automatic download: Enabled
Download time of day (UTC): 0
Download on: sun, mon, tue, wed, thu, fri, sat
Allow RDNS for lookups: No
Download log:
SmartFilter download at: Fri, 02 Jul 2004 00:13:08 UTC
Checking incremental update
    Installed database version: 152
    Current published version: 153
Incremental download complete
Download size: 42821832
Database version: 153
Database date: Thu, 01 Jul 2004 07:05:00 UTC
Database expires: Thu, 05 Aug 2004 07:05:00 UTC

```

Scheduling Automatic Downloads for SmartFilter

Note: By default, the automatic download setting is enabled (for every day at midnight, UTC) and does not need to be configured unless you want to change the schedule or disable auto-download.

To download the SmartFilter database without creating a schedule, see "Configuring SmartFilter" on page 571.

The Automatic Download tab allows you to set the times at which the SmartFilter database is downloaded. You can specify an automatic download on the day and time you prefer. Because sites become stale quickly, Blue Coat recommends downloading on an automatic schedule frequently.

When the database is downloaded, a log is available that includes the information about how the database was updated, but in a more detailed form. You can view the download log through the Management Console (Statistics>Advanced>Content Filter Service) or the CLI (`enable>show content-filter status`).

Setting SmartFilter Automatic Download Times through the Management Console:

1. Select Configuration>Content Filtering>SmartFilter>Automatic Download.

The Automatic Download tab displays.

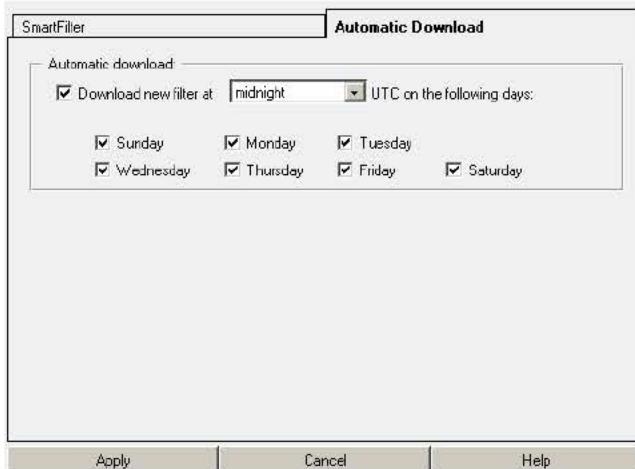


Figure 17-14: SmartFilter Automatic Download Tab

2. To set up a schedule for SmartFilter database downloads, select the Download new filter at checkbox and select the time of day from the drop-down list. The default is Midnight.
3. All days are selected by default. Deselect days as desired.
4. Click Apply when finished.

Setting SmartFilter Automatic Download Times through the CLI:

1. At the (config) command prompt, enter the following commands to enable or disable automatic downloading of the SmartFilter database.

```
SGOS#(config) content-filter
SGOS#(config content-filter) smartfilter
SGOS#(config smartfilter) download auto
-or-
SGOS#(config smartfilter) no download auto
```

2. At the (config smartfilter) command prompt, enter the following command to select the day(s) to automatically download the local database.

```
SGOS#(config smartfilter) download day-of-week {all | none | sun | mon | tue |
wed | thu | fri | sat}
-or-
SGOS#(config smartfilter) no download day-of-week {sun | mon | tue | wed | thu |
fri | sat}
```

where **all** selects all days of the week, and **none** clears all days of the week from the schedule. All days are selected by default; to deselect days, enter **none** and enter specific days. You can only select one day each time, but it is appended to the list. You can also use the **no download day-of-week** command to clear specific days from the schedule.

3. Enter the following command to specify the hour (UTC) of the selected days during which the download should be performed.

```
SGOS#(config smartfilter) download time-of-day 0-23
```

4. (Optional) To download the SmartFilter database now, enter the following command:

```
SGOS# (config smartfilter) download get-now
```

Note: Downloading the database now does not affect the automatic database download schedule.

Configuring SurfControl

Use the ProxySG Management Console or the CLI to configure SurfControl content filtering.

To Configure SurfControl Content Filtering through the Management Console:

1. Select Configuration>Content Filtering>SurfControl.

The SurfControl tab displays.



Figure 17-15: SurfControl Configuration Tab

2. Enter the license key assigned to you for downloading the SurfControl database.
3. The default database download location is displayed in the URL field. If you have been instructed to use a different URL, enter it here. You can restore the default at any time by clicking Set to default.
4. (Optional) To download the SurfControl database right away, complete the following steps.

Note: You can return here at any time to download a database on demand (remember that the automatic download feature, if configured, keeps you up-to-date—see "Scheduling Automatic Downloads for SurfControl" on page 581).

Ordinarily, the ProxySG will check to see if the database has changed before initiating a download. If the database is up to date, then no download is necessary and none is performed. You can override this check and force a download by selecting the Force Full Update checkbox; this option is not needed under normal circumstances.

- a. Click Download Now (if you want to download a full database, first select the Force Full Update checkbox—this option is unnecessary under normal circumstances).

The SurfControl Installation status dialog box displays with the message SurfControl download in progress.

When the operation is complete, the dialog message changes to The new SurfControl filter was successfully downloaded and installed. Use the “Results” button to view full details.

- b. Click Results to see the SurfControl download log:

Download log:

```
SurfControl download at: Thu, 08 Jul 2004 22:43:42 UTC
Downloading from http://listsrv.surfcontrol.com/bluecoat/v4/scdb.md5
Download size: 99279946
Database version: 96
Database date: Thu, 24 Jun 2004 18:27:25 UTC
Database expires: Mon, 23 Aug 2004 18:27:25 UTC
```

5. Click Apply.

To Configure SurfControl Content Filtering through the CLI:

The following commands allow you to enter the username and define the default URL and the default URL location.

1. At the (config) command prompt, enter the following commands:

```
SGOS# (config) content-filter
SGOS# (config content-filter) surfcontrol
SGOS# (config surfcontrol) download license license_key
SGOS# (config surfcontrol) download url {default | url}
```

where:

download license	license_key	Specifies the license key assigned to you for database download.
download url	default	Specifies the use of the default download URL.
	url	The URL is the SurfControl URL. You can change it if directed to do so.

2. (Optional) To download the database now, enter one of the following commands:

```
SGOS# (config surfcontrol) download get-now
-or-
SGOS# (config surfcontrol) download full-get-now
```

where:

download get-now	Initiates an immediate database download. If the database is already up-to-date, no download will be initiated.
download full-get-now	Initiates immediate database download, forcing a download whether or not an update is necessary. This option is unnecessary under most circumstances.

3. (Optional) View the configuration.

```
SGOS#(config surfcontrol) view
Status: Ready
Download License key:
Download URL: http://listsrv.surfcontrol.com/bluecoat/v4/scdb.md5
Automatic download: Enabled
Download time of day (UTC): 0
Download on: sun, mon, tue, wed, thu, fri, sat
Download log:
SurfControl download at: Thu, 08 Jul 2004 22:43:42 UTC
Downloading from http://listsrv.surfcontrol.com/bluecoat/v4/scdb.md5
Download size: 99279946
Database version: 96
Database date: Thu, 24 Jun 2004 18:27:25 UTC
Database expires: Mon, 23 Aug 2004 18:27:25 UTC
```

Using SurfControl Reporter with SGOS 3.x

You can use the SurfControl Reporter with SGOS 3.x access logging to periodically upload information to the SurfControl Reporter reports database.

After you create a SurfControl access logging client, Reporter periodically uploads flat files from the ProxySG. The files are then edited and deleted before loaded into the reports database.

Working with SurfControl Reporter and SGOS 3.x requires several configuration steps. You must:

- Create and configure an access log with SurfControl as the client. For information on configuring a SurfControl access logging client, see "Editing the Custom SurfControl Client" on page 669.
- Download a SurfControl database and configure SurfControl as the content-filtering vendor. For information on downloading a SurfControl database and configuring SurfControl, see "Configuring SurfControl" on page 579.
- Configure the SurfControl server by installing Reporter and configuring the SurfControl Schedule. (Note that the schedule should not be the same as the ProxySG appliance's upload time.) For information on configuring the SurfControl server, refer to the SurfControl server documentation.

Scheduling Automatic Downloads for SurfControl

Note: By default, the automatic download setting is enabled (for every day at midnight, UTC) and does not need to be configured unless you want to change the schedule or disable auto-download.

To download the SurfControl database without creating a schedule, see "Configuring SurfControl" on page 579.

The Automatic Download tab allows you to set the times at which the SurfControl database is downloaded. You can specify an automatic download on the day and time you prefer. Because sites become stale quickly, Blue Coat recommends downloading on an automatic schedule frequently.

When the database is downloaded, a log is available that includes the information about how the database was updated, but in a more detailed form. You can view the download log through the Management Console (Statistics>Advanced>Content Filter Service) or the CLI (`enable>show content-filter status`).

Setting SurfControl Automatic Download Times through the Management Console:

1. Select Configuration>Content Filtering>SurfControl>Automatic Download.

The Automatic Download tab displays.

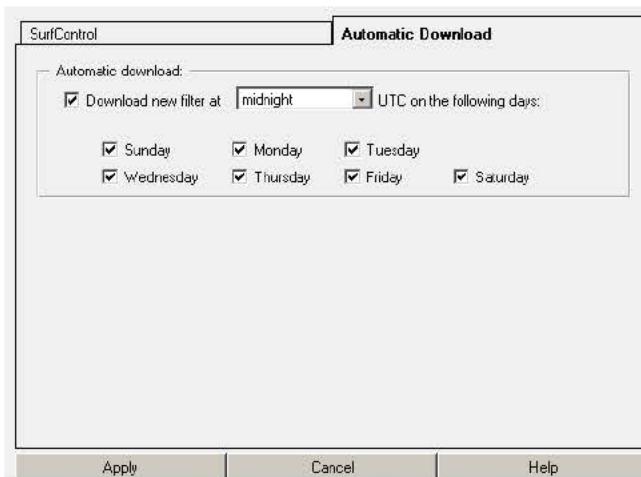


Figure 17-16: SurfControl Automatic Download Tab

2. To set up a schedule for SurfControl database downloads, select the `Download new filter at` checkbox and select the time of day from the drop-down list. The default is `Midnight`.
3. All days are selected by default. Deselect days as desired.
4. Click `Apply` when finished.

Setting SurfControl Automatic Download Times through the CLI:

1. At the `(config)` command prompt, enter the following commands to enable or disable automatic downloading of the SurfControl database.

```
SGOS#(config) content-filter
SGOS#(config content-filter) surfcontrol
SGOS#(config surfcontrol) download auto
-or-
SGOS#(config surfcontrol) no download auto
```

2. At the `(config surfcontrol)` command prompt, enter the following command to select the day(s) to automatically download the local database.

```
SGOS#(config surfcontrol) download day-of-week {all | none | sun | mon | tue |
wed | thu | fri | sat}
-or-
SGOS#(config surfcontrol) no download day-of-week {sun | mon | tue | wed | thu |
fri | sat}
```

where `all` selects all days of the week, and `none` clears all days of the week from the schedule. All days are selected by default; to deselect days, enter `none` and enter specific days. You can only select one day each time, but it is appended to the list. You can also use the `no download day-of-week` command to clear specific days from the schedule.

3. Enter the following command to specify the hour (UTC) of the selected days during which the download should be performed.

```
SGOS# (config surfcontrol) download time-of-day 0-23
```

4. (Optional) To download the SurfControl database now, enter the following command:

```
SGOS# (config surfcontrol) download get-now
```

Downloading the database now does not affect the automatic database download schedule.

Configuring Websense

Use the ProxySG Management Console or the CLI to configure Websense content filtering.

To Configure the Database through the Management Console:

1. Select Configuration>Content Filtering>Websense>Websense.

The Websense download tab displays.

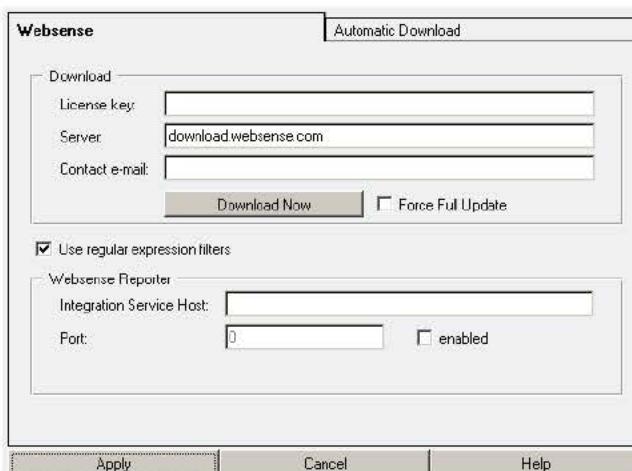


Figure 17-17: Websense Configuration Tab

2. Fill in the fields as appropriate:

- License Key—Enter the license key assigned to you for downloading the Websense database.
- Server—Enter the Websense server from which you wish to download. Your licensing information may suggest an alternate value; otherwise, use the default (`download.websense.com`).
- Contact e-mail—(Optional) Enter an email address through which Websense can contact you.

Important: Websense uses regular expression filters to categorize some Web sites. You can disable these filters if instructed to do so.

Disabling regular expressions prevents Websense from properly categorizing some Web sites and increases the likelihood of the ProxySG serving inappropriate content.

3. (Optional—not recommended) If you do not want to use regular expression filters, de-select the checkbox.
4. To use the Websense Reporter, you must enable the Websense Integration Service.
 - a. In the Integrator Service Host field, enter the Integrator Service Host IP (which has the same IP address as the Websense Log Server).
 - b. In the Port field, specify the port of the Websense Integration Service. It must be between 0 and 65535 and match the port selected on the Integration Service host.
 - c. Click the enabled checkbox to enable the service.

Note: The Policy Server, the Log Server, and Reporter must be installed and enabled on your PC before Reporter can be used. For information on Websense products, refer to <http://www.websense.com/support/documentation/integrationservice>.

You must also set up access logging on the ProxySG with Websense as the client. For more information on configuring a Websense access logging client, see "Editing the Websense Client" on page 671.

5. (Optional) To download the Websense database right away, complete the following steps.

Note: You can return here at any time to download a database on demand (remember that the automatic download feature, if configured, keeps you up-to-date—see "Scheduling Automatic Downloads for Websense" on page 587).

Ordinarily, the ProxySG will check to see if the database has changed before initiating a download. If the database is up to date, then no download is necessary and none is performed. If an incremental update is available on the server, then it is downloaded (an incremental update contains only the changes between the current installed version and the latest published version of the database, and is much smaller than a full copy of the database). You can override this process and force a download of the full database by selecting the Force Full Update checkbox; this option is not needed under normal circumstances.

- a. Click Download Now (if you want to download a full database, first select the Force Full Update checkbox—this option is unnecessary under normal circumstances).

The Websense Installation status dialog box displays with the message Websense download in progress.

When the operation is complete, the dialog message changes to The new Websense filter was successfully downloaded and installed. Use the "Results" button to view full details.

- b. Click Results to view the Websense download log:

```
Download log:  
Websense download at: Thu, 29 Jan 2004 01:36:32 UTC  
    Downloading from download.websense.com  
    Download size: 63642227  
    Database version: 71919  
    Database date: 2004-01-28  
    License expires: Sun, 28 Nov 2004 08:00:00 UTC  
    License max users: 25  
    Licenses in use: 1
```

6. Click Apply.

To Configure Websense through the CLI:

1. At the `(config)` command prompt, enter the following commands to configure the Websense download:

```
SGOS#(config) content-filter  
SGOS#(config content-filter) websense  
  
SGOS#(config websense) download email-contact email_address  
SGOS#(config websense) download server hostname_or_ip_address  
SGOS#(config websense) download license license_key  
SGOS#(config websense) use-regexes | no use-regexes
```

where:

download	email_address	(Optional) Specifies an email address through which Websense can contact you.
email-contact		
download server	hostname_or_ip_address	Specifies the Websense server from which you wish to download. Your licensing information may suggest an alternate value; otherwise, use the default (download.websense.com).
download license	license_key	Specifies the license key assigned to you for downloading the Websense database.
use-regexes		Specifies whether or not to use regular expression filters. Blue Coat strongly recommends that you use regular expression filters.
-or-		
no use-regexes		

2. (Optional) To download the database now, enter one of the following commands:

```
SGOS#(config websense) download get-now  
-or-  
SGOS#(config websense) download full-get-now
```

where:

download get-now	Initiates an immediate database download. An incremental update will be requested.
download full-get-now	Initiates an immediate full-size database download. This option is unnecessary under most circumstances.

3. (Optional) View the configuration.

```
SGOS#(config websense) view
Status: Ready
Download License key: ABC123DEF456GHI789
Download Server: download.websense.com
Email contact:
Automatic download: Enabled
Download time of day (UTC): 0
Download on: sun, mon, tue, wed, thu, fri, sat
Use regular expression filters: Yes
Integration Server: Disabled
Integration Server host:
Integration Server port: 0
Download log:
Websense download at: Sat, 03 Jul 2004 00:27:46 UTC
No database is currently installed
Attempting full download
Downloading from download.websense.com
Processing download file
Retrieved full update
Download size: 74067548
Database version: 82036
Database date: 2004-07-02
License expires: Thu, 29 Jul 2004 08:00:00 UTC
License max users: Unlimited
```

To Configure the Websense Integration Service through the CLI:

Enter the following commands to enable (or disable) and configure the Websense Integration Service through the CLI:

```
SGOS#(config) content-filter
SGOS#(config content-filter) websense
SGOS#(config websense) integration-service {enable | disable}
SGOS#(config websense) integration-service port integer
SGOS#(config websense) integration-service host ip_address_or_hostname
```

where:

port	<i>integer</i>	Specifies the port of the Websense Integration Service. The integer must be between 0 and 65535, and match the port selected on the Integration Service host.
host	<i>ip_address_or_hostname</i>	Specifies the hostname or IP address of the Websense Integration Service, which is the name or IP address of the Websense Log Server.

Note: The Policy Server, the Log Server, and Reporter must be installed and enabled on your PC before Reporter can be used. For information on configuring Websense products, refer to the Websense documentation.

You must also set up access logging on the ProxySG with Websense as the client. For more information on configuring a Websense access logging client, see "Editing the Websense Client" on page 521".

Scheduling Automatic Downloads for Websense

Note: By default, the automatic download setting is enabled (for every day at midnight, UTC) and does not need to be configured unless you want to change the schedule or disable auto-download.

To download the Websense database without creating a schedule, see "Configuring Websense" on page 583.

The Automatic Download tab allows you to set the times the Websense database will download. You can specify an automatic download on the day and time you prefer. Because sites become stale quickly, Blue Coat recommends downloading on an automatic schedule frequently.

When you download the database, a log is available that includes the information about how the database was updated, but in a more detailed form. You can view the download log through the Management Console (Statistics>Advanced>Content Filter Service) or the CLI (enable>show content-filter status).

Setting Websense Automatic Download Times through the Management Console:

1. Select Configuration>Content Filtering>Websense>Automatic Download.

The Automatic Download tab displays.

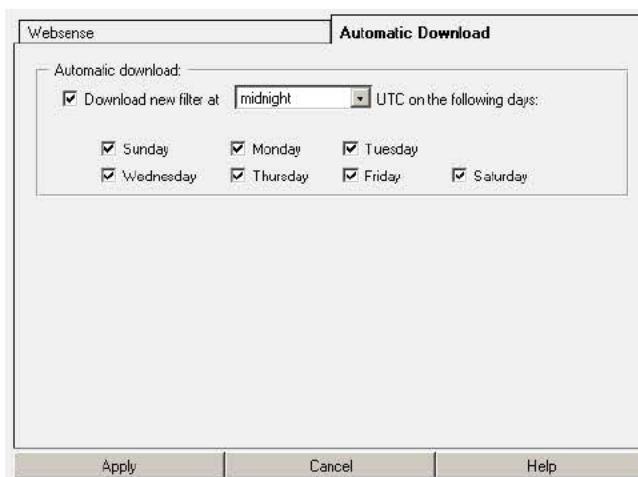


Figure 17-18: Websense Automatic Download Tab

2. To set up a schedule for Websense database downloads, select the Download new filter at checkbox and select the time of day from the drop-down list. The default is Midnight.
3. All days are selected by default. Deselect days as desired.
4. Click Apply when finished.

Setting Websense Automatic Download Times through the CLI:

1. At the `(config)` command prompt, enter the following commands to enable or disable automatic downloading of the Websense database.

```
SGOS#(config) content-filter
SGOS#(config content-filter) websense
SGOS#(config websense) download auto
-or-
SGOS#(config websense) no download auto
```

2. At the `(config websense)` command prompt, enter the following command to select the day(s) to automatically download the local database.

```
SGOS#(config websense) download day-of-week {all | none | sun | mon | tue | wed
| thu | fri | sat}
-or-
SGOS#(config websense) no download day-of-week {sun | mon | tue | wed | thu | fri
| sat}
```

where `all` selects all days of the week, and `none` clears all days of the week from the schedule. All days are selected by default; to deselect days, enter `none` and enter specific days. You can only select one day each time, but it is appended to the list. You can also use the `no download day-of-week` command to clear specific days from the schedule.

3. Enter the following command to specify the hour (UTC) of the selected days during which the download should be done.

```
SGOS#(config websense) download time-of-day 0-23
```

4. (Optional) To download the Websense database now, enter the following command:

```
SGOS#(config websense) download get-now
```

Downloading the database now does not affect the automatic database download schedule.

How to Apply Policy to Categorized URLs

You apply policy to categories in the same way you apply policy to individual URLs: using Content Policy Language. To define policies on the ProxySG, you can either use the Visual Policy Manager or you can manually edit Policy files. For information on managing Policy Files, see Chapter 12: “Managing Policy Files” on page 363.

Note: If you have extensive category definitions, Blue Coat recommends that you put them into a local database rather than into a policy file. The local database stores custom categories in a more scalable and efficient manner, and separates the administration of categories from policy. A local database does, however, have some restrictions that policy does not: no more than 200 separate categories are allowed, category names must be 32 characters or less, and a given URL pattern can appear in no more than four category definitions. You can choose to use any combination of the local database, policy files, and VPM to manage your category definitions. See "Configuring a Local Database" on page 549 for more information.

The CPL trigger `category=` is used to test the category or categories assigned to the request URL, and thus make a policy decision. For example, to block all requests for URLs that are categorized as Sports:

```
DENY category=Sports
```

The following example demonstrates a condition that is true when a request contains the Websense content categories Sexuality and Drugs:

```
<proxy>
    category=(sexuality, drugs)
```

You can block multiple categories with a single rule:

```
category=(Sports, Gambling, Shopping) exception(content_filter_denied)
```

In this example, three categories are blocked and instead the predefined exception page `content_filter_denied` is served; by default this indicates that the request was denied due to its content and specifies the categories found.

The following example shows a condition that includes an extensive number of categories:

```
category=(Abortion, Activist, Adult, Gambling, Illegal, Hacking, Militancy,
Racism, Shopping, Tasteless, Violence, Weapons)
```

Note that URLs which are not categorized are assigned the system category `none`. This is not an error condition; many sites (such as those inside a corporate intranet) are unlikely to be categorized by a commercial service. Use `category=none` to detect uncategorized sites and apply relevant policy. The following example disallows access to uncategorized sites outside of the corporate network:

```
define subnet intranet
    10.0.0.0/8 ; internal network
    192.168.123.45; external gateway
end

<proxy>
    ; allow unrestricted access to internal addresses
    ALLOW url.address=intranet

    ; otherwise (internet), restrict Sports, Shopping and uncategorized sites
    DENY category=(Sports, Shopping, none)
```

Such category tests can also be combined with other types of triggers to produce more complex policy, such as:

- Restrict access by category and time: block sports from 6 am to 6 pm:

```
category=Sports time=0600..1800 DENY
```

- Restrict by category and user identity: only members of the group Sales are permitted to visit Shopping sites:

```
category=Shopping group!=Sales DENY
```

- Require special authentication for access to certain categories:

```
category=Hacking authenticate(restricted.realm)
```

where *restricted.realm* is an authentication realm you have configured.

- Log certain types of access:

```
category=Adult action.Log_adult_site_access(yes)
```

where *Log_adult_site_access* is a policy action defined elsewhere that records extra information about this request in the event log.

In general, `category=` can be used in policy anywhere that a basic URL test can be used. Refer to the *Blue Coat Content Policy Language Guide* for more details.

Depending on which provider you have selected and whether you have defined any of your own categories in policy (see "Defining Custom Categories in Policy" on page 592), you have a number of possible category names that can be used with `category=`. To review the valid category names, use the `categories` CLI command or click **View Categories** in the Management Console (as described in "Selecting Category Providers" on page 546).

The `category=` expressions are normally put in <Proxy> Layers (Web Access Layers in the VPM), because the goal of content-filtering policy is usually to control requests from users. They can also be used in <Cache> (Web Content in the VPM) Layers. Either way, policy is enforced on all user requests.

It is possible for an attempt to categorize a URL to fail—for example, if no database is loaded, your license is expired, or if a system error occurs. In such a case, the category is considered *unavailable* and triggers such as:

```
category=Sports
```

are false, even if the URL is actually a Sports site, because the ProxySG is unable to determine the category. When the policy depends on the category of a URL, you do not want such errors to inadvertently allow ordinarily restricted content to be served by the ProxySG. You can control how the ProxySG treats these situations with the condition:

```
category=unavailable
```

which is true in these cases. In continuing with the example, to make sure that Sports is always blocked, even when errors occur (this is a mode of operation called *fail-closed*), use a rule such as:

```
category=(sports, unavailable) exception(name_of_exception_page)
```

This rule is true if the category is sports or if the category could not be determined, and in either case the proper exception page is served instead of the restricted content.

The category *unlicensed* is assigned in addition to *unavailable* when the failure to categorize occurred because of license expiry. That can be caused by the expiration of your Blue Coat license to use content filtering, or because of expiration of your license from the provider. You can use

```
category=unlicensed
```

to detect this situation as a distinct case from other causes of unavailability.

You can also use this feature with custom exception pages (see Chapter 14: “Advanced Policy” on page 473):

```
<proxy>
    category=sports time=0800..1800 exception(sports_during_bus_hours)
    category=unlicensed exception(contact_admin_re_license)
    category=unavailable exception(content_filter_unavailable)
```

where *sports_during_bus_hours* is a custom exception page you have created to respond to requests for Sports pages between 8 am and 6 pm local time. *contact_admin_re_license* is another page that instructs the user to inform the administrator about license expiry, and is served if a license check fails. When the category is unavailable for some other reason, the pre-defined exception (*content_filter_unavailable*) is served.

Note that the most common reason (other than license expiry) why categories are unavailable is that a provider is selected but no database is installed. Barring hardware or network problems that might cause a downloaded database to become corrupted and unreadable, it is unlikely that the database will suddenly become unavailable.

To define policies on the ProxySG, use either the Visual Policy Manager or manually edit Policy files. Content filtering policies are usually found in `<Proxy>` and `<Cache>` layers.

If you are using content filtering to manage a type of content globally, create these rules in the `<Cache>` layer.

However, if your content filtering policy is dependent on user identity or request characteristics, create these rules in the `<Proxy>` layer.

Using Content-Filtering Vendors with ProxySG Policies

The ProxySG provides the ability to define flexible Web access and control policies. With content filtering, you can set up policies to provide a customized level of Web-site access control. With vendor-based content filtering, these policies use and can supplement vendor categories. By supplementing content-filtering vendor categories, you can further refine the type of content filtering the ProxySG performs. For example, if *Travel* is a vendor-defined content category, you can define a policy that allows only Human Resources staff to access travel sites. You can define policies that filter by a variety of conditions, including category, protocol (including MMS and RTSP streaming protocols), time of day, and user or user groups.

Example

Policy: Limit employee access to travel Web sites.

The first step is to rephrase this policy as a set of rules. In this example, the model of a general rule and exceptions to that rule is used:

- Rule 1: All users are denied access to travel sites
- Rule 2: As an exception to the above, Human Resources users are allowed to visit Travel sites

Before you can write the policy, you must be able to identify users in the Human Resources group. You can do this with an external authentication server, or define the group locally on the ProxySG. For information on identifying and authenticating users, see Chapter 9: “Using Authentication Services” on page 233.

In this example, a group called `human_resources` is identified and authenticated through an external server called `my_auth_server`.

This then translates into a fairly straightforward policy written in the local policy file:

```
<proxy>
; Ensure all access is authenticated
    Authenticate(my_auth_server)

<proxy>
; Rule 1: All users denied access to travel
    DENY category=travel

<proxy>
; Rule 2: Exception for HR
    ALLOW category=travel group=human_resources
    DENY category=sites
```

Example

Policy: Student access to Health sites is limited to a specified time of day, when the Health 100 class is held.

This time the policy contains no exceptions:

- Rule 1: Health sites can be accessed Monday, Wednesday, and Friday from 10-11am.
- Rule 2: Health sites can not be accessed at other times.

```
define condition Health_class_time
    weekday=(1, 3, 5)    time=1000..1100
end

<proxy>
; 1) Allow access to health while class in session
    ALLOW category=health condition=health_class_time
; 2) at all other times, deny access to health
    DENY category=health
```

Defining Custom Categories in Policy

You can use CPL to create your own categories and assign URLs to them. This is done with the `define category` construct (for more complete information on the `define category` construct, refer to *Blue Coat Content Policy Language Guide*). To add URLs to a category, simply list them in the definition. You only need to specify a partial URL:

- hosts and subdomains within the domain you specify will automatically be included
- if you specify a path, all paths with that prefix will be included (if you specify no path, the whole site is included)

Example:

```
define category Grand_Canyon
  kaibab.org
  www2.nature.nps.gov/air/webcams/parks/grcacam
  nps.gov/grca
  grandcanyon.org
end
```

Any URL at `kaibab.org` is now put into the `Grand_Canyon` category (in addition to any category it might be assigned by a provider). Only those pages in the `/grca` directory of `nps.gov` are put in this category.

Nested Definitions and Subcategories

You can define subcategories and nest category definitions by adding a `category=<name>` rule. To continue the example, you could add:

```
define category Yellowstone
  yellowstone-natl-park.com
  nps.gov/yell/
end
define category National_Parks
  category=Grand_Canyon; Grand_Canyon is a subcategory of National_Parks
  category=Yellowstone; Yellowstone is a subcategory of National_Parks
  nps.gov/yose; Yosemite - doesn't have its own category (yet)
end
```

With these definitions, pages at `kaibab.org` are assigned TWO categories: `Grand_Canyon` and `National_Parks`. You can add URLs to the `Grand_Canyon` category and they are automatically added by implication to the `National_Parks` category as well.

Multiple unrelated categories can also be assigned by CPL. For instance, by adding:

```
define category Webcams
  www2.nature.nps.gov/air/webcams/parks/grcacam
end
```

the URL, `http://www2.nature.nps.gov/air/webcams/parks/grcacam/grcacam.htm`, will have three categories assigned to it:

- `Grand_Canyon` (because it appears in the definition directly)
- `National_Parks` (because `Grand_Canyon` is included as a subcategory)
- `Webcams` (because it also appears in this definition)

However, the other sites in the `Grand_Canyon` category are not categorized as `Webcams`. This can be seen by testing the URL (or any other you want to try) using the Test button on the Management Console or the `test-url` command in the CLI, as described in "Selecting Category Providers" on page 546.

You can test for any of these categories independently. For example, the following example is a policy that depends on the above definitions, and assumes that your provider has a category called `Travel` into which most national park sites probably fall. The policy is intended to prevent access to travel sites during the day, with the exception of those designated `National_Parks` sites. But the `Grand_Canyon` webcam is an exception to that exception.

Example:

```
<proxy>
    category=Webcams DENY
    category=National_Parks ALLOW
    category=Travel time =0800..1800 DENY
```

Remember that you can use the **Test** button on the Management Console or the `test-url` command in CLI to validate the categories assigned to any URL. This can help you to ensure that your policy rules have the expected effect (refer to “Configuring Policy Tracing” in the *Blue Coat Content Policy Language Guide*).

If you are using policy-defined categories and a content-filter provider at the same time, be sure that your custom category names do not coincide with the ones supplied by your provider. You can also use the same names—this adds your URLs to the existing categories, and extends those categories with your own definitions. For example, if the webcam mentioned above was not actually categorized as Travel by your provider, you could do the following to add it to the Travel category (for the purpose of policy):

```
define category Travel ; extending a vendor category
    www2.nature.nps.gov/air/webcams/parks/grcacam/ ; add the GC webcam
end
```

Note: The policy definitions described in this section can also be used as definitions in a local database. See “Configuring a Local Database” on page 549 for information about Local Databases.

Tips

- When you use an expired database, the category *unlicensed* will be assigned to all URLs and no lookups will be done on the database. This can occur even if your download license with the database vendor is still valid, but you haven’t downloaded a database for a long time (databases expire after a certain number of days). You can view the date that your database expires (or expired) in the download log or by using the `view` command in the CLI.

When you download a database through the CLI, you can see the download log as soon as the download is complete. To see the download log when you download a database through the Management Console, click the **Results** button in the Installation Status dialog when the download is complete.

To see the last download log without doing another download, enter the following CLI (config) commands:

```
SGOS# (config) content-filter
SGOS# (config content-filter) view
```

- When your license with the database vendor expires, you can no longer download. This does not have an immediate effect—you can still use the database you have for a period of time. But eventually, the database will expire and you will get the category *unlicensed*, as described above.

- If a requested HTTPS host is categorized in a content filtering database, then filtering will apply. However, if the request contains a path and the categorization relies on the host/relative path, content filtering only filters on the host name because the path is not accessible. This might result in a different categorization than if the host plus path were used.
- If you receive an error message when downloading a content-filtering database, check the error message (in the Management Console, click the Results button on the Installation status dialog; in the CLI, the results message appears in the event of an error). If you see an error message such as "ERROR: HTTP 401 - Unauthorized," check that you entered your username and password correctly. For example, the following error message was generated by entering an incorrect username and attempting to download a SmartFilter database:

```
Download log:  
SmartFilter download at: Thu, 08 Apr 2004 18:03:08 UTC  
Checking incremental update  
    Checking download parameters  
    Fetching:http://example.com/  
    Warning: HTTP 401 - Unauthorized  
Downloading full control file  
    SmartFilter download at: Thu, 08 Apr 2004 18:03:17 UTC  
    Downloading from http://example.com/  
    Fetching:http://example.com/  
    ERROR: HTTP 401 - Unauthorized  
    Download failed  
Download failed  
Previous download:  
...
```


Chapter 18: Configuring the Upstream Networking Environment

The ProxySG must interact not only with the local network, but with the upstream network environment to fill requests. To control upstream interaction, various options are supported, such as forwarding, SOCKS gateways, ICP (Internet Caching Protocol), and WCCP (Web Cache Control Protocol).

- Forwarding—Allows you to define the hosts and groups of hosts to which client requests can be redirected. Those hosts can be servers or proxies, including additional ProxySG Appliances. Rules to redirect requests are set up in policy.
Forwarding is available for HTTP, HTTPS, FTP, Windows Media, RTSP, Telnet, and TCP tunnels.
- SOCKS gateways—SOCKS servers provide application level firewall protection for an enterprise. The SOCKS protocol provides a generic way to proxy HTTP.
- ICP—ICP is a service to handle ICP queries from other caching devices looking for cached data. The devices that can access this service can be controlled. ICP can also be used by the ProxySG to locate cached data in other systems.
- WCCP—WCCP is a Cisco®-developed protocol that allows you to establish redirection of the traffic that flows through routers. (For more information on WCCP, see Appendix C: "Using WCCP" on page 785.)

This chapter contains the following topics:

- "Forwarding Configuration"
- "SOCKS Gateway Configuration"
- "Internet Caching Protocol (ICP) Configuration"

Forwarding, SOCKS gateways, and ICP all work together to identify the network topology. Forwarding and SOCKS Gateway each have has a single configuration created either through the CLI or through installable lists. ICP configuration must be created through installable lists.

Note: In SGOS 3.x, ICP, Forwarding, and SOCKS gateways are treated separately.

Forwarding Configuration

Forwarding allows you to define the hosts and groups of hosts to which client requests can be redirected. Those hosts can be servers or proxies, including additional ProxySG Appliances. Rules to redirect requests are configured in policy.

Forwarding stores forwarding hosts' configuration information in the registry; policy is used to create rules for forwarding hosts.

Configuration can be created through the CLI or through installable lists that you can create.

To set the default load-balancing and host-affinity values, you must use the high level load-balance and host-affinity commands (see "Configuring Load Balancing" on page 604 or "Configuring Host Affinity" on page 606). However, three methods are available to you for setting per host or per group settings. You can:

- Use the `(config forwarding) create` command (see "Creating Forwarding Hosts or Host Groups" on page 598).
- Use the `(config forwarding host_alias)` or `(config forwarding group_alias)` commands (see "Editing a Forwarding Host" on page 601 or "Editing a Forwarding Host Group" on page 603).
- Use the `(config forwarding) load-balance` or `(config forwarding) host-affinity` commands (see "Configuring Load Balancing" on page 604 or "Configuring Host Affinity" on page 606).

Note: Forwarding is available for HTTP, HTTPS, FTP, Windows Media, RTSP, Telnet, and TCP tunnels.

The host/group aliases cannot be CPL keywords, such as `no`, `default`, or `forward`.

Configuring Forwarding through the CLI

You can use the CLI to configure your forwarding hosts and describe the upstream network. If you prefer to create an installable list instead of using the CLI, see "Using Forwarding Directives to Create an Installable List" on page 608.

Creating Forwarding Hosts or Host Groups

You can create a maximum of 32 groups, and each group can contain a maximum of 512 hosts. You can create 512 individual hosts that do not belong to any group.

To Create a Host or Host Group through the CLI:

The only required entries under the `create` option (for a host) are the `host_alias`, `host_name`, a protocol, and a port number. The port number can be defined explicitly (such as `http=8080`), or it can take on the default port value of the protocol, if one exists (such as enter `http`, and the default port value of 80 is entered automatically).

To create a host group, you must also include the `group=group_name` command. If this is the first mention of the group, `group_name`, then that group is automatically created with this host as its first member. Do not use this command when creating an independent host.

1. At the `(config)` command prompt, create a forwarding host:

```
SGOS#(config) forwarding
SGOS#(config forwarding) create host_alias host_name [default-schemes]
[http[=port | =no]] [https[=port | =no]] [ftp[=port | =no]] [mms[=port | =no]]
[rtsp[=port | =no]] [tcp=port] [telnet[=port | =no]] [ssl-verify-server[=yes |
=no]] [group=group_name] [server | proxy] [load-balance={no | round-robin |
least-connections}] [host-affinity={no | client-ip-address |
accelerator-cookie}] [host-affinity-ssl={no | client-ip-address |
accelerator-cookie | ssl-session-id}]
```

where:

<i>host_alias</i>		This is the alias for use in policy. Define a meaningful name.
<i>host_name</i>		The name of the host domain, such as <code>www.bluecoat.com</code> , or its IP address.
<i>default-schemes</i>		If you use <i>default-schemes</i> in the directive, all protocols, along with their default ports are selected. This directive is only available for proxy hosts.
<code>http</code> <code>https</code> <code>ftp</code> <code>mms</code> <code>rtsp</code> <code>telnet</code>	<code>=port =no</code>	No protocol is selected by default if the forwarding host is a server. You must choose at least one protocol where <code>port=0</code> to <code>65535</code> . If only one protocol is configured, the ProxySG configures the default port for that protocol. You can use <i>default-schemes</i> and then eliminate protocols by selecting the protocol you do not want; for example, <code>http=no</code> . If you do not want to use the default ports for the protocols, you must also specify them here. HTTPS protocols are not allowed if the host is a proxy.
<code>tcp</code>	<code>=port</code>	If you choose to add a TCP protocol, a TCP port must be specified. TCP protocols are not allowed if the host is a proxy.
<code>ssl-verify-server</code>	<code>=yes =no</code>	Sets SSL to specify that the ProxySG checks the CA certificate of the upstream server. The default for <i>ssl-verify-server</i> is <code>yes</code> . To disable this feature, you must specify <code>ssl-verify-server=no</code> in the installable list or CLI.
<code>group</code>	<code>=group_name</code>	Specifies the group (or server farm or group of proxies) to which this host belongs. If this is the first mention of the group <code>group_name</code> then that group is automatically created with this host as its first member. The ProxySG uses load balancing to evenly distribute forwarding requests to the origin servers or group of proxies. Do not use the <code>group=</code> option when creating independent hosts
<code>server proxy</code>		<code>server</code> specifies to use the relative path for URLs in the HTTP header because the next hop is a Web server, not a proxy server. <code>Proxy</code> is the default.

load-balance	=no =round-robin =least-connections	Specifies either the least-connections or round-robin method of load balancing. Select no to disable load balancing for this forwarding host or host group. If these settings are not specified for a particular host or host group, then the global default settings are used. To configure the settings for a specific host or host group, use the <code>edit host alias</code> or <code>edit group alias</code> commands (see "Editing a Forwarding Host" on page 601 or "Editing a Forwarding Host Group" on page 603).
host-affinity	=no =client-ip-address =accelerator-cookie	Specifies non-SSL host affinity via either a client IP address or an accelerator cookie. Select no to disable non-SSL host affinity for this forwarding host or host group. If these settings are not specified for a particular host or host group, then the global default settings are used. To configure the settings for a specific host or host group, use the <code>edit host alias</code> or <code>edit group alias</code> commands (see "Editing a Forwarding Host" on page 601 or "Editing a Forwarding Host Group" on page 603).
host-affinity-ssl	=no =client-ip-address =accelerator-cookie =ssl-session-id	Specifies SSL host affinity via a client IP address, an accelerator cookie, or an SSL session ID. Select no to disable SSL host affinity for this forwarding host or host group. If these settings are not specified for a particular host or host group, then the global default settings are used. To configure the settings for a specific host or host group, use the <code>edit host alias</code> or <code>edit group alias</code> commands (see "Editing a Forwarding Host" or "Editing a Forwarding Host Group").

2. Repeat step 1 to create additional forwarding hosts or host groups.
3. Complete the configuration by entering the following commands as necessary:

```
SGOS# (config forwarding) download-via-forwarding disable | enable
SGOS# (config forwarding) failure-mode closed | open
SGOS# (config forwarding) integrated-host-timeout minutes
SGOS# (config forwarding) delete {all | group group_name | host host_alias}
SGOS# (config forwarding) path url
SGOS# (config forwarding) no path
```

where:

download-via-forwarding	enable disable	Specifies whether to allow configuration file downloads using forwarding.
failure-mode	closed open	Specifies the default failure mode for forwarding hosts if an operation is unsuccessful.
integrated-host-timeout	minutes	An integrated host is an Origin Content Server (OCS) that has been added to the health check list. The host, added through the <code>integrate_new_hosts</code> property, ages out after being idle for the specified time. The default is 60 minutes.
delete	all group <code>group_name</code> host <code>host_alias</code>	Deletes all forwarding hosts and groups (<code>delete all</code>) or a specific forwarding group (<code>delete group <code>group_name</code></code>) or host (<code>delete host <code>host_alias</code></code>).
path	<code>url</code>	(Optional) Specifies the download path to use if you download forwarding settings through directives.
no	path	Clears the network path URL to download forwarding settings.

Editing a Forwarding Host

Once you have created a forwarding host, you can edit its configuration.

To Edit the Settings of a Forwarding Host through the CLI:

- At the `(config)` command prompt, enter the following commands to configure the settings of a forwarding host:

```
SGOS#(config) forwarding
SGOS#(config forwarding) edit host_alias

SGOS#(config forwarding host_alias) {ftp | http | https | mms | rtsp |
telnet} [port]
SGOS#(config forwarding host_alias) group group_name
SGOS#(config forwarding host_alias) host host_name
SGOS#(config forwarding host_alias) host-affinity method {accelerator-cookie |
client-ip-address | default}
-or-
SGOS#(config forwarding host_alias) host-affinity ssl-method {accelerator-cookie |
client-ip-address | default | ssl-session-id}
SGOS#(config forwarding host_alias) load-balance method {default |
least-connections | round-robin}
SGOS#(config forwarding host_alias) proxy | server
SGOS#(config forwarding host_alias) ssl-verify-server
SGOS#(config forwarding host_alias) tcp port
```

where:

<code>ftp http https mms rtsp telnet</code>	<code>[port]</code>	Adds the protocol and optional port for this host if it was not set previously or changes the port number for the specified protocol if it was. If you do not enter a port number, the default port number is used. HTTPS protocols are not allowed if the host is a proxy.
<code>tcp</code>	<code>port</code>	Changes the port number for the TCP protocol for this host. You must enter a port number if you use the TCP protocol. TCP protocols are not allowed if the host is a proxy.
<code>group</code>	<code>group_name</code>	Changes the group membership for this host.
<code>host</code>	<code>host_name</code>	Changes this host's name.
<code>host-affinity</code>	<code>method {accelerator-cookie client-ip-address default}</code> <code>ssl-method {accelerator-cookie client-ip-address default ssl-session-id}</code>	Changes the non-SSL host affinity method for this host. Changes the SSL host affinity method for this host.
<code>load-balance</code>	<code>method {default least-connections round-robin}</code>	Changes the load balancing method for this host.
<code>proxy</code>		Defines this host as a proxy instead of a server; any HTTPS or TCP port is deleted.
<code>server</code>		Defines this host as a server instead of a proxy.
<code>ssl-verify-server</code>		Sets SSL to specify that the ProxySG checks the CA certificate of the upstream server for this host.

2. (Optional) Enter the following commands to negate or disable settings for this host:

```
SGOS#(config forwarding host_alias) no {ftp | http | https | mms | rtsp | tcp | telnet)
-or-
SGOS#(config forwarding host_alias) no group
SGOS#(config forwarding host_alias) no host-affinity {method | ssl-method}
-or-
SGOS#(config forwarding host_alias) no load-balance method
-or-
SGOS#(config forwarding host_alias) no ssl-verify-server
```

where:

<code>no {ftp http https mms rtsp tcp telnet}</code>		Clears the specified protocol and port from this host.
<code>no group</code>		Removes this host from any and all groups.
<code>no host-affinity</code>	<code>method ssl-method</code>	Disables the host affinity method (non-SSL or SSL) for this host.
<code>no load-balance</code>	<code>method</code>	Disables the load balancing method for this host.
<code>no ssl-verify-server</code>		Disables SSL verification for this host.

Example

```
SGOS# (config) forwarding
SGOS# (config forwarding) edit testhost
SGOS# (config forwarding testhost) server
    ok
SGOS# (config forwarding testhost) no ftp
    ok
SGOS# (config forwarding testhost) exit
SGOS# (config forwarding) exit
SGOS# (config)
```

Editing a Forwarding Host Group

Once you have created a forwarding host group, you can edit its configuration.

To Edit the Settings of a Forwarding Host Group through the CLI:

- At the `(config)` command prompt, enter the following commands to configure the settings of a forwarding host group:

```
SGOS# (config) forwarding
SGOS# (config forwarding) edit group_alias

SGOS# (config forwarding group_alias) host-affinity method {accelerator-cookie
| client-ip-address | default}
-or-
SGOS# (config forwarding group_alias) host-affinity ssl-method
{accelerator-cookie | client-ip-address| default | ssl-session-id}
SGOS# (config forwarding group_alias) load-balance hash {default | domain | url}
-or-
SGOS# (config forwarding group_alias) load-balance method {default |
least-connections | round-robin}
```

where:

host-affinity	method {accelerator-cookie client-ip-address default}	Changes the non-SSL host affinity method for this group.
	ssl-method {accelerator-cookie client-ip-address default ssl-session-id}	Changes the SSL host affinity method for this group.
load-balance	hash {default domain url}	Changes if and how load balancing hashes between group members for this group.
	method {default least-connections round-robin}	Changes the load balancing settings of the method specified for this group.

2. (Optional) Enter the following commands to disable settings for a forwarding host group:

```
SGOS#(config forwarding group_alias) no host-affinity {method | ssl-method}
-or-
SGOS#(config forwarding group_alias) no load-balance {hash | method}
```

where:

no host-affinity	method ssl-method	Disables a host affinity method (non-SSL or SSL) for this group.
no load-balance	hash method	Disables the specified load balancing setting for this group.

Example

```
SGOS#(config) forwarding
SGOS#(config forwarding) edit testgroup
SGOS#(config forwarding testgroup) host-affinity method client-ip-address
    ok
SGOS#(config forwarding testgroup) no load-balance hash
    ok
SGOS#(config forwarding testgroup) exit
SGOS#(config forwarding) exit
SGOS#(config)
```

Configuring Load Balancing

Load-balancing of groups has two stages:

- In the first stage, you optionally apply a hash (a domain name or full URL) to select one host from the group.
- In the second stage, you apply a method (round-robin, least-connections, or none) to the IP addresses of the selected host (the host must have more than one IP address).

If the hash in the first stage is disabled, all of the IP addresses in the group are gathered together and the selected method is applied to the whole set of IP addresses. If the hash in the first stage is enabled and has more than one IP address, it will select one of the member hosts of the group, and that selected host will then have the load balancing method applied to its set of IP addresses.

Load balancing defaults can be configured globally. Each individual host or group will use those defaults unless it is optionally configured to its own private values which override those defaults. See "Creating Forwarding Hosts or Host Groups" on page 598, "Editing a Forwarding Host" on page 601, or "Editing a Forwarding Host Group" on page 603 for ways to set a host or group's individual load-balance configuration (including ways to return it to using the global defaults). The top level load-balance commands shown below can be used to set the global defaults. Those top level commands also provide an alternative way to set the override values for a particular host or group or to return a host or group to using the global defaults.

To Set Load Balancing through the CLI:

```
SGOS# (config) forwarding
SGOS# (config forwarding) load-balance hash {domain | no | url}
SGOS# (config forwarding) load-balance method {least-connections | no | round-robin}
```

where:

hash	{domain no url}	If you use the hash for load balancing, you can choose to hash the domain or the full URL or you can choose no to disable hashing, and the load balancing method applies across a group.
method	{least-connections no round-robin}	If you use method for load balancing, you can select the round-robin method or the least-connections method, or you can specify no to disable load balancing.

To Configure Group Load Balancing through the CLI:

```
SGOS# (config) forwarding
SGOS# (config forwarding) load-balance hash {default | domain | no | url} group_alias
SGOS# (config forwarding) load-balance method {default | least-connections | no | round-robin} host_or_group_alias
```

where:

hash	{default domain no url} <i>group_alias</i>	You can specify a group to apply the load-balancing hash setting to only that group.
method	{default least-connections no round-robin} <i>host_or_group_alias</i>	You can specify a host or group to apply the load-balancing method to only that host or group.

Example

```
SGOS#(config forwarding) load-balance method least-connections test-host-name
ok
```

Configuring Host Affinity

Host affinity is the attempt to direct multiple connections by a single user to the same group member. Host affinity affects load balancing behavior.

Host affinity defaults can be configured globally. Each individual host or group will use those defaults unless it is optionally configured to its own private values which override those defaults. See "Creating Forwarding Hosts or Host Groups" on page 598, "Editing a Forwarding Host" on page 601, or "Editing a Forwarding Host Group" on page 603 for ways to set a host or group's individual host-affinity configuration (including ways to return it to using the global defaults). The top level host-affinity commands shown below can be used to set the global defaults. Those top level commands also provide an alternative way to set the override values for a particular host or group or to return a host or group to using the global defaults.

Note: The non-SSL host affinity methods are implemented for HTTP only and the SSL host affinity methods are implemented for HTTPS only.

To Configure Host Affinity through the CLI:

```
SGOS#(config) forwarding
SGOS#(config forwarding) host-affinity method {accelerator-cookie |
client-ip-address | no}
-or-
SGOS#(config forwarding) host-affinity ssl-method {accelerator-cookie |
client-ip-address | ssl-session-id | no}
SGOS#(config forwarding) host-affinity timeout minutes
```

where:

method	{accelerator-cookie client-ip-address no}	Sets which non-SSL host-affinity method to use (accelerator cookie or client-ip-address) or you can use no to disable non-SSL host affinity.
ssl_method	{accelerator-cookie client-ip-address default ssl-session-id no}	Sets which SSL host-affinity method to use (accelerator cookie, client-ip-address, or ssl-session-id) or you can use no to disable SSL host affinity.
timeout	minutes	Determines how long a user's IP address, SSL ID, or cookie remains valid.

To Configure Group Specific Host-Affinity Settings through the CLI:

```
SGOS# (config) forwarding
SGOS# (config forwarding) host-affinity method {accelerator-cookie |
client-ip-address | default | no} host_or_group_alias
-or-
SGOS# (config forwarding) host-affinity ssl-method {accelerator-cookie |
client-ip-address | default | no | ssl-session-id} host_or_group_alias
```

where:

method	{accelerator-cookie client-ip-address default no} host_or_group_alias	You can choose which non-SSL host-affinity method to use (accelerator cookie or client-ip-address) for a specific host or group, or you can use no to disable non-SSL host affinity for a specific host or group. You can also apply the global non-SSL host-affinity method to a specific host or group.
ssl-method	{accelerator-cookie client-ip-address default no ssl-session-id} host_or_group_alias	You can choose which SSL host-affinity method to use (accelerator cookie, client-ip-address or ssl-session-id) for a specific host or group, or you can use no to disable SSL host affinity for a specific host or group. You can also apply the global SSL host-affinity method to a specific host or group.

Example

```
SGOS# (config forwarding) host-affinity method client-ip-address
      ok
SGOS# (config forwarding) host-affinity ssl-method no test-group-name
      ok
SGOS# (config forwarding) host-affinity timeout 45
      ok
```

Creating a Default Sequence

The default sequence defines the order in which forwarding hosts are used in case of failover and which host to use first (only one default sequence is allowed). All members must be pre-existing hosts and groups, and no member can be in the group more than once.

Note: The default sequence replaces the deprecated `default` and `backup` settings. The default sequence (if present) is applied only if no applicable forwarding gesture is in policy.

A default failover sequence (and any sequence specified in policy) works by allowing healthy hosts to take over for an unhealthy host (one that is failing its DNS Resolution or its health check). The sequence specifies the order of failover, with the second host taking over for the first host, the third taking over for the second, and so on.

If all hosts are unhealthy, the operation fails either open or closed, depending upon your settings.

This configuration is generally created and managed through policy. If no forwarding policy applies, you can create a default sequence through the CLI. This single default sequence consists of a single default host (or group) plus one or more hosts to use if the preceding ones are unhealthy.

To Create a Default Sequence through the CLI:

From the `(config)` prompt, enter the following commands:

```
SGOS# (config forwarding) sequence add alias_name
SGOS# (config forwarding) sequence clear
SGOS# (config forwarding) sequence demote alias_name
SGOS# (config forwarding) sequence promote alias_name
SGOS# (config forwarding) sequence remove alias_name
```

where:

<code>add</code>	<code>alias_name</code>	Adds an alias to the end of the default failover sequence.
<code>clear</code>		Clears the default failover sequence.
<code>demote</code>	<code>alias_name</code>	Moves an alias one place towards the end of the default failover sequence.
<code>promote</code>	<code>alias_name</code>	Moves an alias one place towards the start of the default failover sequence.
<code>remove</code>	<code>alias_name</code>	Removes an alias from the default failover sequence.

Example

```
SGOS# (config forwarding) sequence clear
ok
```

Note: Any host or group in the default sequence is considered in use by policy. As a result, if you try to delete a host or group while it is in the default sequence, you will get an error message. You must remove the host/group from the sequence first, then delete.

Using Forwarding Directives to Create an Installable List

You can use either directives or the CLI to create and configure forwarding hosts. To use the CLI, see "Configuring Forwarding through the CLI" on page 598.

The forwarding configuration includes directives that:

- Create the forwarding hosts and groups
- Provide load balancing and host affinity

Table 18.1: Forwarding Directives

Directive	Meaning	See
<code>fwd_fail</code>	Determines whether the forwarding host should fail open or fail closed if an operation does not succeed. Fail open is a security risk.	"Setting Fail Open/Closed and Host Timeout Values" on page 611.

Table 18.1: Forwarding Directives

fwd_host	Create a forwarding host and set configuration parameters for it, including protocols and ports.	"Creating Forwarding Host and Group Directives" on page 609.
host_affinity	The attempt to direct multiple connections by a single user to the same group member.	"Configuring Host Affinity Directives" on page 613.
integrated_host_timeout	An origin content server that has been added to the health check list is called an integrated host. The host ages out after being idle for the specified time.	"Setting Fail Open/Closed and Host Timeout Values" on page 611.
load_balance	The attempt to manage the load among forwarding hosts in a group, or among multiple IP addresses of a host.	"Configuring Load Balancing Directives" on page 612.
sequence alias_list	where <i>alias_list</i> is a space separated list of one or more forwarding host and group aliases.	"Creating a Default Sequence" on page 613.

Creating Forwarding Host and Group Directives

You can add directives into the forwarding installable list that allows you to create and delete the forwarding host and associate protocols and ports with the host.

You can create a maximum of 32 groups, and each group can contain a maximum of 512 hosts. You can create 512 individual hosts that do not belong to any group.

To create a forwarding host, choose the protocols you want to use, or optionally add the forwarding host to a group, enter the following into your installable list. You should create a `fwd_host` directive for each forwarding host you want to create.

```
fwd_host host_alias host_name [default-schemes] [http[=port | =no]] [https[=port | =no]] [ftp[=port | =no]] [mms[=port | =no]] [rtsp[=port | =no]] [tcp=port] [telnet[=port | =no]] [ssl-verify-server[=yes | =no]] [group=group_name] [server | proxy] [load-balance={no | round-robin | least-connections}] [host-affinity={no | client-ip-address | accelerator-cookie}] [host-affinity-ssl={no | client-ip-address | ssl-session-id}]
```

where:

<i>host_alias</i>		This is the alias for use in policy. Define a name meaningful to you.
<i>host_name</i>		The name of the host domain, such <code>www.bluecoat.com</code> , or its IP address.
<i>default-schemes</i>		If you use default-schemes in the directive, all protocols, along with their default ports are selected. This directive is only available for proxy hosts.

http https ftp mms rtsp telnet	=port =no	No protocol is selected by default if the forwarding host is a server. You must choose at least one protocol where port=0 to 65535. If only one protocol is configured, the ProxySG configures the default port for that protocol. You can use default-schemes and then eliminate protocols by selecting the protocol you do not want; for example, http=no. If you do not want to use the default ports for the protocols, you must also specify them here. HTTPS protocols are not allowed if the host is a proxy.
tcp	=port	If you choose to add a TCP protocol, a TCP port must be specified. TCP protocols are not allowed if the host is a proxy.
ssl-verify-server	=yes =no	Sets SSL to specify that the ProxySG checks the CA certificate of the upstream server. The default for ssl-verify-server is yes. To disable this feature, you must specify ssl-verify-server=no in the installable list or CLI. In other words, you can configure ssl-verify-server=yes in three ways: do nothing (yes is the default), specify ssl-verify-server, or specify ssl-verify-server=yes.
group	=group_name	Specifies the group (or server farm or group of proxies) to which this host belongs. If this is the first mention of the group <i>group_name</i> then that group is automatically created with this host as its first member. The ProxySG uses load balancing to evenly distribute forwarding requests to the origin servers or group of proxies. Do not use the group= option when creating independent hosts.
server proxy		<i>server</i> specifies to use the relative path for URLs in the HTTP header because the next hop is a Web server, not a proxy server. The default is proxy.

load-balance	=no =round-robin =least-connections	Specifies either the least-connections or round-robin method of load balancing. Select no to disable load balancing for this forwarding host or host group. If these settings are not specified for a particular host or host group, then the global default settings are used. To configure the settings for a specific host or host group, use the <code>edit host_alias</code> or <code>edit group_alias</code> commands (see "Editing a Forwarding Host" on page 601 or "Editing a Forwarding Host Group" on page 603).
host-affinity	=no =client-ip-address =accelerator-cookie	Specifies non-SSL host affinity via either a client IP address or an accelerator cookie. Select no to disable non-SSL host affinity for this forwarding host or host group. If these settings are not specified for a particular host or host group, then the global default settings are used. To configure the settings for a specific host or host group, use the <code>edit host_alias</code> or <code>edit group_alias</code> commands (see "Editing a Forwarding Host" on page 601 or "Editing a Forwarding Host Group" on page 603).
host-affinity-ssl	=no =client-ip-address =accelerator-cookie =ssl-session-id	Specifies SSL host affinity via a client IP address, an accelerator cookie, or an SSL session ID. Select no to disable SSL host affinity for this forwarding host or host group. If these settings are not specified for a particular host or host group, then the global default settings are used. To configure the settings for a specific host or host group, use the <code>edit host_alias</code> or <code>edit group_alias</code> commands (see "Editing a Forwarding Host" on page 601 or "Editing a Forwarding Host Group" on page 603).

Example

```
fwd_host www.bluecoat1.com 10.25.36.48 default-schemes ssl-verify-server=no
group=bluecoat
```

Setting Fail Open/Closed and Host Timeout Values

Using directives, you can determine if the forwarding host fails open or closed, if an operation does not succeed, and the interval it takes for integrated hosts to be aged out.

An integrated host is an Origin Content Server (OCS) that has been added to the health check list. If the policy property `integrate_new_hosts` applies to a forwarding request, Blue Coat makes a note of each OCS and starts health checking to help future accesses to those systems. If the host is idle for the interval you specify, it is aged out. Sixty minutes is the default.

The syntax is:

```
fwd_fail {open | closed}  
integrated_host_timeout minutes
```

where:

<code>fwd_fail</code>	<code>{open closed}</code>	Determines whether the forwarding host should fail open or fail closed if an operation does not succeed. Fail open is a security risk, and fail closed is the default if no setting is specified. This setting can be overridden by policy, (using the <code>forward.fail_open(yes no)</code> property).
<code>integrated_host_timeout</code>	<code>minutes</code>	An OCS that has been added to the health check list is called an integrated host. The host ages out after being idle for the specified time.

Examples

```
fwd_fail open  
integrated_host_timeout 90
```

Configuring Load Balancing Directives

Load balancing shares the load among a set of IP addresses, whether a group or a host with multiple IPs.

The syntax is:

```
load_balance hash {domain | no | url} [group_alias]  
load_balance method {least-connections | round-robin | no} [host_or_group_alias]
```

where:

<code>hash</code>	<code>{domain no url}</code> [<code>group_alias</code>]	If you use the hash for load balancing, you can choose to hash the domain or the full URL, or you can choose <code>no</code> to disable hashing and the load-balancing method will apply across a group. If you do not specify a group, the settings apply as the default for all groups.
-------------------	--	---

method	{least-connections no round-robin} [host_or_group_alias]	If you use method for load balancing, you can select the least-connections method or the round-robin method, or you can specify no to disable load balancing (hashing will still occur if it is set). If you do not specify a host or group, the settings apply as the default for all hosts or groups.
--------	--	---

Example

```
load_balance method least_connections
```

Configuring Host Affinity Directives

Host affinity is the attempt to direct multiple connections by a single user to the same group member.

The syntax is:

```
host_affinity method {accelerator-cookie | client-ip-address | no}  
[host_or_group_alias]  
host_affinity ssl_method {client-ip-address | no | ssl-session-id}  
[host_or_group_alias]  
host_affinity timeout seconds
```

where:

method	{accelerator-cookie client-ip-address no} [host_or_group_alias]	You can choose which non-SSL host-affinity method to use (accelerator cookie or client-ip-address), or you can use no to disable non-SSL host affinity. If you do not specify a host or group, the settings apply as the default for all hosts or groups.
ssl_method	{accelerator-cookie client-ip-address no ssl-session-id} [host_or_group_alias]	You can choose which SSL host-affinity method to use (client-ip-address or ssl-session-id), or you can use no to disable SSL host affinity. If you do not specify a host or group, the settings apply as the default for all hosts or groups.
timeout	minutes	Determines how long a user's IP address, SSL ID, or cookie remains valid.

Example

```
host_affinity ssl_method 10.25.36.48  
host_affinity timeout 5
```

Creating a Default Sequence

A default sequence defines the order in which forwarding hosts are used. Only one default sequence is allowed. All members must be pre-existing hosts and groups, and no member can be in the group more than once.

Note: The default sequence, completely overridden by policy, replaces the deprecated `default` and `backup` settings.

A default failover sequence works by allowing healthy hosts to take over for an unhealthy host (one that is failing its DNS Resolution or its health check). The sequence specifies the order of failover, with the second host taking over for the first host, the third taking over for the second, and so on).

If all hosts are unhealthy, the operation fails either open or closed, depending upon your settings.

This configuration is generally created and managed through policy. If no forwarding policy applies, you can create a default sequence through the CLI. This single default sequence consists of a single default host (or group) plus one or more hosts to use if the preceding ones are unhealthy.

The syntax is

```
sequence alias_list alias_list
```

where `alias_list` is a space-separated list of one or more forwarding host and group aliases.

Example

```
sequence bluecoat
```

Creating a Forwarding Installable List

You can create and install the forwarding installable list with the following methods:

- Use the ProxySG Text Editor, which allows you to enter the installable list of directives (or copy and paste the contents of an already-created file) directly onto the ProxySG.
- Create a local file on your local system; the ProxySG can browse to the file and install it.
- Enter a remote URL, where you placed an already-created file on an FTP or HTTP server to be downloaded to the ProxySG.
- Use the CLI `inline` command.

When the Forwarding Installable List is installed, it updates the forwarding directives on the ProxySG. The directives remain in effect until they are overwritten by another installable list; the list can be modified or overwritten using CLI commands.

Note: During the time that a forwarding installable list is being compiled and installed, forwarding is not available. Any transactions that come into the ProxySG during this time will not be forwarded properly and will be denied.

Installation of forwarding installable lists should be done outside peak traffic times.

To Create a Forwarding Installable List through the Management Console:

1. Select Configuration>Forwarding>Forwarding Hosts.

The Forwarding Hosts tab displays.

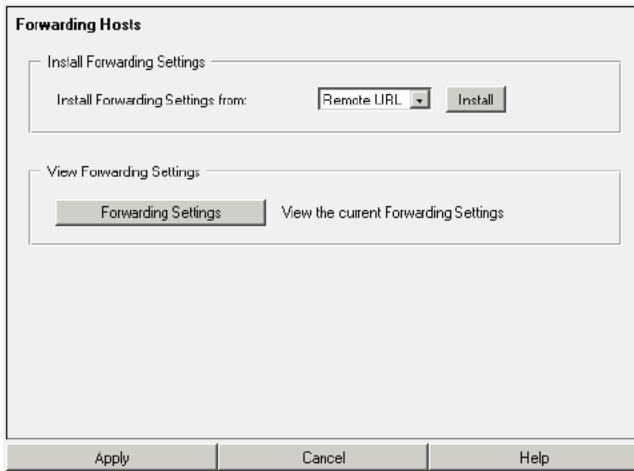


Figure 18-1: Selecting the Forwarding Hosts Download Method

2. From the drop-down list, select the method to use to install the forwarding installable list; click Install.

Remote URL:

Enter the fully-qualified URL, including the filename, where the installable list is located. To view the file before installing it, click View. Click Install. Examine the installation status that displays; click OK.

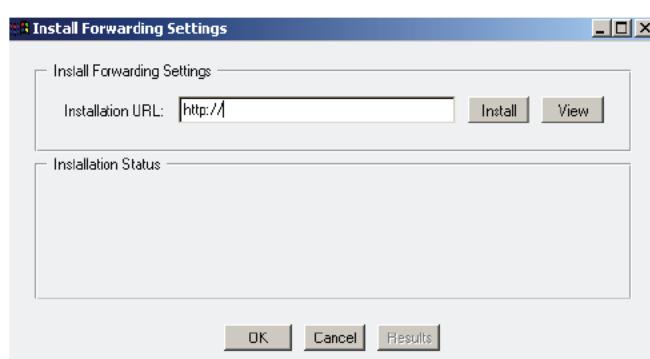


Figure 18-2: Specifying the Remote Location of a Forwarding Configuration

Local File:

Click Browse to bring up the Local File Browse window. Browse for the installable list file on the local system. Open it and click Install. When the installation is complete, a results window opens. View the results, close the window, click Close.

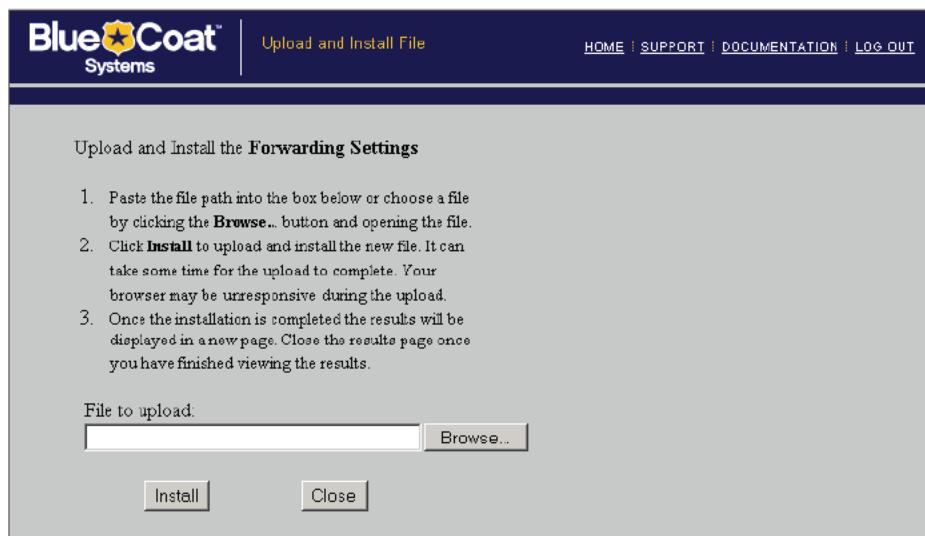


Figure 18-3: Specifying the Local Location of a Forwarding Configuration

Text Editor:

The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click **Install**. When the installation is complete, a results window opens. View the results, close the window, click **Close**.

Note: The Management Console text editor is a way to enter an installable list for forwarding. It is not a way to enter CLI commands. The directives are understood only by the installable list parser for forwarding.

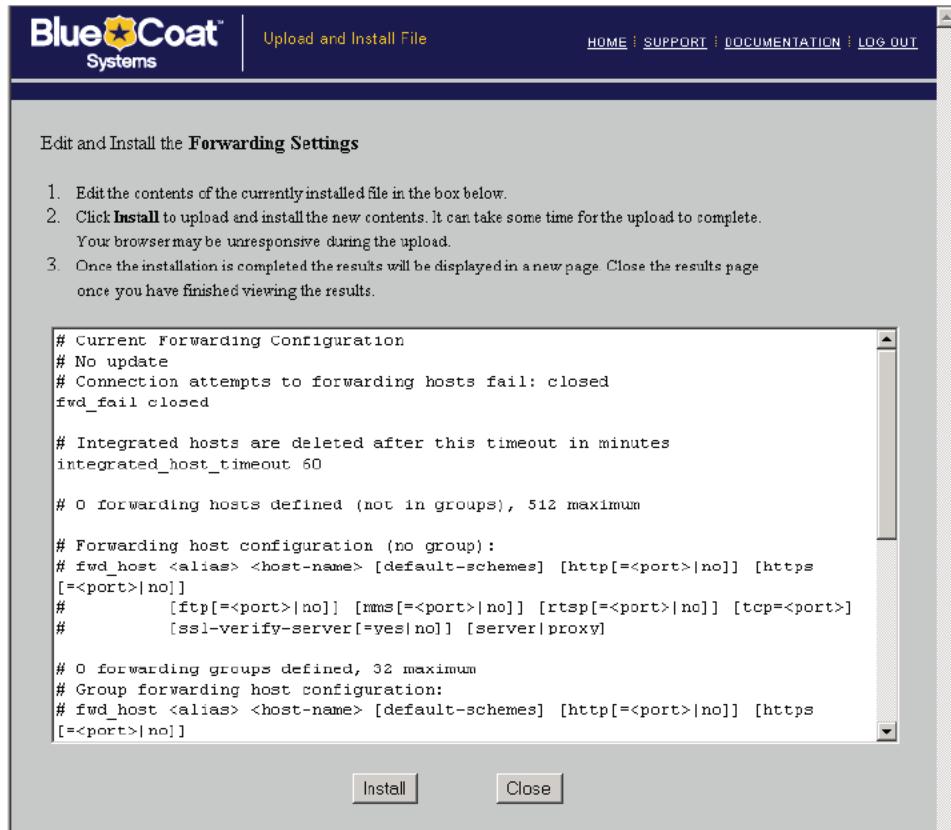


Figure 18-4: Using the ProxySG Text Editor

3. Click Apply.

To Create a Remote Forwarding Installable List through the CLI:

At the (config) command prompt, enter the following commands:

```

SGOS#(config) forwarding
SGOS#(config forwarding) path url

```

where *url* is a fully-qualified URL, including the filename, where the installable list is located.

```

SGOS#(config forwarding) exit
SGOS#(config) load forwarding

```

To Create Forwarding Settings on the ProxySG through the CLI:

1. At the `(config)` command prompt, enter the following commands to create an inline set of commands. You can use any of the forwarding directives, but host affinity and load balancing are mutually exclusive. The procedure below demonstrate the creation of an inline forwarding configuration, using the non-SSL host affinity method:

```
SGOS#(config) inline forwarding eof
fwd_host test 10.25.36.47 default-schemes
host_affinity method client-ip-address
host_affinity timeout 45
eof
ok
```

where:

<code>forwarding</code>	Identifies the kind of inline settings you are creating.
<code>eof</code>	Indicates the marker you use to tell the CLI that you are beginning or ending the set of commands. You can use any characters as the end-of-file marker.

The limitation to using the `inline` command to create a configuration is that you cannot create mistakes except on the current line. If you find an error farther back than that, you must start over after exiting the current file.

2. View the results.

```
SGOS#(config) show forwarding
download-via-forwarding: enabled
Connection attempts to forwarding hosts fail: closed.
Forwarding Groups: (* = host unresolved)
  Group: techpubs
    test3          10.25.36.47 http=80 ftp=21 rtsp=554
  Individual Hosts: (* = host unresolved)
    No individual hosts defined.
  Load balancing hash: domain
  Load balancing method: no
  Host affinity method (non-SSL): client-ip-address
  Host affinity method (SSL): client-ip-address
  Host affinity timeout: 45 minutes
```

To Delete Forwarding Settings on the ProxySG through the CLI

From the `(config)` prompt, enter the following commands to delete a host, a group, or all hosts and groups from the forwarding configuration:

```
SGOS#(config) forwarding
SGOS#(config forwarding) delete {all | group group_name | host host_alias}
```

Note: Any host or group in the default sequence is considered in use by policy. As a result, if you try to delete a host or group while it is in the default sequence, you receive an error message. You must remove the host/group from the sequence first, then delete.

SOCKS Gateway Configuration

The ProxySG implementation of SOCKS includes the following:

- A SOCKS proxy server that supports both SOCKSv4/4a and SOCKSv5, running on the ProxySG.
- Support for forwarding through SOCKS gateways.

To configure a SOCKS proxy server on the ProxySG, see "Configuring a SOCKS Proxy" on page 160. To use SOCKS gateways when forwarding, continue with the next section.

Note: SOCKS gateway aliases cannot be CPL keywords, such as no, default, forward, or socks_gateways.

Using SOCKS Gateways

SOCKS servers provide application level firewall protection for an enterprise. The SOCKS protocol provides generic way to proxy HTTP.

SOCKS gateways, like ICP and forwarding, can use installable lists for configuration. You can configure the installable list using directives. You can also use the CLI to create a SOCKS gateways configuration.

Using the CLI to Create SOCKS Gateways Settings

If you prefer, you can use SOCKS gateways CLI commands, instead of an installable list, to create SOCKS gateways settings.

To Create a SOCKS Gateways Host through the CLI:

1. At the (config) command prompt, enter the following commands:

```
SGOS# (config) socks-gateways
SGOS# (config socks-gateways) create gateway_alias gateway_host SOCKS_port
[version =4 | =5 [user=username password=password]]
```

where:

<i>gateway_alias</i>		A name, meaningful to you.
<i>gateway_host</i>		The IP address or the host name of the gateway where traffic will be directed. The host name must DNS resolve.
<i>SOCKS_port</i>		The port number of the SOCKS gateway.
<i>version</i>	=4 =5	The version that SOCKS gateways can support. (SOCKS v5 is recommended, if you have a choice). If no version is configured, the default is version 4.
<i>user</i>	= <i>username</i>	(Optional, and only if you use v5) The username of the user on the SOCKS gateway. The username already must exist on the gateway. If you use user=, you must also use password=.

password	=password	(Optional, and only if you use v5) The password of the user on the SOCKS gateway. The password must match the gateway's information. If you use user=, you must also use password=.
----------	-----------	---

2. Repeat for step 1 for each gateway you want to create. The **failure-mode** command applies to all SOCKS gateways configured on the system. The default failure mode can be overridden using policy.
3. Complete the configuration by entering the following commands as necessary:

```
SGOS# (config socks-gateways) failure-mode {open | closed}
SGOS# (config socks-gateways) delete {all | gateway gateway_alias}
SGOS# (config socks-gateways) path url
SGOS# (config socks-gateways) no path
```

where:

failure-mode	open closed	If the health checks fail, open specifies that the connection be attempted without use of any SOCKS gateway (whether to an origin content server or a forwarding target); closed specifies that the connection be aborted.
delete	all gateway <i>gateway_alias</i>	Deletes all SOCKS gateways (delete all) or a specific SOCKS gateway (delete gateway <i>gateway_alias</i>).
path	<i>url</i>	(Optional) Specifies the download path to use if you download SOCKS-gateways settings through directives.
no	path	Clears the network path URL to download SOCKS gateway settings.

4. View the results.

```
SGOS# (config socks-gateways) view
SOCKS Gateways: (* = gateway unresolved)
Sec_App1          10.25.36.47 1080  V5
```

Editing a SOCKS Gateways Host

Once you have created a SOCKS gateways host, you can edit the settings.

To Edit the Settings of a SOCKS Gateways Host:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) socks-gateways
SGOS# (config socks-gateways) edit gateway_alias
```

```
SGOS# (config socks-gateways gateway_alias) host gateway_host
SGOS# (config socks-gateways gateway_alias) no {password | user}
SGOS# (config socks-gateways gateway_alias) password password
SGOS# (config socks-gateways gateway_alias) port socks_port
SGOS# (config socks-gateways gateway_alias) user username
SGOS# (config socks-gateways gateway_alias) version {4 | 5}
```

where:

host	<i>gateway_host</i>	Changes the host name.
no	password user	Optional, and only if you use version 5. Deletes the version 5 password or username.
password	<i>password</i>	Optional, and only if you use version 5. Changes the version 5 password.
port	<i>socks_port</i>	Changes the SOCKS port.
user	<i>username</i>	Optional, and only if you use version 5. Changes the version 5 username.
version	4 5	Changes the SOCKS version.

Example

```
SGOS# (config) socks-gateways
SGOS# (config socks-gateways) edit testsocks
SGOS# (config socks-gateways testsocks) port 23
    ok
SGOS# (config socks-gateways testsocks) version 5
    ok
SGOS# (config socks-gateways testsocks) exit
SGOS# (config socks-gateways) exit
SGOS# (config)
```

Creating a Default Sequence

A default sequence defines the order in which SOCKS gateways hosts are used. Only one default sequence is allowed. All members must be pre-existing hosts, and no member can be in the group more than once.

Note: The default sequence replaces the deprecated `default` and `backup` settings. The default sequence (if present) is applied only if no applicable forwarding gesture is in policy.

A default failover sequence works by allowing healthy hosts to take over for an unhealthy host (one that is failing its DNS Resolution or its health check). The sequence specifies the order of failover, with the second host taking over for the first host, the third taking over for the second, and so on.

If all hosts are unhealthy, the operation fails either open or closed, depending upon your settings.

This configuration is generally created and managed through policy. If no SOCKS-gateways policy applies, you can create a default sequence through the CLI. This single default sequence consists of a single default host (or group) plus one or more hosts to use if the preceding ones are unhealthy.

The syntax is:

```
sequence alias_name alias_name
```

where *alias_name* is a space-separated list of one or more SOCKS gateways.

To create a default failover sequence, enter the following commands from the (config) prompt:

```
SGOS#(config) socks-gateways
SGOS#(config socks-gateways) sequence add gateway-alias
SGOS#(config socks-gateways) sequence promote | demote gateway-alias
SGOS#(config socks-gateways) sequence clear | remove gateway-alias
```

where:

sequence	add	Adds an alias to the end of the default fail-over sequence.
	clear	Clears the default fail-over sequence.
	demote	Demotes an alias one place towards the end of the default fail-over sequence.
	promote	Promotes an alias one place towards the start of the default fail-over sequence.
	remove	Removes an alias from the default fail-over sequence.

Using SOCKS Gateways Configuration Directives to Create an Installable List

To configure a SOCKS gateway you must create an installable list and load it on the ProxySG. Alternately, you can use the CLI to configure SOCKS gateways. To use the CLI, see "Using the CLI to Create SOCKS Gateways Settings" on page 619.

For information on installing the file itself, see "Creating a SOCKS Gateway Installable List" on page 624.

The SOCKS gateways configuration includes SOCKS directives that:

- Names the SOCKS gateway hosts
- Specifies the SOCKS version
- (Optional, if using Version 5) Specifies user name and password

Available directives are described in the table below.

Table 18.2: SOCKS Gateway Directives

Directive	Meaning
gateway	Specifies the gateway alias and name, SOCKS port, version supported, usernames and password.
socks_fail	In case connections cannot be made, specifies whether to abort the connection attempt or to connect to the origin content server
sequence	Specifies the order in which hosts should be used for failover.

Syntax for the SOCKS directives are:

```

gateway gateway_alias gateway_host SOCKS_port [version={4 | 5 [user=username
password=password]}]
socks_fail {open | closed}
sequence gateway_name

```

where:

gateway		Configures the SOCKS gateway host.
	gateway_alias	A meaningful name that is used for policy rules.
	gateway_host	The IP address or host name of the gateway where traffic will be directed. The host name must DNS resolve.
	SOCKS_port	The port number of the SOCKS gateway.
	version={4 5}	The version that SOCKS gateways can support.
	user=username	(Optional, if you use v5) The username of the user on the SOCKS gateway. It already must exist on the gateway.
	password=password	(Optional, if you use v5) The password of the user on the SOCKS gateway. It must match the gateway's information.
socks_fail	{open closed}	If health checks fail, socks_gateway.fail_open specifies that the connection be attempted without using a SOCKS gateway (for example, go to the original server or forwarding target); socks_gateway.fail_closed specifies that the connection be aborted. The default is closed. Fail open is a security risk, and fail closed is the default if no setting is specified. This setting can be overridden by policy, (using the forward.fail_open(yes no) property).
sequence	gateway_name	Specifies the order in which hosts should be used for failover.

Example

```

gateway Sec_App1 10.25.36.47 1022 version=5 user=username password=password
socks_gateway.fail_open no

```

Important: The username and password display in clear text if you run the show config command.

A default sequence defines the order in which forwarding hosts are used. Only one default sequence is allowed. All members must be pre-existing hosts and groups, and no member can be in the sequence more than once.

Note: The default sequence replaces the deprecated `default` and `backup` settings. The default sequence (if present) is applied only if no applicable forwarding gesture is in policy.

A default failover sequence works by allowing healthy hosts to take over for an unhealthy host (one that is failing its DNS Resolution or its health check). The sequence specifies the order of failover, with the second host taking over for the first host, the third taking over for the second, and so on).

If all hosts are unhealthy, the operation fails either open or closed, depending upon your settings.

This configuration is generally created and managed through policy. If no SOCKS-gateways policy applies, you can create a default sequence through the CLI. This single default sequence consists of a single default host (or group) plus one or more hosts to use if the preceding ones are unhealthy.

The syntax is

```
sequence gateway_name gateway_name  
where gateway_name is a space-separated list of one or more SOCKS gateway aliases.
```

Example

```
sequence gateway_alias
```

Creating a SOCKS Gateway Installable List

You can create and install the SOCKS gateway installable list with the following methods:

- Use the ProxySG Text Editor, which allows you to enter directives (or copy and paste the contents of an already-created file) directly onto the ProxySG.
- Create a local file on your local system; the ProxySG can browse to the file and install it.
- Use a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the ProxySG.

When the SOCKS gateway installable list is created, it overwrites any previous SOCKS gateway configurations on the ProxySG. The installable list remains in effect until it is overwritten by another installable list; it can be modified or overwritten using CLI commands.

Note: During the time that a SOCKS gateway installable list is being compiled and installed, forwarding is not available. Any transactions that come into the ProxySG during this time will not be forwarded properly and will be denied.

Installation of SOCKS gateways installable-list configuration should be done outside peak traffic times.

To Create a SOCKS Gateways Installable List through the Management Console:

1. Select Configuration>Forwarding>SOCKS Gateways.

The SOCKS Gateways tab displays.

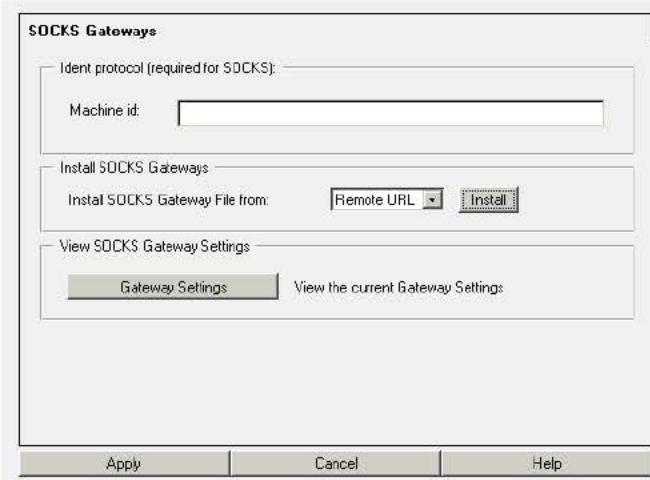


Figure 18-5: Selecting the SOCKS Gateways Tab

2. If you use a SOCKS gateway server for the primary or alternate forwarding gateway, you must specify the ProxySG ID for the Identification (Ident) protocol used by the SOCKS gateway in SOCKS' server handshakes. The default is BLUECOAT SYSTEMS.
3. From the drop-down list, select the method used to install the SOCKS gateway configuration; click **Install**.

Remote URL:

Enter the fully-qualified URL, including the filename, where the configuration is located. To view the file before installing it, click **View**. Click **Install**. Examine the installation status that displays; click **OK**.

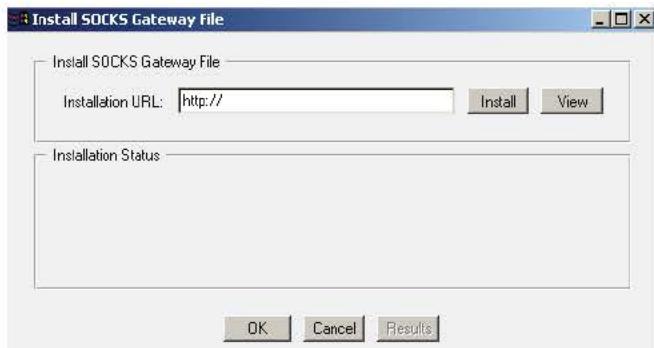


Figure 18-6: Specifying the Remote Location of the SOCKS Gateways Configuration

Local File:

Click **Browse** to bring up the Local File Browse window. Browse for the file on the local system. Click **Install**. When the installation is complete, a results window opens. View the results, close the window, click **Close**.

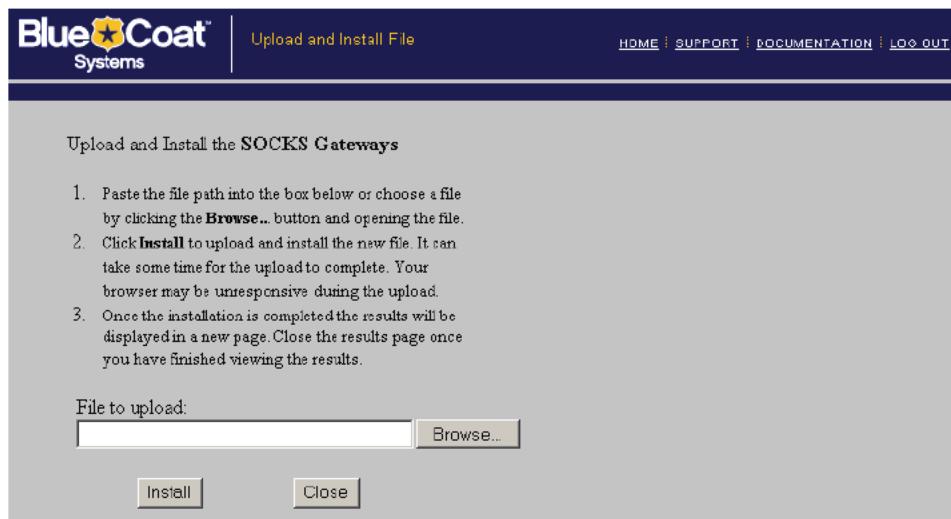


Figure 18-7: Specifying the Local Location of the SOCKS Gateways Configuration

Text Editor:

The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click **Install**. When the installation is complete, a results window opens. View the results, close the window, click **Close**.

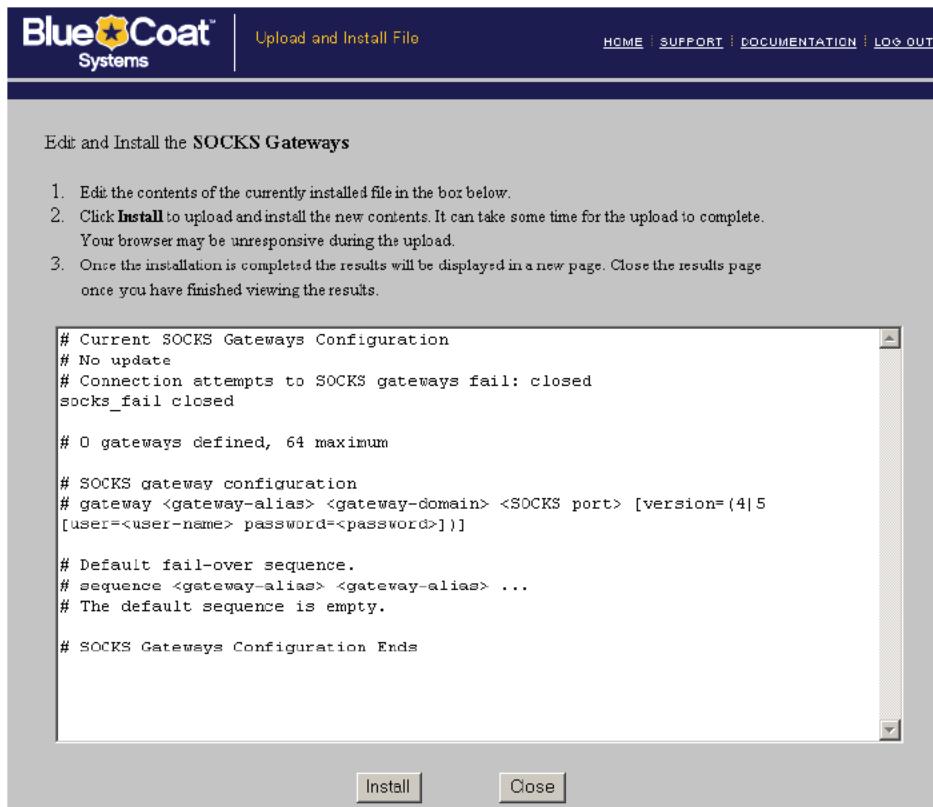


Figure 18-8: Using the ProxySG Text Editor

4. Click Apply.

To Specify the SOCKS Gateway Machine ID through the CLI:

Note: This is an optional command. The default is BLUE COAT SYSTEMS.

At the config command prompt, enter the following command:

```
SGOS#(config) socks-machine-id machine_ID
```

To Create a Remote SOCKS Gateways Installable List through the CLI:

At the (config) prompt, enter the following commands:

```
SGOS#(config) socks-gateways
SGOS#(config socks-gateways) path url
```

where *url* is a fully-qualified URL, including the filename, where the configuration is located.

```
SGOS#(config) socks-gateways) exit
SGOS#(config) load socks-gateways
```

Tip for SOCKS Configuration

By default, SOCKS treats all incoming requests destined to port 80 as HTTP, allowing the usual HTTP policy to be done on them, including ICAP scanning. If the SOCKS connection is being made to a server on another port, you should write policy on the ProxySG to match on the server host and port and specify that it is HTTP using SOCKS.

Internet Caching Protocol (ICP) Configuration

ICP is a communication protocol for caches. It allows a cache (not necessarily a ProxySG) to query other caches for an object, without actually requesting the object. By using ICP, the cache can determine if the object is available from a neighboring cache, and which cache will provide the fastest response.

Note: The ProxySG (assuming ICP is configured) does ICP queries only if no forwarding host or SOCKS gateway is identified as an upstream target. If ICP is used by the ProxySG, it prompts other cache devices for the item, and upon a positive response re-directs the upstream request to that cache device instead of the content origin server.

Only use ICP if you have ICP hosts available or if you want the ProxySG to support requests from other ICP hosts.

By default, the ICP protocol requires the requesting host to wait up to two seconds for all ICP hosts to respond to the request for an object (the time is configurable).

If the ICP service is configured and running, the service is used if no forwarding or SOCKS gateway target was specified. In other words, the policy rule `icp(yes)` is the default, assuming that the ICP service is available. You can disable ICP with the policy rule `icp(no)` to control ICP queries for requests.

Configuring ICP

An ICP *hierarchy* is comprised of a group of caches, with defined parent and sibling relationships. A cache parent is one that can return the object if it is in the cache, or request the object from the source on behalf of the requester if the object is not in the cache. A cache sibling is a device that can only return the object if it is in the cache. One cache acting as a parent can also act as a sibling to other cache devices.

- When an object is not cached, the cache device sends an ICP query to its neighbors (parents and siblings) to see if any of its peers holds the object.
- Each neighbor that holds the requested object returns an `ICP_HIT` reply.
- Each neighbor that does not hold the object returns an `ICP_MISS` reply.

Based on the responses, the cache can determine where to request the object: from one of its neighbors or from the source. If an `ICP_HIT` reply is received, the request is sent to the host that returned the first reply. If no `ICP_HIT` reply is received, the request is forwarded to the first parent that replied. If no parents respond or are configured, the request is made directly to the source.

Using ICP Configuration Directives to Create an Installable List

To configure ICP you must create an installable list and load it on the ProxySG. The ICP protocol contains a number of *directives*, commands used to create a list that can be installed on the ProxySG.

For information on installing the file itself, see "Creating an ICP Installable List" on page 632.

The ICP configuration includes directives that:

- Name the ICP hosts
- Restrict ICP access to only these hosts

Available directives are listed in Table 18.3.

Table 18.3: ICP Directives

Directive	Meaning	Where used
icp_host	The <code>icp_host</code> directive describes cache peers in the hierarchy. There should be one entry for each ProxySG you want to use.	Names the ICP hosts. See "Naming the IP Hosts" on page 630.
icp_access_domain	The <code>icp_access_domain</code> directive is used to control which ICP queries are accepted. The <code>icp_access_domain</code> directive requires a reverse DNS lookup of each ICP query to validate the IP address.	Restricts access. See "Restricting Access" on page 631.
icp_access_ip	The <code>icp_access_ip</code> directive works like the <code>icp_access_domain</code> command, except you can specify an IP address and subnet mask rather than a domain.	Restricts access. See "Restricting Access" on page 631.
icp_port	The <code>icp_port</code> directive sets the port the ProxySG uses to listen for ICP requests. The default port is 3130. If you set the port to 0, ICP is disabled.	Connects to other ICP hosts. See "Connecting to other ICP Hosts" on page 632.
neighbor_timeout	The <code>neighbor_timeout</code> directive sets the number of seconds the ProxySG waits for ICP replies. When the cache device sends an ICP request, it waits for all hosts to reply or for the <code>neighbor_timeout</code> to expire. The default timeout is 2 seconds.	Connects to other ICP hosts. See "Connecting to other ICP Hosts" on page 632.
icp_failcount	The <code>icp_failcount</code> directive sets the number of consecutive failures the cache device can receive before considering the ICP host as failed. By default, the ICP failure count is set to 20. Each time a request fails, the failure count is incremented. When a request succeeds, the failure count is reset to zero.	Connects to other ICP hosts. See "Connecting to other ICP Hosts" on page 632.

Table 18.3: ICP Directives (Continued)

<code>http_failcount</code>	The <code>http_failcount</code> directive sets the number of consecutive failures the cache device can receive before considering the HTTP host as failed. By default, the HTTP failure count is set to 5. The failure count increments each time a request fails. When a request succeeds, the failure count is reset to zero. When an HTTP host fails, the cache device waits five minutes before attempting to use it again as a forwarding target. If the next request fails, the cache device continues to wait five minutes between attempts until the cache becomes available.	Connects to other ICP hosts. See "Connecting to other ICP Hosts" on page 632.
<code>host_fail_notify</code>	The <code>host_fail_notify</code> directive tells the cache device to send event notification email when a connect fails persistently.	Connects to other ICP hosts. See "Connecting to other ICP Hosts" on page 632.
<code>host_recover_notify</code>	The <code>host_recover_notify</code> directive tells the cache device to send event notification email when a failed host recovers.	Connects to other ICP hosts. See "Connecting to other ICP Hosts" on page 632.

Naming the IP Hosts

The `icp_host` directive describes peers in the hierarchy. One entry is required for each ProxySG you want to use.

```
icp_host hostname peertype HTTPport ICPport [default | backup | feeder]
```

where:

<i>hostname</i>		The host name of the ProxySG.
<i>peertype</i>	{parent sibling}	Relationship of the ProxySG to the cache device you are configuring.
<i>HTTPport</i>		TCP port where the ProxySG accepts HTTP requests. The common HTTP port is 80 or 8080.
<i>ICPport</i>		UDP port where the ProxySG accepts ICP requests. The common ICP port is 3130.
<i>default</i>		If specified, designates a ProxySG host parent to be the default ICP parent. If no ICP reply is received, all requests will be forwarded to the default parent.
<i>backup</i>		If specified, designates the cache device host parent to be the backup default ICP parent. If the default parent is not available, the cache device uses the backup default parent.
<i>feeder</i>		If specified, designates the ProxySG host sibling as a feeder-type host, using ICP request loops to populate the ProxySG.

The following are sample `icp_host` directives that can be entered into the ICP configuration:

```
; Define ICP parent and sibling hosts.
icp_host cm1.bluecoat.com parent 8080 3130 default
icp_host cm2.bluecoat.com sibling 8080 3130
icp_host cm3.bluecoat.com sibling 8080 3130
icp_host cm4.bluecoat.com sibling 8080 3130
icp_host cm5.bluecoat.com parent 8080 3130
```

Restricting Access

You can restrict access to ProxySG acting as caches by other ICP hosts using the `icp_access_domain` and `icp_access_ip` directives. By default, when ICP is configured, all ICP hosts are allowed access. You should deny access to all domains other than the ICP hosts you want to use.

icp_access_domain Directive

The `icp_access_domain` directive defines which hosts can request objects from the Web cache using ICP. The default action is to allow all requests. When you use `icp_access_domain`, each ICP query requires a reverse DNS lookup to validate the IP address. Depending on the number of ICP requests, these lookups can consume ProxySG resources.

```
icp_access_domain {allow | deny} domain
```

where:

allow deny	Allows or denies ICP queries from neighbors that match the domain specification.
domain	The domain to match. All ICP queries from neighbors that match the specified domain are handled by the host. The special domain of <i>all</i> defines the default action when there is no domain match.

The following are sample `icp_access_domain` directives to be entered into the ICP configuration:

```
; allow ICP access to this Blue Coat Systems ProxySG Appliance from the
; bluecoat.com domain
icp_access_domain allow bluecoat.com
icp_access_domain deny all
; the deny all option should always be specified to deny all other
; domains
```

icp_access_ip Directive

The `icp_access_ip` directive works like the `icp_access_domain` command, except you can specify an IP address and subnet mask rather than a domain. The following describes the parameters for the `icp_access_ip` command:

```
icp_access_ip {allow | deny} subnet mask
```

where:

allow deny	Allow or deny ICP queries from neighbors that match the address specification.
--------------	--

address/subnet mask	The address and subnet mask to match. All ICP queries that match the specified address will be handled by the ICP host. The special address of 0.0.0.0 defines the default action when there is no address match.
---------------------	---

The following are sample `icp_access_ip` directives to be entered into the ICP configuration:

```
; allow ICP access to this Blue Coat Systems ProxySG Appliance from the local
subnet
icp_access_ip allow 192.168.10.0/255.255.255.0
icp_access_ip deny 10.25.36.47
; the deny all option should always be specified to deny all other domains
```

Connecting to other ICP Hosts

In addition to the ICP directives described in the sections above, you can specify the following directives in the ICP configuration:

```
icp_port 0
neighbor_timeout 2
icp_failcount 20
http_failcount 5
host_fail_notify on
host_recover_notify on
```

where:

<code>icp_port</code>	The default port is 3130. If you set the port to 0, ICP is disabled.
<code>neighbor_timeout</code>	When the cache device sends an ICP request, it waits for all hosts to reply or for the <code>neighbor_timeout</code> to expire. The default timeout is 2 seconds.
<code>http_failcount</code>	By default, the HTTP failure count is set to 5. The failure count increments each time a request fails. When a request succeeds, the failure count is reset to zero. When an HTTP host fails, the cache device waits five minutes before attempting to use it again as a forwarding target.
<code>icp_failcount</code>	By default, the ICP failure count is set to 20. Each time a request fails, the failure count is incremented. When a request succeeds, the failure count is reset to zero.
<code>host_fail_notify</code>	<code>on</code> tells the cache to send event notification e-mail when a connect fails persistently; <code>off</code> disables this setting.
<code>host_recover_notify</code>	<code>on</code> tells the cache to send event notification e-mail when a failed host recovers; <code>off</code> disables this setting.

Creating an ICP Installable List

You can create the ICP installable list with the following methods:

- Use the ProxySG Text Editor, which allows you to enter directives (or copy and paste the contents of an already-created file) directly onto the ProxySG.
- Create a local file on your local system; the ProxySG can browse to the file and install it.

- Use a remote URL, where you place an already-created file on an FTP or HTTP server to be downloaded to the ProxySG.
- Use the CLI `inline` command.

When the ICP installable list is created and installed, it overwrites any ICP settings on the ProxySG.

To Create an ICP Installable List through the Management Console:

1. Select Configuration>Forwarding>ICP.

The ICP tab displays.

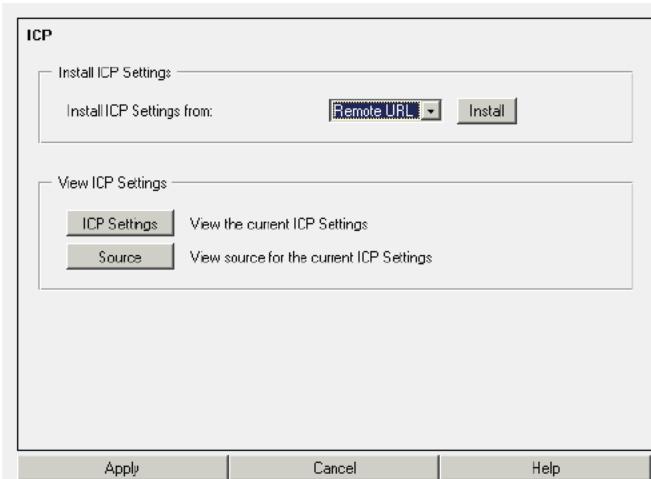


Figure 18-9: Selecting the ICP Download Method

2. From the drop-down list, select the method you want to use to install the ICP configuration; then click **Install**.

Remote URL:

Enter the fully-qualified URL, including the filename, where the configuration is located. To view the file before installing it, click **View**. Click **Install**. Examine the installation status that displays; click **OK**.

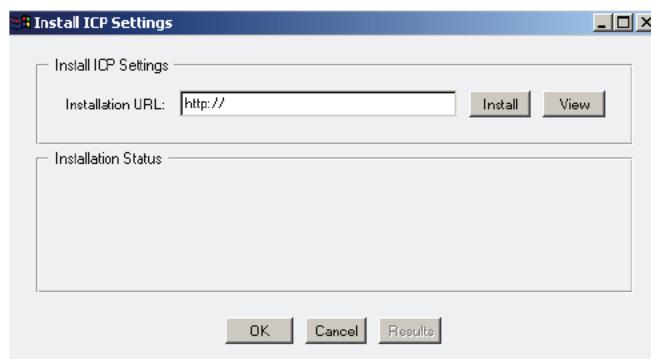


Figure 18-10: Specifying the Remote Location for an ICP Configuration

Local File:

Click **Browse** to bring up the Local File Browse window. Browse for the file on the local system. Click **Install**. When the installation is complete, a results window opens. View the results, close the window, click **Close**.

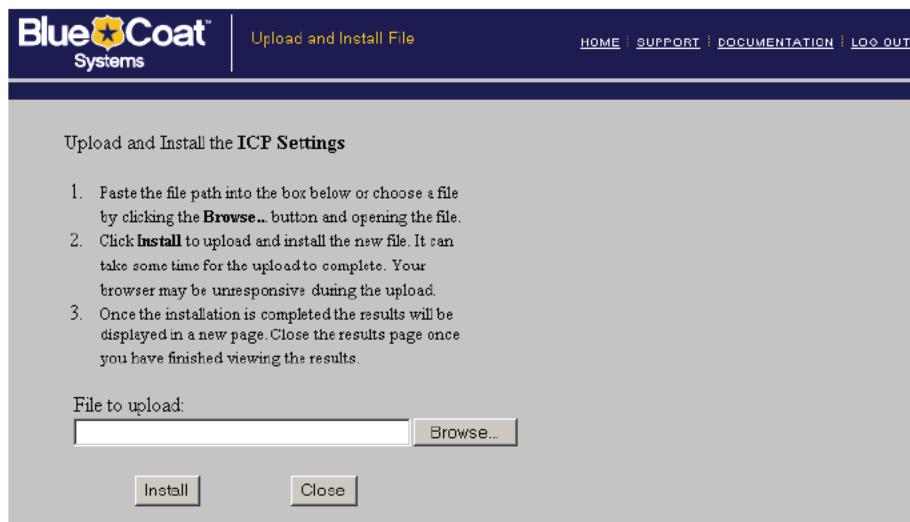


Figure 18-11: Specifying the Local Location for an ICP Configuration

Text Editor:

The current configuration is displayed in installable list format. You can customize it or delete it and create your own. Click **Install**. When the installation is complete, a results window opens. View the results, close the window, click **Close**.

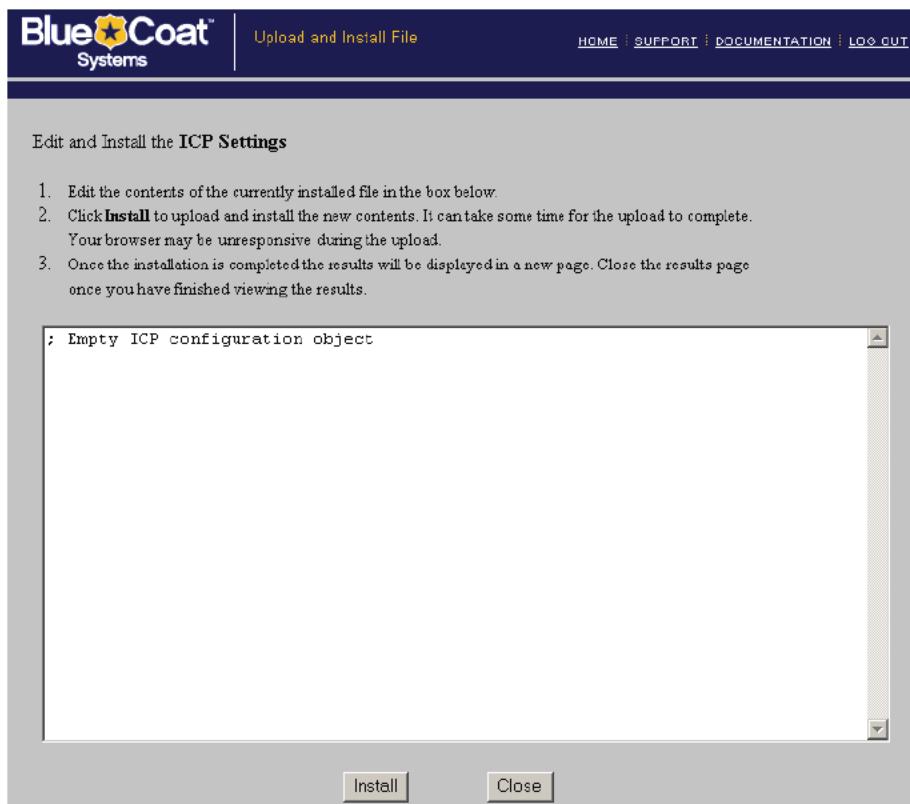


Figure 18-12: Creating an ICP File on the ProxySG

3. Click **Apply**.

To Create a Remote ICP Installable List through the CLI:

At the `(config)` command prompt, enter the following commands:

```
SGOS#(config) icp path url
where url is a fully -qualified URL, including the filename, where the configuration is located.
```

```
SGOS#(config) load icp-settings
```

To Create ICP Settings on the ProxySG through the CLI:

From the `(config)` prompt, enter the following commands to create an inline set of commands. You can use any of the ICP directives, not just the ones displayed here.

```
SGOS#(config) inline icp-settings eof
icp_port 0
neighbor_timeout 2
icp_failcount 20
http_failcount 5
eof
ok
```

where:

<code>icp-settings</code>	Identifies the type of inline settings you are creating.
<code>eof</code>	Specifies the marker that tells the CLI that you are using to begin and end the set of commands. You can use any characters as the end-of-file marker.

The drawback to using the inline command to create a configuration is that you cannot correct mistakes except on the current line. If you find an error farther back than that, you must start over after exiting the current file.

Enabling ICP

ICP must be running and at least one forwarding host configured before ICP can be used in the ProxySG environment. ICP can be enabled or disabled through the policy rule `icp`. The default is `icp(yes)`. You can disable ICP with the policy rule `icp(no)` to control ICP queries for requests.

Using Policy to Manage Forwarding

Once ICP, forwarding, and the SOCKS gateways are configured, you can use policy to create and manage forwarding rules. Forwarding, ICP, and SOCKS gateway rules should go in the `<Forward>` layer of your Forwarding Policy file or your VPM Policy file (if you use the VPM).

Note: Because the contents of the Forward policy file are overwritten by the CLI `restore-sgos2-config` or `restore-cacheos4-config` commands, you should back up the file before using them.

The separate `<Forward>` layer (and `server_url` triggers in place of `url` triggers) is provided because the `url` can undergo URL rewrites before the request is fetched. This rewritten URL is accessed as `server_url` and decisions about upstream connections are based on that, requiring a separate layer. All policy commands allowed in the `<Forward>` layer are described in Table 18.4.

Table 18.4: Forwarding Conditions, Properties, Actions, and Definitions

Forwarding Conditions	Description
<code>client_address=</code>	Tests the IP address of the client. Can also be used in <code><Exception></code> and <code><Proxy></code> layers.
<code>client.host=</code>	Tests the hostname of the client (obtained through RDNS). Can also be used in <code><Admin></code> , <code><Proxy></code> , and <code><Exception></code> layers.
<code>client.host.has_name=</code>	Tests the status of the RDNS performed to determine <code>client.host</code> . Can also be used in <code><Admin></code> , <code><Proxy></code> , and <code><Exception></code> layers.
<code>client.protocol=</code>	Tests true if the client transport protocol matches the specification. Can also be used in <code><Exception></code> and <code><Proxy></code> layers.
<code>date[.utc]=</code>	Tests true if the current time is within the <code>startdate..enddate</code> range, inclusive. Can be used in all layers.

Table 18.4: Forwarding Conditions, Properties, Actions, and Definitions (Continued)

Forwarding	Description
day=	Tests if the day of the month is in the specified range or an exact match. Can be used in all layers.
has_client=	has_client= is used to test whether or not the current transaction has a client. This can be used to guard triggers that depend on client identity.
hour[.utc]=	Tests if the time of day is in the specified range or an exact match. Can be used in all layers.
im.client=	Tests the type of IM client in use. Can also be used in <Proxy>, <Exception>, and <Cache> layers.
im.message.reflected=	Tests whether IM reflection occurred. Can also be used in <Proxy> and <Cache> layers.
minute[.utc]=month[.utc]=	Tests if the minute of the hour is in the specified range or an exact match. Can be used in all layers.
proxy_address=	Tests the IP address of the network interface card (NIC) on which the request arrives. Can also be used in <Admin> and <Proxy> layers.
proxy_card=	Tests the ordinal number of the network interface card (NIC) used by a request. Can also be used in <Admin> and <Proxy> layers.
proxy_port=	Tests if the IP port used by a request is within the specified range or an exact match. Can also be used in <Admin> and <Proxy> layers.
server_url[.case_sensitive .no_lookup]=	Tests if a portion of the requested URL exactly matches the specified pattern.
server_url.address=	Tests if the host IP address of the requested URL matches the specified IP address, IP subnet, or subnet definition.
server_url.domain[.case_sensitive .no_lookup]=	Tests if the requested URL, including the domain-suffix portion, matches the specified pattern.
server_url.extension[.case_sensitive]=	Tests if the filename extension at the end of the path matches the specified string.
server_url.host.has_name=	Tests whether the server URL has a resolved DNS hostname.
server_url.host[.exact .substring .prefix .suffix .regex] [.no_lookup]=	Tests if the host component of the requested URL matches the IP address or domain name.
server_url.host.is_numeric=	This is true if the URL host was specified as an IP address.
server_url.host.no_name=	This is true if no domain name can be found for the URL host.
server_url.host.regex=	Tests if the specified regular expression matches a substring of the domain name component of the requested URL.
server_url.is_absolute=	Tests whether the server URL is expressed in absolute form.
server_url.path[.exact .substring .prefix .suffix .regex] [.case_sensitive]=	Tests if a prefix of the complete path component of the requested URL, as well as any query component, matches the specified string.
server_url.path.regex=	Tests if the regex matches a substring of the path component of the request URL.

Table 18.4: Forwarding Conditions, Properties, Actions, and Definitions (Continued)

Forwarding	Description
server_url.port=	Tests if the port number of the requested URL is within the specified range or an exact match.
server_url.query.regex=	Tests if the regex matches a substring of the query string component of the request URL.
server_url.regex=	Tests if the requested URL matches the specified pattern.
server_url.scheme=	Tests if the scheme of the requested URL matches the specified string.
socks=	This condition is true whenever the session for the current transaction involves SOCKS to the client.
socks.version=	Switches between SOCKS 4/4a and 5. Can also be used in <Exception> and <Proxy> layers.
streaming.client=	yes no. Tests the user agent of a Windows, Real Media, or QuickTime player.
time[.utc]=	Tests if the time of day is in the specified range or an exact match. Can be used in all layers.
tunneled=	yes no. Tests TCP tunneled requests, HTTP CONNECT requests, and unaccelerated SOCKS requests
weekday[.utc]=	Tests if the day of the week is in the specified range or an exact match. Can be used in all layers.
year[.utc]=	Tests if the year is in the specified range or an exact match. Can be used in all layers.
Properties	
access_server()	Determines whether the client can receive streaming content directly from the OCS. Set to no to serve only cached content.
ftp.transport()	Determines the upstream transport mechanism. Note that this setting is not definitive. It depends on the capabilities of the selected forwarding host.
forward()	Determines forwarding behavior. Note that there is a box-wide configuration setting (<config>>forwarding>failure-mode) for the forward failure mode. The optional specific settings can be used to override the default.
forward.fail_open()	Controls whether the ProxySG terminates or continues to process the request if the specified forwarding host or any designated backup or default cannot be contacted.
http.refresh.recv.timeout()	Sets the socket timeout for receiving bytes from the upstream host when performing refreshes. Can also be used in <Cache> layers.
http.server.connect_attempts()	Sets the number of attempts to connect performed per-address when connecting to the upstream host.
http.server.recv.timeout()	Sets the socket timeout for receiving bytes from the upstream host. Can also be used in <Proxy> layers.
icp()	Determines when to consult ICP. The default is yes if ICP hosts are configured and if no forwarding host or SOCKS gateway is identified as an upstream target.

Table 18.4: Forwarding Conditions, Properties, Actions, and Definitions (Continued)

Forwarding	Description
im.transport()	Sets the type of upstream connection to make for IM traffic.
integrate_new_hosts()	Determines whether to add new host addresses to health checks and load balancing. The default is no. If it is set to yes, any new host addresses encountered during DNS resolution of forwarding hosts are added to health checks and load balancing.
reflect_ip()	Determines how the client IP address is presented to the origin server for explicitly proxied requests. Can also be used in <Proxy> layers.
socks_gateway()	The socks_gateway() property determines the gateway and the behavior of the request if the gateway cannot be contacted. Note that there is a box-wide configuration setting for the SOCKS failure mode. The optional specific settings can be used to override the default.
socks_gateway.fail_open()	Controls whether the ProxySG terminates or continues to process the request if the specified SOCKS gateway or any designated backup or default cannot be contacted.
streaming.transport()	Determines the upstream transport mechanism. Note that this setting is not definitive. The ability to use streaming.transport() depends on the capabilities of the selected forwarding host.
trace.request()	Determines whether detailed trace output is generated for the current request. The default value is no, which produces no output
trace.rules()	Determines whether trace output is generated that shows each policy rule that fired. The default value of no suppresses output.
trace.destination()	Used to change the default path to the trace output file. By default, policy evaluation trace output is written to an object in the cache accessible using a console URL of the following form: <code>http://ProxySG_IP_address:8081/Policy/Trace/path</code>
Actions	
notify_email()	Sends an email notification to the list of recipients specified in the Event Log mail configuration. Can be used in all layers.
notify_snmp()	The SNMP trap is sent when the transaction terminates. Can be used in all layers.
log_message	Writes the specified string to the ProxySG event log.
Definitions	
define server_url.domain condition name	Binds a user-defined label to a set of domain suffix patterns for use in a condition= expression.

Chapter 19: Access Logging

Access logging allows you to track Web usage for the entire network or specific information on user or department usage patterns. These logs and reports can be made available in real-time or on a scheduled basis.

Overview

Multiple access logs are supported in SGOS 3.x. *Log* is a generic term that includes a single access log in a single format plus its customizable components such as log format, upload schedule, and the like.

The following protocols support configurable access logging:

- Windows Media
- RealMedia/QuickTime
- HTTP/HTTPS
- ICP
- FTP/FTPS
- Instant Messaging
- SOCKS
- TCP Tunnel
- Telnet Proxy

The ProxySG can create access logs with any one of a number of formats. Four of the formats are reserved and cannot be configured. However, you can create additional formats using custom or ELFF format strings. The formats are:

- NCSA common log format
- SQUID-compatible format
- ELFF (W3C Extended Log File Format)
- Custom, using the strings you enter
- SmartReporter, a log format compatible with SmartFilter's SmartReporter
- SurfControl, a log format compatible with the SurfControl Reporter tool
- Websense, a log format compatible with the Websense Reporter tool

The logs, each containing a single logical file and supporting a single log format, are managed by policy (created through VPM or CPL), which specifies the destination log for a protocol.

Terms

- *Log*: A separate entity that contains a single logical file and supports a single log format. It also contains the log's configuration and upload schedule information as well as other configurable information, such as how often to rotate (switch to a new log file) the log files at the destination, any passwords needed, and the point at which the log can be uploaded.
- *Encrypted Log*: A log is encrypted using an external certificate associated with a private key. Encrypted logs can only be decrypted by someone with access to the private key. The private key is not accessible to the ProxySG.
- *Log Format*: The type of log that is used: NCSA/Common, SQUID, ELFF, SurfControl, or Websense. The log uses a log format for logging the log entries.
- *Log Tail*: The access log tail shows the log entries as they get logged. With high traffic on the ProxySG, not all access log entries are necessarily displayed. However, you can display all access log information after uploading the log.
- *NCSA common log format*: A log format that contains only basic HTTP access information.
- *SQUID-compatible format*: A format that was designed for cache statistics.
- *ELFF-compatible format*: A log format defined by the W3C that is general enough to be used with any protocol.
- *SurfControl*: A proprietary log format that is compatible with the SurfControl reporter tool.
- *Websense*: A proprietary log format that is compatible with the Websense reporter tool.

Customizing the Log Procedures

You should first decide what protocols you want to use and the upload schedules you plan to follow. Then decide which log format you want to use or create a new custom or ELFF log format. Then you can do the following:

- Associate a log format with the log.
- Associate a log with a protocol and/or create policies for protocol association and to manage the access logs and generate entries in them (if you do both, policy takes precedence).
- Determine the upload parameters for the log.

Customizing the Log: Creating and Editing Log Formats

The Format tab allows you to create a format to use for your logs. Several log formats ship with the ProxySG, and they might be sufficient for your needs. If so, you do not need to use the Format tab and can skip to "Customizing the Log: Creating an Access Log" on page 646. If the formats that exist do not meet your needs, you can use the Format tab to create a custom or ELFF format and specify the string and other qualifiers used.

Note: If you change log formats on the fly, the ProxySG continues logging to the same log object, resulting in a log upload of a file that contains two different formats. If you use Blue Coat Reporter, the log file is no longer usable, because the file contains two separate logging formats but only the ELFF header for the first format.

Several log formats already exist. For a description of each value, see Appendix B: “Access Log Formats” on page 751.

- im (Instant Messaging): This is an ELFF format with the custom strings of:

```
date time c-ip cs-username cs-protocol x-im-method x-im-user-id x-im-user-name
x-im-user-state x-im-client-info x-im-buddy-id x-im-buddy-name x-im-buddy-state
x-im-chat-room-id x-im-chat-room-type x-im-chat-room-members x-im-message-text
x-im-message-size x-im-message-route x-im-message-type x-im-file-path
x-im-file-size s-action
```

- main: This is an ELFF format with custom strings of:

```
date time time-taken c-ip sc-status s-action sc-bytes cs-bytes cs-method
cs-uri-scheme cs-host cs-uri-path cs-uri-query cs-username s-hierarchy
s-supplier-name cs(Content-Type) cs(User-Agent) sc-filter-result
sc-filter-category x-virus-id s-ip s-sitename
```

- ncsa: This is a reserved format that cannot be edited. The NCSA/Common format contains the following strings:

```
remotehost rfc931 authuser [date] "request" status bytes
```

The ELFF/custom access log format strings that represent the strings above are:

```
$(c-ip) - $(cs-username) $(localtime) $(cs-request-line) $(sc-status)
$(sc-bytes)
```

- smartreporter: This is a reserved format that cannot be edited. It contains the following string:

```
localtime s-computername c-ip c-uri sc-filter-result cs-categories cs-user
sc-bytes
```

- squid: This is a reserved format that cannot be edited. You can create a new SQUID log format using custom strings. The default SQUID format is SQUID-1.1 and SQUID-2 compatible.

SQUID uses several definitions for its field formats:

```
SQUID-1:time elapsed remotehost code/status/peerstatus bytes method URL
SQUID-1.1: time elapsed remotehost code/status bytes method URL rfc931
peerstatus/peerhost type
```

SQUID-2 has the same fields as SQUID-1.1, although some of the field values have changed.

- streaming: This is an ELFF format with custom strings of:

```
c-ip date time c-dns cs-uri-stem c-starttime x-duration c-rate c-status
c-playerid c-playerversion c-playerlanguage cs(User-Agent) cs(Referer) c-hostexe
c-hostexever c-os c-osversion c-cpu filelength filesize avgbandwidth protocol
transport audiocodec videocodec channelURL sc-bytes c-bytes s-pkts-sent
c-pkts-received c-pkts-lost-client c-pkts-lost-net c-pkts-lost-cont-net
c-resendreqs c-pkts-recovered-ECC c-pkts-recovered-reSENT c-buffercount
c-totalbuffertime c-quality s-ip s-dns s-totalclients s-cpu-util x-cache-user
x-cache-info x-client-address
```

- surfcontrol and surfcontrolv5: These are reserved formats that cannot be edited.

- websense: This is a reserved format that cannot be edited.

Note: If you had previously created formats with the name smartreporter or surfcontrolv5 and you upgrade your ProxySG, those formats will be changed to "smartreporter_user" or "surfcontrolv5_user." If you already have a log format named "smartreporter_user" or "surfcontrolv5_user," then the names will be "smartreporter_user1" or "surfcontrolv5_user1." This naming protocol continues (_user2, _user3...) as long as necessary. The logs associated with these formats will automatically be associated with the new format name.

Creating a Custom or ELFF Log Format

If you are using one of the already-existing formats, skip to "Customizing the Log: Creating an Access Log" on page 646. Complete the following steps to create a custom or ELFF log format.

To Create and Edit the Log Format through the Management Console:

1. Select Configuration>Access Logging>Formats.

The Format tab displays, with the current log formats.

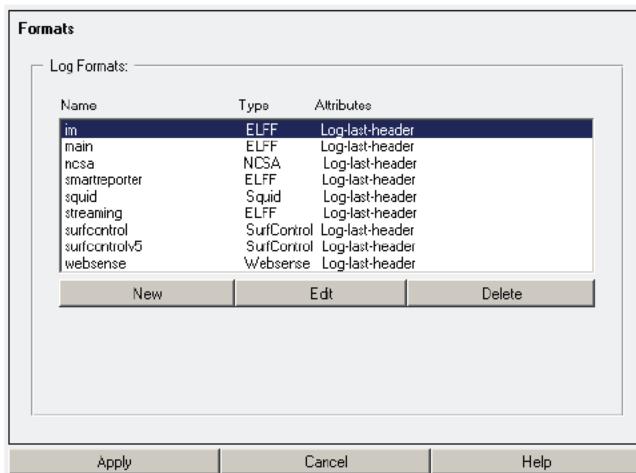


Figure 19-1: Log Format Tab

2. To create or edit a new custom or ELFF log format, click the New button; to edit an existing ELFF log format (im, main, or streaming), highlight the format to be changed and click the Edit button. If you choose an unconfigurable format, you will see an error message.

The Create/Edit Format dialog displays.

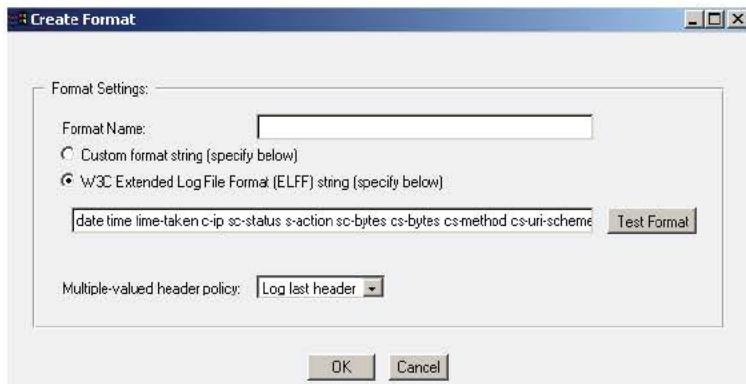


Figure 19-2: Create Format Dialog

3. If you are creating a new format, provide a name meaningful to you.
4. Use a Format Settings radio button to select the log format you need; specify the string in the field below.

Note: ELFF strings cannot start with spaces.

5. Click the Test Format button to test whether the format-string syntax is correct.

When you click the Test Format button, a line displays below the field that indicates that testing is in progress and then gives a result, such as Format is valid.

6. From the Multiple-valued header policy drop-down list, select the header you want to log: Log last header, log first header, log all headers.

The Multiple valued header policy allows you to determine what will be done with HTTP-headers that have multiple headers.

7. Click OK; click Apply.

To Create and Edit a Custom or ELFF Log Format through the CLI:

1. To create a custom or ELFF log format name, enter the following commands from the (config) command prompt (skip to step 2 to edit an existing ELFF format log):

```
SGOS# (config) access-log
SGOS# (config access-log) create format format_name
```

2. To edit a newly created or existing log format:

```
SGOS# (config access-log) edit format format_name
```

The prompt changes to:

```
SGOS# (config format format_name)
```

3. To customize the log format:

```
SGOS# (config format format_name) type {custom | elff} format_string
SGOS# (config format format_name) multi-valued-header-policy {log-all-headers | log-first-header | log-last-header}
```

where:

type	{custom elff} <i>format_string</i>	Specifies the log type.
multi-valued-header-policy	log-all-headers log-first-header log-last-header	(Optional) Specifies which headers should be logged. The default is log-last-header.

4. (Optional) View the results.

```
SGOS#(config format testformat) view
Settings:
Format name: testformat
  Type elff "date time time-taken c-ip sc-status s-action sc-bytes cs-bytes
  cs-method cs-uri-scheme cs-host cs-uri-path cs-uri-query cs-username s-hierarchy
  s-supplier-name cs(Content-Type) cs(User-Agent) sc-filter-result
  sc-filter-category
  x-virus-id s-ip s-sitename"
  Multiple-header-policy log-last-header
```

5. (Optional) To delete a log format:

```
SGOS#(config) access-log
SGOS#(config access-log) delete format format_name
```

Customizing the Log: Creating an Access Log

You can use existing logs and modify them for your needs. You can also create new logs for special circumstances, such as associating the SurfControl log format with a log. To create new logs, continue with the next section. If you need to edit an existing log, skip to "Customizing the Log: Editing an Existing Log" on page 648.

Note: Several logs have already been created. Before creating a new one, check the existing ones to see if they fit your needs. If you want to use a custom log format with the new log, you must create the log format before associating it with a log (see "Customizing the Log: Creating and Editing Log Formats" on page 642).

To Create a Log through the Management Console:

1. Select Configuration>Access Logging>Logs>Logs.

The Log tab displays.

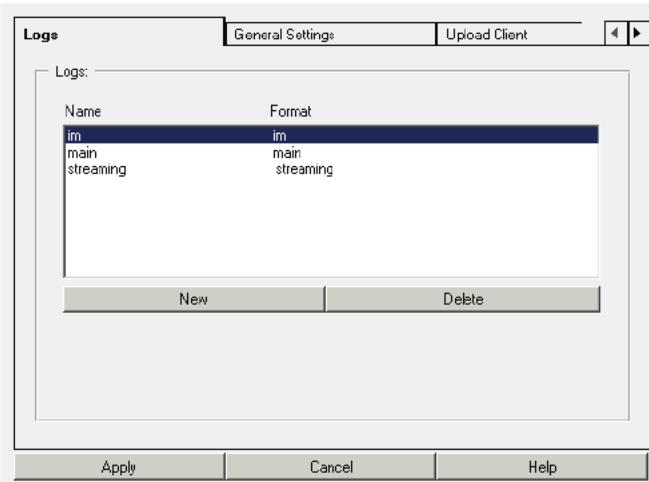


Figure 19-3: Log Tab

2. The logs already created are displayed in the Log tab. To create a new log, click New. The Create Log dialog displays.

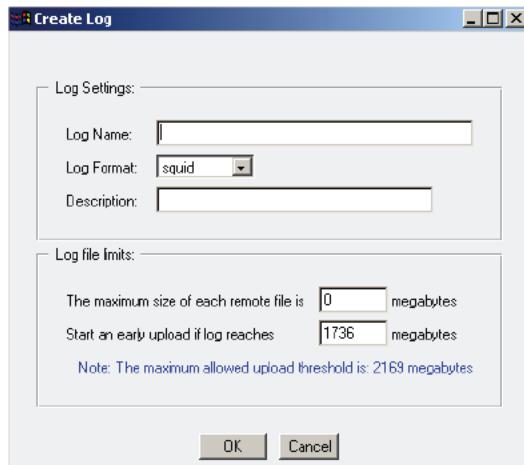


Figure 19-4: Create Log Dialog

3. Fill in the fields as appropriate:
 - Log Name:** Enter a log name that is meaningful to you.
 - Log Format:** Select a log format from the drop-down list.
 - Description:** Enter a meaningful description of the log. It is used for display purposes only.
4. Fill in the Log file limits panel as appropriate. (You can edit these settings later. See "Customizing the Log: Editing an Existing Log" below.)
 - The maximum size for each remote log file (the file on the upload server) defaults to 0, meaning that it continues to send data to the same log file. If you set a maximum size, a new log file opens when the file reaches that size.

- You can specify a size that will trigger an early upload—the maximum upload size varies depending on the size of the ProxySG disks (the maximum allowed upload threshold appears below this field).
5. Click OK; click Apply.

To Create a Log through the CLI:

From the `(config)` command prompt, enter the following commands:

```
SGOS# (config) access-log
SGOS# (config access-log) create log log_name
```

See "Customizing the Log: Editing an Existing Log" below for information on configuring the newly created log.

Customizing the Log: Editing an Existing Log

Three logs exist, each associated with a log format. (For a description of the format, see "Customizing the Log: Creating and Editing Log Formats" on page 642.)

- im (Instant Messaging): Associated with the im format.
- main: Associated with the main format.
- streaming: Associated with the streaming format.

Note: If you change the log format of a log, keep in mind that ELFF formats require an ELFF header in the log (the list of fields being logged are mentioned in the header) and that non-ELFF formats do not require this header.

Make sure you upload the log before you switch the format.

To Edit an Existing Log through the Management Console:

1. Select Configuration>Access Logging>Logs>General Settings.
The General Settings tab displays.

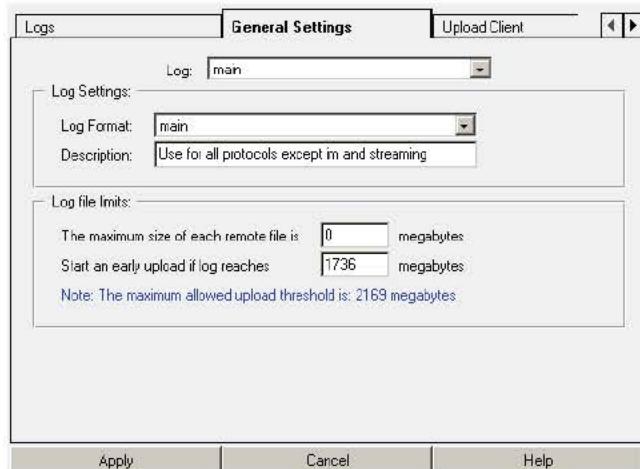


Figure 19-5: General Settings Tab

2. Fill in the fields as appropriate:
 - Log: Select an already-existing log from the Log drop-down list.
 - Log Format: Select the log format from the drop-down list.
 - Description: Enter a meaningful description of the log. (If you chose an existing log format, the default description for that log is displayed. You can change it.)
3. Fill in the Log file limits panel as appropriate:
 - The maximum size for each remote log file (the file on the upload server) defaults to 0, meaning that it continues to send data to the same log file. If you set a maximum size, a new log file opens when the file reaches that size.
 - You can specify a size that will trigger an early upload—the maximum upload size varies depending on the size of the ProxySG disks (the maximum allowed upload threshold appears below this field).
4. Click OK; click Apply.

To View an Existing Log through the CLI:

A log must exist before you can edit it. You can view all the created logs with their configured settings through the CLI. The example below shows the settings for only one log.

To view the existing log types on the system, enter the following command:

```
SGOS#(config) show access-log log
Settings:
  Log name: main
  Format name: main
  Description: Use for all protocols except im and streaming
  Logs uploaded using FTP client
  Logs upload as gzip file
  Wait 60 seconds between server connection attempts
  Log encryption disabled
FTP client:
```

```
Filename format: SG_%f_%c_%l%m%d%H%M%S.log
Filename uses utc time
Use PASV: yes
Use secure connections: no
Primary host site:
Host:
Port: 21
Path:
Username:
Password: *****
Alternate host site:
Host:
Port: 21
Path:
Username:
Password: *****
HTTP client:
Filename format: SG_%f_%c_%l%m%d%H%M%S.log
Filename uses utc time
Use secure connections: no
Primary host site:
Host:
Port: 80
Path:
Username:
Password: *****
Alternate host site:
Host:
Port: 80
Path:
Username:
Password: *****
Custom client:
Primary server: :69
Alternate server: :69
Use secure connections: no
Websense client:
Primary server: :55805
Alternate server: :55805
Log uploading:
Log is uploaded daily at 02:00
A maximum bandwidth of 100 KB/sec will be used
The maximum time between text log packets is 30 seconds
A keep-alive log packet is sent every 300 seconds
Access log size:
Remote log file rotation by size is disabled
```

To Edit an Existing Log through the CLI:

Once you know which log you want to edit, complete the following procedure.

1. From the (config) command prompt, enter the following commands:

```
SGOS# (config) access-log
SGOS# (config access-log) edit log log_name
SGOS# (config log log_name) format-name format_name
SGOS# (config log log_name) early-upload megabytes
SGOS# (config log log_name) remote-size megabytes
```

where:

format-name	<i>format_name</i>	Specifies a log format for this log. The format name can be any format that already exists on the ProxySG.
early-upload	<i>megabytes</i>	Specifies the size that will trigger an early upload—the maximum upload size varies depending on the size of the ProxySG disks (the maximum allowed upload threshold appears below this field).
remote-size	<i>megabytes</i>	Specifies the maximum size for each remote log file (the file on the upload server). The default is 0, meaning that it continues to send data to the same log file. If you set a maximum size, a new log file opens when the file reaches that size.

2. (Optional) View the results.

```
SGOS# (config log testlog) view
Settings:
  Log name: testlog
  Format name: squid
Description:
  Logs uploaded using Websense LogServer client
  Wait 60 seconds between server connection attempts
  Log encryption disabled
...
...
  A maximum bandwidth of 100 KB/sec will be used
  The maximum time between text log packets is 30 seconds
  A keep-alive log packet is sent every 300 seconds
Access log size:
  Start an early upload when log reaches 1736 megabytes
  Remote log file rotation by size is disabled
```

Note: The output you see includes all the defaults for the log, whether or not you configured them. The default values change as you make other configuration settings.

3. (Optional) To delete a log:

```
SGOS# (config) access-log
SGOS# (config delete log log_name)
```

Note: Deleting the log throws away any existing log entries on the ProxySG. To avoid this, upload the access log entries before deleting the logs.

Customizing the Log: Associating a Log with a Protocol

You can associate a log with a protocol at any point in the process.

Note: If you have a policy that defines protocol and log association, that policy will override any settings you make here.

Supported protocols are:

- HTTP/HTTPS
- FTP
- SOCKS
- TCP-Tunnel
- ICP
- Instant Messaging
- Windows Media
- RealMedia/QuickTime
- Telnet Proxy

If you upgraded to SGOS 3.x, some protocols might already be associated with a log format. (Old logs are converted into the main log format.) If your system is new, the protocols will not be associated with a log.

Note: To disable access logging for a particular protocol, you must do two things:

- First, disable the default logging policy for that protocol (see either the Management Console or CLI instructions below) or modify access logging policy in VPM (see "Modify Access Logging" on page 426).
 - Second, stop the log from uploading by clearing the hostname from the upload client settings (see "Editing Upload Clients" on page 659 for information about clearing this setting for each of the client types).
-

To Associate a Log with a Protocol through the Management Console:

1. Select Configuration>Access Logging>General>Default Logging.

The Default Logging tab displays.

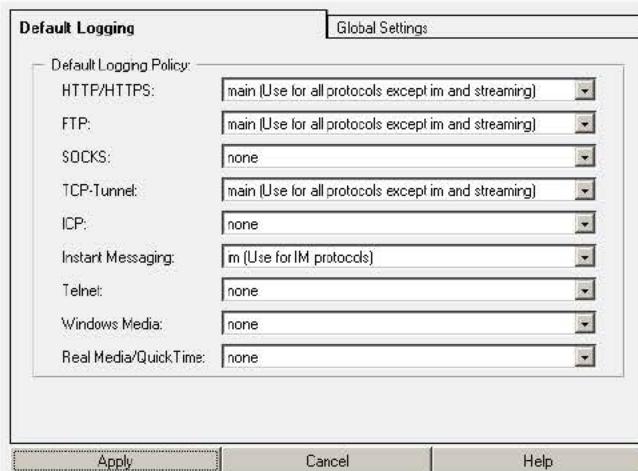


Figure 19-6: Default Logging Tab

2. Select the log you want to use from the drop-down list of the protocol that you want to change. All existing logs, plus the default value **none**, display in these drop-down lists.
3. (Optional) To disable default logging for a protocol, select **none** from the drop-down list of that protocol.
4. Click **Apply**.

To Associate a Log with a Protocol through the CLI:

1. From the **(config)** command prompt, enter the following commands:

```
SGOS#(config) access-log
SGOS#(config access-log) defaultLogging {icp | ftp | http | im | mms | rtsp |
socks | tcp-tunnel | telnet} } log_name
```

where:

icp	log_name	Sets the default log for ICP.
ftp	log_name	Sets the default log for FTP.
http	log_name	Sets the default log for HTTP.
im	log_name	Sets the default log for IM.
mms	log_name	Sets the default log for MMS.
rtsp	log_name	Sets the default log for Real Media/QuickTime.
socks	log_name	Sets the default log for SOCKS.
tcp-tunnel	log_name	Sets the default log for TCP-tunnel.
telnet	log_name	Sets the default log for Telnet Proxy.

2. (Optional) To disable default logging for a protocol, enter the following command:

```
SGOS#(config access-log) no defaultLogging {icp | ftp | http | im | mms | rtsp |
socks | tcp-tunnel | telnet}
```

3. (Optional) View the results.

```
SGOS#(config access-log) view default-logging
Default Logging:
Protocol      Log
-----
http          main
ftp           main
socks         none
tcp tunnel   main
telnet        none
im            im
icp           none
mms           none
rtsp          none
```

Customizing the Log: Configuring Global Settings

You can set global limits for log size and early upload times. These settings can be overridden by individual logs.

To Set Global Log Limits through the Management Console:

1. Select Configuration>Access Logging>General>Global Settings.

The Global Settings tab displays.

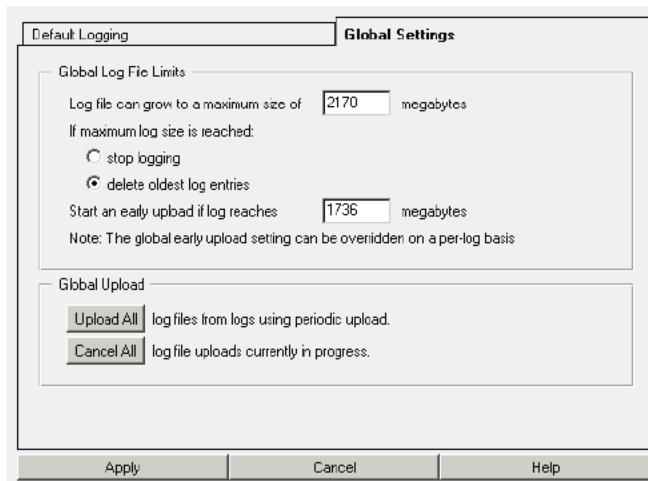


Figure 19-7: Global Settings Tab

2. Fill in the Global Log File Limits panel as appropriate:
 - Configure the maximum size occupied by all of the log files (in megabytes).
 - Determine the behavior of the log when the maximum size is reached. You can have the log stop logging (and do an immediate upload) or have it delete the oldest log entries.
 - Specify the size of the log that triggers an early upload.

3. The Global Upload options affect all logs currently available. They do not affect scheduled upload times. You can upload logs now, using the periodic upload method, or you can cancel all the uploads that are currently in progress.

To Set Global Log Limits through the CLI:

From the `(config)` command prompt, enter the following commands:

```
SGOS#(config) access-log
SGOS#(config access-log) overflow-policy {delete | stop}
SGOS#(config access-log) early-upload megabytes
SGOS#(config access-log) upload {all | log log_name}
SGOS#(config access-log) cancel-upload {all | log log_name}
```

where:

<code>overflow-policy</code>	<code>delete stop</code>
<code>early-upload</code>	<code>megabytes</code>
<code>upload</code>	<code>all log log_name</code>
<code>cancel-upload</code>	<code>all log log_name</code>

When the log reaches its maximum size, you can have the log delete the oldest log entries, or you can have it stop logging (and do an immediate upload).

Specifies the size of the log before an upload can take place.

An immediate upload for all logs or a specified log.

Cancels the current upload for all logs or a specified log.

Customizing the Log: Configuring the Upload Client

Blue Coat supports four types of upload client:

- FTP client, the default
- HTTP client
- Custom client
- Websense client

We also support secure FTP, HTTP, and Custom client.

The Custom client can be used for special circumstances, such as working with SurfControl Reporter. Custom client is based on plain sockets.

Note: You must have a socket server to use the Custom client.

The ProxySG provides access logging with two types of uploads to a remote server: continuous uploading, where the ProxySG continuously streams new access log entries from the ProxySG memory to a remote server, and scheduled (periodic) uploading, where the ProxySG transmits log entries on a scheduled basis. See "Customizing the Log: Configuring the Upload Schedule" on page 673 for more information.

The ProxySG allows you to upload either compressed access logs or plain-text access logs. The ProxySG uses the GZIP format to compress access logs. GZIP-compressed files allow more log entries to be stored in the ProxySG. Advantages of using file compression include:

- Reduces the time and resources used to produce a log file because fewer disk writes are required for each megabyte of log-entry text.
- Uses less bandwidth when the ProxySG sends access logs to an upload server.
- Requires less disk space.

Compressed log files have the extension `.log.gz`. Text log files have the extension `.log`.

Note: You cannot upload GZIP access-log files for the Websense client.

You can configure the ProxySG to encrypt the access log. You must first place an external certificate on the ProxySG (see "Importing an External Certificate" on page 186). The ProxySG derives a session key from the public key in the external certificate and uses it to encrypt the log. When an access log is encrypted, two access log files are produced: an ENC file (extension `.enc`), which is the encrypted access log file, and a DER file (extension `.der`), which contains the ProxySG session key and other information. You need four things to decrypt an encrypted access log:

- The ENC file
- The DER file
- The external (public key) certificate
- The corresponding private key

For information about decrypting a log, see "Decrypting an Encrypted Access Log" on page 659.

Note: The encryption feature is not available for custom or Websense clients.

The general options you enter in the Upload Client tab affect all clients. Specific options that affect individual clients are discussed in the FTP client, HTTP client, Custom client, or Websense client panes or the `access-log ftp-client`, `https-client`, `custom-client`, or `websense-client` CLI commands.

Keep in mind that only one client can be used at any one time. All four can be configured, but only the selected client is used.

To Configure the Upload Client through the Management Console:

1. Select Configuration>Access Logging>Logs>Upload Client.

The Upload Client tab displays.

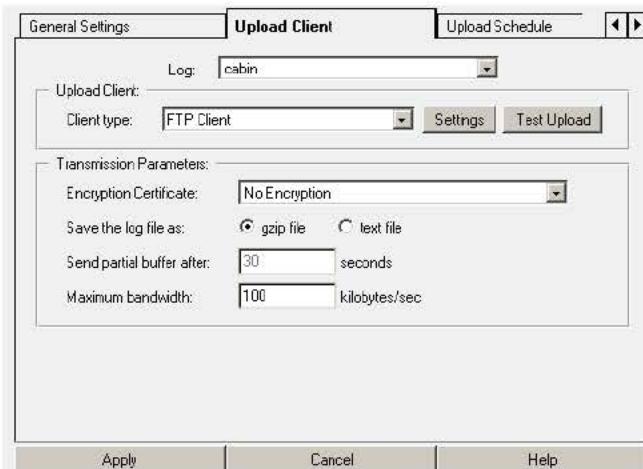


Figure 19-8: Upload Client Tab

2. From the Log drop-down list, select the log you want to configure. The log must exist before it displays in this list.
3. From the Client type drop-down list, select the upload client to use. Only one client can be configured for each log.
4. Click the Settings button to customize the upload client.

For information on customizing the clients, skip to "Editing the FTP Client" on page 659, "Editing the HTTP Client" on page 664, "Editing the Custom Client" on page 668, "Editing the Custom SurfControl Client" on page 669, or "Editing the Websense Client" on page 671.

For information about testing the upload client, see "Testing Access Log Uploading" on page 676.

5. (Optional) To use an external certificate to encrypt the uploaded log, select an external certificate from the Encryption Certificate drop-down list. You must first import the external certificate to the ProxySG (see "Importing an External Certificate" on page 186).

The encryption option is not available for Websense or Custom clients.

6. Select a Save the log file as radio button to determine whether the access log that is uploaded will be compressed (gzip file, the default) or not (text file).

Note: If you are configuring a SurfControl Custom client, select the text file radio button.

7. If you chose text file, you can change the Send partial buffer after *n* seconds field to the time you need (30 seconds is the default).

This field configures the maximum time between text log packets, meaning that it will force a text upload after the specified length of time even if the internal log buffer is not full. If the buffer fills up before the time specified in this setting, the text uploads right away, and is not affected by this maximum setting.

Note: If you chose gzip file, the Send partial buffer after *n* seconds field is not configurable. Also, this setting is only valid for continuous uploading (see "Customizing the Log: Configuring the Upload Schedule" on page 673 for information about continuous uploading).

8. (Optional) Change the Maximum bandwidth field to the bandwidth you need.

You can regulate the amount of bandwidth the ProxySG uses to upload access logs to a remote server. By default, the ProxySG uses a limit of 100 kilobytes. You can specify a bandwidth minimum of 10 kilobytes per second and a maximum of 65535 kilobytes per second. Remember that less bandwidth slows down the upload, while more could flood the network.

9. Click Apply.

To Configure the Upload Client through the CLI:

From the `(config)` command prompt, enter the following commands to make general settings for the upload client.

```
SGOS# (config) access-log
SGOS# (config access-log) edit log log_name
SGOS# (config log log_name) client-type {custom | ftp | http | websense}
SGOS# (config log log_name) upload-type gzip | text
SGOS# (config log log_name) bandwidth kbps
SGOS# (config log log_name) encryption certificate certificate_name
SGOS# (config log log_name) no encryption
SGOS# (config log log_name) ftp-client | http-client | custom-client | websense-client
```

where:

<code>client-type</code>	<code>custom ftp http websense</code>	Specifies which upload client to use. Only one client can be configured for each log.
<code>upload-type</code>	<code>gzip text</code>	Specifies upload as a GZIP or a text file. Websense client always uploads a text file.
<code>bandwidth</code>	<code>kbps</code>	Specifies maximum bandwidth (KBps) to use during log upload. You can specify a bandwidth minimum of 10 kilobytes per second and a maximum of 65535 kilobytes per second. 100 KBps is the default.
<code>encryption</code>	<code>certificate certificate_name</code>	Specifies the access log encryption certificate. Cannot be used for Websense or Custom clients.
<code>no</code>	<code>encryption</code>	Disables access log encryption.
<code>ftp-client</code>		Edits the FTP client configuration. Skip to "Editing the FTP Client" on page 659 for more information.
<code>http-client</code>		Edits the HTTP client configuration. Skip to "Editing the HTTP Client" on page 664 for more information.
<code>custom-client</code>		Edits the Custom client configuration. Skip to "Editing the Custom Client" on page 668 for more information.

websense-client	Edits the Websense client configuration. Skip to "Editing the Websense Client" on page 671 for more information.
-----------------	--

Decrypting an Encrypted Access Log

To decrypt an encrypted access log, you need to concatenate the DER and ENC files (with the DER file in front of the ENC file) and use a program such as OpenSSL for decryption. For example, use the following UNIX command and a tool such as OpenSSL to concatenate the DER and ENC files and decrypt the resulting file:

```
cat path/filename_of_DER_file path/filename_of_ENC_file | openssl smime
-decrypt -inform DER -binary -inkey path/filename_of_private_key -recip
path/filename_of_external_certificate -out path/filename_for_decrypted_log_file
```

You can also download a script based on the OpenSSL tool for decryption. Go to https://download.bluecoat.com/release/SG3/files/accesslog_decrypt.zip.

Editing Upload Clients

Four upload clients are supported by Blue Coat: FTP, HTTP, Custom, and Websense. Each of these clients are described below. You can also create a SurfControl upload client to upload information to the SurfControl Reporter.

Only one upload client can be used at once, but you can configure multiple upload clients for each access log.

Note: To disable access logging, you must do two things:

- First, disable the default logging policy for that protocol (see "Customizing the Log: Associating a Log with a Protocol" on page 652) or modify access logging policy in VPM (see "Modify Access Logging" on page 426).
 - Second, stop the log from uploading by clearing the hostname from the upload client settings (see the procedures that follow for information about clearing this setting for each of the client types).
-

Editing the FTP Client

To Edit the FTP Client through the Management Console:

1. Select Configuration>Access Logging>Logs>Upload Client.

The Upload Client tab displays. See "Customizing the Log: Configuring the Upload Client" on page 655 for configuration information.

2. Select FTP Client from the Client type drop-down list. Click the Settings button.

The FTP Client Settings dialog displays.

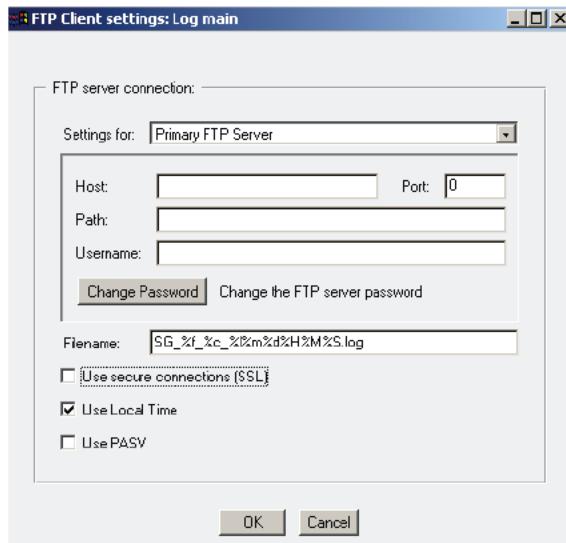


Figure 19-9: Edit FTP Client Dialog

3. Select the primary or alternate FTP server you want to configure from the Settings for drop-down list.
4. Fill in the fields as appropriate:

- Host: The name of the upload client host. If the Use secure connections (SSL) checkbox is selected, the hostname must match the hostname in the certificate presented by the server.

Note: To stop a log from uploading, clear the Host field.

- Port: The default is 21; it can be changed.
- Path: The directory path where the access log will be uploaded on the server.
- Username: This is the username that is known on the host you are configuring.
- Change Password: Change the password on the FTP host by clicking this button.

The Change Password dialog displays.

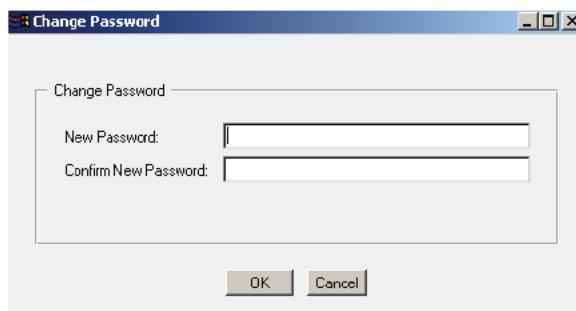


Figure 19-10: Change Password Dialog

Enter and confirm the new password; click OK.

- **Filename:** The **Filename** field is comprised of text and/or specifiers. The default filename includes specifiers and text that indicate the log name (%f), name of the external certificate used for encryption, if any (%c), the fourth parameter of the ProxySG IP address (%l), the date and time (Month: %m, Day: %d, Hour: %H, Minute: %M, Second: %S), and the **.log** or **.gzip.log** file extension.

Note: Be cautious if you change the **Filename** field. If an ongoing series of access logs files are produced and you do not have time-specifiers in this field, each access log file produced will overwrite the old file. Also, if you use more than one external certificate to encrypt a log, you should include the **%c** specifier in the **Filename** field to keep track of which external certificate was used to encrypt the uploaded log file.

If you are creating a SurfControl client, you must change the **.log** file extension to **.tmp**.

- **Secure Connections:** If you use FTPS, select the **Use secure connections (SSL)** checkbox. The remote FTP server must support FTPS.
- **Local Time:** If you want the upload to reflect the local time it was uploaded instead of Universal Time Coordinates (UTC), select the **Local Time** checkbox.
- **Use PASV:** With the **Use PASV** checkbox (the default) selected, the ProxySG connects to the FTP server. With the **Use PASV** checkbox de-selected, the FTP server uses the PORT command to connect to the ProxySG.

5. Click **OK**; click **Apply**.

To Edit the FTP Client through the CLI:

1. At the **(config)** command prompt, configure the FTP client's primary or secondary server information:

```
SGOS# (config) access-log
SGOS# (config access-log) edit log log_name
SGOS# (config log log_name) ftp-client primary host hostname [port]
SGOS# (config log log_name) ftp-client no primary
SGOS# (config log log_name) ftp-client primary path path
SGOS# (config log log_name) ftp-client primary username user_name
SGOS# (config log log_name) ftp-client primary password password
-or-
SGOS# (config log log_name) ftp-client primary encrypted-password
encrypted_password
```

where:

primary host	hostname [port]	Specifies the primary FTP server to which logs should be uploaded. By default, the ProxySG uses port 21.
no primary		To stop a log from uploading, enter an empty string instead of a hostname (i.e., double-quotes).
		Deletes the primary FTP host site.

primary path	<i>path</i>	The path is the directory on the primary FTP server to which logs should be uploaded.
primary username	<i>user_name</i>	Specifies the username on the primary FTP server to which logs should be uploaded. The <i>user_name</i> must have write privileges in the access log file upload directory.
primary password -or- primary encrypted-password	<i>password</i> <i>encrypted_password</i>	Specifies the password for the <i>user_name</i> in the previous command. Note that the primary use of the <i>encrypted-password</i> command is to allow the ProxySG to load a password that it encrypted.

2. (Optional) Repeat these steps for the secondary server, replacing primary with alternate.

```
SGOS#(config log log_name) ftp-client alternate host hostname [port]
SGOS#(config log log_name) ftp-client no alternate
SGOS#(config log log_name) ftp-client alternate path path
SGOS#(config log log_name) ftp-client alternate username user_name
SGOS#(config log log_name) ftp-client alternate password password
-or-
SGOS#(config log log_name) ftp-client alternate encrypted-password
encrypted_password
```

3. Enter the following commands to complete configuration of the FTP client.

```
SGOS#(config log log_name) ftp-client filename format
-or-
SGOS#(config log log_name) ftp-client no filename
SGOS#(config log log_name) ftp-client pasv {yes | no}
SGOS#(config log log_name) ftp-client secure {yes | no}
SGOS#(config log log_name) ftp-client time-format {local | utc}
```

where:

filename	<i>format</i>	The Filename field is comprised of text and/or specifiers. The default filename includes specifiers and text that indicate the log name (%f), name of the external certificate used for encryption, if any (%c), the fourth parameter of the ProxySG IP address (%1), the date and time (Month: %m, Day: %d, Hour: %H, Minute: %M, Second: %S), and the .log or .gzip.log file extension.
		Be cautious if you change the Filename field. If an ongoing series of access log files are produced and you do not have a time-specifier in this field, each access log file produced will overwrite the old file. Also, if you use more than one external certificate to encrypt a log, you should include the %c specifier in the Filename field to keep track of which external certificate can decrypt the uploaded file.
no filename		If you are creating a SurfControl client, you must change the .log file extension to .tmp.

Deletes the FTP client configuration parameters.

<code>pasv</code>	<code>yes no</code>	Specifies whether the ProxySG connects to the FTP server or if the FTP server connects to the ProxySG. The default is <code>yes</code> , using the <code>PORT</code> command only on failure.
<code>secure</code>	<code>yes no</code>	Specifies whether FTPS is used. The default is <code>no</code> . If <code>yes</code> , the <i>hostname</i> in Step 2 must match the hostname in the certificate presented by the server.
<code>time-format</code>	<code>local utc</code>	Specifies whether Universal Time Coordinates (UTC) or the local time is used. UTC is the default. UTC was formerly known as Greenwich Mean Time (GMT).

4. (Optional) View the results.

```
SGOS# (config log testlog) view
Settings:
  Log name: testlog
  Format name: squid
Description:
  Logs uploaded using FTP client
  Logs upload as gzip file
  Wait 60 seconds between server connection attempts
  Log encryption disabled
FTP client:
  Filename format: SG_%f_%c_%l%m%d%H%M%S.log
  Filename uses utc time
  Use PASV: yes
  Use secure connections: no
  Primary host site:
    Host:Host:granite.bluecoat.com
    Port: 21
    Path:granite.bluecoat.com/logs
    Username:testname
    Password: *****
  ...
  ...
```

Tip: Doing a Manual Upload for FTP Upload Client through the CLI

Sometimes, an FTP connection is established with the FTP server and is left open. If you try to use the `upload-now` command while the connection is still open, the command fails with the error message:

```
User upload request failed. There is an open-connection. Try closing the
connection.
```

To Close the Connection:

```
SGOS# (config access-log) edit log log_name
SGOS# (config log log_name) commands close-connections
ok
```

Editing the HTTP Client

Access log uploads done through an HTTP/HTTPS client use the HTTP PUT method. The destination HTTP server (where the access logs are being uploaded) must support this method. Microsoft's IIS allows the server to be directly configured for write (PUT/DELETE) access. Other servers, such as Apache, require installing a new module for the PUT method for access log client uploads.

You can create either an HTTP or an HTTPS upload client through the HTTP Client dialog. (You create an HTTPS client by checking the **Use secure connections (SSL)** checkbox.)

Note: To create an HTTPS client, you must also import the appropriate CA Certificate. For information, see "Importing a CA-Certificate" on page 190.

To Edit the HTTP Client through the Management Console:

1. Select Configuration>Access Logging>Logs>Upload Client.

The Upload Client tab displays. See "Customizing the Log: Configuring the Upload Client" on page 655 for configuration information.

2. Select **HTTP Client** from the Client type drop-down list. Click the **Settings** button.

The HTTP Client Settings dialog displays.

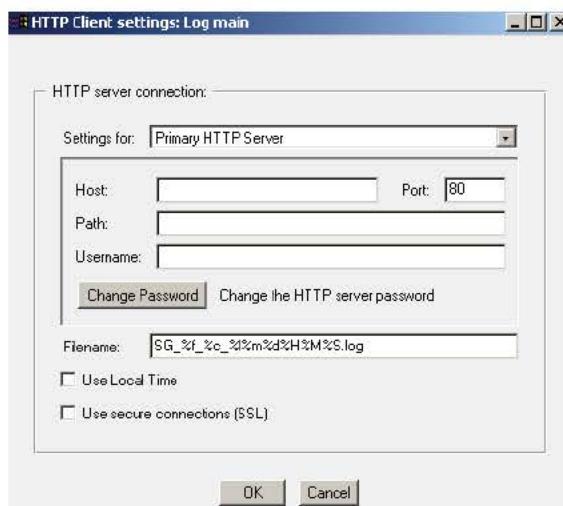


Figure 19-11: Edit HTTP Client Dialog

3. From the **Settings for** drop-down list, select the primary or alternate HTTP server you want to configure.
4. Fill in the fields as appropriate:
 - **Host:** The name of the upload host. If the **Use secure connections (SSL)** checkbox is selected, the hostname must match the hostname in the certificate presented by the server.

Note: To stop a log from uploading, clear the Host field.

- **Port:** The default is 80, but you can change it.

Note: For HTTPS, change the port to 443.

- ❑ **Path:** The directory path where the access log will be uploaded on the server.
 - ❑ **Username:** This is the username that is known on the host you are configuring.
 - ❑ **Change Password:** Change the password on the HTTP host by clicking this button.
- The Change Password dialog displays.



Figure 19-12: Change Password Dialog

Enter and confirm the new password. Click OK.

- ❑ **Filename:** The **Filename** field is comprised of text and/or specifiers. The default filename includes specifiers and text that indicate the log name (%f), name of the external certificate used for encryption, if any (%c), the fourth parameter of the ProxySG IP address (%l), the date and time (Month: %m, Day: %d, Hour: %H, Minute: %M, Second: %S), and the **.log** or **.gzip.log** file extension.

Note: Be cautious if you change the **Filename** field. If an ongoing series of access log files are produced and you do not have time-specifiers in this field, each access log file produced will overwrite the old file. Also, if you use more than one external certificate to encrypt a log, you should include the %c specifier in the **Filename** field to keep track of which external certificate can decrypt the uploaded log file.

If you are creating a SurfControl client, you must change the **.log** file extension to **.tmp**.

- ❑ **Local Time:** If you want the upload to reflect the local time it was uploaded instead of Universal Time Coordinate (UTC), select the Local Time checkbox.
- ❑ **Use secure connections (SSL):** Select this checkbox to create an HTTPS client. To create an HTTPS client, you must also create a keypair, import or create a certificate, and, if necessary, associate the keypair and certificate (called a keyring), with the SSL-client.

5. Click OK; click Apply.

To Edit the HTTP Client through the CLI:

1. At the **(config)** command prompt, configure the HTTP client's primary or secondary server information:

```
SGOS#(config) access-log
SGOS#(config access-log) edit log log_name
SGOS#(config log log_name) http-client primary host hostname [port]
SGOS#(config log log_name) http-client no primary
SGOS#(config log log_name) http-client primary path path
SGOS#(config log log_name) http-client primary username user_name
SGOS#(config log log_name) http-client primary password password
-or-
SGOS#(config log log_name) http-client primary encrypted-password
encrypted_password
```

where:

primary host	hostname [port]	Specifies the primary HTTP server to which logs should be uploaded. By default, the ProxySG uses port 80.
no primary		To stop a log from uploading, enter an empty string instead of a hostname (i.e., double-quotes).
primary path	path	For HTTPS, change the port to 443.
primary username	user_name	Deletes the primary HTTP host site.
primary password	password -or- primary encrypted-password	The path is the directory on the primary HTTP server to which logs should be uploaded.
		Specifies the username on the primary HTTP server to which logs should be uploaded. The user_name must have write privileges in the access log file upload directory.
		Specifies the password (or encrypted password) for the user_name in the previous command. Note that the primary use of the encrypted-password command is to allow the ProxySG to load a password that it encrypted.

2. Repeat these steps for the secondary server, replacing primary with alternate

```
SGOS#(config access-log) edit log log_name
SGOS#(config log log_name) http-client alternate host hostname [port]
SGOS#(config log log_name) http-client no alternate
SGOS#(config log log_name) http-client alternate path path
SGOS#(config log log_name) http-client alternate username user_name
SGOS#(config log log_name) http-client alternate password password
-or-
SGOS#(config log log_name) http-client alternate encrypted-password
encrypted_password
```

3. (Optional) To stop the log from uploading to a primary or secondary server, clear the hostname by entering an empty string (i.e., double-quotes) in the following command:

```
SGOS#(config log log_name) http-client primary ""
-or-
SGOS#(config log log_name) http-client alternate ""
```

4. Enter the following commands to complete configuration of the HTTP client.

```
SGOS# (config log log_name) http-client secure {no | yes}
SGOS# (config log log_name) http-client filename log_name
SGOS# (config log log_name) http-client no filename
SGOS# (config log log_name) http-client time-format {utc | local}
```

where:

secure	no yes	Specifies if you want to use SSL connections. The default is no. If yes, the <i>hostname</i> in Step 2 must match the hostname in the certificate presented by the server.
filename	<i>log_name</i>	The Filename field is comprised of text and/or specifiers. The default filename includes specifiers and text that indicate the log name (%f), name of the external certificate used for encryption, if any (%c), the fourth parameter of the ProxySG IP address (%l), the date and time (Month: %m, Day: %d, Hour: %H, Minute: %M, Second: %S), and the .log or .gzip.log file extension. Be cautious if you change the Filename field. If an ongoing series of access log files are produced and you do not have a time-specifier in this field, each access log file produced will overwrite the old file. Also, if you use more than one external certificate to encrypt a log, you should include the %c specifier in the Filename field to keep track of which external certificate can decrypt the uploaded log file.
no filename		If you are creating a SurfControl client, you must change the .log file extension to .tmp.
time-format	utc local	Deletes the HTTP client configuration parameters. Specifies whether Universal Time Coordinates (UTC) or the local time is used. UTC is the default.

5. (Optional) View the results.

```
SGOS# (config log test) view
Settings:
  Log name: testlog
  Format name: squid
Description:
  Logs uploaded using HTTP client
  Logs upload as gzip file
  Wait 60 seconds between server connection attempts
  Log encryption disabled
  ...
HTTP client:
  Filename format: SG_%f_%c_%l%m%d%H%M%S.log
  Filename uses utc time
  Use secure connections: no
  Primary host site:granite
  Host:granite.example.com/logs
  Port: 443
```

```
Path:  
Username:jsmith  
Password: *****  
...  
...
```

Editing the Custom Client

To Edit the Custom Client through the Management Console:

1. Select Configuration>Access Logging>Logs>Upload Client.

The Upload Client tab displays. See "Customizing the Log: Configuring the Upload Client" on page 655 for configuration information.

2. Select Custom Client from the Client type drop-down list. Click the Settings button.

The Custom Client Settings dialog displays.



Figure 19-13: Edit Custom Client Dialog

3. From the Settings for drop-down list, select the primary or alternate custom server you want to configure.
4. Fill in the fields as appropriate:

- Host: Enter the hostname of the upload destination. If the Use secure connections (SSL) checkbox is selected, the hostname must match the hostname in the certificate presented by the server.

Note: To stop a log from uploading, clear the Host field.

- Port: The default is 69; it can be changed.
- Use secure connections (SSL): Select this checkbox if you are using secure connections.

5. Click OK; click Apply.

To Edit the Custom Client through the CLI:

1. At the `(config)` command prompt, configure the Custom client's primary or secondary server information:

```
SGOS# (config access-log
SGOS# (config access-log) edit log log_name
SGOS# (config log log_name) custom-client primary hostname [port]
-or-
SGOS# (config log log_name) custom-client alternate hostname [port]
```

where *hostname* specifies the primary or alternate server to which logs should be uploaded.
By default the ProxySG uses port 69.

2. Enter the following command to complete configuration of the Custom client:

```
SGOS# (config log log_name) custom-client secure {no | yes}
```

which specifies whether SSL connections are used. The default is no. If yes, the hostname in Step 1 must match the hostname in the certificate presented by the server.

3. (Optional) To stop the log from uploading to a primary or secondary server, clear the hostname by entering an empty string (i.e., double-quotes) in the following command:

```
SGOS# (config log log_name) custom-client primary ""
-or-
SGOS# (config log log_name) custom-client alternate ""
```

4. (Optional) View the results.

```
SGOS# (config log test) view
Settings:
  Log name: testlog
  Format name: squid
Description:
  Logs uploaded using custom client
  Logs upload as gzip file
  Wait 60 seconds between server connection attempts
  Log encryption disabled
  ...
Custom client:
  Primary server: :69
  Alternate server: :69
  Use secure connections: no
  ...
  ...
```

Editing the Custom SurfControl Client

You can use the Custom Client to create an upload client that will upload information to SurfControl Reporter. Before you begin, be sure that:

- You created a log and associated the SurfControl log format with it.
- Determined the protocol you want to use for uploading and associated the SurfControl log with it.
- Configured the log to fit your environment.

To Edit the SurfControl Client through the Management Console:

1. Select Configuration>Access Logging>Logs>Upload Client.

The Upload Client tab displays. See "Customizing the Log: Configuring the Upload Client" on page 655 for configuration information.

2. From the Log drop-down list, select the SurfControl log that you associated with the SurfControl log format.
3. Make sure the Save the log file as radio button is set to text file, not gzip file.
4. Select the upload client from the Client type drop-down list.
5. Click the Settings button for that client.
6. Customize the upload client for SurfControl Reporter.
 - Enter the hostname, path, and username, if necessary, for the SurfControl Reporter server.

Note: To stop a log from uploading, clear the Host field.

- Make sure the filename is .tmp, not .gzip. SurfControl only recognizes files with a .tmp extension.
- If your SurfControl server supports SSL, select the Use secure connections (SSL) checkbox.

To Edit the Custom SurfControl Client through the CLI:

1. At the `(config)` command prompt, make the customized settings for the SurfControl upload client:

```
SGOS#(config) access-log
SGOS#(config access-log) edit log log_name
SGOS#(config access-log log_name) upload-type text
SGOS#(config access-log log_name) periodic-upload upload-interval {daily 0-23 | hourly hours [minutes]}
SGOS#(config access-log log_name) periodic-upload enable
Note: Continuous upload disabled, to re-enable please use "continuous-upload enable" command
SGOS#(config access-log log_name) custom-client | ftp-client | http-client
```

For specific information on managing upload clients, see "Editing the Custom Client" on page 668, "Editing the FTP Client" on page 659, or "Editing the HTTP Client" on page 664.

2. (Optional) View the results.

```
SGOS#(config log SurfControl) view
Settings:
  Log name: surfcontrol
  Format name: surfcontrol
Description:
  Logs uploaded using FTP client
  Logs upload as text file
  Wait 60 seconds between server connection attempts
  Log encryption disabled
FTP client:
  Filename format: SG_%f_%c_%l%m%d%H%M%S.log
  Filename uses utc time
  Use PASV: yes
  Use secure connections: no
```

```

Primary host site:
Host:granite.example.com
Port: 21
Path:/jsmith/logs/
Username:jsmith
Password: *****
...
...
Log uploading:
Log is uploaded daily at 02:00
A maximum bandwidth of 100 KB/sec will be used
The maximum time between text log packets is 30 seconds
A keep-alive log packet is sent every 300 seconds
Access log size:
Start an early upload when log reaches 1736 megabytes
Remote log file rotation by size is disabled

```

Editing the Websense Client

Before you begin, make sure you have created a Websense log using the Websense log format and configured the log to your environment (see "Customizing the Log Procedures" on page 642).

Note: You cannot upload GZIP access-log files with the Websense client.

To Edit the Websense Client through the Management Console:

1. Select Configuration>Access Logging>Logs>Upload Client.

The Upload Client tab displays. See "Customizing the Log: Configuring the Upload Client" on page 655 for configuration information.

2. Select the Websense Client from the Client type drop-down list. Click the Settings button.

The Websense Client Settings dialog displays.

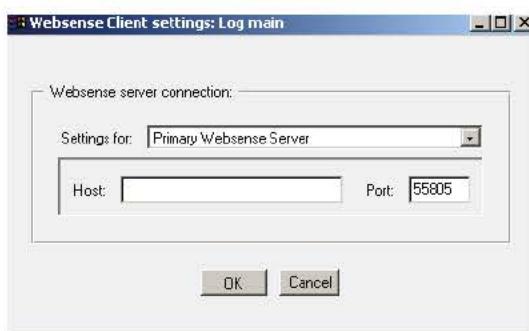


Figure 19-14: Edit Websense Client Dialog

3. From the Settings for drop-down list, select the primary or alternate server you want to configure.
4. Fill in the fields as appropriate:
 - Host: Enter the hostname of the primary Websense Server.

Note: To stop a log from uploading, clear the Host field.

- Port: The default is 55805, but you can change it if the Websense Server is using a different port.
5. Repeat for the Alternate Websense Server.
 6. Click OK; click Apply.

To Edit the Websense Client through the CLI:

1. At the `(config)` command prompt, configure the Websense client's primary or secondary server information:

```
SGOS#(config) access-log  
SGOS#(config access-log) edit log log_name  
SGOS#(config log log_name) websense-client primary hostname [:port]  
-or-  
SGOS#(config log log_name) websense-client alternate hostname [:port]
```

where `hostname` specifies the primary or alternate server to which logs should be uploaded.
By default the ProxySG uses port, which is 55805 by default.

2. (Optional) To stop the log from uploading to a primary or secondary server, clear the hostname by entering an empty string (i.e., double-quotes) in the following command:

```
SGOS#(config log log_name) websense-client primary ""  
-or-  
SGOS#(config log log_name) websense alternate ""
```

3. (Optional) View the results.

```
SGOS#(config log test) view  
Settings:  
  Log name: testlog  
  Format name: squid  
Description:  
  Logs uploaded using Websense LogServer client  
  Wait 60 seconds between server connection attempts  
  Log encryption disabled  
  ...  
  ...  
Websense client:  
  Primary server: :55805  
  Alternate server: :55805  
  Log uploading:  
    Log is uploaded daily at 02:00  
    A maximum bandwidth of 100 KB/sec will be used  
    The maximum time between text log packets is 30 seconds  
    A keep-alive log packet is sent every 300 seconds  
Access log size:  
  Start an early upload when log reaches 1736 megabytes  
  Remote log file rotation by size is disabled
```

Customizing the Log: Configuring the Upload Schedule

The Upload Schedule allows you to configure the frequency of the access logging upload to a remote server, the time between connection attempts, the time between keep-alive packets, the time at which the access log is uploaded, and the protocol that is used.

You can specify either *periodic uploading* or *continuous uploading*. Both periodic and continuous uploading send log information from a ProxySG farm to a single log analysis tool. This allows you to treat multiple ProxySG appliances as a single entity and to review combined information from a single log file or series of related log files.

With periodic uploading, the ProxySG transmits log entries on a scheduled basis (for example, once daily or at specified intervals) as entries are batched, saved to disk, and uploaded to a remote server.

Note: When you configure a log for continuous uploading, it continues to upload until you stop it. To stop continuous uploading, switch to periodic uploading temporarily. This is sometimes required for GZIP or encrypted files, which must stop uploading before you can view them.

With continuous uploading, the ProxySG continuously *streams* new access log entries from the ProxySG memory to a remote server. Note that *streaming* here refers to the real-time transmission of access log information. The ProxySG transmits access log entries using the specified client, such as FTP client. A keep-alive is sent to keep the data connection open.

Continuous uploading allows you to view the latest logging information almost immediately, send log information to a log analysis tool for real-time processing and reporting, maintain ProxySG performance by sending log information to a remote server (avoiding disk writes), and save ProxySG disk space by saving log information on the remote server.

If the remote server is unavailable to receive continuous upload log entries, the ProxySG saves the log information on the ProxySG disk. When the remote server is available again, the appliance resumes continuous uploading.

Note: If you do not need to analyze the upload entries in real time, we recommend that you use periodic uploading because it is more reliable than continuous uploading.

If there is a problem configuring continuous uploading to Microsoft Internet Information Server (IIS), consider using periodic uploading instead.

To Configure the Upload Schedule through the Management Console:

1. Select Configuration>Access Logging>Logs>Upload Schedule.

The Upload Schedule page displays.

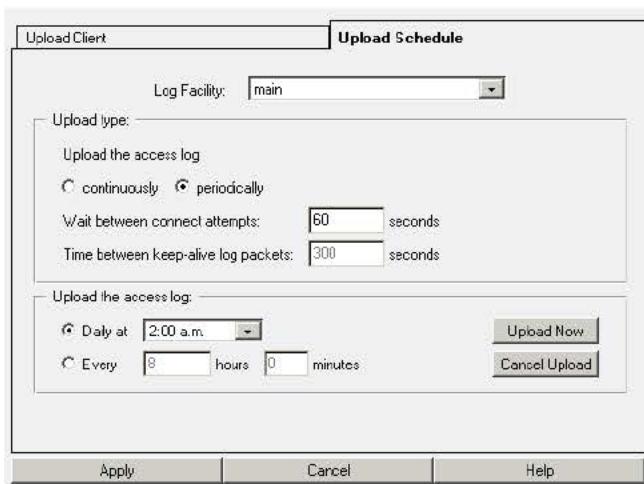


Figure 19-15: Upload Schedule Tab

2. From the Log drop-down list, choose the log whose schedule you are configuring.
3. Select an upload method by choosing the continuously or the periodically radio button; click Apply.
4. To change the time between connection attempts, enter the new time (in seconds) in the Wait between connect attempts field.
5. (Only accessible if you are updating continuously) To change the time between keep-alive packets, enter the new time (in seconds) in the Time between keep-alive log packets field.

Keep-alives maintain the connection during low periods of system usage. When no logging information is being uploaded, the ProxySG sends a keep-alive packet to the remote server at the interval you specify, from 1 to 65535 seconds. If you set this to 0 (zero), you effectively disable the connection during low usage periods. The next time that access log information needs to be uploaded, the ProxySG automatically reestablishes the connection.

6. (Optional) From the Daily at drop-down list, specify the time of day you want the access log updated or rotated (if you are doing continuous uploads).
7. (Optional) If you don't want the log uploaded or rotated on a daily basis, select the Every radio button and enter the time between uploads.

Log rotation helps prevent logs from growing excessively large. Especially with a busy site, logs can grow quickly and become too big for easy analysis. With log rotation, the ProxySG periodically creates a new log file, and archives the older one without disturbing the current log file.

8. (Optional) You can upload the access logs now or you can cancel any access-log upload currently in progress (if you are doing periodic uploads). You can rotate the access logs now (if you are doing continuous uploads). These actions will not affect the next scheduled upload time.

The Cancel upload button (for periodic uploads) allows you to stop repeated upload attempts if the Web server becomes unreachable while an upload is in progress. Clicking this button sets log uploading back to idle if the log is waiting to retry the upload. If the log file is in the process of uploading, it will take time for it to take effect.

9. Click OK; click Apply.

To configure an upload schedule through the CLI:

1. From the (config) command prompt, enter the following commands.

```
SGOS# (config access-log) edit log log_name
SGOS# (config log log_name) upload-type {gzip | text}
```

2. Configure either a continuous upload schedule or a periodic upload schedule by using the options in the continuous-upload or periodic-upload commands.

Note: If you are configuring a SurfControl upload client you must use periodic-upload, not continuous-upload. If you configure a Websense upload client, you should set it to continuous-upload.

```
SGOS# (config log log_name) continuous-upload {enable | keep-alive seconds |
lag-time seconds | rotate-remote {daily 0-23 | hourly hours [minutes]}}
-or-
SGOS# (config log name) periodic-upload {enable | upload-interval {daily 0-23 |
hourly hours [minutes]}}
```

where:

upload-type	gzip text	Specifies using a compressed file (GZIP) or a text file for uploading.
continuous-upload	enable	Specifies continuous upload (automatically disables periodic upload).
	keep-alive seconds	Specifies the interval between keep-alive log packets. Acceptable values are between 0 and 65535 seconds.
	lag-time seconds	Specifies the maximum time between log packets (text upload only). Acceptable values are between 0 and 65535 seconds.
	rotate-remote {daily 0-23 hourly hours [minutes]}	This setting configures the maximum time between text log packets, meaning that it will force a text upload after the specified length of time even if the internal log buffer is not full. If the buffer fills up before the time specified in this setting, the text uploads right away, and is not affected by this maximum setting.
periodic-upload	enable	Specifies when to rotate to new remote log file: enter the time of day for a daily rotation or enter how often to rotate (every <i>n</i> hours/minutes) for an hourly rotation. To rotate more than once an hour, enter 0 hours and specify <i>n</i> minutes.
		Specifies periodic upload (automatically disables continuous upload).

upload-interval {daily 0-23 hourly <i>hours</i> [<i>minutes</i>] }	Specifies when to upload a log file: enter the time of day for a daily upload or enter how often to upload (every <i>n</i> hours/minutes) for an hourly upload. To upload more than once an hour, enter 0 hours and specify <i>n</i> minutes.
--	---

3. Specify the time between connection attempts between the ProxySG and the remote server:

```
SGOS# (config log log_name) connect-wait-time seconds
```

4. (Optional) Use the *log_name* submode commands options to upload an access log immediately, to cancel an access log upload, to switch immediately to a new remote log file, or to permanently delete all access logs on the ProxySG:

```
SGOS# (config log log_name) commands upload-now  
SGOS# (config log log_name) commands cancel-upload  
SGOS# (config log log_name) commands rotate-remote-log  
SGOS# (config log log_name) commands delete-logs
```

Ordinarily, the ProxySG automatically deletes the local copies of access logs from the ProxySG after the logs have been uploaded. You can manually delete access logs from the ProxySG, but it is not recommended.

5. (Optional) View the results.

```
SGOS# (config log log_name) view  
...  
Log uploading:  
    Log is uploaded continuously  
    The remote log file will be rotated every 0 hour(s) 30 minute(s)  
A maximum bandwidth of 100 KB/sec will be used  
The maximum time between text log packets is 225 seconds  
A keep-alive log packet is sent every 65535 seconds  
Access log size:  
    Start an early upload when log reaches 1736 megabytes  
    Remote log file rotation by size is disabled
```

6. (Optional) To delete an individual log:

```
SGOS# (config) access-log  
SGOS# (config access-log) delete log log_name
```

Testing Access Log Uploading

For the duration of the test, configure the event log to use the verbose event level (see "Configuring Which Events to Log" on page 699). This logs more complete log information. After you test uploading, you can check the event log through the Management Console for the test upload event and determine whether any errors occurred (go to Statistics>Event Logging). You cannot check the event log through the CLI.

To Test Access Log Uploading through the Management Console:

You can do a test access log upload. Before you begin, make sure you have configured the upload client completely.

1. Select Configuration>Access Logging>Logs>Upload Client.
2. Click the Test Upload button.
The Test upload dialog appears.
3. Click OK in the Test upload dialog that appears.
4. Check the event log for upload results: go to Statistics>Event Logging.

To Test Access Log Uploading through the CLI:

For the duration of the test, configure the event log to use the verbose event level. This logs more complete log information. After you test uploading, you can check the event log under the Statistics tab for the test upload event and determine whether any errors occurred.

1. At the (config) command prompt, enter the following commands:

```
SGOS#(config) access-log
SGOS#(config access-log) edit log log_name
SGOS#(config log log_name) commands test-upload
```

2. In the Management Console, select Statistics>Event Logging.
3. Click the forward arrow and back arrow buttons to move through the event list.
4. Locate the following event log message entry: Access Log: Transfer complete.
If you do not see the message, check for other Access Log messages from the appropriate time frame. Use these to help in troubleshooting.
5. To check for a successful test upload at the remote server, locate the file *logname_upload_result* or, for an encrypted test upload, locate the file *logname_upload_result.enc*. If you locate the file, the test was successful.

If you cannot locate the file, use the steps above to open the ProxySG event log, locate the test upload event, and determine whether any errors occurred.

The following is a sample of the test file contents.

```
***** START OF TEST FILE *****

NOTE: This is a verification file sent to test access log uploading.
Please check the file for correctness and the event log for errors.
For security purposes, please delete this file after perusal.

ProxySG Appliance Date: 2003-04-05
ProxySG Appliance Time: 02:17:23 UTC
ProxySG Appliance Name: 10.25.36.47 - Blue Coat SG800
ProxySG Appliance IP: 10.25.36.47
ProxySG Appliance Type: Blue Coat SG800

Sent to FTP server using the following configuration:

Host: 10.25.45.35
Port: 21
Path:
User: joe
Password: *****
This file should contain approx. 819 bytes
```

***** END OF TEST FILE *****

Viewing Access-Log Statistics

Access-log statistics can be viewed from the Management Console Statistics>Access Logging tab. They can also be viewed through the CLI. (To view the access log statistics through the CLI, see "Viewing All Access-Log Statistics through the CLI" on page 681.)

Viewing the Access Log Tail

This option is not available through the CLI.

To Display the Access Log Tail through the Management Console:

1. Select Statistics>Access Logging>Log Tail.

The Log Tail tab displays.

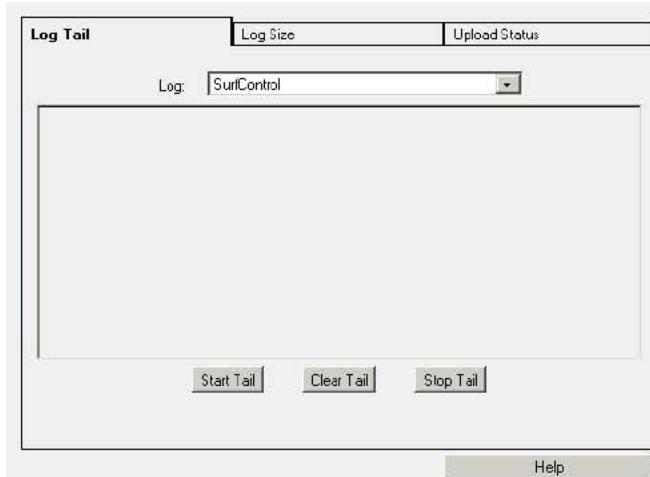


Figure 19-16: Viewing the Access Log Tail

2. From the Log drop-down list, select the log you want to view.
3. Click Start Tail to display the access log tail.

The ProxySG displays a maximum of 500 lines. Entries that pre-date these 500 lines are not displayed.

4. Click Stop Tail to stop the display or Clear Tail to clear the display.

Viewing the Log File Size

The Log Size tab displays current log statistics:

- Whether the log is being uploaded (Table 19.1 describes upload statuses)

Table 19.1: Log Writing Status Description

Status	Description
active	Log writing is active.
active - early upload	The early upload threshold has been reached.
disabled	An administrator has disabled logging.
idle	Log writing is idle.
initializing	The system is initializing.
shutdown	The system is shutting down.
stopped	The access log is full. The maximum log size has been reached.
unknown	A system error has occurred.

- The current size of all access log objects
- Disk space usage
- Last modified time
- Estimated size of the access log file, once uploaded

Estimated compressed size of the uploaded access log and ProxySG access log size might differ during uploading. This occurs because new entries are created during the log upload.

1. Select Statistics>Access Logging>Log Size.

The Log Size tab displays.

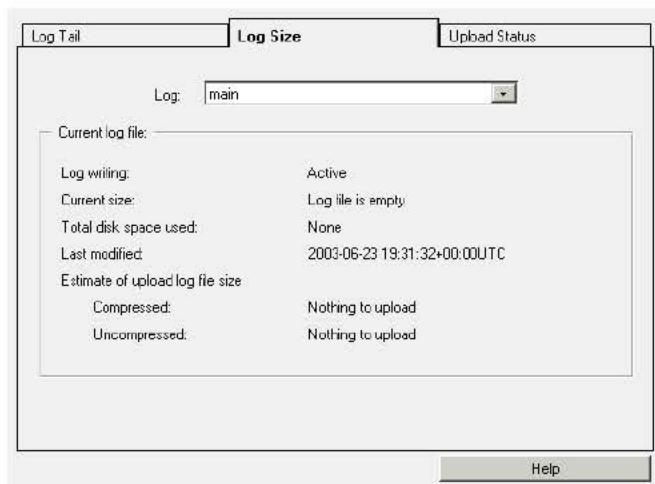


Figure 19-17: Checking the Log Size Statistics

2. From the Log drop-down list, select the log you want to view.

Viewing Access Logging Status

The ProxySG displays the current access logging status on the Management Console. This includes separate status information about:

- The writing of access log information to disk
- The client the ProxySG uses to upload access log information to the remote server

To View Access Logging Status through the Management Console:

1. Select Statistics>Access Logging>Upload Status.

The Upload Status tab displays.

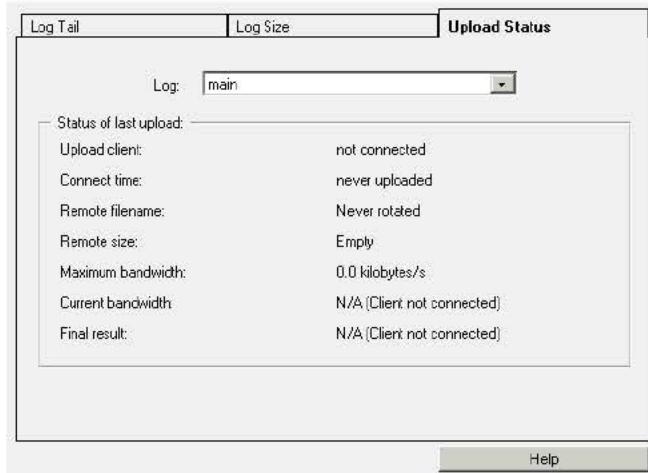


Figure 19-18: Viewing Upload Status Statistics

2. Under Status of Last Upload, check the appropriate status information displayed in the Upload client field.
3. Check the other status information. For information about the status, see the table below.

Table 19.2: Upload Status Information

Status	Description
Connect time	The last time a client connection was made or attempted.
Remote filename	The most recent upload filename. If an access log was encrypted, only the encrypted access log file (the ENC file) displays.
Remote size	The current size of the upload file. If an access log was encrypted, only the encrypted access log file size (the ENC file) displays. The private key file (the DER file) varies, but is usually about 1 Kb.
Maximum bandwidth	The maximum bandwidth used in the current or last connection.
Current bandwidth	The bandwidth used in the last second (available only if currently connected).
Final result	The result of the last upload attempt (success or failure). This is only available if not connected.

Viewing All Access-Log Statistics through the CLI

In the CLI, the statistics are not broken down the way they are in the Management Console. Every log is listed and every statistic is displayed. In this example, only two logs are displayed. For details of the meaning of these statistics, see "Viewing the Log File Size" on page 678 and "Viewing Access Logging Status" on page 679.

```
SGOS#(config) show access-log statistics
Statistics:
Access Log (http_log) Statistics:
Log Manager Version 3
Log entry lifetime counter: 7270
System Status:
Log manager: enabled and running
Upload client: not connected
Log writer: idle
Log reader: idle
Log Information:
Current log size: 134 bytes
Early upload threshold: 3500 MB
Maximum log size: 4375 MB
Max size policy: stop logging
Bytes in write buffer: 0
Tail sockets in use: 0
Modified time: 2003-04-07 23:14:18+00:00UTC
Next Upload:
Client type: ftp
Next attempt: 9190 seconds
Connect type: daily upload
Connect reason: regular upload
Estimated upload size:
compressed: 134 bytes
uncompressed: 1523 bytes
Upload format: text
Last Upload Attempt:
Time: 2003-04-07 02:00:00+00:00UTC
Maximum bandwidth: 0.00 KB/sec
Result: success
Current/Last Upload File:
Remote filename: N/A
Remote size: 0 bytes
Access Log (joe) Statistics:
Log Manager Version 3
Log entry lifetime counter: 353
System Status:
Log manager: enabled and running
Upload client: not connected
Log writer: idle
Log reader: idle
Log Information:
Current log size: 5312 bytes
Early upload threshold: 3448 MB
Maximum log size: 4311 MB
Max size policy: delete oldest entries
```

```
Bytes in write buffer:          0
Tail sockets in use:          0
Modified time:                2003-04-07 23:14:18+00:00UTC
Next Upload:
  Client type:                ftp
  Next attempt:               9185 seconds
  Connect type:               daily upload
  Connect reason:              regular upload
Estimated upload size:
  compressed:                 5312 bytes
  uncompressed:              44695 bytes
  Upload format:              gzip
Last Upload Attempt:
  Time:                       2003-04-07 23:13:23+00:00UTC
  Maximum bandwidth:           0.00 KB/sec
  Result:                     failure
Current/Last Upload File:
  Remote filename:             SG_f_10406020000.log.gz
  Remote size:                  0 bytes
```

Using Access Logging with Policy Rules

After configuration is complete, you must create rules to manage the access logs you set up. You can create rules through the Visual Policy Manager module of the Management Console, or you can use Content Policy Language (CPL) directly (refer to the *Blue Coat Content Policy Language Guide*).

Actions you can do to manage access logging:

- Reset logging to its default
- Disable all logging
- Add logging to a log file
- Disable logging to a log file
- Override specific access-log fields

You can also set the list of logs to be used, but you must use CPL to create this action. It is not available through VPM.

The first two actions—reset logging to its default and disable all logging—are referred to as constant actions, just like the allow/deny actions. You should select only one per rule.

All of the actions are allowed in all layers. If you use VPM, the access-logging actions display in the VPM policy; if you use CPL, you can put the actions into any file, but Blue Coat recommends you use the Local file.

Example: Using VPM to Prevent Entries Matching a Source IP Address from Being Logged

Complete the following steps to prevent a source IP address from being logged.

To Prevent a Source IP Address from Being Logged:

1. Create a Web Access Layer:

- Select Configuration>Policy>Visual Policy Manager; click the Launch button.
- Select Policy>Add Web Access Layer from the menu of the Blue Coat VPM window that appears.

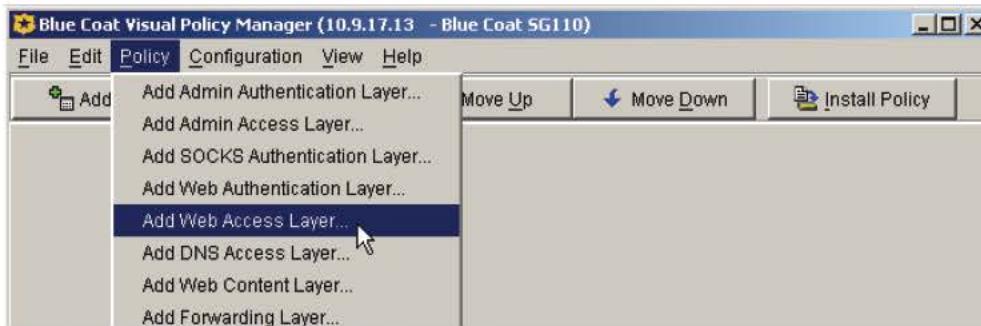


Figure 19-19: Select Add Web Access Layer

- Type a layer name into the dialog that appears and click OK.
- 2. Add a Source object:
 - Right click on the item in the Source column; select Set.
 - Click New in the Set Source Object dialog that appears; select Client IP Address/Subnet.

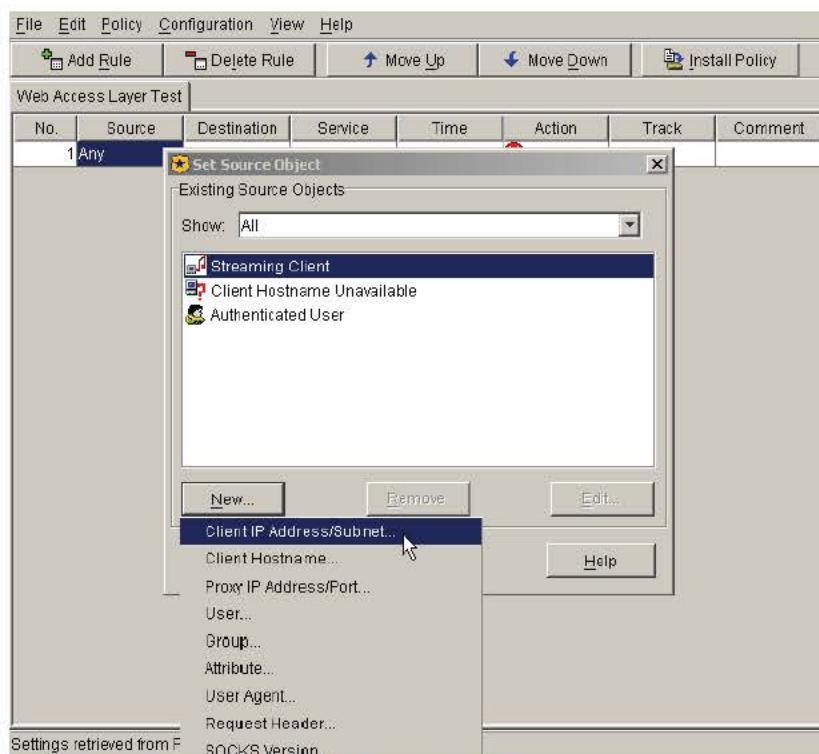


Figure 19-20: Select Client IP Address/Subnet

- Enter an IP address or Subnet Mask in the dialog that appears and click Add; click Close (or add additional addresses and then click Close); click OK.
3. Add an Action object to this rule:
- Right-click on the item in the Action column; select Set.

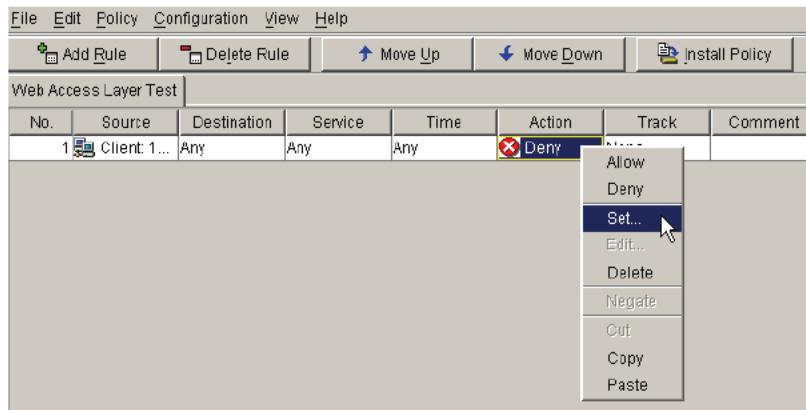


Figure 19-21: Right-Click Action and Select Set

- Click the New button in the Set Action Object dialog that appears; select Modify Access Logging.

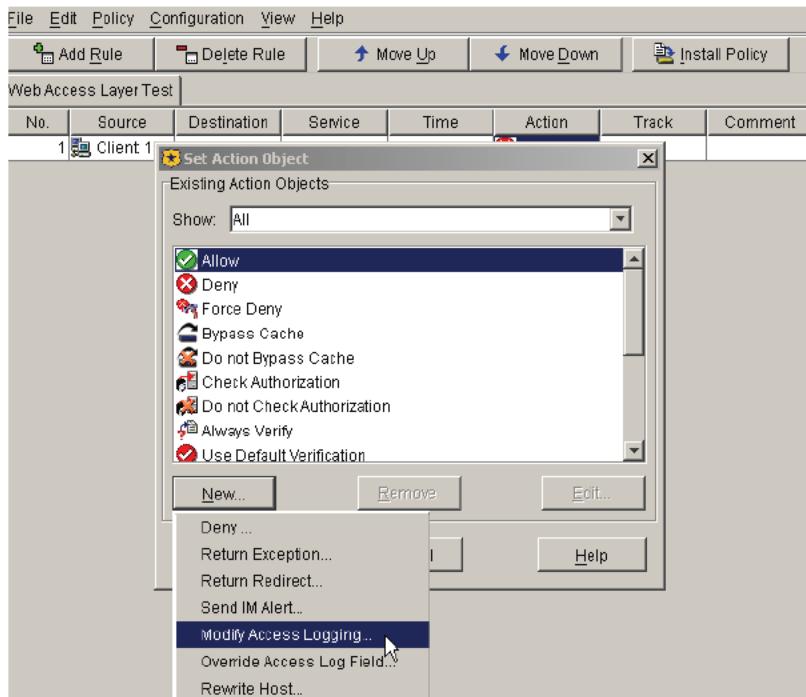


Figure 19-22: Disable Access Logging

- To disable a particular log, click the Disable logging to radio button and select that log from the drop-down list; to disable all access logging, click the Disable all access logging radio button.

- Click OK; click OK again; close the VPM window and click Yes in the dialog to save your changes.

Chapter 20: Maintaining the ProxySG

The Maintenance tabs provide a set of tools for managing and configuring an array of system-wide parameters, such as restarting the ProxySG, restoring system defaults, configuring SNMP, and managing the ProxySG.

This chapter contains the following sections:

- Restarting the ProxySG
- Restoring System Defaults
- Purging the DNS Cache
- Clearing the System Cache
- Upgrading the ProxySG
- Managing ProxySG Systems
- Event Logging and Notification
- Configuring SNMP
- Disk Reinitialization
- Deleting Objects from the ProxySG

Restarting the ProxySG

The restart options control the restart attributes of the ProxySG in case a restart is needed due to a system fault.

Important: The default settings of the Restart option suits most systems. Changing them without assistance from Blue Coat Systems Technical Support is not recommended.

Hardware and Software Restart Options

The Restart settings determine if the ProxySG performs a faster software-only restart, or a more comprehensive hardware and software restart. The latter can take several minutes longer, depending upon the amount of memory and number of disk drives in the ProxySG.

The default setting of Software only will suit most situations. Restarting both the hardware and software is recommended in situations where a hardware fault is suspected.

For information about the Core Image settings, see "Core Image Restart Options" on page 845.

Note: If you change restart option settings and you want them to apply to the next ProxySG restart, be sure to click **Apply**.

To Restart the ProxySG through the Management Console:

1. Select Maintenance>General.

The General tab displays.

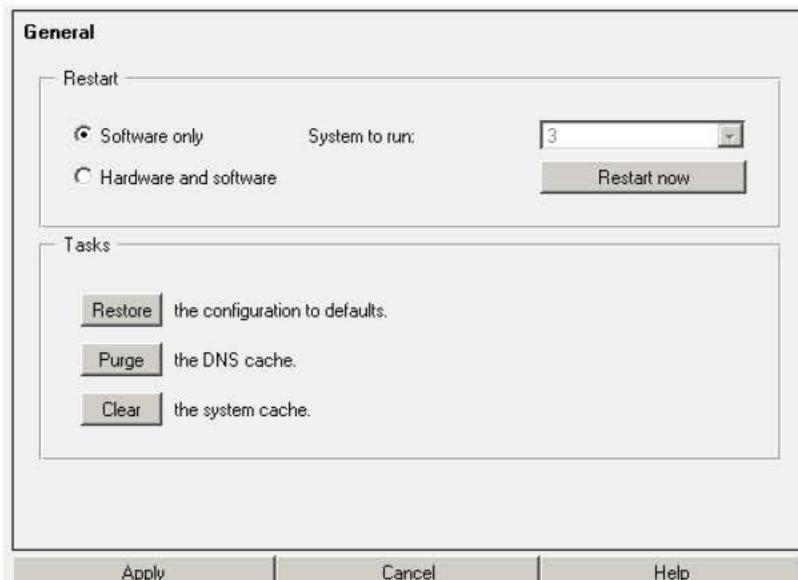


Figure 20-1: Restarting the ProxySG

2. In the Restart field, select either Software only or Hardware and software.
3. If you select the Hardware and software option, select a system from the System to run drop-down list.
The default system is pre-selected.
4. Click Apply.
5. Click the Restart now button.
6. Click OK to confirm and restart the ProxySG.

To Configure the Hardware/Software Restart Settings through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) restart mode {hardware | software}
```

where:

hardware	Configures the ProxySG for hardware (and software) restart.
software	Configures the ProxySG for software only restart.

To Restart the ProxySG through the CLI:

Do one of the following:

- To restart the system according to the restart settings, enter the following command:

```
SGOS# restart regular
```

- To restart hardware and software with a full core image, enter the following command:
`SGOS# restart abrupt`
- If you have added a new software image and want to restart the system using that image, enter the following command:
`SGOS# restart upgrade`

Restoring System Defaults

The ProxySG allows you to restore some or all of the system defaults. Use these commands with caution. The `restore-defaults` command deletes most but not all system defaults. The `restore-defaults` command with the `factory-defaults` option reinitializes the ProxySG to the original settings it had when it was shipped from the factory. The `restore-defaults` command with the `keep-console` option allows you to restore default settings without losing all IP addresses on the system.

Settings that are deleted when you use the `restore-defaults` command with the `factory-defaults` option include:

- Blue Coat licenses
- Local user accounts
- Hardware serial numbers set by the user
- Keyrings and Certificate Signing Authority (CA) certificates

The only settings that are kept when you use the `restore-defaults` command with the `factory-defaults` option are:

- Trial period information
- The last five installed appliance systems, from which you can pick one for rebooting

Settings that are deleted when you use the `restore-defaults` command without also using the `keep-console` option include:

- All IP addresses
- DNS server addresses
- Installable lists
- All customized configurations
- Third-party vendor licenses, such as SmartFilter
- Blue Coat trusted certificates
- Original SSH (v1 and v2) host keys (new host keys are regenerated)

IP settings retained on all interfaces (except for virtual IP addresses) using the `restore-defaults` command with the `keep-console` option include:

- IP addresses, including default gateway and bridging
- Ethernet maximum transmission unit (MTU) size
- TCP round trip time

- Static routes table information

Using the `keep-console` option retains the settings for all consoles (Telnet, SSH, HTTP, and HTTPS), whether they are enabled, disabled, or deleted. Administrative access settings retained using the `restore-defaults` command with the `keep-console` option include:

- Console username and password
- Front panel pin number
- Console enable password
- SSH (v1 and v2) host keys
- RIP configurations

To Restore System Defaults through the Management Console:

Note: The `keep-console` and `factory-defaults` options are not available through the Management Console.

1. Select Maintenance>General.

The General tab displays.

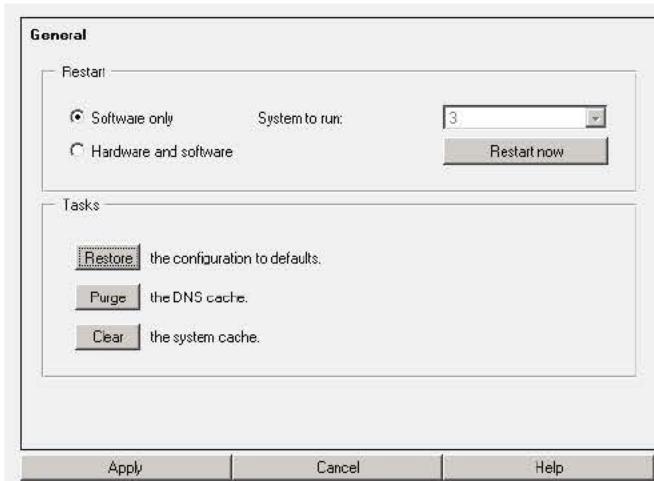


Figure 20-2: Restoring System Defaults

2. From the Tasks field of the General Tab, click Restore the configuration to defaults. Keep in mind that, if you restore the configuration from the Management Console, most settings are lost because you cannot use the `keep-console` option.

The Restore Configuration dialog appears.



Figure 20-3: Reset Configuration Confirmation

3. Click OK.

To Restore System Defaults through the CLI:

At the command prompt, enter the following command:

```
SGOS# restore-defaults [keep-console]
```

To Restore System Defaults without Confirmation, Enter:

```
SGOS# restore-defaults [keep-console] force
```

To Restore Factory Defaults through The CLI:

At the command prompt, enter the following command:

```
SGOS# restore-defaults factory-defaults
```

Purging the DNS Cache

You can purge the DNS cache at any time. You might need to do so if you have experienced a problem with your DNS server or if you have changed your DNS configuration.

To Purge the DNS Cache through the Management Console:

1. Select Maintenance>General.
2. In the Tasks field, click the Purge button.
3. Click OK to confirm in the Purge system DNS cache dialog that appears.

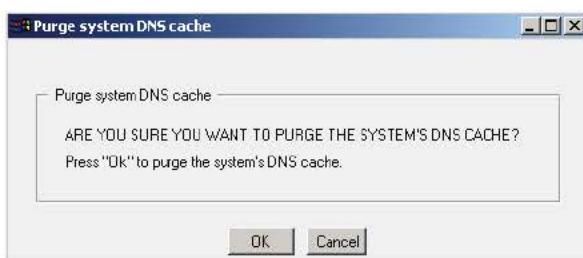


Figure 20-4: Purging the DNS Cache

To Purge the DNS Cache through the CLI:

At the enable command prompt, enter the following command:

```
SGOS# purge-dns-cache
```

Clearing the System Cache

You can clear the system cache at any time.

When you clear the cache, all objects in the cache are set to *expired*. The objects are not immediately removed from memory or disk, but a subsequent request for any object requested is retrieved from the source before it is served.

To Clear the System Cache through the Management Console:

1. Select Maintenance>General.
2. In the Tasks field, click the Clear button.
3. Click OK to confirm in the Clear cache dialog that appears.

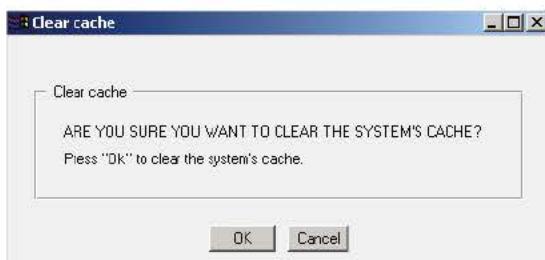


Figure 20-5: Clearing the System Cache

To Clear the System Cache through the CLI:

At the enable command prompt, enter the following command:

```
SGOS# clear-cache
```

Troubleshooting Tip

Occasionally, the Management Console might behave incorrectly because of browser caching, particularly if the browser was used to run different versions of the ProxySG Management Console. This problem might be resolved by clearing the browser cache.

Upgrading the ProxySG

When an upgrade to the ProxySG becomes available, you can download it through the Internet and install it. You can also download it to your PC and install it from there.

The ProxySG 3.x Version Upgrade

The appliance must be running version SGOS 2.1.06 or later in order to upgrade to SGOS 3.x. You cannot directly upgrade from any version of CacheOS.

Note the policy-related considerations in replacing an SGOS 2.3 or later version with the earlier version:

- The earlier version does not use the ProxySG configuration, including any defined ProxySG policies.
- If you defined security-related policies (for example, related to user authentication), those policies do not apply to the earlier version. As a result, the ProxySG might be less secure.
- If a system fault occurs with an SGOS version, the ProxySG can restart with an earlier CacheOS system. In order to maintain continuous operation, CacheOS automatically boots to an earlier version if the current version cannot be booted (for example, as a result of a serious problem). If the next bootable system is a 4.x or earlier version, CacheOS does not use any policies defined for SGOS version 2.x or later.

Note: At least one other system must be unlocked to do the upgrade. If all systems are locked, or all systems except the running system are locked, the Download button in the Management Console is disabled. Similarly, the `load upgrade` command in the CLI generates an error.

To Upgrade the ProxySG through the Management Console:

1. Select Maintenance>Upgrade>Upgrade.

The Upgrade tab displays.

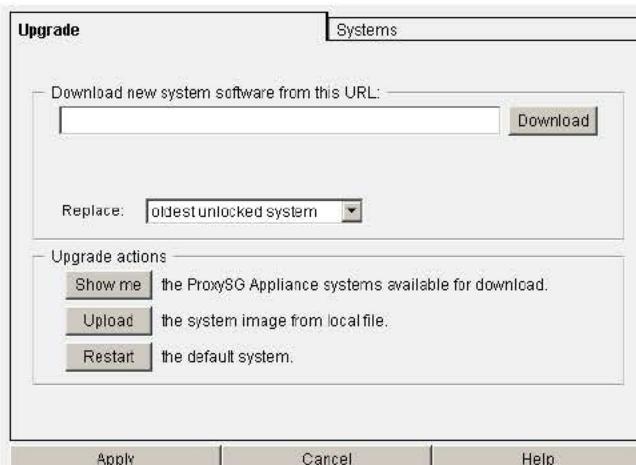


Figure 20-6: Upgrading the ProxySG

2. Click **Show me** to connect to the Blue Coat download page, follow the instructions, and note the URL of the ProxySG upgrade for your system model. Then enter the URL in the **Download new system software from this URL** field and click **Download**.

-or-

(Only if you previously downloaded a system image to your PC) Click **Upload** and **Browse** to the file location, then click **Install**. Note that the upload might take several minutes.

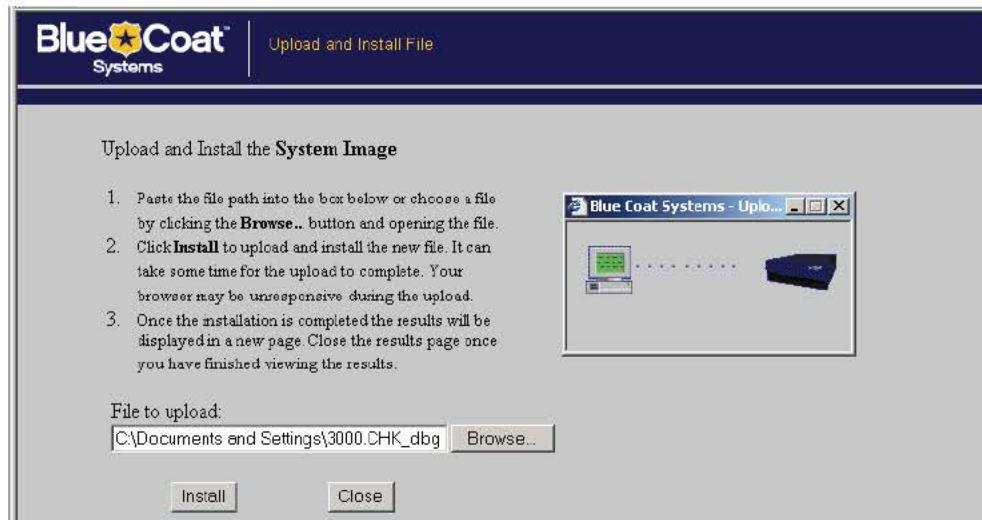


Figure 20-7: Uploading a System Image from a PC

3. (Optional) Select the system to replace in the Replace drop-down list. If you uploaded an image from your PC, refresh the Systems pane to see the new system image.
4. Click Restart.

The Restart system dialog displays.

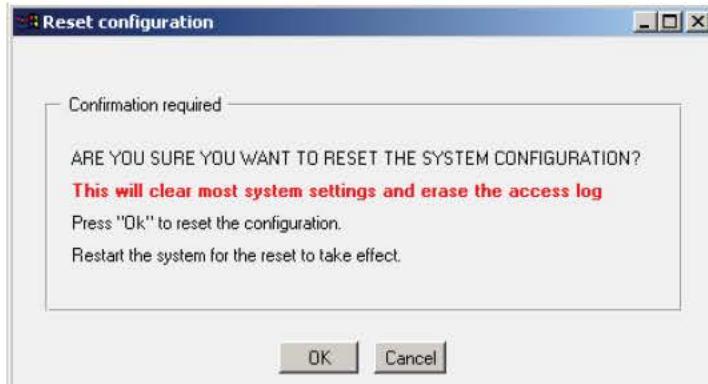


Figure 20-8: Restart System Dialog

5. Click OK to reboot the ProxySG to the default system.

To Upgrade the ProxySG through the CLI:

From the serial console, enter the following commands:

```
SGOS# (config) upgrade-path url
where url is the location of the OS upgrade image.

SGOS# (config) exit
SGOS# load upgrade
SGOS# restart upgrade
```

Managing ProxySG Systems

The ProxySG Systems tab displays the five available ProxySG systems. Empty systems are indicated by the word **Empty**.

The ProxySG system currently running is highlighted in blue and cannot be replaced or deleted.

From this screen, you can:

- Select the SGOS system version to boot.
- Lock one or more of the available SGOS system versions.
- Select the SGOS system version to be replaced.
- Delete one or more of the available SGOS system versions (CLI only).
- View details of the available SGOS system versions.

To View ProxySG System Replacement Options through the Management Console:

Select Maintenance>Upgrade>Systems.

The Systems tab displays.

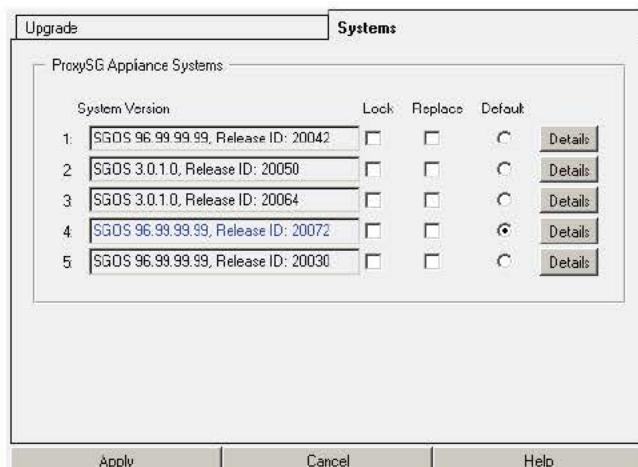


Figure 20-9: Setting SGOS System Version Replacement Properties

To View Details for an SGOS System Version through the Management Console:

1. Select Maintenance>Upgrade>Systems.
2. Click the Details button next to the system for which you want to view detailed information; click OK when you are finished.

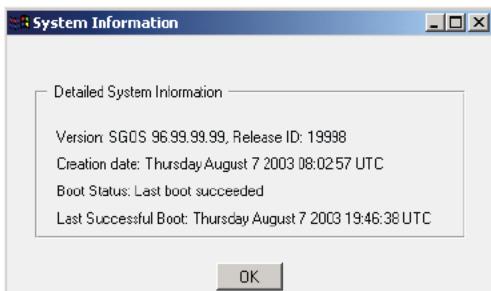


Figure 20-10: SGOS System Version Details

To View Details for an SGOS System Version through the CLI:

At the command prompt:

```
SGOS> show installed-systems
```

Example Session

```
SGOS> show installed-systems
ProxySG Appliance Systems
1. Version: SGOS 96.99.99.99, Release ID: 20042
    Thursday August 21 2003 08:08:58 UTC, Lock Status: Unlocked
    Boot Status: Last boot succeeded, Last Successful Boot: Thursday August 21
    2003 17:51:50 UTC
2. Version: SGOS 3.0.1.0, Release ID: 20050
    Friday August 22 2003 04:43:34 UTC, Lock Status: Unlocked
    Boot Status: Last boot succeeded, Last Successful Boot: Friday August 22 2003
    16:47:53 UTC
3. Version: SGOS 96.99.99.99, Release ID: 20021
    Tuesday August 12 2003 20:02:42 UTC, Lock Status: Unlocked
    Boot Status: Last boot succeeded, Last Successful Boot: Thursday August 14
    2003 17:57:06 UTC
4. Version: SGOS 96.99.99.99, Release ID: 20029
    Thursday August 14 2003 20:01:55 UTC, Lock Status: Unlocked
    Boot Status: Last boot succeeded, Last Successful Boot: Thursday August 14
    2003 20:49:02 UTC
5. Version: SGOS 96.99.99.99, Release ID: 20030
    Friday August 15 2003 08:01:47 UTC, Lock Status: Unlocked
    Boot Status: Last boot succeeded, Last Successful Boot: Friday August 15 2003
    19:20:32 UTC
Default system to run on next hardware restart: 2
Default replacement being used. (oldest unlocked system)
Current running system: 2
```

When a new system is loaded, only the system number that was replaced is changed.
The ordering of the rest of the systems remains unchanged.

Setting the Default Boot System

This setting allows you to select the system to be booted on the next hardware restart. If a system starts successfully, it is set as the default boot system. If a system fails to boot, the next most recent system that booted successfully becomes the default boot system.

To Set the ProxySG to Run on the Next Hardware Restart through the Management Console:

1. Select Maintenance>Upgrade>Systems.
2. Select the preferred ProxySG System version in the Default column.
3. Click Apply.

Note: An empty system cannot be specified as default, and only one system can be specified as the default system.

To Set the ProxySG to Run on the Next Hardware Restart through the CLI:

At the (config) command prompt:

```
SGOS# (config) installed-systems
SGOS# (config installed-systems) default system_number
where system_number is the default system version.
```

Locking and Unlocking ProxySG Systems

Any system can be locked, except a system that has been selected for replacement. If all systems, or all systems except the current system are locked, the ProxySG cannot load a new system.

If a system is locked, it cannot be replaced or deleted.

To Lock a System through the Management Console:

1. Select Maintenance>Upgrade>Systems.
2. Select the system(s) to lock in the Lock column.
3. Click Apply.

To Lock a System through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) installed-systems
SGOS# (config installed-systems) lock system_number
where system_number is the system you want to lock.
```

To Unlock a System through the Management Console:

1. Select Maintenance>Upgrade>Systems.
2. Deselect the system(s) to unlock in the Lock column.
3. Click Apply.

To Unlock a System through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) installed-systems  
SGOS#(config installed-systems) no lock system_number
```

where *system_number* is the system you want to unlock.

Replacing a ProxySG System

You can specify the system to be replaced when a new system is downloaded. If no system is specified, the oldest unlocked system will be replaced by default. You cannot specify a locked system for replacement.

To Specify the System to Replace through the Management Console:

1. Select Maintenance>Upgrade>Systems.
2. Select the system to replace in the Replace column.
3. Click Apply.

To Specify the System to Replace through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) installed-systems  
SGOS#(config installed-systems) replace system_number
```

where *system_number* is the system to be replaced.

Deleting a ProxySG System

You can delete any of the ProxySG system versions except the current running system. A locked system must be unlocked before it can be deleted. If the system you want to delete is the default boot system, you need to select a new default boot system before the system can be deleted.

You cannot delete a system version through the Management Console; you must use the CLI.

To Delete a System through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) installed-systems  
SGOS#(config installed-systems) delete system_number
```

where *system_number* is the system you want to delete.

Event Logging and Notification

You can configure the ProxySG to log system events as they occur. *Event logging* allows you to specify the types of system events logged, the size of the event log, and to configure Syslog monitoring. The ProxySG can also notify you by email if an event is logged.

Configuring Which Events to Log

The event level options are listed from the most to least important events. Because each event requires some disk space, setting the event logging to log all events fills the event log more quickly.

To Set the Event Logging Level through the Management Console:

1. Select Maintenance>Event Logging>Level.

The Level tab displays.

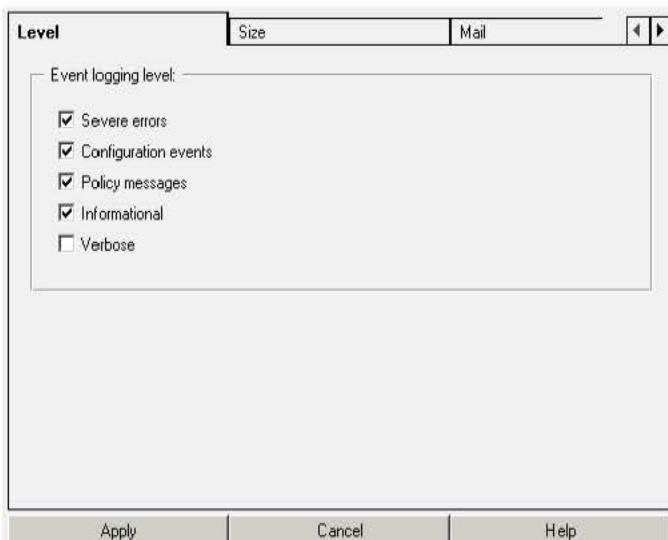


Figure 20-11: Selecting Which Events are Logged

2. Select the events you want to log.

When you select an event level, all levels above the selection are included. For example, if you select Verbose, all event levels are included.

Note: To enable ICAP and health check notification, you must set the event logging level to Informational or Verbose.

3. Click Apply.

To Set the Event Logging Level through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS# (config) event-log
SGOS# (config event-log) level {severe | configuration | policy | informational | verbose}
```

where:

severe	Writes only severe error messages to the event log.
configuration	Writes severe and configuration change error messages to the event log.

policy	Writes severe, configuration change, and policy event error messages to the event log.
informational	Writes severe, configuration change, policy event, and information error messages to the event log.
verbose	Writes all error messages to the event log.

Setting Event Log Size

You can limit the size of the ProxySG's event log and specify what the appliance should do if the log size limit is reached.

To Set Event Log Size through the Management Console:

1. Select Maintenance>Event Logging>Size.

The Size tab displays.

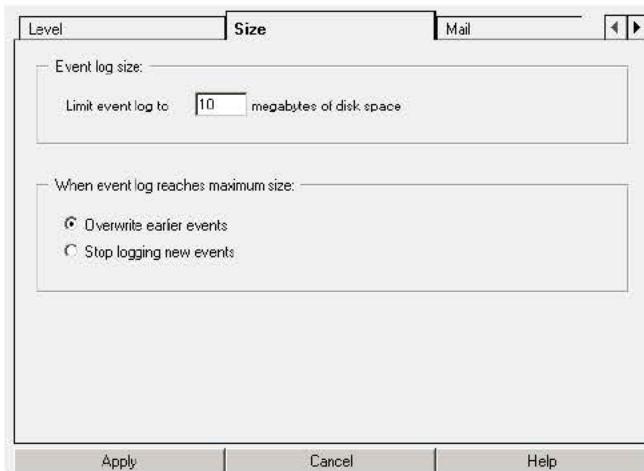


Figure 20-12: Configuring Event Log Size

2. In the Event log size field, enter the maximum size of the event log in megabytes.
3. Select either Overwrite earlier events or Stop logging new events to specify the desired behavior when the event log reaches maximum size.
4. Click Apply.

To Set Event Log Size through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS#(config) event-log
SGOS#(config event-log) log-size megabytes
SGOS#(config event-log) when-full {overwrite | stop}
```

Specifies event logging behavior should the event log become full.

Enabling Event Notification

The ProxySG can send event notifications to Internet email addresses using SMTP. You can also send event notifications directly to Blue Coat for support purposes. For information on configuring diagnostic reporting, see "Archive Configuration" on page 59.

Note: The ProxySG must know the host name or IP address of your SMTP mail gateway to mail event messages to the email address(es) you have entered. If you do not have access to an SMTP gateway, you can use the Blue Coat default gateway to send event messages directly to Blue Coat.

The Blue Coat SMTP gateway will only send mail to Blue Coat. It will not forward mail to other domains.

To Enable Event Notifications through the Management Console:

1. Select Maintenance>Event Logging>Mail.

The Mail tab displays.

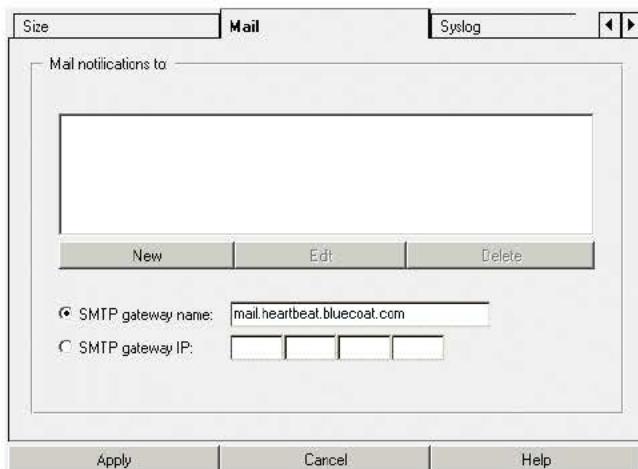


Figure 20-13: Enabling Event Notification

2. Click New to add a new email address; click OK in the Add list item dialog that appears.
3. In the SMTP gateway name field, enter the host name of your mail server; or in the SMTP gateway IP field, enter the IP address of your mail server.
4. Click Apply.

To Enable Event Notifications through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) event-log
SGOS#(config event-log) mail smtp-gateway gateway
```

where *gateway* is a domain name or an IP address.

```
SGOS#(config event-log) mail add recipient@url  
SGOS#(config event-log) exit  
SGOS#(config) policy notify
```

Sends event notifications directly to Blue Coat for support purposes.

Syslog Event Monitoring

Syslog is an event-monitoring scheme that is especially popular in UNIX environments. Sites that use syslog typically have a log host node, which acts as a sink for several devices on the network. You must have a syslog daemon operating in your network to use syslog monitoring. The syslog format is: Date Time Hostname Event.

Most clients using syslog have multiple devices sending messages to a single syslog daemon. This allows viewing a single chronological event log of all of the devices assigned to the syslog daemon. An event on one network device might trigger an event on other network devices, which, on occasion, can point out faulty equipment.

To Enable Syslog Monitoring through the Management Console:

1. Select Maintenance>Event Logging>Syslog.

The Syslog tab displays.

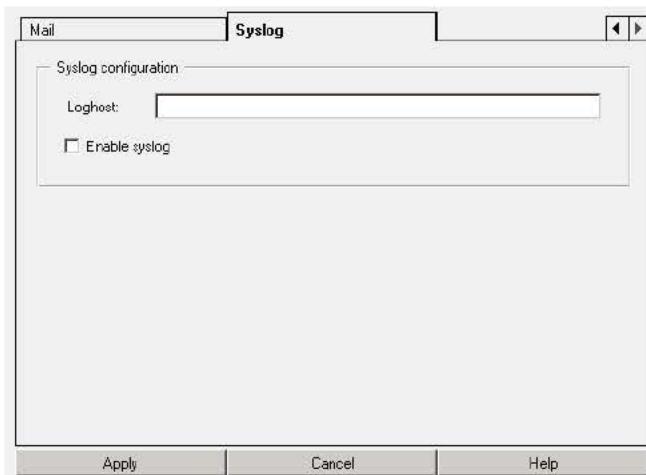


Figure 20-14: Setting Up Syslog Monitoring

2. In the Loghost field, enter the domain name or IP address of your loghost server.
3. Select Enable Syslog.
4. Click Apply.

To Enable Syslog Monitoring through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) event-log  
SGOS#(config event-log) syslog loghost loghost
```

where *loghost* is the log host domain name or IP address.

```
SGOS# (config event-log) syslog enable
```

Viewing Event Log Configuration and Content through the CLI

You can view the system event log through the CLI, either in its entirety or selected portions of it.

Viewing the Event Log Configuration through the CLI

You can view the event log configuration, from `show` or from `view` in the event-log configuration mode.

To view the event long configuration, enter the following command:

- From anywhere in the CLI:

```
SGOS>show event-log configuration
Settings:
  Event level: severe + configuration + policy + informational
  Event log size: 10 megabytes
  If log reaches maximum size, overwrite earlier events
  Syslog loghost: <none>
  Syslog notification: disabled
  Syslog facility: daemon
Event recipients:
  SMTP gateway:
    mail.heartbeat.bluecoat.com
```

-or-

- From the (config) prompt:

```
SGOS# (config) event-log
SGOS# (config event-log) view configuration
Settings:
  Event level: severe + configuration + policy + informational
  Event log size: 10 megabytes
  If log reaches maximum size, overwrite earlier events
  Syslog loghost: <none>
  Syslog notification: disabled
  Syslog facility: daemon
Event recipients:
  SMTP gateway:
    mail.heartbeat.bluecoat.com
```

Viewing the Event Log Contents through the CLI

Again, you can view the event log contents from the `show` command or from the event-log configuration mode.

The syntax for viewing the event log contents is

```
SGOS# show event-log  
-or-  
SGOS# (config event-log) view  
[start [YYYY-mm-dd] [HH:MM:SS]] [end [YYYY-mm-dd] [HH:MM:SS]] [regex regex |  
substring string]
```

Pressing <Enter> shows the entire event log without filters.

The order of the filters is unimportant. If `start` is omitted, the start of the recorded event log is used. If `end` is omitted, the end of the recorded event log is used.

If the date is omitted in either `start` or `end`, it must be omitted in the other one (that is, if you supply just times, you must supply just times for both `start` and `end`, and all times refer to today). The time is interpreted in the current timezone of the ProxySG.

Understanding the Time Filter

The entire event log can be displayed, or either a starting date/time or ending date/time can be specified. A date/time value is specified using the notation ([YYYY-MM-DD] [HH:MM:SS]). Parts of this string can be omitted as follows:

- If the date is omitted, today's date is used.
- If the time is omitted for the starting time, it will be 00:00:00
- If the time is omitted for the ending time, it will be 23:59:59

At least one of the date or the time must be provided. The date/time range is inclusive of events that occur at the start time as well as dates that occur at the end time.

Note: If the notation includes a space, such as between the start date and the start time, the argument in the CLI should be quoted.

Understanding the Regex and Substring Filters

A regular expression can be supplied, and only event log records that match the regular expression will be considered for display. The regular expression is applied to the text of the event log record not including the date and time. It is case-sensitive and not anchored. You should quote the regular expression.

Since regular expressions can be difficult to write properly, you can use a substring filter instead to search the text of the event log record, not including the date and time. The search is case sensitive.

Regular expressions use the standard regular expression syntax as defined by policy. If both regex and substring are omitted, then all records are assumed to match.

Example

```
SGOS# show event-log start "2004-10-22 9:00:00" end "2004-10-22 9:15:00"
2004-10-22 09:00:02+00:00UTC "Snapshot sysinfo_stats has fetched /sysinfo-stats
" 0 2D0006:96 .../Snapshot_worker.cpp:183
2004-10-22 09:05:49+00:00UTC "NTP: Periodic query of server ntp.bluecoat.com,
system clock is 0 seconds 682 ms fast compared to NTP time. Updated system clock.
" 0 90000:1 .../ntp.cpp:631
```

Configuring SNMP

You can view a ProxySG using a Simple Network Management Protocol (SNMP) management station. The ProxySG supports MIB-2 (RFC 1213), Proxy MIB, and the RFC2594 MIB, and can be downloaded at the following URL: <http://download.bluecoat.com/release/SGOS3/index.html>. (The SNMP link is in the lower right-hand corner.).

Enabling SNMP

To view a ProxySG from an SNMP management station, you must enable and configure SNMP support on the ProxySG.

To Enable and Configure SNMP through the Management Console:

1. Select Maintenance>SNMP>SNMP General.

The SNMP General tab displays.



Figure 20-15: Enabling SNMP

2. Select Enable SNMP.
3. In the sysLocation field, enter a string that describes the ProxySG's physical location.

4. In the **sysContact** field, enter a string that identifies the person responsible for administering the ProxySG.
5. Click **Apply**.

To Enable and Configure SNMP through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) snmp  
SGOS#(config snmp) enable  
SGOS#(config snmp) sys-location location
```

where *location* specifies the ProxySG's physical location.

```
SGOS#(config snmp) sys-contact contact
```

where *contact* identifies the person responsible for administering the ProxySG.

Configuring SNMP Community Strings

Use *community strings* to restrict access to SNMP data. To read SNMP data on the ProxySG, specify a *read community* string. To write SNMP data to the ProxySG, specify a *write community* string. To receive traps, specify a *trap community* string. By default, all community string passwords are set to public.

Note: If you enable SNMP, make sure to change all three community-string passwords to values that are difficult to guess. Use a combination of uppercase, lowercase, and numeric characters. An easily-guessed community-string password makes it easier to gain unauthorized access to the ProxySG and network.

To Set or Change Community Strings through the Management Console:

1. Select Maintenance>SNMP>Community Strings.

The Community Strings tab displays.

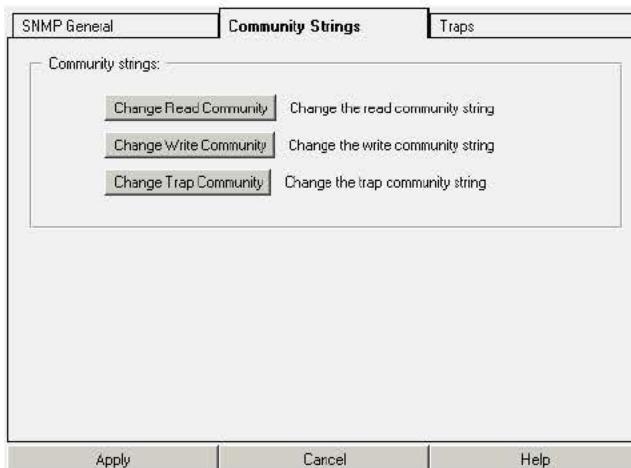


Figure 20-16: Configuring SNMP Community Strings

2. Click the community string button you want to change.

The Change Read/Write/Trap Community dialog displays.

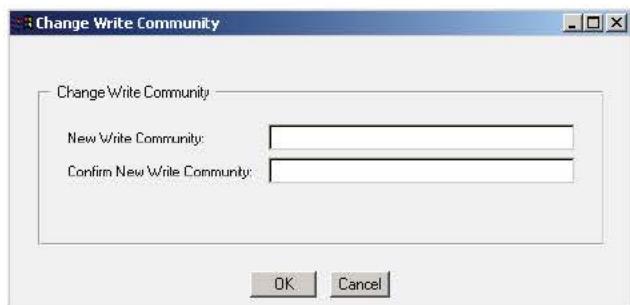


Figure 20-17: SNMP Change Community String Dialog

3. Enter and confirm the community string; click OK.
4. Click Apply.

To Configure or Change Community Strings through the CLI:

You can set the community strings in either cleartext or encrypted form.

To set them in cleartext:

```
SGOS# (config) snmp
SGOS# (config snmp) enable
SGOS# (config snmp) read-community password
SGOS# (config snmp) write-community password
SGOS# (config snmp) trap-community password
```

To set them as encrypted:

```
SGOS# (config) snmp
SGOS# (config snmp) enable
SGOS# (config snmp) encrypted-read-community encrypted-password
SGOS# (config snmp) encrypted-write-community encrypted-password
SGOS# (config snmp) encrypted-trap-community encrypted-password
```

Configuring SNMP Traps

The ProxySG can send SNMP traps to a management station as they occur. By default, all system-level traps are sent to the address specified. You can also enable authorization traps to send notification of attempts to access the ProxySG Management Console.

Note: The SNMP trap for CPU utilization is sent only if the CPU continues to stay up for 32 or more seconds.

To Enable SNMP Traps through the Management Console:

Note: You cannot configure SNMP traps to go out through a particular interface.

1. Select Maintenance>SNMP>Traps.

The Traps tab displays.

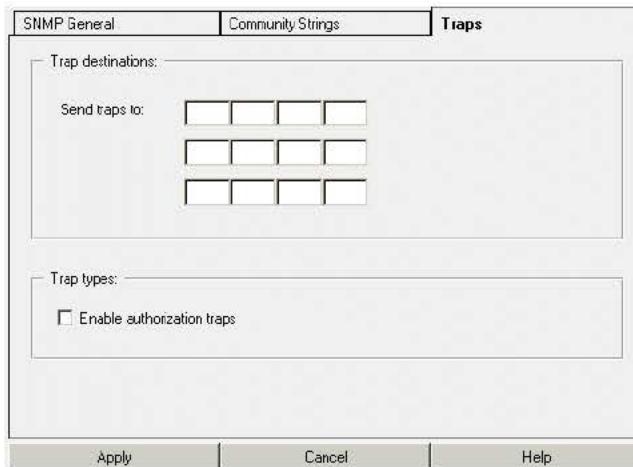


Figure 20-18: Configuring SNMP Traps

2. In the Send traps to fields, enter the IP address(es) of the workstation(s) where traps are to be sent.
3. To receive authorization traps, select Enable authorization traps.
4. Click Apply.

To Enable SNMP Traps through the CLI:

Note: You cannot configure SNMP traps to go out through a particular interface.

1. At the (config) command prompt, enter the following commands:

```
SGOS# (config) snmp  
SGOS# (config snmp) enable  
SGOS# (config snmp) trap-address 1 ip_address
```

To add additional trap addresses, repeat using trap-address 2 or trap-address 3 to specify the IP address for traps 2 and 3.

2. (Optional) To enable authorization traps, enter the following command:

```
SGOS# (config snmp) authorize-traps
```

Disk Reinitialization

You can reinitialize disks on a multi-disk ProxySG. You cannot reinitialize the disk on a single-disk ProxySG: If you suspect a disk fault in a single-disk ProxySG, contact Blue Coat Technical Support for assistance.

Note: If a disk containing an unmirrored event or access log is reinitialized, the logs are lost. Similarly, if two disks containing mirrored copies of the logs are reinitialized, both copies of the logs are lost.

Multi-Disk ProxySG

On a multi-disk ProxySG, the master disk is the leftmost valid disk. “Valid” means that the disk is online, has been properly initialized, and is not marked as invalid or unusable.

If the current master disk is taken offline, reinitialized, or declared invalid or unusable, the leftmost valid disk that has not been reinitialized since restart becomes the master disk. Thus, as disks are reinitialized in sequence, a point is reached where no disk can be chosen as the master. At this point, the current master disk is the last disk. If this disk is taken offline, reinitialized, or declared invalid or unusable, the ProxySG is restarted.

On a multi-disk ProxySG, a disk is reinitialized by setting it to empty and copying pre-boot programs, boot programs, and starter programs, and system images from the master disk to the reinitialized disk.

Reinitialization is done online without rebooting the ProxySG. (For more information, refer to the `#disk` command in the *Blue Coat Command Line Interface Reference*.) ProxySG operations, in turn, are not affected, although during the time the disk is being reinitialized, that disk is not available for caching. Note that only the master disk reinitialization will restart the ProxySG.

Only persistent objects are copied to a newly-reinitialized disk. This is usually not a problem because most of these objects are replicated or mirrored. If the reinitialized disk contained one copy of these objects (which is lost), another disk will contain another copy.

You cannot reinitialize all of the ProxySG disks over a very short period of time. Attempting to reinitialize the last disk in a ProxySG before critical components can be replicated to other disks in the system causes a warning message to appear.

Immediately after reinitialization is complete, the ProxySG automatically starts using the reinitialized disk for caching.

Single-Disk ProxySG

The disk on a single-disk ProxySG cannot be reinitialized by the customer. If you suspect a disk fault in a single-disk ProxySG, contact Blue Coat Technical Support for assistance.

Deleting Objects from the ProxySG

The ability to delete either individual or multiple objects from the ProxySG makes it easy to delete stale or unused data and make the best use of the storage in your system.

Note: The maximum number of objects that can be stored in a ProxySG is roughly a million. The number is based on the 4GB RAM on the motherboard and is not user-configurable.

This feature is not available in the Management Console. Use the CLI instead.

To Delete a Single Object from the ProxySG through the CLI:

At the (config) prompt, enter the following command:

```
SGOS# (config) content delete url url
```

To Delete Multiple Objects from the ProxySG through the CLI:

At the (config) prompt, enter the following command:

```
SGOS#(config) content delete regex regex
```

Chapter 21: Statistics

The Statistics tabs of the Management Console allows you to graphically view the status of many system operations, as well as to take disks offline and put them online. Many statistics are available through the CLI, but without the benefit of graphical display.

The CLI also provides detailed system information. Using the `show ?` command in privileged mode lists the many subcommands to view a great deal of system configuration information in addition to the statistics discussed here. Refer to the *Blue Coat Command Line Interface Reference* for detailed information on using the `show` command.

Selecting the Graph Scale

Some statistics are reported in the form of bar graphs. Most bar graphs offer the option to show all values in the graph or to clip a percentage of the peak values, which means that a percentage is allowed to fall off the scale. For example, if you select clip 25% of peaks, the top 25% of the values will be allowed to exceed the scale for the graph, showing greater detail for the remaining 75% of the values. To set the graph scale, select a value from the Graph scale should drop-down list. Some of the graphs offer the option of viewing statistics in bytes or objects. On these pages, you can switch among viewing modes by selecting bytes served or objects served mode from the Graph shows or Percentages reflect drop-down list.

General Statistics

The General statistics tabs (Summary, Environment, and Disks) provide information about system configuration and the status of hardware sensors and allow you to take disks offline and put them online.

Note: The ProxySG 400 Series Appliances do not have an Environment tab.

System Summary

The device provides a variety of information on its status. The fields on the Summary tab are described below:

- Disks Installed—the number of disk drives installed in the device. The Disks tab displays the status of each drive.
- Memory installed—the amount of RAM installed in the device.
- CPUs installed—the number of CPUs installed in the device.
- Software image—the version and release number of the device image.
- Serial number—the serial number of the machine, if available.
- System started—the time and date the device was started.

- CPU utilization—the current percent utilization of the device CPU.

Viewing the System Summary

To View the System Summary:

Select Statistics>General>Summary.

The General Summary tab displays.

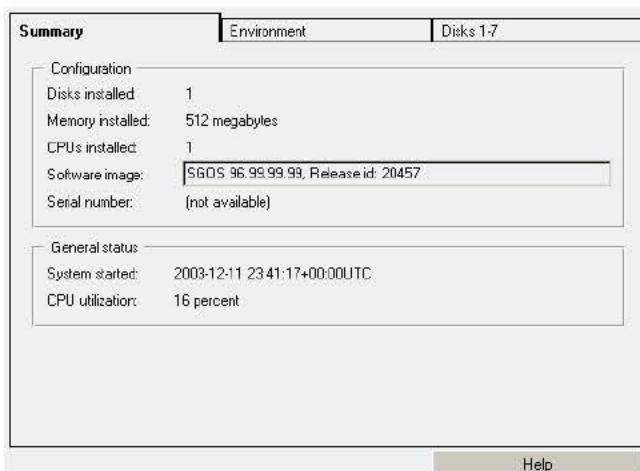


Figure 21-1: General Summary Tab

Viewing System Environment Sensors

The icons on the Environment tab are green when the related hardware environment is within acceptable parameters, and red when an out-of-tolerance condition exists. If an icon is red, click **View Sensors** to view detailed sensor statistics to learn more about the out-of-tolerance condition.

Note: You cannot view environment statistics on a ProxySG 400 Series Appliance.

To View a System Environment:

1. Select Statistics>General>Environment.

The Environment tab displays.

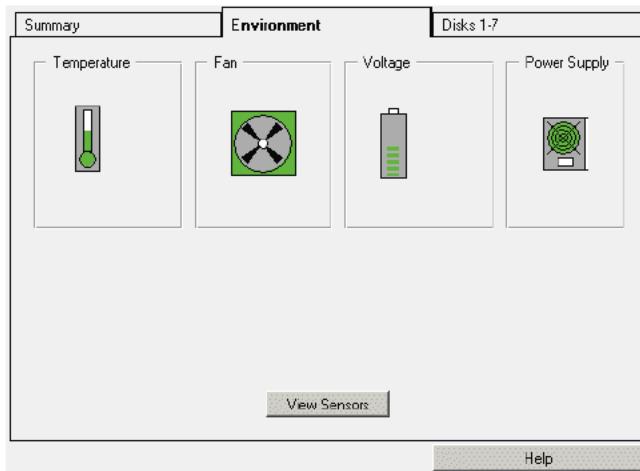


Figure 21-2: Environment Tab

2. Click View Sensors to see detailed sensor values; close the window when you are finished.

Sensor statistics		
Sensor Name	Reading	Status
Bus temperature #1	26.0 C	OK
Bus temperature #2	23.0 C	OK
Fan #1		OK
Fan #2		OK
Bus voltage #1	1.4 volts	OK
Power supply #1		OK
Power supply #2		OK

Figure 21-3: Sensor Statistics Window

Viewing Disk Status

You can view the status of each of the disks in the system and take a disk offline if needed.

To View Disk Status or Take A Disk Offline:

1. Select Statistics>General>Disks.

The Disks tab displays, providing information about the disk in slot 1.

Note: The name of this tab differs, depending on the range of disks available to the ProxySG model you use.

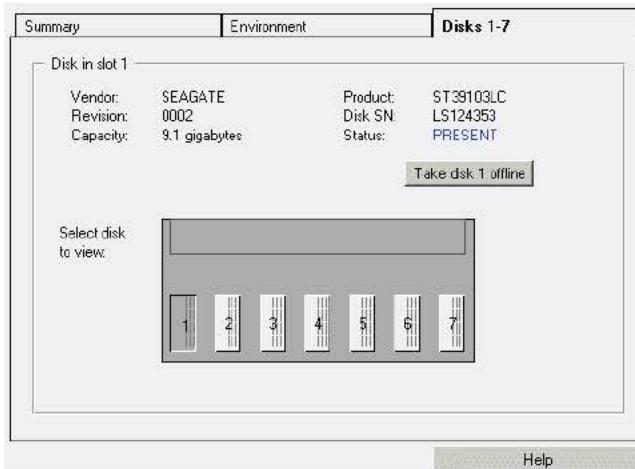


Figure 21-4: Disks Tab

2. Select the disk to view by clicking the appropriate disk number.
3. To take the disk offline, click the Take disk x offline button (where x is the number of the disk you have selected).
4. Click OK in the Take disk offline dialog that displays.



Figure 21-5: Take Disk Offline Dialog

System Usage Statistics

The System Usage tabs (CPU, Bandwidth Gain, Freshness, and Refresh Bandwidth) display bar graphs that illustrate the last 60 minutes, 24 hours, and 30 days for CPU utilization, bandwidth gain, freshness of objects in the cache, and the average network bandwidth used to maintain freshness.

You view graphs in either objects served or bytes served. Objects served is the default, but if you switch one tab to bytes served, all of the tabs switch to that view.

If you hover your cursor over a particular area of any of the graphs, a figure or set of figures appropriate to that graph will display. An example of this feature is shown in Figure 21-7.

Viewing CPU Utilization

The CPU tab illustrates the average CPU utilization for the device over the last 60 minutes, 24 hours, and 30 days. The default view is show all values.

To view CPU utilization:

1. Select Statistics>System Usage>CPU.

The CPU tab displays.

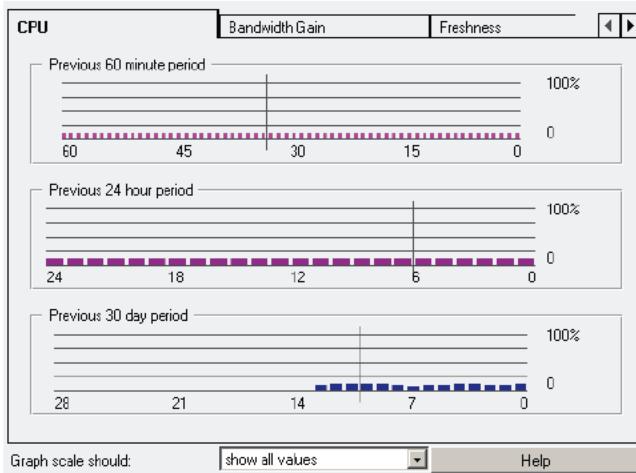


Figure 21-6: CPU Tab

2. (Optional) To set the graph scale to clip a percentage of the peaks in value, select a percentage from the Graph scale should drop-down list.

Viewing Bandwidth Gain

The Bandwidth Gain tab illustrates bandwidth gain over the last 60 minutes, 24 hours, and 30 days.

To View Bandwidth Gain:

1. Select Statistics>System Usage>Bandwidth Gain.

The Bandwidth Gain tab displays.

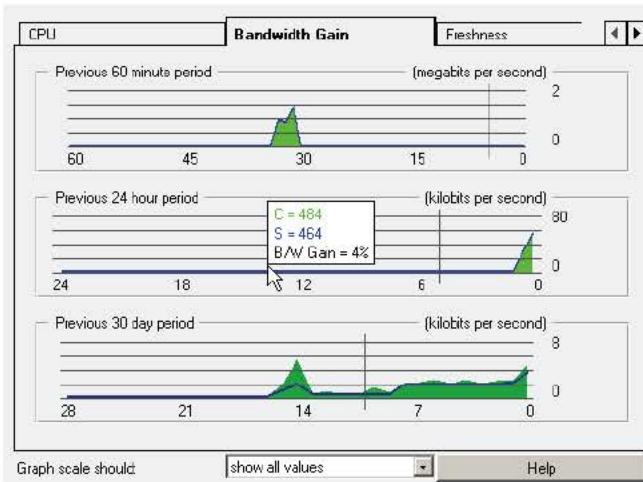


Figure 21-7: Bandwidth Gain Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

The green display represents client data; the blue display represents server data.

The top chart displays the bandwidth gain measured at each minute of operation and includes the most recent 60 minutes of operation.

The middle chart displays the bandwidth gain at each hour of operation and includes the most recent 24 hours.

The bottom chart displays the bandwidth gain at each day of operation and includes the most recent 30 days; the same query applies with respect to the previous collection of 24 hours being reflected in the most recent (right-most) day marker.

It is normal to see 100% markers in places where there has been no client-use for the activity. This means that, of the server side traffic being expended, 100% of it is being expended for ProxySG internal usage, such as asynchronous adaptive refresh.

Viewing Cache Freshness

The Freshness tab illustrates the estimated freshness of objects in the cache over the last 60 minutes, 24 hours, and 30 days.

Freshness applies only to objects that are cached (all objects that are not cached are always 100% fresh). For example, if the estimated freshness is 99%, that means when you request an object there is a 99% chance that object is fresh in the cache.

To View Cache Freshness:

1. Select Statistics>System Usage>Freshness.

The Freshness tab displays.

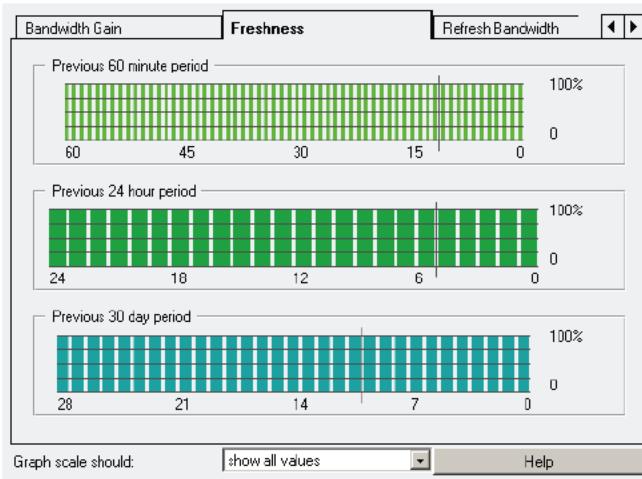


Figure 21-8: Freshness Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

Viewing Refresh Bandwidth Statistics

The Refresh Bandwidth tab illustrates the average network bandwidth used to maintain freshness in the cache over the last 60 minutes, 24 hours, and 30 days.

To View Refresh Bandwidth:

1. Select Statistics>System Usage>Refresh Bandwidth.

The Refresh Bandwidth tab displays.

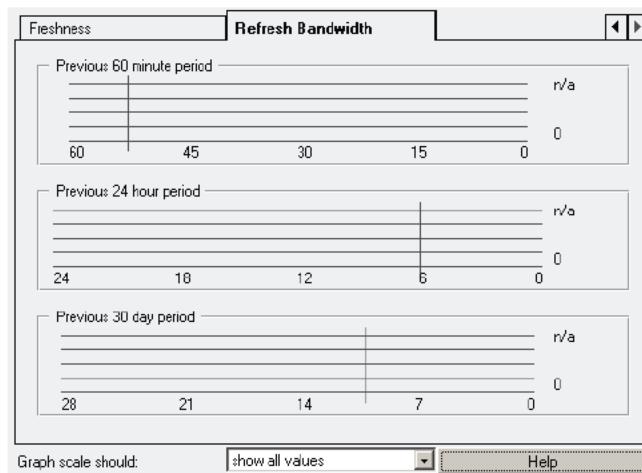


Figure 21-9: Refresh Bandwidth Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

HTTP/FTP History Statistics

The HTTP/FTP History tabs (HTTP/FTP Objects, HTTP/FTP Bytes, and HTTP/FTP Clients) display bar graphs that illustrate the last 60 minutes, 24 hours, and 30 days for the number of objects served, the number of bytes served, and the maximum number of active clients processed.

The bar graphs in the HTTP/FTP History tabs offer the option to show all values in the graph or to clip a percentage of the peak values, which means that a percentage is allowed to fall off the scale. For example, if you select clip 25% of peaks, the top 25% of the values will be allowed to exceed the scale for the graph, showing greater detail for the remaining 75% of the values. The default is show all values, but if you switch one tab to another value, all of the tabs switch to that view.

If you hover your cursor over a particular area of any of the graphs, a figure or set of figures appropriate to that graph will display. An example of this feature is shown in Figure 21-7.

Viewing the Number of Objects Served

The HTTP/FTP Objects tab illustrates the device activity over the last 60 minutes, 24 hours, and 30 days. These charts illustrate the total number of objects served from either the cache or from the Web. To review the number of cached objects versus non-cached objects, display the Efficiency tabs.

Note: The maximum number of objects that can be stored in a ProxySG is roughly a million. The number is based on the 4GB RAM on the motherboard and is not user configurable.

To View the Number of Objects Served:

1. Select Statistics>HTTP/FTP History>HTTP/FTP Objects.

The HTTP/FTP Objects tab displays.

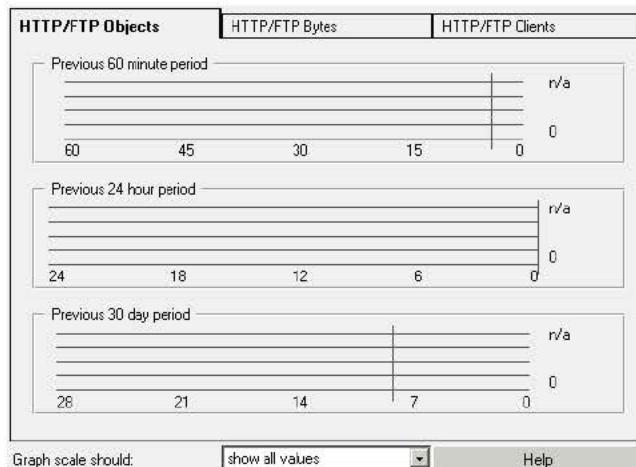


Figure 21-10: HTTP/FTP Objects Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

Viewing the Number of Bytes Served

The Bytes tab shows the sum total of the number of bytes served from the device over the last 60 minutes, 24 hours, and 30 days. The chart shows the total number of bytes for objects served by the device, including both cache hits and cache misses.

To View the Number of Bytes Served:

1. Select Statistics>HTTP/FTP History>HTTP/FTP Bytes.

The HTTP/FTP Bytes tab displays.

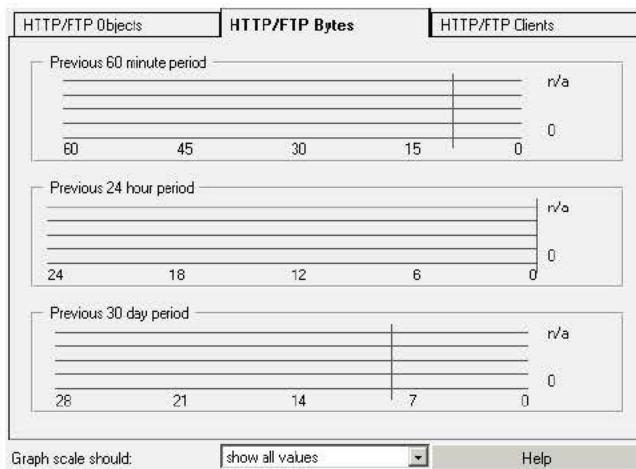


Figure 21-11: HTTP/FTP Bytes Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

Viewing Active Client Connections

The HTTP/FTP Clients tab shows the maximum number of clients with requests processed over the last 60 minutes, 24 hours, and 30 days. This does not include idle client connections (connections that are open but that have not made a request). These charts allow you to monitor the maximum number of active clients accessing the ProxySG at any one time. In conjunction with the HTTP/FTP Objects and HTTP/FTP Bytes tabs, you can determine the number of clients supported based on load, or load requirements for your site based on a specific number of clients.

To View the Number of Active Clients:

1. Select Statistics>HTTP/FTP History>HTTP/FTP Clients.

The HTTP/FTP Clients tab displays.

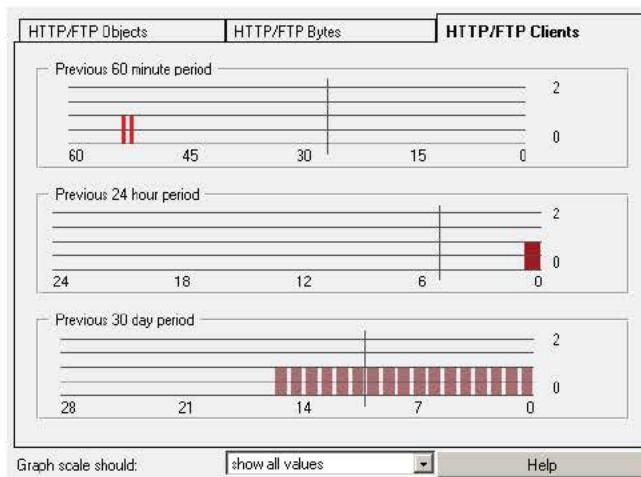


Figure 21-12: HTTP/FTP Clients Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

Streaming History Statistics

The Streaming History tabs (Windows Media, Real Media, QuickTime, Current Streaming Data and Total Streaming Data) display bar graphs that illustrate the number of active client connections over the last 60 minutes, 24 hours, and 30 days, and display real-time values for current connection and live traffic activity on the ProxySG.

The bar graphs in the Streaming History tabs offer the option to show all values in the graph or to clip a percentage of the peak values, which means that a percentage is allowed to fall off the scale. For example, if you select clip 25% of peaks, the top 25% of the values will be allowed to exceed the scale for the graph, showing greater detail for the remaining 75% of the values. The default is show all values, but if you switch one tab to another value, all of the tabs switch to that view.

If you hover your cursor over a particular area of any of the graphs, a figure or set of figures appropriate to that graph will display. An example of this feature is shown in Figure 21-7.

Viewing Windows Media Statistics

The Windows Media tab shows the number of active Windows Media client connections over the last 60 minutes, 24 hours, and 30 days.

To View Windows Media Client Statistics:

1. Select Statistics>Streaming History>Windows Media.

The Windows Media tab displays.

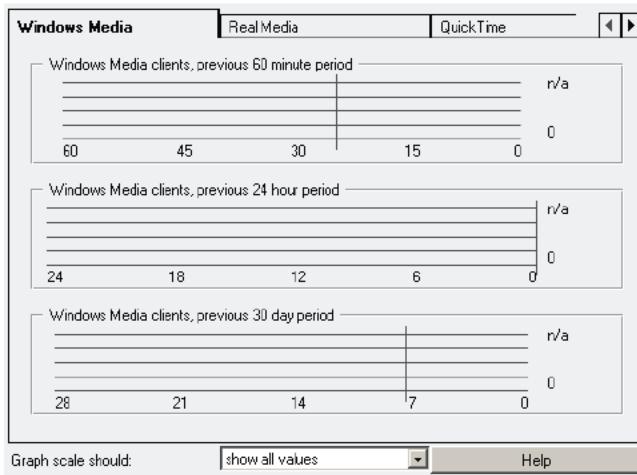


Figure 21-13: Windows Media Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

Viewing Real Media Statistics

The Real Media tab shows the number of active Real Media client connections over the last 60 minutes, 24 hours, and 30 days.

To View Real Media Data Statistics:

1. Select Statistics>Streaming History>Real Media.

The Real Media tab displays.

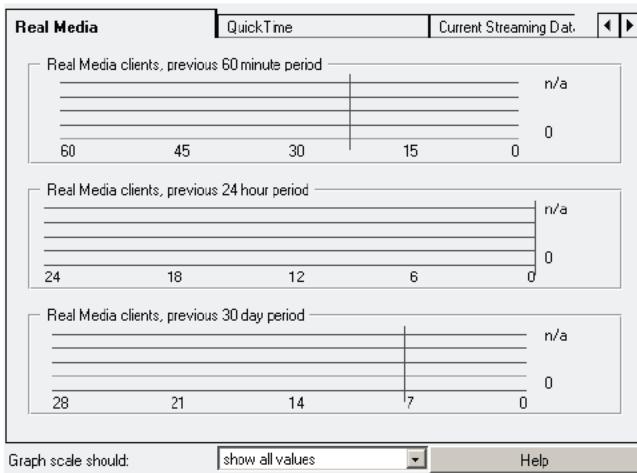


Figure 21-14: Real Media Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

Viewing QuickTime Statistics

The QuickTime tab shows the number of active QuickTime client connections over the last 60 minutes, 24 hours and 30 days.

To View QuickTime Data Statistics:

1. Select Statistics>Streaming History>QuickTime.

The QuickTime tab displays.

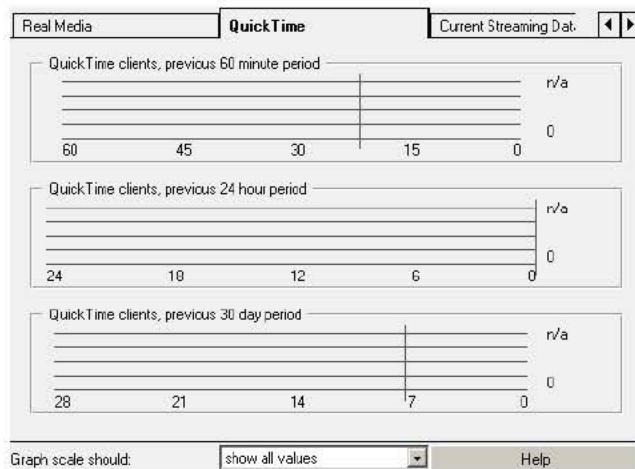


Figure 21-15: QuickTime Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

Viewing Current Streaming Data Statistics

The Current Streaming Data tab shows real-time values for Windows Media, Real Media, and QuickTime activity on the ProxySG.

To View Current Streaming Data Statistics:

1. Select Statistics>Streaming History>Current Streaming Data.

The Current Streaming Data tab displays.

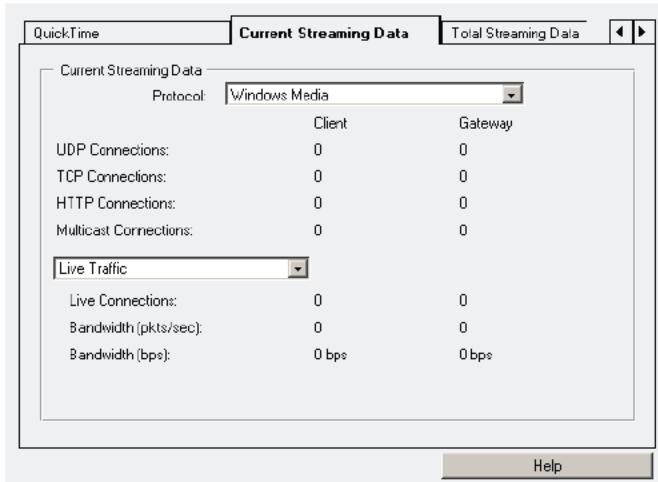


Figure 21-16: Current Streaming Data Tab

2. Select a streaming protocol from the Protocol drop-down list.
3. Select a traffic connection type (Live, On-Demand, or Pass-thru) from the drop-down list.

Viewing Total Streaming Data Statistics

The Total Streaming Data tab shows the total values for Windows Media, Real Media, and QuickTime activity on the ProxySG.

To View Total Streaming Data Statistics:

1. Select Statistics>Streaming History>Total Streaming Data.

The Total Streaming Data tab displays.

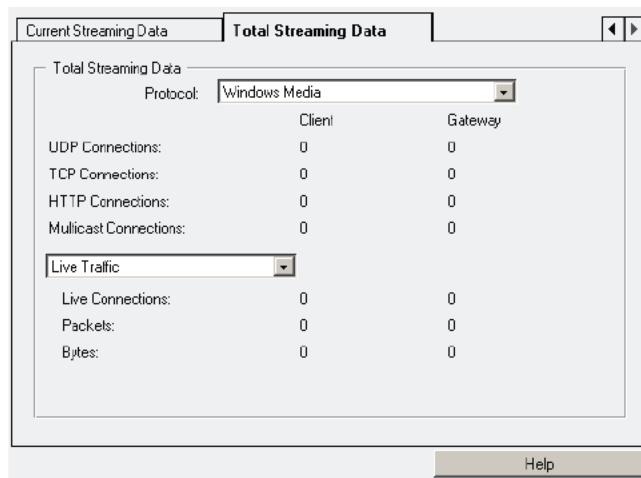


Figure 21-17: Total Streaming Data Tab

2. Select a streaming protocol from the Protocol drop-down list.

3. Select a traffic connection type (Live, On-Demand, or Passthru) from the drop-down list.

SOCKS History Statistics

The SOCKS History tabs (SOCKS Clients, SOCKS Connections, and SOCKS Bytes) displays client data, Connect, Bind, and UPD Associate requests, and client and server UDP and TCP requests.

The bar graphs in the SOCKS History Clients tab offers the option to show all values in the graph or to clip a percentage of the peak values, which means that a percentage is allowed to fall off the scale. For example, if you select clip 25% of peaks, the top 25% of the values will be allowed to exceed the scale for the graph, showing greater detail for the remaining 75% of the values. The default is show all values, but if you switch one tab to another value, all of the tabs switch to that view.

If you hover your cursor over a particular area of any of the graphs, a figure or set of figures appropriate to that graph will display. An example of this feature is shown in Figure 21-7.

Viewing SOCKS Clients

The SOCKS Clients tab displays SOCKS Client data.

To View Socks Client Data:

Select Statistics>SOCKS History>SOCKS Clients.

The SOCKS Clients tab displays.

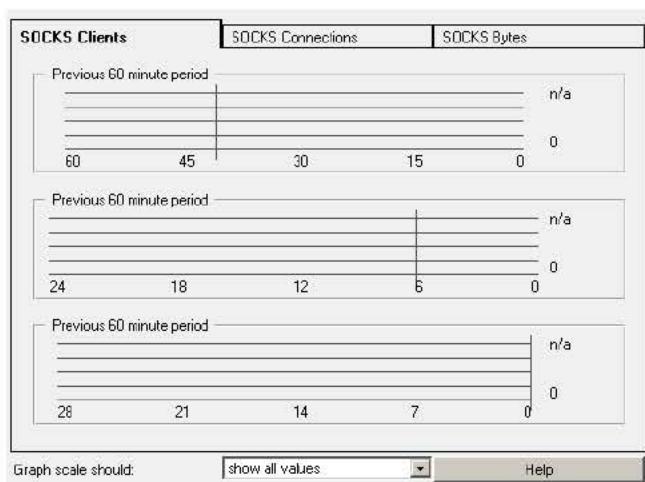


Figure 21-18: SOCKS Client Tab

Viewing SOCKS Connections

The SOCKS Connections tab displays SOCKS Connection data.

To view SOCKS Connection Data:

Select Statistics>SOCKS History>SOCKS Connections.

The SOCKS Connections tab displays.

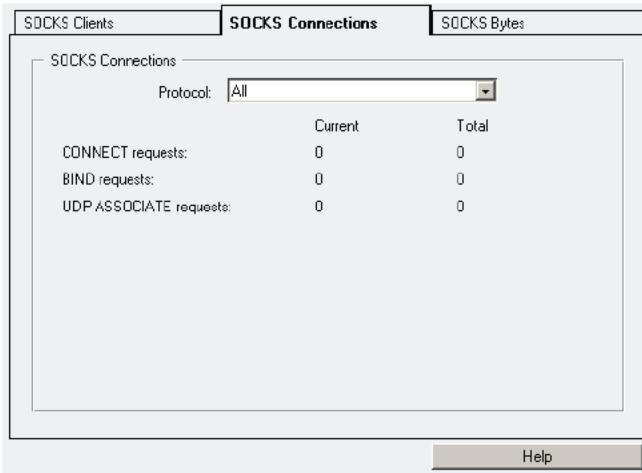


Figure 21-19: SOCKS Connections Tab

Viewing SOCKS Bytes

The SOCKS Bytes tab displays SOCKS Bytes data.

To View SOCKS Bytes Data:

Select Statistics>SOCKS History>SOCKS Bytes.

The SOCKS Bytes tab displays.

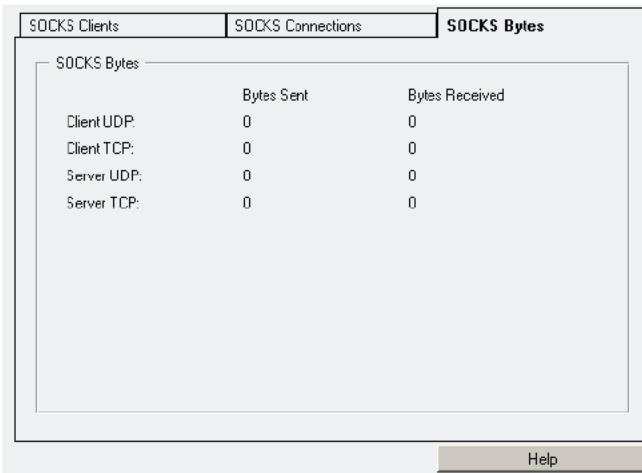


Figure 21-20: SOCKS Bytes Tab

Shell History Statistics

The Shell History tab displays client connections on a per hour, per day, and per month basis.

The bar graphs in the Shell History Clients tab offers the option to show all values in the graph or to clip a percentage of the peak values, which means that a percentage is allowed to fall off the scale. For example, if you select clip 25% of peaks, the top 25% of the values will be allowed to exceed the scale for the graph, showing greater detail for the remaining 75% of the values. The default is show all values, but if you switch one tab to another value, all of the tabs switch to that view.

If you hover your cursor over a particular area of any of the graphs, a figure or set of figures appropriate to that graph will display. An example of this feature is shown in Figure 21-7.

To View Shell History Statistics:

1. Select Statistics>Shell History.

The Shell Clients tab displays.

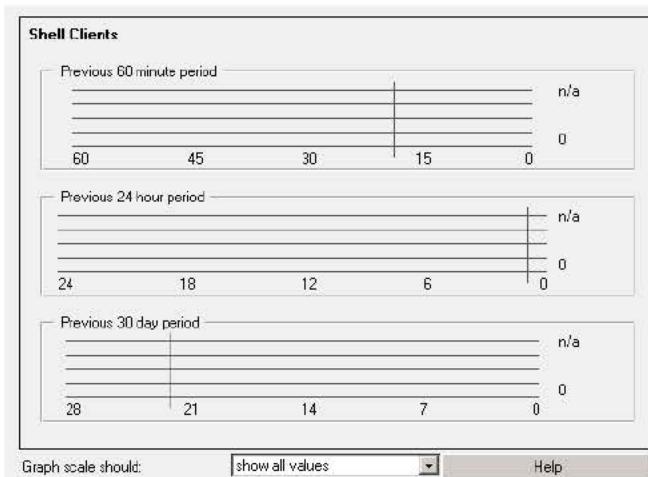


Figure 21-21: Shell Clients History Tab

2. (Optional) To set the graph scale to a different value, select a value from the Graph scale should drop-down list.

Resources Statistics

The Resources tabs (Disk Use, Memory Use, and Data) allow you to view information about how disk space and memory are being used, and how disk and memory space are allocated for cache data.

Viewing Disk Use

The Disk Use tab shows the ProxySG disk usage. The fields on the tab are:

- System Objects—the percentage of storage resources currently used for non-access-log system objects.
- Access log—the percentage of storage resources currently used for the access log.
- Cache in Use—the percentage of non-system, non-access-log resources currently in use for cached objects.

- Cache available—the percentage of non-system, non-access-log resources still available for caching objects.

To View Disk Use:

Select Statistics>Resources>Disk Use.

The Disk Use tab displays.

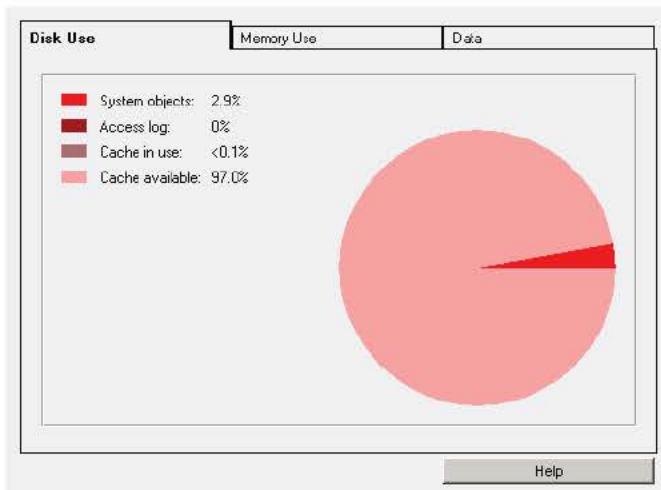


Figure 21-22: Disk Use Tab

Viewing Memory Use

The Memory Use tab shows the amount of memory used for RAM, the ProxySG itself, and for network buffers. The fields on the Memory use tab are:

- RAM Cache—the amount of RAM that is used for caching.
- System allocation—the amount of RAM allocated for the device system.
- Network buffers—the amount of RAM currently allocated for network buffers.

To View Memory Use:

Select Statistics>Resources>Memory Use.

The Memory Use tab displays.

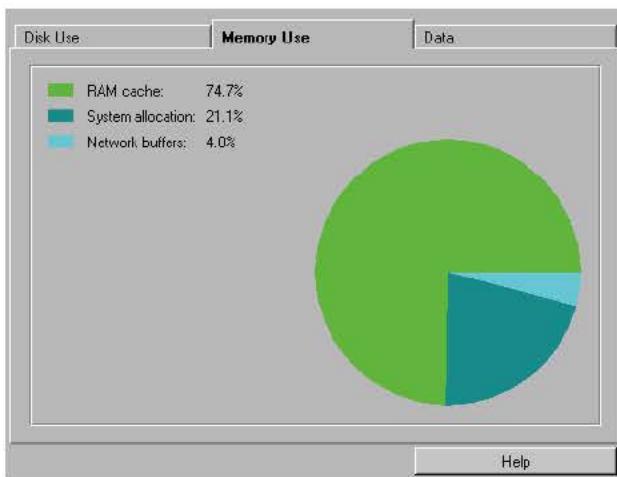


Figure 21-23: Memory Use Tab

Viewing Data Allocation in RAM and on Disk

The Data tab shows the total and available disk space and RAM, and how they are currently allocated. The fields on the Data tab are:

- Maximum objects supported—the maximum number of objects that can be supported.
- Cached objects—the number of objects that are currently cached.
- Disk used by system objects—the amount of disk space used by the system objects.
- Disk used by access log—the amount of disk space used for access logs.
- Total disk installed—the total amount of disk space installed on the device.
- RAM used by cache—the amount of RAM allocated for caching.
- RAM used by system—the amount of RAM allocated for system use.
- RAM used by network—the amount of RAM allocated for network use.
- Total RAM installed—the total amount of RAM installed.

To View Data Allocation:

Select Statistics>Resources>Data.

The Data tab displays.

Disk Use	Memory Use	Data
Maximum objects supported:	1,119,930 objects	
Cached Objects:	0 objects	
Disk used by system objects:	512.63 megabytes	
Disk used by access log:	0 bytes	
Total disk installed:	16.95 gigabytes	
RAM used by cache:	653.83 megabytes	
RAM used by system:	93.28 megabytes	
RAM used by network:	20.88 megabytes	
Total RAM installed:	768 megabytes	

Figure 21-24: Resources Data Tab

Efficiency Statistics

The Efficiency tabs (Summary, Non-cacheable, Access Pattern, and Data) allow you to see information about the flow of both cacheable and non-cacheable data through the ProxySG. You can also see information about how data is being served (such as, RAM, disk, origin).

You can select to view the graphs in either objects or bytes served. Objects served is the default, but if you switch one tab to bytes served, all of the tabs switch to that view.

Viewing the Cache Efficiency Summary

The Summary tab shows the percent of objects served from cache, the percent loaded from the network, and the percent that were non-cacheable. The data dates from the last device reset. The values shown are either objects served or bytes served, based on the Values reflect field at the bottom of the tab. The fields on the Summary tab are:

- **Served from cache**—the percentage of requests the device was able to serve from the cache.
- **Loaded from source**—the percentage of requests the device had to retrieve from the Web and was able to store in the cache.
- **Non-cacheable**—the percentage of requests for non-cacheable objects.

To View the Cache Efficiency Summary:

1. Select Statistics>Efficiency>Summary.

The Summary tab displays.

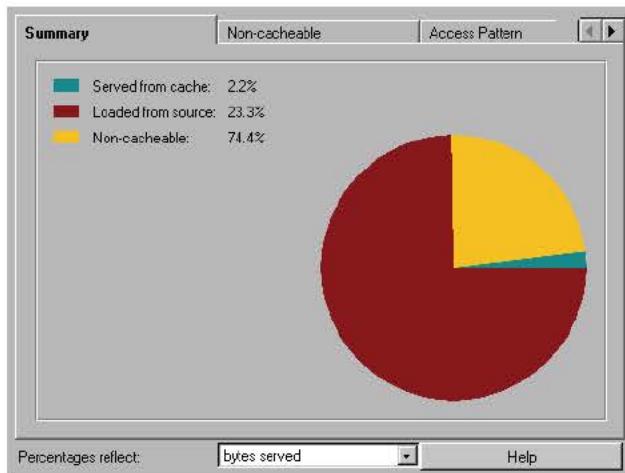


Figure 21-25: Efficiency Summary Tab

2. (Optional) To switch the view between objects served and bytes served, select either **bytes served** or **objects served** from the Percentages reflect drop-down list.

Viewing a Breakdown of Non-Cacheable Data

The Non-cacheable tab shows a breakdown of non-cacheable objects. It shows how many of the various types of non-cacheable requests have been handled. The non-cacheable request types are:

- Pragma no-cache—requests that specify non-cached objects, such as when a user clicks the refresh button in the Web browser.
- Password provided—requests that include a client password.
- Data in request—requests that include additional client data.
- Not a GET request—only the HTTP method Get request can be cached. These are all other methods (PUT, HEAD, POST, DELETE, LINK, and UNLINK).
- Cookie in response—responses that include an HTTP cookie.
- Password required—responses that require a client password.
- Negative response—failed responses, such as when a server or object is not available. This value is zero if the Cache Negative Responses option is enabled.
- Client unique CGI responses—unique responses generated by a CGI application for a specific client.

To View a Breakdown of Non-Cacheable Data:

Select Statistics>Efficiency>Non-cacheable.

The Non-cacheable tab displays.

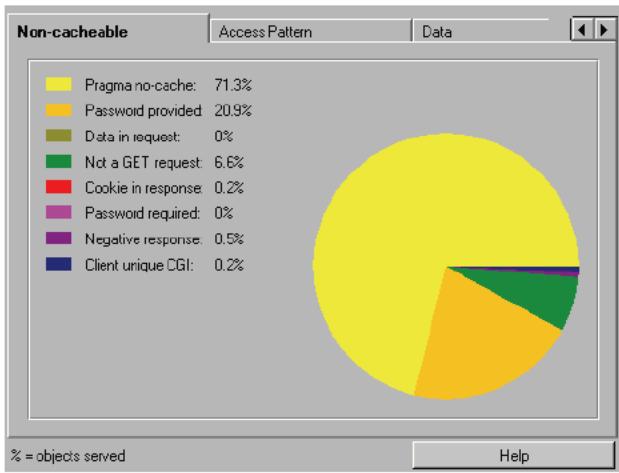


Figure 21-26: Non-Cacheable Tab

Viewing the Cache Data Access Pattern

The Access Pattern tab shows the number of cached requests served from RAM and disk. Cached objects are stored first in RAM. As time passes without additional requests for an object, the object is migrated to disk.

To View the Cache Data Access Pattern:

Select Statistics>Efficiency>Access Pattern.

The Access Pattern tab displays.

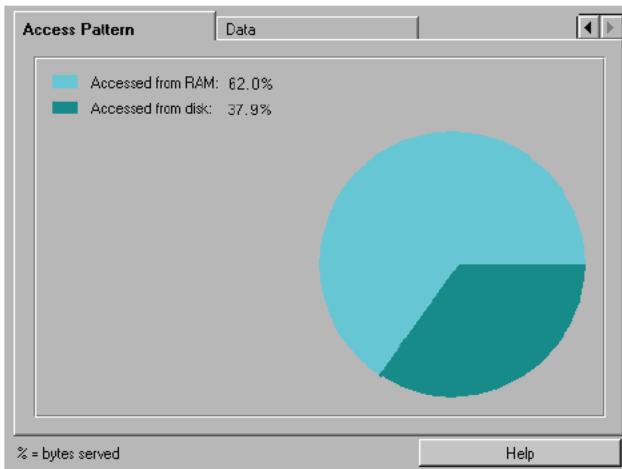


Figure 21-27: Access Pattern Tab

Viewing Totals for Bytes Served

The Data tab lists a breakdown of all requests served. The fields are:

- Served from cache—the number of objects served from the cache.
- Loaded from source—the number of objects that could not be served from the cache and were retrieved from the Web.
- Non-cacheable—the number of objects served that could not be cached.
- Pragma no-cache—requests that specify non-cached objects, such as when a user clicks the refresh button in a Web browser.
- Password provided—requests that include a client password.
- Data in Request—requests that include additional client data.
- Not a GET request—requests that include an invalid HTTP method.
- Cookie in response—responses that include an HTTP cookie.
- Password required—responses that require a client password.
- Negative response—failed responses, such as when a server or object is not available. This information is only displayed if the Cache Negative Responses option is disabled.
- Client unique CGI—responses that contain unique CGI data.
- Accessed from RAM—the total number of bytes served from the RAM cache.
- Accessed from disk—the total number of bytes served from the disk cache.

To View Totals For Bytes Served:

1. Select Statistics>Efficiency>Data.

The Data tab displays.

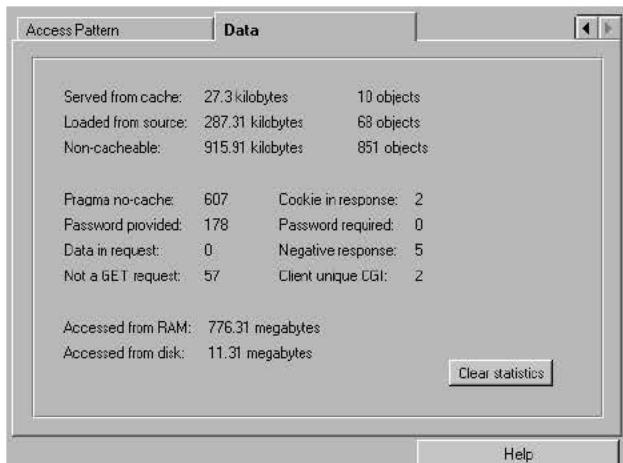


Figure 21-28: Efficiency Data Tab

2. (Optional) To clear all statistics, click the Clear statistics button.

Contents Statistics

The Contents tabs (Distribution and Data) allow you to see information about objects currently stored or served organized by size. The cache contents include all objects currently stored by the ProxySG. The cache contents are not cleared when the ProxySG is powered off.

Viewing Cached Objects by Size

The Distribution tab shows the objects currently stored by the ProxySG, ordered by size.

To View the Distribution of Cache Contents:

Select Statistics>Contents>Distribution.

The Distribution tab displays.

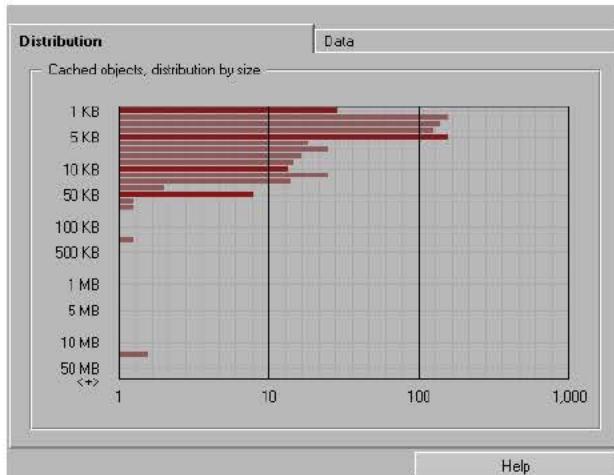


Figure 21-29: Contents Distribution Tab

Viewing the Number of Objects Served by Size

The Data tab displays the number of objects served by the ProxySG, organized by size. This chart shows you how many objects of various sizes have been served.

To View the Number of Objects Served:

Select Statistics>Contents>Data.

The Data tab displays.

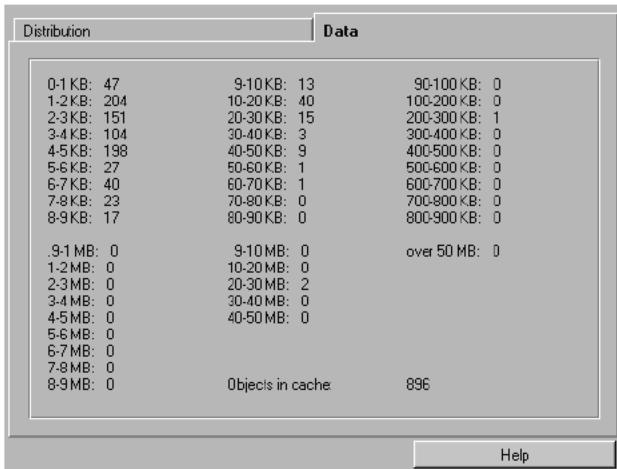


Figure 21-30: Contents Data Tab

Event Logging

Viewing the Event Log

The event log contains all events that have occurred on the ProxySG. Configure the level of detail available by selecting Maintenance>Event Logging>Level (see "Configuring Which Events to Log" on page 699 for details).

To View the Event Log:

1. Select Statistics>Event Logging.

The Event Viewer tab displays.

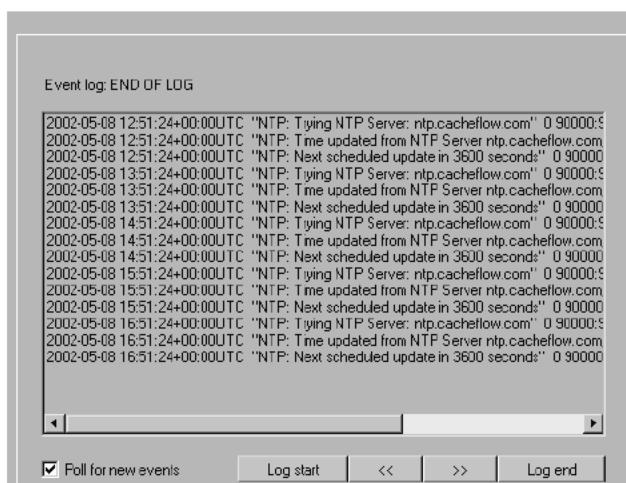


Figure 21-31: Event Viewer

2. Click Log start or Log end or the forward and back arrow buttons to move through the event list.

3. (Optional) Click the Poll for new events checkbox to poll for new events that occurred while the log was being displayed.

Note: The Event Log cannot be cleared.

Failover Statistics

At any time, you can view statistics for any failover group you have configured on your system.

Viewing Failover Status

To View Failover Status:

1. Go to Statistics>Failover.

The Status tab displays.

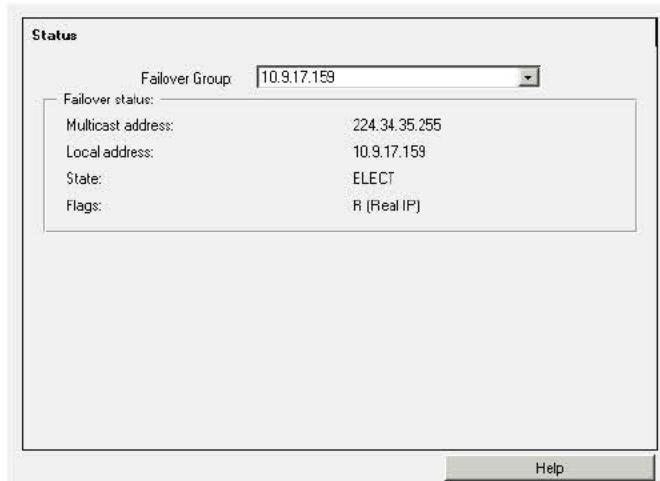


Figure 21-32: Failover Status Tab

2. From the drop-down list, select the group whose statistics you want to view.

The information displayed includes the multicast address, the local address, the state, and any flags, where V indicates the group name is a virtual IP address, R indicates the group name is a physical IP address, and M indicates this machine can be configured to be the master if it is available.

Advanced Statistics

A variety of system statistics are conveniently located in one place and accessible by clicking the links listed in the Advanced tab of the Management Console.

To View System-wide Advanced Statistics:

1. Select Statistics>Advanced.

The Advanced tab displays.



Figure 21-33: Advanced Tab

2. Click the appropriate link for the service you want to view.

A list of categories for that service will appear.

Note: If you upgraded from SGOS 2.x or CacheOS 4.x and have log files generated by those versions, you can view or retrieve them through the Statistics>Advanced>Access Log>Show Old Logs URL.

3. To view the statistics for a particular category, click that category's link.
A window will open detailing the relevant statistics.
4. Close the window when you have finished viewing the statistics.
5. To return to the list of links, either reselect Statistics>Advanced or click your browser's Back button.

Appendix A: Using the Authentication/Authorization Agent

The Blue Coat Systems Authentication and Authorization Agent (BCAAA) allows SGOS 3.x to manage authentication and authorization for NTLM and Netegrity SiteMinder realms.

- NTLM: The BCAA service does not talk directly to an NTLM server. The BCAA service must be installed on a domain controller or member server. The BCAA service authenticates users in all domains trusted by the computer on which it is running.
- SiteMinder: When a SiteMinder realm is referenced in policy, a BCAA process is created. The ProxySG then sends a configuration request that describes the servers to use. The BCAA service logs in to the appropriate servers and determines configuration information to be passed back to the ProxySG (such as the kind of credentials required). Responses from the SiteMinder policy servers are translated into appropriate BCAA protocol responses and returned to the ProxySG.

Important: You must use the 3.2 release of the BCAA service with SGOS 3.2 and higher. You can also use the BCAA service in place of the deprecated CAASNT application for SGOS 2.x and SGOS 3.1.x. You cannot use CAASNT with SGOS 3.2 and higher.

Operating system requirements are:

- NTLM: Windows NT 4 (SP6 or greater and Windows installer 2.0 or greater), Windows 2000 or later. SSL is not supported on Windows NT 4.
- SiteMinder: Windows 2000 or later.

The appendix discusses:

- "Installing the BCAA Service on a Windows or Windows NT System"
- "NTLM and the BCAA Service"
- "SiteMinder and the BCAA Service"
- "Troubleshooting Authentication Agent Problems"
- "Common BCAA Event Messages"

Installing the BCAA Service on a Windows or Windows NT System

All images in this section are from a Windows 2000 system.

Note: If you have an existing CAASNT service on your system, it will be stopped and deleted as part of the BCAA installation procedure.

To Install the Authentication Agent:

1. Download the file from the Blue Coat download site at <https://download.bluecoat.com/>
2. Launch the install wizard.



Figure A-1: BCAA Installation Wizard Launch

3. Click Next to select the destination folder.

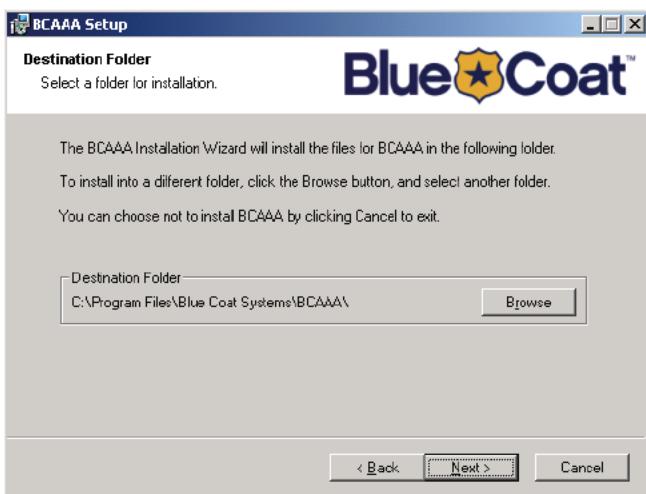


Figure A-2: Destination Folder for BCAA Application

Note: When doing an upgrade from one version of BCAA to another version of BCAA, you must install into the previous BCAA folder to retain your settings. If you install to a different folder, a new .ini file will be created with default settings.

When upgrading from CAASNT to BCAA, the settings from CAASNT are copied to the new installation directory.

4. Click Browse if you want to choose a different destination folder for the BCAA service.
5. Click Next to accept the default and select the port number.

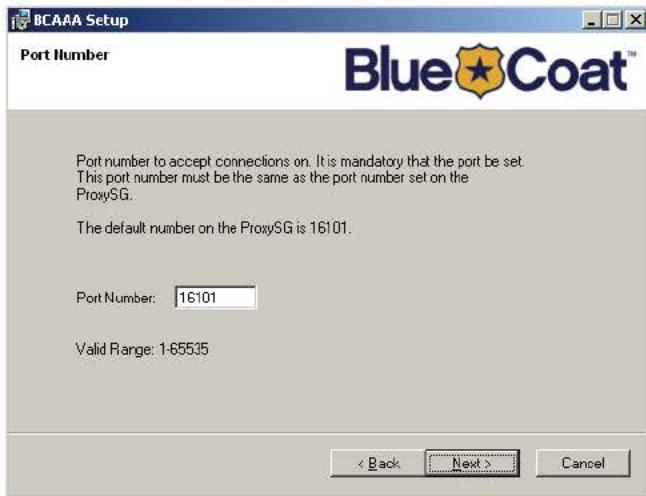


Figure A-3: Selecting BCAA Port Number

6. The port number must match the port number you specify on the ProxySG for the BCAA service. The default is 16101.
7. Click Next to select the number of threads.

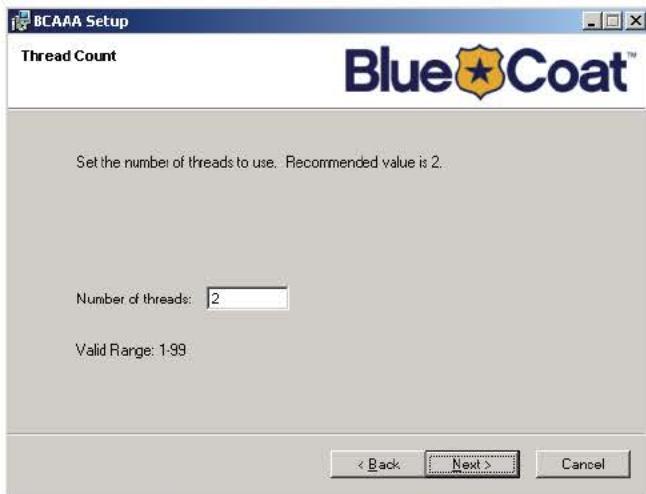


Figure A-4: Thread Count

8. The recommended (and default) value is 2. The maximum number of threads allowed is 99 per ProxySG. After selecting the number, click Next to specify the SSL requirements.

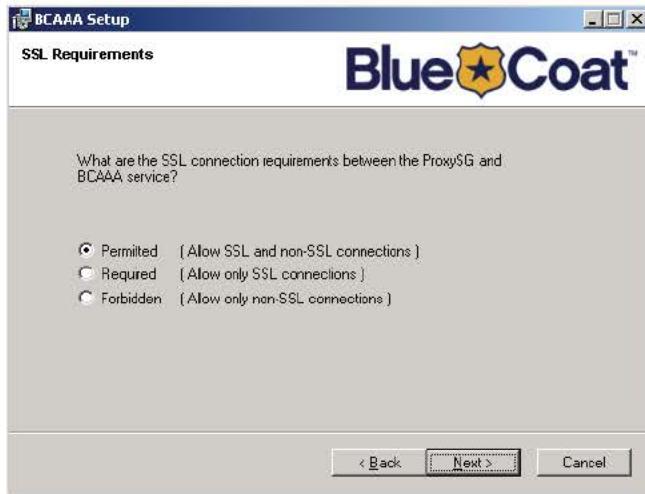


Figure A-5: SSL Requirements

9. The default is that SSL is Permitted, allowing both SSL and non-SSL connections. This setting must be compatible with the setting on the ProxySG.

Note: If you are installing the BCAAA service on an NT4 system, this screen is not available.

10. Click Next to specify the subject of the SSL certificate.

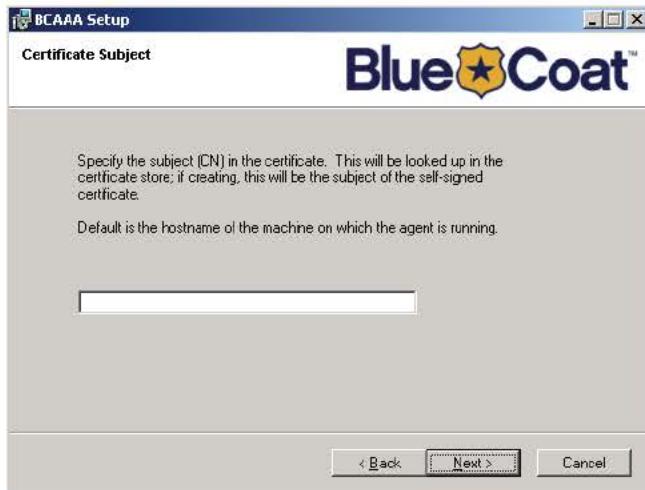


Figure A-6: Specifying the Subject of the Certificate

11. Specify the subject of the certificate.

Note: If you are installing the BCAAA service on an NT4 system, this screen is not available.

The BCAAA service looks up the specified subject in the service's certificate store. If it finds the subject, it uses it instead of generating a new certificate. If not, it generates a self-signed certificate with that subject. This generated certificate can be saved (as specified on the next screen).

12. Click Next to specify save options for the certificate.

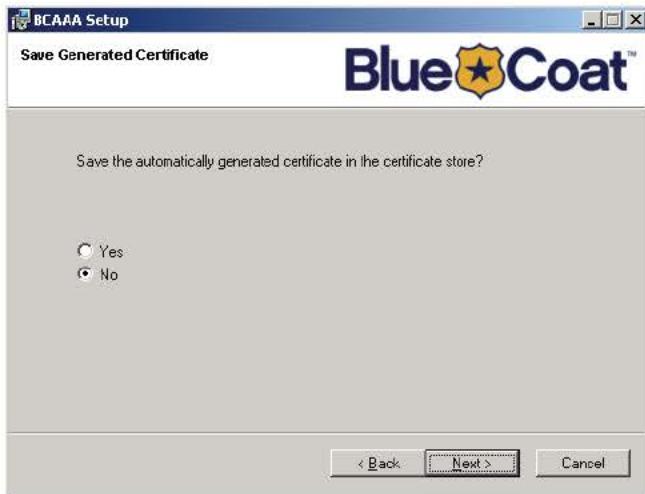


Figure A-7: Saving the Generated Certificate

Note: If you are installing the BCAA service on an NT4 system, this screen is not available.

13. Click Next to specify whether the ProxySG must provide a valid certificate when connecting to the BCAA service.



Figure A-8: Verify ProxySG Certificate

14. To force the ProxySG to provide a valid certificate to connect to the BCAA service, select the Yes radio button. The default is No.

Note: If you are installing the BCAA service on an NT4 system, this screen is not available.

15. Click Next to view the summary of the changes you made.



Figure A-9: BCAA Summary

16. Click **Install** to install the BCAA service using the settings you configured.

When installation completes, the final BCAA screen displays.



Figure A-10: Completing BCAA Installation

To Modify Settings or Uninstall the Authentication Agent:

1. Launch the install wizard.

The Application Maintenance page displays.



Figure A-11: Applications Maintenance Page

2. Click **Modify** to re-enter the installation wizard; click **Remove** to uninstall the BCAA service from the system

Note: For instructions on using the installation wizard, see "Installing the BCAA Service on a Windows or Windows NT System" on page 737.



Figure A-12: Uninstalling the BCAA Service

3. Click **Next** to start the procedure.
4. Click **Finish** to exit the uninstall application.

To View the Application Event Log:

The BCAA service logs all errors to the Windows 2000 Application Event Log under the name BCAA.

1. Launch the Event Log.
2. Doubleclick the information message BCAA service to see that the BCAA service has been automatically started.

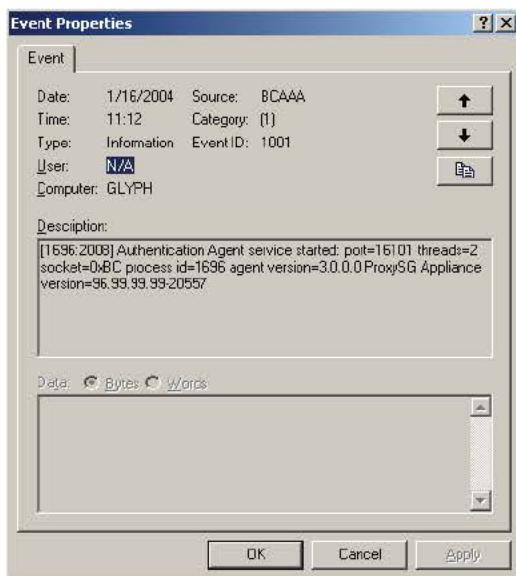


Figure A-13: BCAA Information Message

To View the BCAA Service:

The BCAA service logs all errors to the Windows 2000 Application Event Log under the name BCAA.

1. Launch the Event Viewer.
2. Right-click on BCAA and select Properties to manage the service. For example, to make the BCAA service start only manually, set the Startup Type to Manual. (Automatic is the default setting.)

NTLM and the BCAA Service

The BCAA service acts as an agent allowing the ProxySG to access Windows NT Lan Manager (NTLM) domain controllers. A single installation of the BCAA service can support multiple ProxySG appliances.

Note: SSL is not supported on Windows NT 4.

SiteMinder and the BCAA Service

Before you can use the BCAA service with SiteMinder, you must configure the SiteMinder realm to work with SiteMinder. The realm can be configured from the SiteMinder configuration tabs in the Management Console or from the CLI.

For specific information about configuring the SiteMinder realm to work with the Netegrity policy servers, see "Section G: Netegrity SiteMinder" on page 290 in Chapter 9: "Using Authentication Services".

Troubleshooting Authentication Agent Problems

This section describes some common problems you might encounter when setting up or using the BCAA service on a Windows platform.

To troubleshoot the BCAA service, launch the event viewer.

The Properties pane displays, providing information about the status of the BCAA service at that time. What's of most interest to you is the Type and the Event ID. The description below the Type/Event ID lists the problem. You can often find more information about the problem and suggestions for its solution in "Common BCAA Event Messages" on page 745.

Common problems:

- If an attempt to start the BCAA service is issued when BCAA is already started, the following error message displays:

The requested service has already been started.

- If another application is using the same port number as the BCAA service, the following messages are displayed:

The BCAA service could not be started.

A system error has occurred.

System error 10048 has occurred.

Only one usage of each socket address (protocol/network address/port) is normally permitted.

Common BCAA Event Messages

Following are the most common event messages that can be logged to the Windows 2000 Application Event Log. Most of the event messages not listed here are error status messages returned by Win32 function calls. When a Win32 call fails, the error code and error text containing the reason for the error displays in the event log under the name BCAA.

To View the BCAA Event Log:

1. Right click on My Computer and select Manage.
The Computer Management window displays.
2. Select System Tools>Event Viewer>Application.

Note: When running under Windows NT4, the error text is unavailable for some error codes. In these cases, only the error code displays. This limitation does not apply to Windows 2000.

For each BCAA event message, the event message is displayed along with the event number.

Table A.1: BCAA Event Messages

Message ID	Message	Description
200	Various messages	The associated message provides information about a condition that is not an error.
300	Various messages	The associated message warns about an unexpected condition that does not prevent operation.
400	Various messages	The associated message describes an error condition that prevents normal operation.
1001	Authentication Agent service started: port=# threads=# socket=0x# process id=# agent version=# ProxySG Appliance version=#	This indicates successful startup and provides information about the agent.
1002	Authentication Agent stopped	This indicates normal shutdown of the service.
1003	ProxySG Appliance (a.b.c.d) connected; Process # spawned as #	This indicates a ProxySG has connected to the agent (Windows only).
1004	ProxySG Appliance agent process exited (normal logout)	This indicates normal logout by a ProxySG.
1005	Process %d has terminated, ExitCode=0x#, link=0x#	This indicates an unexpected termination of an agent process (Windows only).
1006	Service dispatcher exited.	This indicates an unexpected termination of the service dispatcher.
1007	CreateNamedPipe failed, pipe='%'	The agent dispatcher could not create the named pipe for the reason given.
1008	ConnectNamedPipe failed, pipe='%'	The agent process could not obtain the information from the dispatcher on the named pipe for the reason given.
1009	WriteFile failed, pipe='%'	The dispatcher could not write information to the named pipe for the reason given.
1011	CreateThread (ProcessTimerThread) failed	The dispatcher could not create its timer thread.
1012	Failed to create ProxySG Appliance process '%'	The dispatcher could not create an agent process.
1015	Various	Too many groups were configured in policy on the ProxySG, or the total length of the group names was too long.
1019	Various	The dispatcher was unable to determine the exit status of an agent process.
1020	Terminating ProxySG Appliance process #, ProcNum=# Handle=0x#	An agent process was active when the Windows service was shut down.
1022	Various	The associated message reports the status of a ProxySG login attempt.
1101	BasicAuth: CloseHandle failed; user 'xx\\xx'	The agent was unable to close the login handle for the specified user.
1102	Username: '%s\\%s' too long	The ProxySG offered the specified username, which is too long.

Table A.1: BCAA Event Messages (Continued)

Message ID	Message	Description
1106	Various	An attempted authentication using BASIC credentials failed for the reason given.
1107	User Right 'Act as part of the operating system' required for Basic Authentication	The agent does not have the necessary privileges to do BASIC authentication
1108	Various	The agent was unable to determine information about the user for the reason given.
1202	Unable to create GroupsOfInterest mutex 'xx' - already exists	The agent could not create the Windows mutex needed for group authorization checks because it already exists.
1203	Unable to create GroupsOfInterest mutex 'xx'	The agent could not create the Windows mutex needed for group authorization checks.
1204	OpenMutex failed for AuthGroups mutex '%s', group='%'s'	The agent was unable to open the Windows mutex needed for group authorization checks.
1205	Various	The agent was unable to close the Windows mutex named for the reason given.
1207	GetAclInformation failed	The agent was unable to obtain ACL information needed to do group authorization checks.
1209	GetKernelObjectSecurity failed for AuthGroup='%'s'	The agent was unable to obtain security information about the specified group.
1210	SetKernelObjectSecurity failed	The agent was unable to set up security information for the reason specified.
1211	InitializeSecurityDescriptor failed	The agent was unable to initialize the security descriptor for the reason specified.
1212	GetSecurityDescriptorDacl failed	The agent was unable to get the discretionary access control list (DACL) for the reason specified.
1213	SetSecurityDescriptorDacl failed	The agent was unable to set the discretionary access control list (DACL) for the reason specified.
1214	InitializeAcl failed	The agent was unable to initialize the access control list (ACL) for the reason specified.
1215	GetUserName failed for AuthGroup='%'s'	The agent was unable to determine the username while processing the specified group.
1217	GetAce failed for AuthGroup='%'s'	The agent was unable to get the access control entry (ACE) for the specified group.
1218	AddAce failed	The agent was unable to add the necessary access control entry (ACE) for the reason specified.
1219	AddAccessAllowedAce failed	The agent was unable to add the necessary "access allowed" access control entry (ACE).
1220	Could not establish groups-of-interest: result=0x##	The agent was unable to initialize groups-of-interest checking.
1221	AuthGroup '%s' does not exist	The specified group does not exist.
1222	NTLM RevertSecurityContext failed, user='%'s'	The agent could not revert the security context for the specified user.
1223	BASIC: RevertToSelf failed, user='%'s'	The agent could not revert the security context for the specified user.

Table A.1: BCAA Event Messages (Continued)

Message ID	Message	Description
1224	Error calling OpenProcessToken	The agent's call to OpenProcessToken failed for the specified reason.
1225	Error calling LookupPrivilegeValue	The agent could not get information about a needed privilege.
1226	Error calling AdjustTokenPrivileges	The agent could not adjust its privileges as required.
1227	ImpersonateLoggedOnUser failed; Group access denied for user '%s'	The agent could not impersonate the specified user.
1228	NTLM: ImpersonateSecurityContext failed; Group access denied for user '%s'	The agent could not impersonate the specified user.
1301	NOTE: Pending ContextLink=### timed out; deleting SecurityContext h=## TS=## now=##	The ProxySG did not provide a response to a challenge quickly enough.
1302	Various	An authentication request from a ProxySG referenced an in-progress request that has timed out or does not exist.
1304	Various	The agent was unable to delete a security context for the reason given.
1305	AcceptSecurityContext failure, SEC_E_INVALID_HANDLE, ContextLink=### count=#	The agent was provided with an invalid context handle.
1306	Various	The client provided an invalid token to the authentication system.
1308	AcceptSecurityContext failure, ContextLink=# count=#, detail=#(xxx)	Windows rejected the authentication attempt for the reason given.
1310	Various	This records the failure of NTLM authentication or group authorization.
1311	3:Failed NTLM Authentication for user: '%s'	This records the failure of NTLM authentication; the user name was supplied by the client.
1312	Various	The agent could not determine the username from the NTLM type 3 message supplied by the client.
1313	Invalid Type3 message	The client provided an NTLM type 3 message that was invalid.
1314	BASE64_Decode: Length of token exceeds max (%d)	The client provided an NTLM token that was too long.
1316	Unsupported version in request: %d(0x% <i>x</i>)	The ProxySG sent a request with an unsupported version number.
1401	Various	The agent lost communication with the ProxySG.
1403	Various	The agent is aborting for the reason given.
1402	Unexpected thread 0 exit	The agent exited unexpectedly.
1404	Unable to get ProcessInfo from parent process.	The agent could not obtain its information from the dispatcher.
1405	CreateFile failed, pipe='xx'	The agent could not create a handle for the dispatcher's named pipe.
1406	WaitNamedPipe failed, pipe='%'s'	The agent could not wait for the dispatcher's named pipe.

Table A.1: BCAA Event Messages (Continued)

Message ID	Message	Description
1407	ReadFile failed, pipe='%s'	The agent could not read information from the dispatcher's named pipe.
1409	Various	The agent could not create the specified thread for the reason given.
1412	Various	The agent could not create a required Windows event object.
1413	AuthMethod 'xcs' not supported: returning _AuthResult=0x##	The ProxySG requested an unsupported authentication mechanism.
1414	Various	The specified request is unsupported.
1500	Various	The agent has a problem with memory allocation; typically this means there is not enough memory.
1501	Unable to allocate memory for ProcLink buffer.	The agent could not allocate some needed memory.
1502	Unable to allocate memory for ContextLink buffer.	The agent could not allocate some needed memory.
1503	Various	The agent was unable to allocate needed memory.
1604	Service dispatch failed	The Windows service dispatcher failed to start.
1605	RegisterServiceCtrlHandler failed	The agent dispatcher was unable to register the service control handler.
1608	SetServiceStatus failed, g_StatusHandle=%d	The agent was unable to set the service's status.
1610	Unsupported service control code: #	Windows sent a service control code that the agent does not support.
1701	WSASocket failed	The agent could not create a Windows socket for the reason given.
1702	WSAStartup failed.	The agent could not start the Windows socket for the reason given.
1703	Various	The agent could not send data to the ProxySG for the reason given.
1704	Various	The agent could not receive data from the ProxySG for the reason given.
1705	accept failed	The agent dispatcher could not initialize to accept new connections.
1706	bind failed, PortNumber=#	The agent dispatcher could not bind to the specified port.
1707	listen failed.	The agent dispatcher could not listen for new connections.
1708	Various	Windows reported an event wait failure to the agent while doing I/O on the socket.
1709	The agent is already running or the agent's port # is in use by another process	Some other process is already using the port needed by the agent.
1710	WSARecv failed reading bytes from socket	Windows reported an error when the agent tried to receive bytes from the ProxySG.

Table A.1: BCAA Event Messages (Continued)

Message ID	Message	Description
1711	WSASend failed sending bytes to socket.	Windows reported an error when the agent tried to send bytes to the ProxySG.
1712	Various	A socket I/O operation did not complete successfully.
1801	Error calling AcquireCredentialsHandle	The agent could not acquire its credentials from Windows.
1803	Various	The agent could not load a needed library (DLL).
1804	Various	The agent could not locate the needed services in a library (DLL).
1805	Unsupported SSPI Windows platform; PlatformId=#	The reported Windows platform is not supported for NTLM authentication.
1806	Error calling QueryContextAttributes	The agent could not determine the authenticated user's security attributes.
1807	QuerySecurityPackageInfo failed	The agent could not get needed security information from Windows.
1808	Max Token size too long (#); max size is #	The client supplied an NTLM token that is too long.
1809	FreeContextBuffer failed	An attempt to free the NTLM context buffer failed.
1811	Username 'x\\y' too long	The reported user name is too long.
1901	Admin Services Error: Access denied to domain/user/group information	The agent was unable to access necessary information.
1902	Admin Services Error: Invalid computer from which to fetch information	The computer to be used to get security information is invalid.
1903	Admin Services Error: Group not found	The requested group could not be found.
1904	Various	The reported error was encountered while browsing.
1905	Admin services error: could not translate context to Unicode	The requested object for browsing could not be translated to Unicode
1906	Admin service out of memory	The browsing service ran out of memory.
1907	Search request object too long: # > #	The requested object for browsing is too long.
2000	AcquireCredentialsHandle failed: 0x#	The agent could not acquire the credentials needed for an SSL session.
2001	Various	The agent was unable to negotiate an SSL session for the reason given.
2002	Various	An I/O error occurred during an SSL session .
2003	Various	The specified cryptographic error occurred during an SSL session.
2004	Various	The specified problem occurred with a certificate during SSL negotiation.

Appendix B: Access Log Formats

The ProxySG can create access logs in one of the following formats:

- "Custom or W3C ELFF Format"
 - "SQUID-Compatible Format"
 - "NCSA Common Access Log Format"

ELFF is a log format defined by the W3C that contains information about Windows Media and RealProxy logs.

The ProxySG can create access logs with any one of six formats. Four of the six are reserved formats and cannot be configured. However, you can create additional logs using custom or ELFF format strings.

When using an ELFF or custom format, a blank field is represented by a dash character. When using the SQUID or NCSA log format, a blank field is represented according to the standard of the format.

Custom or W3C ELFF Format

The W3C Extended Log File Format (ELFF) is a subset of the Blue Coat Systems format. The ELFF format is specified as a series of space delimited fields. Each field is described using a text string. The types of fields are described in Table B.1.

Table B.1: Field Types

Field type	Description								
Identifier	A type unrelated to a specific party, such as date and time.								
prefix-identifier	Describes information related to a party or a transfer, such as c-ip (client's IP) or sc-bytes (how many bytes were sent from the server to the client)								
prefix (header)	<p>Describes a header data field. The valid prefixes are:</p> <table> <tbody> <tr> <td>c = Client</td> <td>cs = Client to Server</td> </tr> <tr> <td>s = Server</td> <td>sc = Server to Client</td> </tr> <tr> <td>r = Remote</td> <td>rs = Remote to Server</td> </tr> <tr> <td>sr = Server to Remote</td> <td></td> </tr> </tbody> </table>	c = Client	cs = Client to Server	s = Server	sc = Server to Client	r = Remote	rs = Remote to Server	sr = Server to Remote	
c = Client	cs = Client to Server								
s = Server	sc = Server to Client								
r = Remote	rs = Remote to Server								
sr = Server to Remote									

ELFF formats are created by selecting a corresponding custom log format using the table below. Note that ELFF does not support character strings and require a space between fields, unlike the Blue Coat custom format.

Selecting the ELFF format does the following:

- Puts one or more W3C headers into the log file. Each header contains the following lines:

```
#Software: SGOS x.x.x  
#Version: 1.0  
#Date: 2002-06-06 12:12:34  
#Fields:date time cs-ip...
```

- Changes all spaces within fields to + or %20. The ELFF standard requires that spaces only be present between fields.

ELFF formats are described in Table B.2.

Table B.2: Blue Coat Custom Format and Extended Log File Format

Blue Coat Custom Format	Extended Log File Format	Description
space character	N/A	Multiple consecutive spaces are compressed to a single space.
%	-	Denotes an expansion field.
%%	-	Denotes '%' character.
%a	c-ip	IP address of the client.
%b	sc-bytes	Number of bytes sent from appliance to client.
%c	rs(Content-Type)	Response header: Content-Type
%d	s-supplier-name	Hostname of the upstream host (not available for a cache hit).
%e	time-taken	Time taken (in milliseconds) to process the request.
%f	sc-filter-category	Content filtering category of the request URL.
%g	timestamp	UNIX type timestamp.
%h	c-dns	Hostname of the client (uses the client's IP address to avoid reverse DNS).
%i	cs-uri	The 'log' URL.
%j	-	[Not used.]
%k	-	[Not used.]
%l	x-bluecoat-special-empty	Resolves to an empty string.
%m	cs-method	Request method used from client to appliance.
%n	-	[Not used.]
%o	-	[Not used.]
%p	r-port	Port from the outbound server URL.
%q	-	[Not used.]
%r	cs-request-line	First line of the client's request.
%s	sc-status	Protocol status code from appliance to client.
%t	gmftime	GMT date and time of the user request in format: [DD/MM/YYYY:HH:MM:SS GMT]
%u	cs-user	Qualified username for NTLM. Relative username for other protocols.
%v	cs-host	Hostname from the client's request URL. If URL rewrite policies are used, this field's value is derived from the 'log' URL.
%w	s-action	What type of action did the appliance take to process this request.
%x	date	GMT Date in YYYY-MM-DD format.
%y	time	GMT time in HH:MM:SS format.
%z	s-icap-status	ICAP response status.

Table B.2: Blue Coat Custom Format and Extended Log File Format (Continued)

Blue Coat Custom Format	Extended Log File Format	Description
%A	cs (User-Agent)	Request header: User-Agent.
%B	cs-bytes	Number of bytes sent from client to appliance.
%C	cs (Cookie)	Request header: Cookie.
%D	s-supplier-ip	IP address used to contact the upstream host (not available for a cache hit).
%E	-	[Not used.]
%F	-	[Not used.]
%G	-	[Not used.]
%H	s-hierarchy	How and where the object was retrieved in the cache hierarchy.
%I	s-ip	IP address of the appliance on which the client established its connection.
%J	-	[Not used.]
%K	-	[Not used.]
%L	localtime	Local date and time of the user request in format: [DD/MMM/YYYY:hh:mm:ss +nnnn]
%M	-	[Not used.]
%N	s-computername	Configured name of the appliance.
%O	-	[Not used.]
%P	s-port	Port of the appliance on which the client established its connection.
%Q	cs-uri-query	Query from the 'log' URL.
%R	cs (Referer)	Request header: Referer.
%S	s-sitename	Service used to process the transaction.
%T	duration	Time taken (in seconds) to process the request.
%U	cs-uri-path	Path from the 'log' URL. Does not include query.
%V	cs-version	Protocol and version from the client's request, e.g. HTTP/1.1.
%W	sc-filter-result	Content filtering result: Denied, Proxied or Observed.
%X	cs (X-Forwarded-For)	Request header: X-Forwarded-For.
%Y	-	[Not used.]
%Z	s-icap-info	ICAP response information.

Example Access Log Formats

Squid log format: %g %e %a %w/%s %b %m %i %u %H/%d %c

NCSA common log format: %h %l %u %t "%r" %s %b

NCSA extended log format: %h %l %u %L "%r" %s %b "%R" "%A"

Microsoft IIS format: %a, -, %x, %y, %s, %N, %I, %e, %b, %B, %s, 0, %m, %U, -

The Blue Coat custom format allows any combination of characters and format fields. Multiple spaces are compressed to a single space in the actual access log. You can also enter a string, such as My default is %d. The ProxySG goes through such strings and finds the relevant information. In this case, that information is %d.

SQUID-Compatible Format

The SQUID-compatible format contains one line for each request. For SQUID-1.1, the format is:

```
time elapsed remotehost code/status bytes method URL rfc931 peerstatus/peerhost
type
```

For SQUID-2, the columns stay the same, though the content within may change a little.

Action Field Values

Table B.3 describes the possible values for the action field.

Table B.3: Action Field Values

Value	Description
ACCELERATED	(SOCKS only) The request was handed to the appropriate protocol agent for handling.
ALLOWED	An FTP method (other than the data transfer method) is successful.
DENIED	Policy denies a method.
FAILED	An error or failure occurred.
LICENSE_EXPIRED	(SOCKS only) The request could not be handled because the associated license has expired.
TUNNELED	Successful data transfer operation.
TCP_	Refers to requests on the HTTP port.
TCP_AUTH_HIT	The requested object requires upstream authentication, and was served from the cache.
TCP_AUTH_MISS	The requested object requires upstream authentication, and was not served from the cache. This is part of CAD (Cached Authenticated Data).
TCP_AUTH_REDIRECT	The client was redirected to another URL for authentication.
TCP_CLIENT_REFRESH	The client forces a revalidation with the origin server with a Pragma: no-cache. If the server returns 304 Not Modified, this appears in the Statistics:Efficiency file as In Cache, verified Fresh.
TCP_DENIED	Access to the requested object was denied by a filter.
TCP_ERR_MISS	An error occurred while retrieving the object from the origin server.
TCP_HIT	A valid copy of the requested object was in the cache.
TCP_LOOP	The current connection is dropped because the upstream connection would result in a looped connection.
TCP_MEM_HIT	The requested object was, in its entirety, in RAM.
TCP_MISS	The requested object was not in the cache.
TCP_NC_MISS	The object returned from the origin server was non-cacheable.
TCP_PARTIAL_MISS	The object is in the cache, but retrieval from the origin server is in progress.
TCP_POLICY_REDIRECT	The client was redirected to another URL due to policy.

Table B.3: Action Field Values (Continued)

Value	Description
TCP_REFRESH_HIT	A GIMS request to the server was forced and the response was 304 Not Modified, this appears in the Statistics:Efficiency file as In Cache, verified Fresh.
TCP_REFRESH_MISS	A GIMS request to the server was forced and new content was returned.
TCP_RESCAN_HIT	The requested object was found in the cache but was rescanned because the virus-scanner-tag-id in the object was different from the current scanner tag.
TCP_SPLASHED	The user was redirected to a splash page.
TCP_SWAPFAIL	The object was believed to be in the cache, but could not be accessed.
TCP_TUNNELED	The CONNECT method was used to tunnel this request (generally proxied HTTPS).
UDP_	Refers to requests on the ICP port (3130).
UDP_DENIED	Access was denied for this request.
UDP_HIT	A valid copy of the requested object was in the cache. This value is also used with ICP queries.
UDP_INVALID	The ICP request was corrupt, short, or otherwise unintelligible.
UDP_MISS	The requested object was not in the cache. This value is also used with ICP queries.
UDP_MISS_NOFETCH	An ICP request was made to this cache for an object not in the cache. The requestor was informed that it could not use this cache as a parent to retrieve the object. (This is not supported at this time.)
UDP_OBJ	An ICP request was made to this cache for an object that was in cache, and the object was returned through UDP. (This is not supported at this time. This functionality is deprecated in the current ICP specification.)

NCSA Common Access Log Format

The common log format contains one line for each request. The format of each log entry is shown below:

```
remotehost rfc931 authuser [date] "request" status bytes
```

Each field is described in Table B.4.

Table B.4: Common Log Format Entries

Field Name	Description
remotehost	DNS hostname or IP address of remote server.
rfc931	The remote log name of the user. This field is always —.
authuser	The username as which the user has authenticated himself.
[date]	Date and time of the request.
"request"	The request line exactly as it came from the client.
status	The HTTP status code returned to the client.
bytes	The content length of the document transferred.

Access Log Filename Formats

Table B.5 details the specifiers for the access log upload filenames.

Table B.5: Specifiers for the Access Log Upload Filenames

Specifier	Description
%%	Percent sign.
%a	Abbreviated weekday name.
%A	Full weekday name.
%b	Abbreviated month name.
%B	Full month name.
%c	The certificate name used for encrypting the log file (expands to nothing in non-encrypted case).
%C	The ProxySG name.
%d	Day of month as decimal number (01 – 31).
%f	The log name.
%H	Hour in 24-hour format (00 – 23).
%i	First IP address of the ProxySG, displayed in x_x_x_x format, with leading zeros removed.
%I	Hour in 12-hour format (01 – 12).
%j	Day of year as decimal number (001 – 366).
%l	The fourth part of the ProxySG's IP address, using three digits (001.002.003.004)
%m	Month as decimal number (01 – 12).
%M	Minute as decimal number (00 – 59).
%p	Current locale's A.M./P.M. indicator for 12-hour clock.
%S	Second as decimal number (00 – 59).
%U	Week of year as decimal number, with Sunday as first day of week (00 – 53).
%w	Weekday as decimal number (0 – 6; Sunday is 0).
%W	Week of year as decimal number, with Monday as first day of week (00 – 53).
%y	Year without century, as decimal number (00 – 99).
%Y	Year with century, as decimal number.
%z, %Z	Time-zone name or abbreviation; no characters if time zone is unknown.

Fields Available for Creating Access Log Formats

The following table lists all fields available for creating access log formats. When creating an ELFF format, you must use the values from the ELFF column. When creating a custom format, you can use values from the ELFF, CPL, or custom column.

The available format fields are organized in the following categories:

- bytes
- connection
- dns
- packets
- req_rsp_line
- streaming
- time
- instant messaging (im)
- url
- user

- special_token
- status
- ci_request_header
- si_response_header

Table B.6: Access Log Format Fields

Category: bytes			
ELFF	CPL	Custom	Description
cs-bodylength			Number of bytes in the body (excludes header) sent from client to appliance
cs-bytes		%B	Number of bytes sent from client to appliance
cs-headerlength			Number of bytes in the header sent from client to appliance
rs-bodylength			Number of bytes in the body (excludes header) sent from upstream host to appliance
rs-bytes			Number of bytes sent from upstream host to appliance
rs-headerlength			Number of bytes in the header sent from upstream host to appliance
sc-bodylength			Number of bytes in the body (excludes header) sent from appliance to client
sc-bytes		%b	Number of bytes sent from appliance to client
sc-headerlength			Number of bytes in the header sent from appliance to client
sr-bodylength			Number of bytes in the body (excludes header) sent from appliance to upstream host
sr-bytes			Number of bytes sent from appliance to upstream host
sr-headerlength			Number of bytes in the header sent from appliance to upstream host

Category: connection			
ELFF	CPL	Custom	Description
cs-ip	proxy.address		IP address of the destination of the client's connection
c-connect-type			The type of connection made by the client to the appliance: 'Transparent' or 'Explicit'
c-dns		%h	Hostname of the client (uses the client's IP address to avoid reverse DNS)

Table B.6: Access Log Format Fields (Continued)

x-cs-dns	client.host		The hostname of the client obtained through reverse DNS.
c-ip	client.address	%a	IP address of the client
x-cs-connection-negotiated-cipher	client.connection.negotiated_cipher		OpenSSL cipher suite negotiated for the client connection
x-cs-connection-negotiated-cipher-strength	client.connection.negotiated_cipher.strength		Strength of the OpenSSL cipher suite negotiated for the client connection
r-dns			Hostname from the outbound server URL
r-ip			IP address from the outbound server URL
r-port		%p	Port from the outbound server URL
r-supplier-dns			Hostname of the upstream host (not available for a cache hit)
r-supplier-ip			IP address used to contact the upstream host (not available for a cache hit)
r-supplier-port			Port used to contact the upstream host (not available for a cache hit)
sc-adapter	proxy.card		Adapter number of the client's connection to the appliance
sc-connection			Unique identifier of the client's connection (i.e. SOCKET)
x-bluecoat-server-connection-socket-errno	server_connection.socket_errno		Error message associated with a failed attempt to connect to an upstream host
s-computername	proxy.name	%N	Configured name of the appliance
s-connect-type			Upstream connection type (Direct, SOCKS gateway, etc.)
s-dns			Hostname of the appliance (uses the primary IP address to avoid reverse DNS)
s-ip		%I	IP address of the appliance on which the client established its connection
s-port	proxy.port	%P	Port of the appliance on which the client established its connection
s-sitename		%S	Service used to process the transaction
x-module-name	module_name		The SGOS module that is handling the transaction
s-supplier-ip		%D	IP address used to contact the upstream host (not available for a cache hit)

Table B.6: Access Log Format Fields (Continued)

s-supplier-name		%d	Hostname of the upstream host (not available for a cache hit)
x-bluecoat-transaction-id	transaction.id		Unique per-request identifier generated by the appliance (note: this value is not unique across multiple appliances)
x-bluecoat-appliance-name	appliance.name		Configured name of the appliance
x-bluecoat-appliance-primary-address	appliance.primary_address		Primary IP address of the appliance
x-bluecoat-proxy-primary-address	proxy.primary_address		Primary IP address of the appliance
x-client-address			IP address of the client
x-client-ip			IP address of the client

Category: dns			
ELFF	CPL	Custom	Description
x-dns-cs-transport	dns.client_transport		The transport protocol used by the client connection in a DNS query
x-dns-cs-address	dns.request.address		The address queried in a reverse DNS lookup
x-dns-cs-dns	dns.request.name		The hostname queried in a forward DNS lookup
x-dns-cs-opcode	dns.request.opcode		The DNS OPCODE used in the DNS query
x-dns-cs-qtype	dns.request.type		The DNS QTYPE used in the DNS query
x-dns-cs-qclass	dns.request.class		The DNS QCLASS used in the DNS query
x-dns-rs-rcode	dns.response.code		The DNS RCODE in the response from upstream
x-dns-rs-a-records	dns.response.a		The DNS A RRs in the response from upstream
x-dns-rs-cname-records	dns.response cname		The DNS CNAME RRs in the response from upstream
x-dns-rs-ptr-records	dns.response.ptr		The DNS PTR RRs in the response from upstream

Category: im			
ELFF	CPL	Custom	Description
x-im-buddy-id			Instant messaging buddy ID
x-im-buddy-name			Instant messaging buddy display name
x-im-buddy-state			Instant messaging buddy state

Table B.6: Access Log Format Fields (Continued)

x-im-chat-room-id			Instant messaging identifier of the chat room in use
x-im-chat-room-members			The list of chat room member Ids
x-im-chat-room-type			The chat room type, one of 'public' or 'public', and possibly 'invite_only', 'voice' and/or 'conference'
x-im-client-info			The instant messaging client information
x-im-user-agent	im.user_agent		The instant messaging user agent string
x-im-file-path			Path of the file associated with an instant message
x-im-file-size			Size of the file associated with an instant message
x-im-http-gateway			The upstream HTTP gateway used for IM (if any)
x-im-message-opcode	im.message.opcode		The opcode utilized in the instant message
x-im-message-reflected	im.message.reflected		Indicates whether or not the IM message was reflected.
x-im-message-route			The route of the instance message
x-im-message-size			Length of the instant message
x-im-message-text			Text of the instant message
x-im-message-type			The type of the instant message
x-im-method			The method associated with the instant message
x-im-user-id			Instant messaging user identifier
x-im-user-name			Display name of the client
x-im-user-state			Instant messaging user state

Category: packets			
ELFF	CPL	Custom	Description
c-pkts-lost-client			Number of packets lost during transmission from server to client and not recovered at the client layer via error correction or at the network layer via UDP resends.
c-pkts-lost-cont-net			Maximum number of continuously lost packets on the network layer during transmission from server to client
c-pkts-lost-net			Number of packets lost on the network layer

Table B.6: Access Log Format Fields (Continued)

c-pkts-received			Number of packets from the server (s-pkts-sent) that are received correctly by the client on the first try
c-pkts-recovered-ECC			Number of packets repaired and recovered on the client layer
c-pkts-recovered-resent			Number of packets recovered because they were resent via UDP.
c-quality			The percentage of packets that were received by the client, indicating the quality of the stream
c-resendreqs			Number of client requests to receive new packets
s-pkts-sent			Number of packets from the server

Category: req_rsp_line			
ELFF	CPL	Custom	Description
cs-method	method	%m	Request method used from client to appliance
x-cs-http-method	http.method		HTTP request method used from client to appliance. Empty for non-HTTP transactions
cs-protocol	client.protocol		Protocol used in the client's request
cs-request-line	http.request_line	%r	First line of the client's request
x-cs-raw-headers-count	request.raw_headers.count		Total number of 'raw' headers in the request
x-cs-raw-headers-length	request.raw_headers.length		Total length of 'raw' headers in the request
cs-version	request.version	%v	Protocol and version from the client's request, e.g. HTTP/1.1
x-bluecoat-proxy-via-http-version	proxy.via_http_version		Default HTTP protocol version of the appliance without protocol decoration (e.g. 1.1 for HTTP/1.1)
x-bluecoat-redirect-location	redirect.location		Redirect location URL specified by a redirect CPL action
rs-response-line			First line (a.k.a. status line) of the response from an upstream host to the appliance
rs-status	response.code		Protocol status code of the response from an upstream host to the appliance
rs-version	response.version		Protocol and version of the response from an upstream host to the appliance, e.g. HTTP/1.1
sc-status		%s	Protocol status code from appliance to client

Table B.6: Access Log Format Fields (Continued)

x-bluecoat-ssl-failure-reason	ssl_failure_reason		Upstream SSL negotiation failure reason
x-cs-http-version	http.request.version		HTTP protocol version of request from the client. Does not include protocol qualifier (e.g. 1.1 for HTTP/1.1)
x-cs-socks-ip	socks.destination_address		Destination IP address of a proxied SOCKS request
x-cs-socks-port	socks.destination_port		Destination port of a proxied SOCKS request
x-cs-socks-method	socks.method		Method of a proxied SOCKS request
x-cs-socks-version	socks.version		Version of a proxied SOCKS request.
x-sc-http-status	http.response.code		HTTP response code sent from appliance to client
x-rs-http-version	http.response.version		HTTP protocol version of response from the upstream host. Does not include protocol qualifier (e.g. 1.1 for HTTP/1.1)
x-sc-http-version			HTTP protocol version of response to client. Does not include protocol qualifier (e.g. 1.1 for HTTP/1.1)
x-sr-http-version			HTTP protocol version of request to the upstream host. Does not include protocol qualifier (e.g. 1.1 for HTTP/1.1)

Category: special_token

ELFF	CPL	Custom	Description
x-bluecoat-special-amp	amp		The ampersand character
x-bluecoat-special-apos	apos		The apostrophe character (a.k.a. single quote)
x-bluecoat-special-cr	cr		Resolves to the carriage return character
x-bluecoat-special-crlf	crlf		Resolves to a carriage return/line feed sequence
x-bluecoat-special-empty	empty	%1	Resolves to an empty string
x-bluecoat-special-esc	esc		Resolves to the escape character (ASCII HEX 1B)
x-bluecoat-special-gt	gt		The greater-than character
x-bluecoat-special-lf	lf		The line feed character
x-bluecoat-special-lt	lt		The less-than character
x-bluecoat-special-quot	quot		The double quote character

Table B.6: Access Log Format Fields (Continued)

x-bluecoat-special-slash	slash		The forward slash character
--------------------------	-------	--	-----------------------------

Category: status			
ELFF	CPL	Custom	Description
x-bluecoat-release-id	release.id		The release ID of the ProxySG operating system
x-bluecoat-release-version	release.version		The release version of the ProxySG operating system
cs-categories			All content categories of the request URL
cs-categories-external			All content categories of the request URL that are defined by an external service.
cs-categories-policy			All content categories of the request URL that are defined by CPL.
cs-categories-local			All content categories of the request URL that are defined by a Local database.
cs-categories-provider			All content categories of the request URL that are defined by the current 3rd-party provider.
cs-categories-qualified			All content categories of the request URL, qualified by the provider of the category.
cs-category			Single content category of the request URL (a.k.a. sc-filter-category)
r-hierarchy			How and where the object was retrieved in the cache hierarchy.
sc-filter-category	category	%f	Content filtering category of the request URL
sc-filter-result		%w	Content filtering result: Denied, Proxied or Observed
s-action		%w	What type of action did the appliance take to process this request.
s-cpu-util			Average load on the proxy's processor (0%-100%)
s-hierarchy		%H	How and where the object was retrieved in the cache hierarchy.
s-icap-info		%z	ICAP response information
s-icap-status		%z	ICAP response status
x-bluecoat-surfcontrol-category-id			The SurfControl specific content category ID.

Table B.6: Access Log Format Fields (Continued)

x-bluecoat-surfcontrol-is-denied			'1' if the transaction was denied, else '0'
x-bluecoat-surfcontrol-is-proxied			'0' if transaction is explicitly proxied, '1' if transaction is transparently proxied
x-bluecoat-surfcontrol-reporter-id			Specialized value for SurfControl reporter
x-bluecoat-surfcontrol-reporter-v4			The SurfControl Reporter v4 format
x-bluecoat-surfcontrol-reporter-v5			The SurfControl Reporter v5 format
x-bluecoat-websense-category-id			The Websense specific content category ID
x-bluecoat-websense-keyword			The Websense specific keyword
x-bluecoat-websense-reporter-id			The Websense specific reporter category ID
x-bluecoat-websense-status			The Websense specific numeric status
x-bluecoat-websense-user			The Websense form of the username
x-bluecoat-websense-reporter-protocol-3			The Websense reporter format protocol version 3
x-exception-company-name	exception.company_name		The company name configured under exceptions
x-exception-contact	exception.contact		Describes who to contact when certain classes of exceptions occur, configured under exceptions (empty if the transaction has not been terminated)
x-exception-details	exception.details		The configurable details of a selected policy-aware response page (empty if the transaction has not been terminated)
x-exception-header	exception.header		The header to be associated with an exception response (empty if the transaction has not been terminated)
x-exception-help	exception.help		Help text that accompanies the exception resolved (empty if the transaction has not been terminated)
x-exception-id	exception.id		Identifier of the exception resolved (empty if the transaction has not been terminated)

Table B.6: Access Log Format Fields (Continued)

x-exception-last-error	exception.last_error		The last error recorded for the current transaction. This can provide insight when unexpected problems are occurring (empty if the transaction has not been terminated)
x-exception-reason	exception.reason		Indicates the reason why a particular request was terminated (empty if the transaction has not been terminated)
x-exception-sourcefile	exception.sourcefile		Source filename from which the exception was generated (empty if the transaction has not been terminated)
x-exception-sourceline	exception.sourceline		Source file line number from which the exception was generated (empty if the transaction has not been terminated)
x-exception-summary	exception.summary		Summary of the exception resolved (empty if the transaction has not been terminated)
x-exception-category-review-message	exception.category_review_message		Exception page message that includes a link allowing content categorization to be reviewed and/or disputed.
x-exception-category-review-url	exception.category_review_url		URL where content categorizations can be reviewed and/or disputed.
x-patience-javascript	patience_javascript		Javascript required to allow patience responses
x-patience-progress	patience_progress		The progress of the patience request
x-patience-time	patience_time		The elapsed time of the patience request
x-patience-url	patience_url		The url to be requested for more patience information
x-virus-id			Identifier of a virus if one was detected
x-virus-details	icap_virus_details		Details of a virus if one was detected
x-icap-error-code	icap_error_code		ICAP error code
x-icap-error-details	icap_error_details		ICAP error details

Category: streaming			
ELFF	CPL	Custom	Description
audiocodec			Audio codec used in stream.

Table B.6: Access Log Format Fields (Continued)

avgbandwidth		Average bandwidth (in bits per second) at which the client was connected to the server.
channelURL		URL to the .nsc file
c-buffercount		Number of times the client buffered while playing the stream.
c-bytes		An MMS-only value of the total number of bytes delivered to the client.
c-cpu		Client computer CPU type.
c-hostexe		Host application
c-hostexever		Host application version number
c-os		Client computer operating system
c-osversion		Client computer operating system version number
c-playerid		Globally unique identifier (GUID) of the player
c-playerlanguage		Client language-country code
c-playerversion		Version number of the player
c-rate		Mode of Windows Media Player when the last command event was sent
c-starttime		Timestamp (in seconds) of the stream when an entry is generated in the log file.
c-status		Codes that describe client status
c-totalbuffertime		Time (in seconds) the client used to buffer the stream
filelength		Length of the file (in seconds).
filesize		Size of the file (in bytes).
protocol		Protocol used to access the stream: mms, http, or asfm.
s-totalclients		Clients connected to the server (but not necessarily receiving streams).
transport		Transport protocol used (UDP, TCP, multicast, etc.)
videocodec		Video codec used to encode the stream.
x-cache-info		Values: UNKNOWN, DEMAND_MISS, DEMAND_PARTIAL_HIT, DEMAND_HIT, LIVE_FROM_ORIGIN, LIVE_PARTIAL_SPLIT, LIVE_SPLIT

Table B.6: Access Log Format Fields (Continued)

x-duration			Length of time a client played content prior to a client event (FF, REW, Pause, Stop, or jump to marker).
x-wm-c-dns			Hostname of the client determined from the Windows Media protocol
x-wm-c-ip			The client IP address determined from the Windows Media protocol
x-cs-streaming-client	streaming.client		Type of streaming client in use (windows_media, real_media, or quicktime).
x-rs-streaming-content	streaming.content		Type of streaming content served. (e.g. windows_media, quicktime)
x-streaming-bitrate	bitrate		The reported client-side bitrate for the stream

Category: time			
ELFF	CPL	Custom	Description
connect-time			Total ms required to connect to the origin server
date	date.utc	%x	GMT Date in YYYY-MM-DD format
dnslookup-time			Total ms cache required to perform the DNS lookup
duration		%T	Time taken (in seconds) to process the request
gmttime		%t	GMT date and time of the user request in format: [DD/MM/YYYY:hh:mm:ss GMT]
x-bluecoat-day-utc	day.utc		GMT/UTC day (as a number) formatted to take up two spaces (e.g. 07 for the 7th of the month)
x-bluecoat-hour-utc	hour.utc		GMT/UTC hour formatted to always take up two spaces (e.g. 01 for 1AM)
x-bluecoat-minute-utc	minute.utc		GMT/UTC minute formatted to always take up two spaces (e.g. 01 for 1 minute past)
x-bluecoat-month-utc	month.utc		GMT/UTC month (as a number) formatted to take up two spaces (e.g. 01 for January)
x-bluecoat-monthname-utc	monthname.utc		GMT/UTC month in the short-form string representation (e.g. Jan for January)
x-bluecoat-second-utc	second.utc		GMT/UTC second formatted to always take up two spaces (e.g. 01 for 1 second past)

Table B.6: Access Log Format Fields (Continued)

x-bluecoat-weekday-utc	weekday.utc		GMT/UTC weekday in the short-form string representation (e.g. Mon for Monday)
x-bluecoat-year-utc	year.utc		GMT/UTC year formatted to always take up four spaces
localtime		%L	Local date and time of the user request in format: [DD/MMM/YYYY:hh:mm:ss +nnnn]
x-bluecoat-day	day		Localtime day (as a number) formatted to take up two spaces (e.g. 07 for the 7th of the month)
x-bluecoat-hour	hour		Localtime hour formatted to always take up two spaces (e.g. 01 for 1AM)
x-bluecoat-minute	minute		Localtime minute formatted to always take up two spaces (e.g. 01 for 1 minute past)
x-bluecoat-month	month		Localtime month (as a number) formatted to take up two spaces (e.g. 01 for January)
x-bluecoat-monthname	monthname		Localtime month in the short-form string representation (e.g. Jan for January)
x-bluecoat-second	second		Localtime second formatted to always take up two spaces (e.g. 01 for 1 second past)
x-bluecoat-weekday	weekday		Localtime weekday in the short-form string representation (e.g. Mon for Monday)
x-bluecoat-year	year		Localtime year formatted to always take up four spaces
time	time.utc	%y	GMT time in HH:MM:SS format
timestamp		%g	Unix type timestamp
time-taken		%e	Time taken (in milliseconds) to process the request
rs-time-taken			Total time taken (in milliseconds) to send the request and receive the response from the origin server
x-bluecoat-end-time-wft			End local time of the transaction represented as a windows file time
x-bluecoat-start-time-wft			Start local time of the transaction represented as a windows file time
x-bluecoat-end-time-mssql			End local time of the transaction represented as a serial date time
x-bluecoat-start-time-mssql			Start local time of the transaction represented as a serial date time

Table B.6: Access Log Format Fields (Continued)

x-cookie-date	cookie_date		Current date in Cookie time format
x-http-date	http_date		Current date in HTTP time format
x-timestamp-unix			Seconds since UNIX epoch (Jan 1, 1970) (local time)
x-timestamp-unix-utc			Seconds since UNIX epoch (Jan 1, 1970) (GMT/UTC)

Category: url			
ELFF	CPL	Custom	Description
cs-host		%v	Hostname from the client's request URL. If URL rewrite policies are used, this field's value is derived from the 'log' URL
cs-uri	log_url	%i	The 'log' URL.
cs-uri-address	log_url.address		IP address from the 'log' URL. DNS is used if URL uses a hostname.
cs-uri-extension	log_url.extension		Document extension from the 'log' URL.
cs-uri-host	log_url.host		Hostname from the 'log' URL.
cs-uri-hostname	log_url.hostname		Hostname from the 'log' URL. RDNS is used if the URL uses an IP address.
cs-uri-path	log_url.path	%U	Path from the 'log' URL. Does not include query.
cs-uri-pathquery	log_url.pathquery		Path and query from the 'log' URL.
cs-uri-port	log_url.port		Port from the 'log' URL.
cs-uri-query	log_url.query	%Q	Query from the 'log' URL.
cs-uri-scheme	log_url.scheme		Scheme from the 'log' URL.
cs-uri-stem			Stem from the 'log' URL. The stem includes everything up to the end of path, but does not include the query.
c-uri	url		The original URL requested.
c-uri-address	url.address		IP address from the original URL requested. DNS is used if the URL is expressed as a hostname.
c-uri-cookie-domain	url.cookie_domain		The cookie domain of the original URL requested
c-uri-extension	url.extension		Document extension from the original URL requested
c-uri-host	url.host		Hostname from the original URL requested
c-uri-hostname	url.hostname		Hostname from the original URL requested. RDNS is used if the URL is expressed as an IP address

Table B.6: Access Log Format Fields (Continued)

c-uri-path	url.path		Path of the original URL requested without query.
c-uri-pathquery	url.pathquery		Path and query of the original URL requested
c-uri-port	url.port		Port from the original URL requested
c-uri-query	url.query		Query from the original URL requested
c-uri-scheme	url.scheme		Scheme of the original URL requested
c-uri-stem			Stem of the original URL requested
sr-uri	server_url		URL of the upstream request
sr-uri-address	server_url.address		IP address from the URL used in the upstream request. DNS is used if the URL is expressed as a hostname.
sr-uri-extension	server_url.extension		Document extension from the URL used in the upstream request
sr-uri-host	server_url.host		Hostname from the URL used in the upstream request
sr-uri-hostname	server_url.hostname		Hostname from the URL used in the upstream request. RDNS is used if the URL is expressed as an IP address.
sr-uri-path	server_url.path		Path from the upstream request URL
sr-uri-pathquery	server_url.pathquery		Path and query from the upstream request URL
sr-uri-port	server_url.port		Port from the URL used in the upstream request.
sr-uri-query	server_url.query		Query from the upstream request URL
sr-uri-scheme	server_url.scheme		Scheme from the URL used in the upstream request
sr-uri-stem			Path from the upstream request URL
s-uri	cache_url		The URL used for cache access
s-uri-address	cache_url.address		IP address from the URL used for cache access. DNS is used if the URL is expressed as a hostname
s-uri-extension	cache_url.extension		Document extension from the URL used for cache access
s-uri-host	cache_url.host		Hostname from the URL used for cache access

Table B.6: Access Log Format Fields (Continued)

s-uri-hostname	cache_url.hostname		Hostname from the URL used for cache access. RDNS is used if the URL uses an IP address
s-uri-path	cache_url.path		Path of the URL used for cache access
s-uri-pathquery	cache_url.pathquery		Path and query of the URL used for cache access
s-uri-port	cache_url.port		Port from the URL used for cache access
s-uri-query	cache_url.query		Query string of the URL used for cache access
s-uri-scheme	cache_url.scheme		Scheme from the URL used for cache access
s-uri-stem			Stem of the URL used for cache access
x-CS(Referer)-uri	request.header.Referer.url		The URL from the Referer header.
x-CS(Referer)-uri-address	request.header.Referer.url.address		IP address from the 'Referer' URL. DNS is used if URL uses a hostname.
x-CS(Referer)-uri-extension	request.header.Referer.url.extension		Document extension from the 'Referer' URL.
x-CS(Referer)-uri-host	request.header.Referer.url.host		Hostname from the 'Referer' URL.
x-CS(Referer)-uri-hostname	request.header.Referer.url.hostname		Hostname from the 'Referer' URL. RDNS is used if the URL uses an IP address.
x-CS(Referer)-uri-path	request.header.Referer.url.path		Path from the 'Referer' URL. Does not include query.
x-CS(Referer)-uri-pathquery	request.header.Referer.url.pathquery		Path and query from the 'Referer' URL.
x-CS(Referer)-uri-port	request.header.Referer.url.port		Port from the 'Referer' URL.
x-CS(Referer)-uri-query	request.header.Referer.url.query		Query from the 'Referer' URL.
x-CS(Referer)-uri-scheme	request.header.Referer.url.scheme		Scheme from the 'Referer' URL.
x-CS(Referer)-uri-stem			Stem from the 'Referer' URL. The stem includes everything up to the end of path, but does not include the query.
x-CS-raw-uri	raw_url		The 'raw' request URL.
x-CS-raw-uri-host	raw_url.host		Hostname from the 'raw' URL.
x-CS-raw-uri-port	raw_url.port		Port string from the 'raw' URL.
x-CS-raw-uri-scheme	raw_url.scheme		Scheme string from the 'raw' URL.

Table B.6: Access Log Format Fields (Continued)

x-cs/raw-uri-path	raw_url.path		Path from the 'raw' request URL. Does not include query.
x-cs/raw-uri-pathquery	raw_url.pathquery		Path and query from the 'raw' request URL.
x-cs/raw-uri-query	raw_url.query		Query from the 'raw' request URL.
x-cs/raw-uri-stem			Stem from the 'raw' request URL. The stem includes everything up to the end of path, but does not include the query.

Category: user			
ELFF	CPL	Custom	Description
cs-auth-group	group		One group that an authenticated user belongs to. If a user belongs to multiple groups, the group logged is determined by the Group Log Order configuration specified in VPM. If Group Log Order is not specified, an arbitrary group is logged.
cs-auth-groups	groups		List of groups that an authenticated user belongs to.
cs-auth-type			Client-side: authentication type (basic, ntlm, etc.)
cs-realm	realm		Authentication realm that the user was challenged in.
cs-user		%u	Qualified username for NTLM. Relative username for other protocols
cs-userdn	user		Full username of a client authenticated to the proxy (fully distinguished)
cs-username	user.name		Relative username of a client authenticated to the proxy (i.e. not fully distinguished)
sc-auth-status			Client-side: Authorization status
x-agent-sso-cookie			The authentication agent single signon cookie
x-cache-user			Relative username of a client authenticated to the proxy (i.e. not fully distinguished) (same as cs-username)
x-cs-auth-domain			The domain of the authenticated user.
x-cs-auth-form-action-url			The URL to submit the authentication form to.

Table B.6: Access Log Format Fields (Continued)

x-cs-auth-form-domain-field			The authentication form input field for the user's domain.
x-cs-auth-request-id			The bas64 encoded string containing the original request information during forms based authentication
x-cs-username-or-ip			Used to identify the user using either their authenticated proxy username or, if that is unavailable, their IP address.
x-radius-splash-session-id			Session ID made available through RADIUS when configured for session management
x-radius-splash-username			Username made available through RADIUS when configured for session management
x-user-x509-issuer	user.x509.issuer		If the user was authenticated via an X.509 certificate, this is the issuer of the certificate as an RFC2253 DN
x-user-x509-serial-number	user.x509.serialNumber		If the user was authenticated via an X.509 certificate, this is the serial number from the certificate as a hexadecimal number.
x-user-x509-subject	user.x509.subject		If the user was authenticated via an X.509 certificate, this is the subject of the certificate as an RFC2253 DN

Category: ci_request_header			
ELFF	CPL	Custom	Description
cs(Accept)	request.header.Accept		Request header: Accept
cs(Accept)-length	request.header.Accept.length		Length of HTTP request header: Accept
cs(Accept)-count	request.header.Accept.count		Number of HTTP request header: Accept
cs(Accept-Charset)	request.header.Accept-Charset		Request header: Accept-Charset
cs(Accept-Charset)-length	request.header.Accept-Charset.length		Length of HTTP request header: Accept-Charset
cs(Accept-Charset)-count	request.header.Accept-Charset.count		Number of HTTP request header: Accept-Charset
cs(Accept-Encoding)	request.header.Accept-Encoding		Request header: Accept-Encoding
cs(Accept-Encoding)-length	request.header.Accept-Encoding.length		Length of HTTP request header: Accept-Encoding
cs(Accept-Encoding)-count	request.header.Accept-Encoding.count		Number of HTTP request header: Accept-Encoding

Table B.6: Access Log Format Fields (Continued)

cs(Accept-Language)	request.header.Accept-Language		Request header: Accept-Language
cs(Accept-Language)-length	request.header.Accept-Language.length		Length of HTTP request header: Accept-Language
cs(Accept-Language)-count	request.header.Accept-Language.count		Number of HTTP request header: Accept-Language
cs(Accept-Ranges)	request.header.Accept-Ranges		Request header: Accept-Ranges
cs(Accept-Ranges)-length	request.header.Accept-Ranges.length		Length of HTTP request header: Accept-Ranges
cs(Accept-Ranges)-count	request.header.Accept-Ranges.count		Number of HTTP request header: Accept-Ranges
cs(Age)	request.header.Age		Request header: Age
cs(Age)-length	request.header.Age.length		Length of HTTP request header: Age
cs(Age)-count	request.header.Age.count		Number of HTTP request header: Age
cs(Allow)	request.header.Allow		Request header: Allow
cs(Allow)-length	request.header.Allow.length		Length of HTTP request header: Allow
cs(Allow)-count	request.header.Allow.count		Number of HTTP request header: Allow
cs(Authentication-Info)	request.header.Authentication-Info		Request header: Authentication-Info
cs(Authentication-Info)-length	request.header.Authentication-Info.length		Length of HTTP request header: Authentication-Info
cs(Authentication-Info)-count	request.header.Authentication-Info.count		Number of HTTP request header: Authentication-Info
cs(Authorization)	request.header.Authorization		Request header: Authorization
cs(Authorization)-length	request.header.Authorization.length		Length of HTTP request header: Authorization
cs(Authorization)-count	request.header.Authorization.count		Number of HTTP request header: Authorization
cs(Cache-Control)	request.header.Cache-Control		Request header: Cache-Control
cs(Cache-Control)-length	request.header.Cache-Control.length		Length of HTTP request header: Cache-Control
cs(Cache-Control)-count	request.header.Cache-Control.count		Number of HTTP request header: Cache-Control
cs(Client-IP)	request.header.Client-IP		Request header: Client-IP
cs(Client-IP)-length	request.header.Client-IP.length		Length of HTTP request header: Client-IP

Table B.6: Access Log Format Fields (Continued)

cs(Client-IP)-count	request.header.Client-IP.count		Number of HTTP request header: Client-IP
cs(Connection)	request.header.Connection		Request header: Connection
cs(Connection)-length	request.header.Connection.length		Length of HTTP request header: Connection
cs(Connection)-count	request.header.Connection.count		Number of HTTP request header: Connection
cs(Content-Encoding)	request.header.Content-Encoding		Request header: Content-Encoding
cs(Content-Encoding)-length	request.header.Content-Encoding.length		Length of HTTP request header: Content-Encoding
cs(Content-Encoding)-count	request.header.Content-Encoding.count		Number of HTTP request header: Content-Encoding
cs(Content-Language)	request.header.Content-Language		Request header: Content-Language
cs(Content-Language)-length	request.header.Content-Language.length		Length of HTTP request header: Content-Language
cs(Content-Language)-count	request.header.Content-Language.count		Number of HTTP request header: Content-Language
cs(Content-Length)	request.header.Content-Length		Request header: Content-Length
cs(Content-Length)-length	request.header.Content-Length.length		Length of HTTP request header: Content-Length
cs(Content-Length)-count	request.header.Content-Length.count		Number of HTTP request header: Content-Length
cs(Content-Location)	request.header.Content-Location		Request header: Content-Location
cs(Content-Location)-length	request.header.Content-Location.length		Length of HTTP request header: Content-Location
cs(Content-Location)-count	request.header.Content-Location.count		Number of HTTP request header: Content-Location
cs(Content-MD5)	request.header.Content-MD5		Request header: Content-MD5
cs(Content-MD5)-length	request.header.Content-MD5.length		Length of HTTP request header: Content-MD5
cs(Content-MD5)-count	request.header.Content-MD5.count		Number of HTTP request header: Content-MD5
cs(Content-Range)	request.header.Content-Range		Request header: Content-Range
cs(Content-Range)-length	request.header.Content-Range.length		Length of HTTP request header: Content-Range
cs(Content-Range)-count	request.header.Content-Range.count		Number of HTTP request header: Content-Range
cs(Content-Type)	request.header.Content-Type		Request header: Content-Type

Table B.6: Access Log Format Fields (Continued)

cs(Content-Type)-length	request.header.Content-Type.length		Length of HTTP request header: Content-Type
cs(Content-Type)-count	request.header.Content-Type.count		Number of HTTP request header: Content-Type
cs(Cookie)	request.header.Cookie	%C	Request header: Cookie
cs(Cookie)-length	request.header.Cookie.length		Length of HTTP request header: Cookie
cs(Cookie)-count	request.header.Cookie.count		Number of HTTP request header: Cookie
cs(Cookie2)	request.header.Cookie2		Request header: Cookie2
cs(Cookie2)-length	request.header.Cookie2.length		Length of HTTP request header: Cookie2
cs(Cookie2)-count	request.header.Cookie2.count		Number of HTTP request header: Cookie2
cs(Date)	request.header.Date		Request header: Date
cs(Date)-length	request.header.Date.length		Length of HTTP request header: Date
cs(Date)-count	request.header.Date.count		Number of HTTP request header: Date
cs(Etag)	request.header.Etag		Request header: Etag
cs(Etag)-length	request.header.Etag.length		Length of HTTP request header: Etag
cs(Etag)-count	request.header.Etag.count		Number of HTTP request header: Etag
cs(Expect)	request.header.Expect		Request header: Expect
cs(Expect)-length	request.header.Expect.length		Length of HTTP request header: Expect
cs(Expect)-count	request.header.Expect.count		Number of HTTP request header: Expect
cs(Expires)	request.header.Expires		Request header: Expires
cs(Expires)-length	request.header.Expires.length		Length of HTTP request header: Expires
cs(Expires)-count	request.header.Expires.count		Number of HTTP request header: Expires
cs(From)	request.header.From		Request header: From
cs(From)-length	request.header.From.length		Length of HTTP request header: From
cs(From)-count	request.header.From.count		Number of HTTP request header: From
cs(Front-End-HTTPS)	request.header.Front-End-HTTPS		Request header: Front-End-HTTPS
cs(Front-End-HTTPS)-length	request.header.Front-End-HTTPS.length		Length of HTTP request header: Front-End-HTTPS
cs(Front-End-HTTPS)-count	request.header.Front-End-HTTPS.count		Number of HTTP request header: Front-End-HTTPS

Table B.6: Access Log Format Fields (Continued)

cs(Host)	request.header.Host		Request header: Host
cs(Host)-length	request.header.Host.length		Length of HTTP request header: Host
cs(Host)-count	request.header.Host.count		Number of HTTP request header: Host
cs(If-Match)	request.header.If-Match		Request header: If-Match
cs(If-Match)-length	request.header.If-Match.length		Length of HTTP request header: If-Match
cs(If-Match)-count	request.header.If-Match.count		Number of HTTP request header: If-Match
cs(If-Modified-Since)	request.header.If-Modified-Since		Request header: If-Modified-Since
cs(If-Modified-Since)-length	request.header.If-Modified-Since.length		Length of HTTP request header: If-Modified-Since
cs(If-Modified-Since)-count	request.header.If-Modified-Since.count		Number of HTTP request header: If-Modified-Since
cs(If-None-Match)	request.header.If-None-Match		Request header: If-None-Match
cs(If-None-Match)-length	request.header.If-None-Match.length		Length of HTTP request header: If-None-Match
cs(If-None-Match)-count	request.header.If-None-Match.count		Number of HTTP request header: If-None-Match
cs(If-Range)	request.header.If-Range		Request header: If-Range
cs(If-Range)-length	request.header.If-Range.length		Length of HTTP request header: If-Range
cs(If-Range)-count	request.header.If-Range.count		Number of HTTP request header: If-Range
cs(If-Unmodified-Since)	request.header.If-Unmodified-Since		Request header: If-Unmodified-Since
cs(If-Unmodified-Since)-length	request.header.If-Unmodified-Since.length		Length of HTTP request header: If-Unmodified-Since
cs(If-Unmodified-Since)-count	request.header.If-Unmodified-Since.count		Number of HTTP request header: If-Unmodified-Since
cs(Last-Modified)	request.header.Last-Modified		Request header: Last-Modified
cs(Last-Modified)-length	request.header.Last-Modified.length		Length of HTTP request header: Last-Modified
cs(Last-Modified)-count	request.header.Last-Modified.count		Number of HTTP request header: Last-Modified
cs(Location)	request.header.Location		Request header: Location
cs(Location)-length	request.header.Location.length		Length of HTTP request header: Location
cs(Location)-count	request.header.Location.count		Number of HTTP request header: Location

Table B.6: Access Log Format Fields (Continued)

cs (Max-Forwards)	request.header.Max-Forwards		Request header: Max-Forwards
cs (Max-Forwards)-length	request.header.Max-Forwards.length		Length of HTTP request header: Max-Forwards
cs (Max-Forwards)-count	request.header.Max-Forwards.count		Number of HTTP request header: Max-Forwards
cs (Meter)	request.header.Meter		Request header: Meter
cs (Meter)-length	request.header.Meter.length		Length of HTTP request header: Meter
cs (Meter)-count	request.header.Meter.count		Number of HTTP request header: Meter
cs (P3P)	request.header.P3P		Request header: P3P
cs (P3P)-length	request.header.P3P.length		Length of HTTP request header: P3P
cs (P3P)-count	request.header.P3P.count		Number of HTTP request header: P3P
cs (Pragma)	request.header.Pragma		Request header: Pragma
cs (Pragma)-length	request.header.Pragma.length		Length of HTTP request header: Pragma
cs (Pragma)-count	request.header.Pragma.count		Number of HTTP request header: Pragma
cs (Proxy-Authenticate)	request.header.Proxy-Authenticate		Request header: Proxy-Authenticate
cs (Proxy-Authenticate)-length	request.header.Proxy-Authenticate.length		Length of HTTP request header: Proxy-Authenticate
cs (Proxy-Authenticate)-count	request.header.Proxy-Authenticate.count		Number of HTTP request header: Proxy-Authenticate
cs (Proxy-Authorization)	request.header.Proxy-Authorization		Request header: Proxy-Authorization
cs (Proxy-Authorization)-length	request.header.Proxy-Authorization.length		Length of HTTP request header: Proxy-Authorization
cs (Proxy-Authorization)-count	request.header.Proxy-Authorization.count		Number of HTTP request header: Proxy-Authorization
cs (Proxy-Connection)	request.header.Proxy-Connection		Request header: Proxy-Connection
cs (Proxy-Connection)-length	request.header.Proxy-Connection.length		Length of HTTP request header: Proxy-Connection
cs (Proxy-Connection)-count	request.header.Proxy-Connection.count		Number of HTTP request header: Proxy-Connection
cs (Range)	request.header.Range		Request header: Range
cs (Range)-length	request.header.Range.length		Length of HTTP request header: Range
cs (Range)-count	request.header.Range.count		Number of HTTP request header: Range
cs (Referer)	request.header.Referer	%R	Request header: Referer

Table B.6: Access Log Format Fields (Continued)

cs(Referer)-length	request.header.Referer.length		Length of HTTP request header: Referer
cs(Referer)-count	request.header.Referer.count		Number of HTTP request header: Referer
cs(Refresh)	request.header.Refresh		Request header: Refresh
cs(Refresh)-length	request.header.Refresh.length		Length of HTTP request header: Refresh
cs(Refresh)-count	request.header.Refresh.count		Number of HTTP request header: Refresh
cs(Retry-After)	request.header.Retry-After		Request header: Retry-After
cs(Retry-After)-length	request.header.Retry-After.length		Length of HTTP request header: Retry-After
cs(Retry-After)-count	request.header.Retry-After.count		Number of HTTP request header: Retry-After
cs(Server)	request.header.Server		Request header: Server
cs(Server)-length	request.header.Server.length		Length of HTTP request header: Server
cs(Server)-count	request.header.Server.count		Number of HTTP request header: Server
cs(Set-Cookie)	request.header.Set-Cookie		Request header: Set-Cookie
cs(Set-Cookie)-length	request.header.Set-Cookie.length		Length of HTTP request header: Set-Cookie
cs(Set-Cookie)-count	request.header.Set-Cookie.count		Number of HTTP request header: Set-Cookie
cs(Set-Cookie2)	request.header.Set-Cookie2		Request header: Set-Cookie2
cs(Set-Cookie2)-length	request.header.Set-Cookie2.length		Length of HTTP request header: Set-Cookie2
cs(Set-Cookie2)-count	request.header.Set-Cookie2.count		Number of HTTP request header: Set-Cookie2
cs(TE)	request.header.TE		Request header: TE
cs(TE)-length	request.header.TE.length		Length of HTTP request header: TE
cs(TE)-count	request.header.TE.count		Number of HTTP request header: TE
cs(Trailer)	request.header.Trailer		Request header: Trailer
cs(Trailer)-length	request.header.Trailer.length		Length of HTTP request header: Trailer
cs(Trailer)-count	request.header.Trailer.count		Number of HTTP request header: Trailer
cs(Transfer-Encoding)	request.header.Transfer-Encoding		Request header: Transfer-Encoding

Table B.6: Access Log Format Fields (Continued)

cs(Transfer-Encoding)-length	request.header.Transfer-Encoding.length		Length of HTTP request header: Transfer-Encoding
cs(Transfer-Encoding)-count	request.header.Transfer-Encoding.count		Number of HTTP request header: Transfer-Encoding
cs(Upgrade)	request.header.Upgrade		Request header: Upgrade
cs(Upgrade)-length	request.header.Upgrade.length		Length of HTTP request header: Upgrade
cs(Upgrade)-count	request.header.Upgrade.count		Number of HTTP request header: Upgrade
cs(User-Agent)	request.header.User-Agent	%A	Request header: User-Agent
cs(User-Agent)-length	request.header.User-Agent.length		Length of HTTP request header: User-Agent
cs(User-Agent)-count	request.header.User-Agent.count		Number of HTTP request header: User-Agent
cs(Vary)	request.header.Vary		Request header: Vary
cs(Vary)-length	request.header.Vary.length		Length of HTTP request header: Vary
cs(Vary)-count	request.header.Vary.count		Number of HTTP request header: Vary
cs(Via)	request.header.Via		Request header: Via
cs(Via)-length	request.header.Via.length		Length of HTTP request header: Via
cs(Via)-count	request.header.Via.count		Number of HTTP request header: Via
cs(WWW-Authenticate)	request.header.WWW-Authenticate		Request header: WWW-Authenticate
cs(WWW-Authenticate)-length	request.header.WWW-Authenticate.length		Length of HTTP request header: WWW-Authenticate
cs(WWW-Authenticate)-count	request.header.WWW-Authenticate.count		Number of HTTP request header: WWW-Authenticate
cs(Warning)	request.header.Warning		Request header: Warning
cs(Warning)-length	request.header.Warning.length		Length of HTTP request header: Warning
cs(Warning)-count	request.header.Warning.count		Number of HTTP request header: Warning
cs(X-BlueCoat-Error)	request.header.X-BlueCoat-Error		Request header: X-BlueCoat-Error
cs(X-BlueCoat-Error)-length	request.header.X-BlueCoat-Error.length		Length of HTTP request header: X-BlueCoat-Error
cs(X-BlueCoat-Error)-count	request.header.X-BlueCoat-Error.count		Number of HTTP request header: X-BlueCoat-Error
cs(X-BlueCoat-MC-Client-Ip)	request.header.X-BlueCoat-MC-Client-Ip		Request header: X-BlueCoat-MC-Client-Ip

Table B.6: Access Log Format Fields (Continued)

cs(X-BlueCoat-MC-Client-Ip)-length	request.header.X-BlueCoat-MC-Client-Ip.length		Length of HTTP request header: X-BlueCoat-MC-Client-Ip
cs(X-BlueCoat-MC-Client-Ip)-count	request.header.X-BlueCoat-MC-Client-Ip.count		Number of HTTP request header: X-BlueCoat-MC-Client-Ip
cs(X-BlueCoat-Via)	request.header.X-BlueCoat-Via		Request header: X-BlueCoat-Via
cs(X-BlueCoat-Via)-length	request.header.X-BlueCoat-Via.length		Length of HTTP request header: X-BlueCoat-Via
cs(X-BlueCoat-Via)-count	request.header.X-BlueCoat-Via.count		Number of HTTP request header: X-BlueCoat-Via
cs(X-Forwarded-For)	request.header.X-Forwarded-For	%X	Request header: X-Forwarded-For
cs(X-Forwarded-For)-length	request.header.X-Forwarded-For.length		Length of HTTP request header: X-Forwarded-For
cs(X-Forwarded-For)-count	request.header.X-Forwarded-For.count		Number of HTTP request header: X-Forwarded-For

Category: si_response_header

ELFF	CPL	Custom	Description
rs(Accept)	response.header.Accept		Response header: Accept
rs(Accept-Charset)	response.header.Accept-Charset		Response header: Accept-Charset
rs(Accept-Encoding)	response.header.Accept-Encoding		Response header: Accept-Encoding
rs(Accept-Language)	response.header.Accept-Language		Response header: Accept-Language
rs(Accept-Ranges)	response.header.Accept-Ranges		Response header: Accept-Ranges
rs(Age)	response.header.Age		Response header: Age
rs(Allow)	response.header.Allow		Response header: Allow
rs(Authentication-Info)	response.header.Authentication-Info		Response header: Authentication-Info
rs(Authorization)	response.header.Authorization		Response header: Authorization
rs(Cache-Control)	response.header.Cache-Control		Response header: Cache-Control
rs(Client-IP)	response.header.Client-IP		Response header: Client-IP
rs(Connection)	response.header.Connection		Response header: Connection
rs(Content-Encoding)	response.header.Content-Encoding		Response header: Content-Encoding

Table B.6: Access Log Format Fields (Continued)

rs(Content-Language)	response.header.Content-Language		Response header: Content-Language
rs(Content-Length)	response.header.Content-Length		Response header: Content-Length
rs(Content-Location)	response.header.Content-Location		Response header: Content-Location
rs(Content-MD5)	response.header.Content-MD5		Response header: Content-MD5
rs(Content-Range)	response.header.Content-Range		Response header: Content-Range
rs(Content-Type)	response.header.Content-Type	%c	Response header: Content-Type
rs(Cookie)	response.header.Cookie		Response header: Cookie
rs(Cookie2)	response.header.Cookie2		Response header: Cookie2
rs(Date)	response.header.Date		Response header: Date
rs(Etag)	response.header.Etag		Response header: Etag
rs(Expect)	response.header.Expect		Response header: Expect
rs(Expires)	response.header.Expires		Response header: Expires
rs(From)	response.header.From		Response header: From
rs(Front-End-HTTPS)	response.header.Front-End-HTTPS		Response header: Front-End-HTTPS
rs(Host)	response.header.Host		Response header: Host
rs(If-Match)	response.header.If-Match		Response header: If-Match
rs(If-Modified-Since)	response.header.If-Modified-Since		Response header: If-Modified-Since
rs(If-None-Match)	response.header.If-None-Match		Response header: If-None-Match
rs(If-Range)	response.header.If-Range		Response header: If-Range
rs(If-Unmodified-Since)	response.header.If-Unmodified-Since		Response header: If-Unmodified-Since
rs>Last-Modified	response.header.Last-Modified		Response header: Last-Modified
rs(Location)	response.header.Location		Response header: Location
rs(Max-Forwards)	response.header.Max-Forwards		Response header: Max-Forwards
rs(Meter)	response.header.Meter		Response header: Meter
rs(P3P)	response.header.P3P		Response header: P3P
rs(Pragma)	response.header.Pragma		Response header: Pragma
rs(Proxy-Authenticate)	response.header.Proxy-Authenticate		Response header: Proxy-Authenticate
rs(Proxy-Authorization)	response.header.Proxy-Authorization		Response header: Proxy-Authorization

Table B.6: Access Log Format Fields (Continued)

rs(Proxy-Connection)	response.header.Proxy-Connection		Response header: Proxy-Connection
rs(Range)	response.header.Range		Response header: Range
rs(Referer)	response.header.Referer		Response header: Referer
rs(Refresh)	response.header.Refresh		Response header: Refresh
rs(Retry-After)	response.header.Retry-After		Response header: Retry-After
rs(Server)	response.header.Server		Response header: Server
rs(Set-Cookie)	response.header.Set-Cookie		Response header: Set-Cookie
rs(Set-Cookie2)	response.header.Set-Cookie2		Response header: Set-Cookie2
rs(TE)	response.header.TE		Response header: TE
rs(Trailer)	response.header.Trailer		Response header: Trailer
rs(Transfer-Encoding)	response.header.Transfer-Encoding		Response header: Transfer-Encoding
rs(Upgrade)	response.header.Upgrade		Response header: Upgrade
rs(User-Agent)	response.header.User-Agent		Response header: User-Agent
rs(Vary)	response.header.Vary		Response header: Vary
rs(Via)	response.header.Via		Response header: Via
rs(WWW-Authenticate)	response.header.WWW-Authenticate		Response header: WWW-Authenticate
rs(Warning)	response.header.Warning		Response header: Warning
rs(X-BlueCoat-Error)	response.header.X-BlueCoat-Error		Response header: X-BlueCoat-Error
rs(X-BlueCoat-MC-Client-Ip)	response.header.X-BlueCoat-MC-Client-Ip		Response header: X-BlueCoat-MC-Client-Ip
rs(X-BlueCoat-Via)	response.header.X-BlueCoat-Via		Response header: X-BlueCoat-Via
rs(X-Forwarded-For)	response.header.X-Forwarded-For		Response header: X-Forwarded-For

Appendix C: Using WCCP

This appendix discusses how to configure a Blue Coat Systems ProxySG to participate in a Web Cache Communication Protocol (WCCP) scheme, when a WCCP-capable router collaborates with a set of WCCP-configured ProxySG Appliances to service requests. If you are already familiar with WCCP version 2 and want to get your router and ProxySG up and running right away, see the "Quick Start" on page 787.

Overview

WCCP is a Cisco®-developed protocol that allows you to establish redirection of the traffic that flows through routers.

The main benefits of using WCCP are:

- **Scalability.** With no reconfiguration overhead, redirected traffic can be automatically distributed to up to 32 ProxySG Appliances.
- **Redirection safeguards.** If no ProxySG Appliances are available, redirection stops and the router forwards traffic to the original destination address.

WCCP has two versions, version 1 and version 2, both of which are supported by Blue Coat. However, only one protocol version can be active on the ProxySG at a time. The active WCCP protocol set up in the ProxySG configuration must match the version running on the WCCP router.

Using WCCP and Transparent Redirection

A WCCP-capable router operates in conjunction with the ProxySG Appliances to transparently redirect traffic to a set of caches that participate in the specified WCCP protocol. IP packets are redirected based on fields within each packet. For instance, WCCP version 1 only redirects destination TCP port 80 (default HTTP traffic) IP packets. WCCP version 2 allows you to redirect traffic from other ports and protocols.

Load balancing is achieved through a redirection hash table to determine which ProxySG will receive the redirected packet.

WCCP Version 1

In WCCP version 1, the WCCP-configured home router transparently redirects TCP port 80 packets to a maximum of 32 ProxySG Appliances. (A ProxySG is seen as a cache in WCCP protocol.)

One of the caches participating in the WCCP service group is automatically elected to configure the home router's redirection tables. This way, caches can be transparently added and removed from the WCCP service group without requiring operator intervention. WCCP version 1 supports only a single service group.

Figure C-1: "A Typical WCCP Version 1 Configuration" on page 786 illustrates a typical WCCP version 1 implementation.

Each applicable client IP packet received by the home router is transparently redirected to a cache. A ProxySG from the group is selected to define the home router's redirection hash table for all caches. All caches periodically communicate with the home router to verify WCCP protocol synchronization and ProxySG availability within the service group. In return, the home router responds to each cache with information as to which ProxySG Appliances are available in the service group.

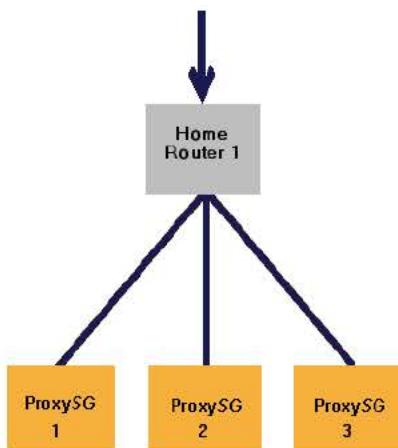


Figure C-1: A Typical WCCP Version 1 Configuration

Note the following WCCP version 1 caveats:

- The home router IP must be configured on all participating interfaces and must match the home router address configured on the ProxySG.
- The interface connected to the ProxySG must be Ethernet or Fast Ethernet.
- For Cisco routers using WCCP version 1, minimum IOS releases are 11.1(18)CA and 11.2(13)P. Note that releases prior to IOS 12.0(3)T only support WCCP version 1. Ensure that you are using the correct IOS software for the router and that the ProxySG configuration protocol version number and router protocol version number match.

For more information on WCCP Version 1, refer to the Cisco Web site. The rest of this appendix discusses WCCP version 2 only.

WCCP Version 2

For Cisco routers using WCCP version 2, minimum IOS releases are 12.0(3)T and 12.0(4). Note that release 12.0(5) and later releases support WCCP versions 1 and 2. Ensure that you use the correct IOS software for the router and that you have a match between the ProxySG configuration WCCP version number and router protocol version number.

WCCP version 2 protocol offers the same capabilities as version 1, along with increased protocol security and multicast protocol broadcasts. Version 2 multicasting allows caches and routers to discover each other via a common multicast service group and matching passwords. In addition, up to 32 WCCP-capable routers can transparently redirect traffic to a set of up to 32 ProxySG Appliances. Version 2 WCCP-capable routers are capable of redirecting IP traffic to a set of ProxySG Appliances based on various fields within those packets.

Version 2 allows routers and caches to participate in multiple, simultaneous service groups. Routers can transparently redirect IP packets based on their formats. For example, one service group could redirect HTTP traffic and another could redirect FTP traffic.

Note: Blue Coat recommends that WCCP-compliant caches from different vendors be kept separate and that only one vendor's routers be used in a service group.

One of the caches participating in the WCCP service group is automatically elected to configure the home router's redirection tables. This way, caches can be transparently added and removed from the WCCP service group without requiring operator intervention. WCCP version 2 supports multiple service groups.

Figure C-2, below, illustrates a WCCP version 2 implementation using multiple routers and ProxySG Appliances. In this scenario, routers 1 through n and caches 1 through m participate in the same service group. As in version 1, an appliance from the group is selected to define the redirection hash table in all routers for all caches. All caches periodically communicate with all routers to verify WCCP protocol synchronization and ProxySG and router availability within the service group. In return, each router responds to caches with information as to what caches and discovered routers are available in the service group.

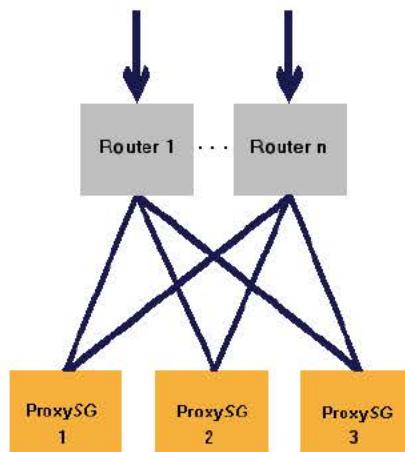


Figure C-2: A Version 2 Configuration Using Packet Redirection to Multiple Routers and Caches

Quick Start

Two tasks must be completed to get WCCP running: configuring the router and configuring the ProxySG. If you have a standard router and ProxySG configuration, use the Quick Start below. Otherwise, begin with the instructions in the procedure "To Do Initial Router Configuration:", below, and "To Create a ProxySG WCCP Configuration File and Enable WCCP:" on page 788.

If you require a more complicated configuration, start with "Configuring a WCCP Version 2 Service on the Router".

To Do Initial Router Configuration:

1. From the router (config) mode, tell WCCP which service group you want use. The web-cache service group redirects port 80 (HTTP) traffic only.

```
Router(config)#ip wccp web-cache
```

2. Enter the (config-if) submode by telling WCCP which IP address to use.

```
Router(config)#int interface
```

where *interface* is the interface with an IP address. The prompt changes to configuration interface submode.

3. Enable packet redirection on an outbound (Internet facing) interface.

```
Router(config-if)# ip wccp web-cache redirect out
```

4. Prevent packets received on an interface from being checked for redirection and allow the use of Blue Coat bypass lists.

```
Router(config-if)# ip wccp redirect exclude in
```

For more information on WCCP router configuration, see "Configuring a WCCP Version 2 Service on the Router" on page 788.

To Create a ProxySG WCCP Configuration File and Enable WCCP:

1. Create a WCCP configuration file through either the ProxySG's CLI inline commands or through a text editor. Make sure that the home router you enter here is the home router that was named in the router's configuration. If you do have a mismatch, you must correct it before continuing. See "Identifying a Home Router/Router ID Mismatch" on page 807.

For more information on creating a configuration file, see "Creating a ProxySG WCCP Configuration File" on page 795.

If you used the inline commands, you have completed WCCP configuration for both the router and the ProxySG and you have enabled WCCP on the ProxySG. No further steps are needed.

2. If you used a text editor, copy the file to an HTTP server accessible to the ProxySG.
3. Enable WCCP and download the configuration file to the ProxySG.

```
SGOS#(config) wccp enable  
SGOS#(config) wccp path http://205.66.255.10/files/wccp.txt  
SGOS#(config) load wccp-settings
```

Configuring a WCCP Version 2 Service on the Router

Configuring a router requires that you work with two different types of configuration commands:

- Creating a service group (which uses global settings).
- Configuring the Internet-Connected Interface (which uses interface settings).

Define service group settings before defining interface settings.

Setting up a Service Group

Services are of two types:

- Well known services (web-cache for port 80—HTTP— redirection)
The `web-cache` service group is supported by both Cisco and Blue Coat.
- Dynamic services (which can be used for other services, such as FTP, RTSP redirection, and reverse proxy).
Dynamic service uses identifiers ranging from 0-99 to name the service group.

WCCP global settings allow you to name the service group and then define the characteristics for that service group. Even if you use the pre-defined web-cache service group, you should:

- configure a multicast group address
- create and identify a redirection access list and associate it with a service group
- create and identify a cache bypass list and associate it with a service group
- create password authentication for messages sent by the service group to the router

Syntax for configuring a service group (global settings):

```
ip wccp {web-cache | service-number} [group-address groupaddress] [redirect-list  
access-list] [group-list access-list] [password password]
```

where:

`web-cache` Enables port 80 (HTTP) service.

`service-number` The identification number of the cache service group being controlled by the router. Services are identified using a value from 0 to 99. The reverse-proxy service is indicated using the value 99, although any value can be used for reverse proxy.

`group-address` (Optional) If no redirect list is defined (the default), all traffic will be redirected. The `groupaddress` option directs the router to use a specified multicast IP address to coalesce the “I See You” responses to the “Here I Am” messages that it has received on this address. The `groupaddress` argument requires a multicast address used by the router to determine which cache engine should receive redirected messages. The response is sent to the group address, as well. If no group address is defined (the default), all “Here I Am” messages are responded to with a unicast reply.

`redirect-list` (Optional) Directs the router to use an access list to control traffic redirected to the defined service group. The `access-list` parameter specifies either a number from 1 to 99 identifying a predefined standard or extended access list number, or a name (up to 64 characters long) identifying an existing standard or extended access list. The access list itself specifies which traffic may be redirected.

`group-list` (Optional) If no group list is defined (the default), all caches may participate in the service group.

The `group-list` option directs the router to use an access list to determine which caches are allowed to participate in the service group. The `access-list` parameter specifies either a number from 1 to 99 identifying a predefined standard or extended access list number or a name (up to 64 characters long) identifying an existing standard or extended access list. The access list itself specifies which caches are permitted to participate in the service group.

<code>password password</code>	(Optional) By default, password authentication is not configured and authentication is disabled. The password option increases authentication security to messages received from the service group specified by the service-number. Messages that do not pass authentication are discarded. The password can be up to eight characters long. Note that if you specify a password in the router configuration, you must also configure the same password separately on each cache.
------------------------------------	---

Naming a Service Group and Enabling WCCP

WCCP version 2 is enabled when you name a WCCP service group. (Version 1 requires a specific `enable` command.) The service group can already exist, such as `web-cache`, or it could be a new group, such as 36.

To Name a Service Group and Enable WCCP:

From the router `(config)` mode, enter the following command:

```
Router#(config) ip wccp web-cache  
-or-  
Router#(config) ip wccp 36
```

Configuring a Global Multicast Group Address

Benefits of using a multicast address include reduced WCCP protocol traffic and the ability to easily add and remove caches and routers from a service group without having to reconfigure all service group members. Multicast addresses fall within the range of 224.0.0.0 to 239.255.255.255.

Use the following syntax to configure a global multicast group address for multicast cache discovery.

```
ip wccp {web-cache | service-number} [group-address group_address]
```

To Configure a Multicast Address:

From the router `(config)` mode, name the group that will use the multicast address, provide the address, then tell the router which interface will be used:

```
Router(config)# ip wccp 36 group-address 225.1.1.1  
Router(config)# interface ethernet 0  
Router(config-if)# end
```

Creating a Redirection Access List and Associating it with a Service Group

Redirection access lists can contain commands redirecting packets from one network or cache to another. The lists also can be used to determine which caches participate in which service groups.

The two lists, although similar, have different purposes, and are applied to the router differently. The redirection lists are applied with the `redirect-list` option. The cache bypass lists are applied with the `group-list` argument. Both lists can be identified with either a name or a number.

Use the following syntax to create a redirection access list. Note that this is partial syntax for this command. Access lists are very complicated; refer to the Cisco Web site for complete syntax.

```
access-list acl_ID [deny | permit] protocol {[source_addr source_mask] |  
[local_addr local_mask]}
```

where:

<i>acl_ID</i>	Names the access list you are creating. You can use either a name or number.
<i>deny</i>	Indicates that you do not want to allow a packet to traverse the Cisco router. By default, the router firewall denies all inbound or outbound packets unless you specifically permit access.
<i>permit</i>	Selects a packet to traverse the PIX firewall. By default, the router firewall denies all inbound or outbound packets unless you specifically permit access.
<i>protocol</i>	Identifies, by name or number, an IP protocol. This parameter can be one of the keywords <code>icmp</code> , <code>ip</code> , <code>tcp</code> , or <code>udp</code> , or an integer in the range 1 to 254 representing an IP protocol number. To match any Internet protocol, including ICMP, TCP, and UDP, use the keyword <code>ip</code> .
<i>source_addr</i>	Indicates the address of the network or host from which the packet is being sent. Use the keyword <code>any</code> as an abbreviation for an address of 0.0.0.0.
<i>source_mask</i>	Specifies the netmask bits (mask) to be applied to <code>source_addr</code> , if the source address is for a network mask. Use the keyword <code>any</code> as an abbreviation for a mask of 0.0.0.0.
<i>local_addr</i>	Indicates the address of the network or host local to the PIX firewall. The <code>local_addr</code> is the address after NAT has been performed. Use the keyword <code>host</code> , followed by <code>address</code> , as an abbreviation for a mask of 255.255.255.255.
<i>local_mask</i>	Specifies the netmask bits (mask) to be applied to <code>local_addr</code> , if the local address is a network mask. Use the keyword <code>host</code> followed by <code>address</code> as an abbreviation for a mask of 255.255.255.255.

To Create a Redirection Access List or a Cache Bypass List:

From the router (config) prompt, name an access list and assign rules to it.

```
Router(config)# access-list 100 deny ip any host 126.10.10.10
Router(config)# access-list 100 permit ip any any
Router#
```

- The commands above gave the access list a name of 100.
- Denied packets from any protocol to be sent from any host on the 126.10.10.10 network.
- Permitted packets from any protocol to be sent from any other network.

To Associate a Redirection Access List with a Specific Service Group:

1. Create a redirection access list.
2. Associate the access list with a specified service group.

```
ip wccp {web-cache | service-number} [redirect-list access-list]
Router(config)# interface ethernet 0/0
Router(config-if)# ip wccp web-cache redirect-list 100
Router(config-if)# end
Router#
```

To Associate a Cache Bypass Access List with a Specific Service Group:

1. Create a redirection access list, using the syntax discussed above.
2. Associate the access list with a specified service group.

```
ip wccp {web-cache | service-number} [group-list access-list]
Router(config)# interface ethernet 0/0
Router(config-if)# ip wccp web-cache group-list 120
Router(config-if)# end
Router#
```

Configuring the Internet-Connected Interface

WCCP interface settings allow you to configure the Internet-connected interface that will redirect Web traffic to the content engine.

Using the interface commands allows you to:

- Enable and prevent packet redirection
- Enable reception of multicast packets for service group member routers

Syntax for configuring an internet-connected interface (interface settings):

```
ip wccp [{web-cache | service-number} redirect out | group-listen] | redirect
exclude in
```

where:

web-cache Enables the web cache service group.

service-number The identification number of the cache service group being controlled by the router. Services are identified using a value from 0 to 99. The reverse-proxy service is indicated using the value 99.

redirect out Enables packet redirection on an outbound (Internet facing) interface.

group-listen On a router that is a member of a service group, enables the reception of pre-defined IP multicast packets.

redirect exclude in Prevents packets received on an interface from being checked for redirection. Note that if the cache *service-group* is located on a separate router interface, the possibility exists that bypass filters could be enabled on the cache.

Using Packet Redirection

WCCP communication among the routers and the ProxySG Appliances can be done by either directly addressing protocol packets to each router's and cache's IP address (as illustrated in Figure C-1 on page 786) or by sending these packets to a common multicast address as illustrated in Figure C-3, below:

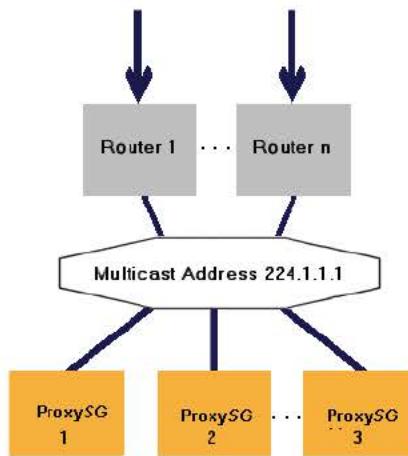


Figure C-3: A Version 2 Configuration Using Multicast Packet Redirection

You can configure redirection on inbound or outbound interfaces.

To Configure Redirection on the Outbound Interfaces:

Use the following syntax to configure redirection on the outbound interface.

```
ip wccp {web-cache | service-number} redirect out
```

From the router (config) prompt, enter the following:

```
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# end
```

To Exclude Packet Redirection on an Inbound Interface:

Use the following command to prevent packets received on an interface from being checked for redirection.

```
ip wccp redirect exclude in
```

The following example shows how to exclude Blue Coat interface (xx, in this case) and allow use of Blue Coat bypass lists:

From the router (config) prompt, enter the following:

```
Router(config)# int xx
Router(config-if)# ip wccp redirect exclude in
Router(config-if)# end
```

Enabling Reception of Multicast Packets

Benefits of using a multicast address include reduced WCCP protocol traffic and the ability to easily add and remove caches and routers from a service group without having to reconfigure all service group members. You (optionally) set up a multicast group address in "Configuring a Global Multicast Group Address". In the following procedure, you enable the reception of the pre-defined IP multicast packets to routers that are members of the group.

Multicast addresses fall within the range 224.0.0.0 to 239.255.255.255.

Use the following syntax to configure for multicast discovery of the cache(s).

```
ip wccp {web-cache | service-number} group-listen
```

The following example configures the router to use the WCCP 36 service group to redirect port 80 destination traffic. WCCP protocol traffic will be using multicast address 225.1.1.1. Interface "Ethernet 0" is used to receive the multicast WCCP traffic.

```
Router(config)# ip wccp 36 group-address 225.1.1.1
Router(config)# interface ethernet 0
Router(config-if)# ip wccp web-cache group-listen
Router(config-if)# end
```

Saving and Viewing Changes

Once you have made all the changes, you must permanently save them to disk. If not, the changes will be lost at the next reboot of the router.

To Save Router Configuration:

```
Router# write memory
```

To Display all Current WCCP Configuration Settings:

Use the following syntax to verify the settings in the new router configuration and to ensure that the appropriate cache engines are visible to the router.

```
show ip wccp {web-cache | service-number} [view | detail]
```

where

view (Optional) Lists all members of the identified service group and whether they have been detected.

detail (Optional) Displays IP and protocol version information about the router. Displays IP, protocol version, state, initial and assigned hash, hash allotment, redirected packet, and connection time information about the associated cache engine (ProxySG).

For example:

```
Router# show ip wccp web-cache view

Global WCCP Information:
Service Name: web-cache:
Number of Cache Engines:1
Number of Routers:1
Total Packets Redirected:186
Redirect Access-list:120
Total Packets Denied Redirect:57
Total Packets Unassigned:-none-
Group Access-list:0
Total Messaged Denied to Group:0
Total Authentication Failures:0
```

WCCP Router Informed of:

```
86.135.77.10  
186.135.77.20  
  
WCCP Cache Engines Visible:  
186.135.77.11  
186.135.77.12  
  
WCCP Cache Engines Not Visible:  
-none-
```

Creating a ProxySG WCCP Configuration File

Once you have the router global and interface settings complete, you must create a WCCP configuration file for the ProxySG. These configurations should include the following:

- Identify the service group
- Identify the queuing priorities for all defined service groups
- Identify the protocol
- Load balancing caches in a service group
- Identify ports
- Identify the home router as defined in the router configuration
- Identify the packet forwarding method

Understanding Packet Forwarding

By default, Cisco's GRE encapsulation (Generic Routing Encapsulation) is used to forward packets from the WCCP router to the caches. If you have a version 2 WCCP router, you can alternatively use Layer 2 (L2) rewrites to forward packets, which is faster than GRE and saves network bandwidth.

Using GRE, redirected packets are encapsulated in a new IP packet with a GRE header.

Using L2, redirected packets are not encapsulated; the packet's destination MAC address is replaced with the MAC address of the target cache. This different way of directing packets saves you the overhead of creating the GRE packet at the router and decoding it at the cache. Also, you save network bandwidth that would otherwise be consumed by the GRE header.

If you want to continue using GRE, you need not change any settings. To use L2 packet redirection, you must add the forwarding option to the ProxySG configuration file.

If WCCP version 2 is supported, the router sends out a list of forwarding mechanisms supported by the router in the first WCCP2_I_SEE_YOU message. The cache responds with a WCCP2_HERE_I_AM message. If the router does not send the list, the cache aborts its attempt to join the WCCP service group. If the method of forwarding mechanism is not supported by the router, the WCCP2 messages from the cache are ignored.

Caveats for using L2 redirection:

- You must use WCCP version 2.
- If a cache is not connected directly to a router, the router will not allow the cache to negotiate the rewrite method.

- The same rewrite method must be used for both packet forwarding and packet return.

Understanding Cache Load Balancing

If you use WCCP version 2, you can balance the load on the caches in a service group. When a router receives an IP packet for redirection, it hashes fields within the packet to yield an index within the hash table. The packet then is forwarded to the “owner” ProxySG for servicing. The proportion of redirection hash table assigned to each ProxySG can be altered to provide a form of load balancing between caches in a service group.

A hash table is configured by a dynamically elected ProxySG participating in a service group, enabling the simultaneous interception of multiple protocols on multiple ports. You can configure up to 100 dynamic or standard service groups plus standard service groups. A single service can intercept up to eight port numbers.

Each element in this 256-entry hash table refers to an active ProxySG within the service group. By default, each ProxySG is assigned roughly an even percentage of the 256-element redirection hash table. Multiple network cards within a ProxySG can participate in the same service group. To the routers and other caches, each interface appears as a unique cache. Using this strategy, redirected traffic can be better distributed among network interfaces in a cache.

Using Figure C-4, below, all caches would be assigned $1/m$ of the redirection hash table, but since Cache 2 and Cache 3 are physically located within the same ProxySG Appliance, that appliance would actually be assigned $2/m$ of the redirection hash table.

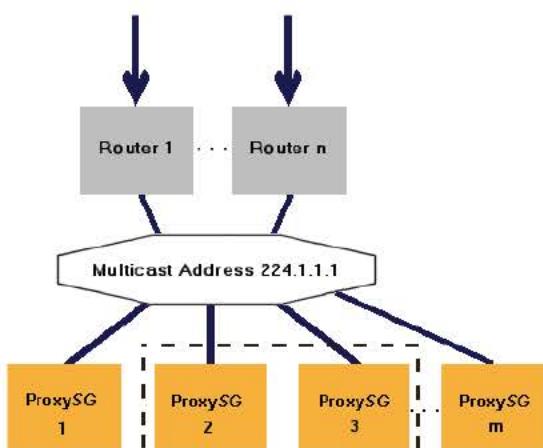


Figure C-4: A Version 2 Configuration Using Multicast Packet Redirection to Multiple Routers, Multiple Caches, and a Service Group

Assigning Percentages

You can override the default of each ProxySG being assigned roughly an even percentage; the relative distribution of the redirection hash table can be specified for each cache. Multiple hash-distributions are supported. Also, all, none, or part of a source and/or destination IP address or port number can be used in the hash. Each ProxySG can be assigned a primary-hash-weight value to determine the proportion of the 256-element hash table to be assigned.

If all caches are configured with a 0 primary-hash-weight value (the default) then each ProxySG is assigned an equal proportion of the redirection hash table. However, if any ProxySG is configured with a non-zero primary-hash-weight, each ProxySG is assigned a relative proportion of the table.

For instance, consider a configuration with five caches that use a primary-hash-weight defined as {25, 200, 0, 50, 25}. The total requested weight value is $25+200+0+50+25=300$ and, therefore, the proportion of the hash table assigned to each ProxySG will be $25/300$, $200/300$, $0/300$, $50/300$, and $25/300$.

Note that since one cache did not specify a non-zero primary-hash-weight, that cache will not be assigned any elements within the redirection hash table and, therefore, will not receive any redirected traffic. Also note that the hash weight can be specified for each caching member within a ProxySG. In Figure C-4, Cache 2 and Cache 3 can be assigned different weight values.

Alternate Hash Table

In some cases, a Web site becomes an Internet *hot spot*, receiving a disproportional number of client traffic relative to other sites. This situation can cause a larger request load on a specific ProxySG since the hash element associated with the popular site receives more activity than other hash elements.

To balance the redirection traffic load among the caches, a service group can be configured to use an alternate hash function when the number of GRE packets forwarded to the cache exceeds a certain number. (If you use L2 forwarding, the ProxySG counts MAC addresses.) Therefore, when a router receives an IP packet that hashes to an element flagged as a hot spot, the alternate hash function is computed. The ProxySG specified by the new index in the redirection hash table receives the redirected packet.

Each ProxySG can dynamically determine a hot spot within its assigned portion of the redirection hash table.

Alternate hash tables are only used for dynamic service groups that specify alternate-hash flags within their service-flags. Note that the default web-cache service group cannot use an alternate hash table. Instead, a comparable dynamic service group must be created.

To use hot spot detection, the ProxySG's WCCP configuration file must specify:

```
service-flags source-ip-hash
service-flags destination-port-alternate-hash
```

Creating a Configuration File

An example of a file using a dynamic service, as opposed to the default web-cache service, is shown below:

Note that if you are using the default web-cache service, the service group settings *priority*, *protocol*, *service flags*, and *ports* are not used.

```
wccp enable
wccp version 2
service-group 9
forwarding-type L2
priority 1
protocol 6
service-flags destination-ip-hash
service-flags ports-defined
ports 80 21 1755 554 80 80 80 80
```

```
interface 6
home-router 10.16.18.2
end
```

You can create a configuration file customized for the environment two ways: CLI inline commands or through a text file. In either case, the configuration file must include the information required by the commands below.

Syntax to create a customized configuration file:

```
service-group {web-cache | service-number}
[priority priority-number]
[protocol protocol-number]
[service-flags hash-bit-identifier]
[ports port1 ... port8]
home-router [ip-address | domain-name]
interface [interface-number]
[password string]
[primary-hash-weight interface-number value]
forwarding-type [GRE | L2]
```

Using Optional Negation Syntax, you can create an alternative WCCP configuration file using these negative commands; this is especially helpful when testing and debugging. This functionality enables you to change some of the configuration settings without altering or reloading the main configuration file.

```
[no] service-group {web-cache | service-number}
[priority priority-number]
[protocol protocol-number]
[no] service-flags hash-bit-identifier
[ports port1 ...port8]
home-router [ip-address | domain-name]
[no] interface [interface-number]
[password string | no password]
[primary-hash-weight interface-number value]
```

where:

<i>web-cache</i>	Enables the Web cache service group. Note that if you use the web-cache service group for WCCP, the dynamic service group settings (priority, protocol, service flags, and ports) are not applicable.
<i>service-number</i>	The identification number of the dynamic service group being controlled by the router. Services are identified using a value from 0 to 99. The reverse-proxy service is indicated using the value 99.
<i>priority-number</i>	(Applies to a dynamic service group only. A dynamic service group is one identified by a service number.) Establishes queuing priorities for all defined service groups, based on a priority number from 0 through 255, inclusive.
<i>protocol-number</i>	(Applies to a dynamic service group only. A dynamic service group is one identified by a service number.) Number of an Internet protocol. Protocol-number must be an integer in the range 0 through 255, inclusive, representing an IP protocol number.

<i>hash-bit-identifier</i>	(Applies to a dynamic service group only. A dynamic service group is one identified by a <i>service number</i> .) Sets the hash index, for load balancing purposes.
	The key associated with the <i>hash-bit-identifier</i> you specify will be hashed to produce the primary redirection hash table index. For instance, if only the <i>destination-ip-hash</i> flag is set, then the packet destination IP address will be used to determine the index. The index is constructed by starting with an initial value of zero and then computing an exclusive OR (XOR) of the fields specified in the hash-bit identifier. If alternative hashing has been enabled, any alternate hash flags are processed in the same way and produce a secondary redirection hash table index. Alternate hash flags end with the suffix “-alternate-hash.” For more information using the hashing table, see “Understanding Cache Load Balancing” on page 796.
<i>source-ip-hash</i> <i>(hash-bit-identifier)</i>	Sets the source IP bit definition within the redirection hash table index.
<i>destination-ip-hash</i> <i>(hash-bit-identifier)</i>	Sets the source IP bit definition within the redirection hash table index.
<i>source-port-hash</i> <i>(hash-bit-identifier)</i>	Sets the source port bit definition within the redirection hash table index.
<i>destination-port-hash</i> <i>(hash-bit-identifier)</i>	Sets the destination port bit definition within the redirection hash table index.
<i>ports-defined</i> <i>(hash-bit-identifier)</i>	Sets the port bit definition within the redirection hash table index.
<i>ports-source</i> <i>(hash-bit-identifier)</i>	Sets the source port bit definition within the redirection hash table index.
<i>source-ip-alternate-hash</i> <i>(hash-bit-identifier)</i>	Sets the alternate source IP bit definition within the redirection hash table index.
<i>destination-ip-alternate-hash</i> <i>(hash-bit-identifier)</i>	Sets the alternate destination IP bit definition within the redirection hash table index.
<i>source-port-alternate-hash</i> <i>(hash-bit-identifier)</i>	The alternate source port bit definition within the redirection hash table index.
<i>destination-port-alternate-hash</i> <i>(hash-bit-identifier)</i>	Sets the alternate destination port bit definition within the redirection hash table index.
<i>port1...port8</i>	(Applies to a dynamic service group only. A dynamic service group is one identified by a <i>service number</i> .) A zero-terminated list of TCP port identifiers. If the <i>service-flags ports-defined</i> flag is set, packets will be matched against the set of ports supplied. If the <i>service-flags ports-source</i> flag is set, the ports are assumed to be source ports. Otherwise, the ports are assumed to be destination ports.

<i>ip-address</i>	Indicates the IP address of your network's home router. For version 2, <i>ip-address</i> can be a multicast address. (Multicast addresses are in the range 224.0.0.0 to 239.255.255.255, inclusive.)
	In version 2, multiple <i>ip-addresses</i> can be specified for unicast addressing. For multicast addresses, only one <i>ip-address</i> can be specified per service group.
	If you choose to specify the home router IP address, it is very important that the actual home router IP address and the home router IP address specified in this ProxySG configuration file match. If you do not already know the IP address of the home router, you can easily determine it from the router CLI by using the <code>show ip wccp</code> command.
<i>domain-name</i>	Specifies the domain name of your network's home router. <i>Domain-name</i> must be a valid domain name string that will successfully resolve on DNS lookup.
<i>interface-number</i>	Specifies the interface number for the service group. Note that you cannot use a colon (0:0 or 0:1, for example).
<i>string</i>	(Applies to a dynamic service group only. A dynamic service group is one identified by a service number.) <i>String</i> can be at least one, and not more than eight, alphanumeric characters long.
	The password string specified here must match the password string declared for the router.
<i>interface-number</i>	(When used with the hash identifiers) Indicates the interface to which the weight factor should be applied to alter the distribution of the primary hash table.
<i>value</i>	Specifies the weight factor value (0 through 255) that should be applied to the interface indicated to alter the distribution of the primary hash table.
<i>forwarding-type</i> [GRE L2]	Switches between GRE encapsulation (the default) and L2 MAC address rewrite for forwarding packets. If this command is not present, GRE encapsulation is used.

You can create a configuration file customized for the environment through the CLI inline commands or through a text file. The CLI inline commands enable WCCP on the ProxySG immediately; the drawback is that if any information changes, you must re-create the whole file using the inline command. With a text file, if any information changes, you can change the individual line; the drawback is that you must download the file again from an HTTP server to the ProxySG.

To use CLI commands to create a configuration file, continue with the next procedure. To use a text editor to create a configuration file, continue with "Creating a Configuration File using a Text File" on page 801.

Creating a Configuration File using CLI Inline Commands

For examples of various types of WCCP configurations, see "Examples" on page 802.

If you choose to configure through the CLI and the `inline` command, refer to the example below:

```
SGOS# configure terminal  
SGOS# (config) inline wccp eof
```

where *eof* marks the beginning and end of the inline commands.

For example:

```
SGOS# (config) inline wccp eof
wccp enable
wccp version 2
service-group 9
forwarding-type L2
priority 1
protocol 1
service-flags destination-ip-hash
service-flags ports-defined
ports 80 21 1755 554 80 80 80 80
interface 1
home-router 10.16.18.2
end
eof
```

You created a WCCP configuration file and enabled WCCP on the ProxySG. WCCP setup is complete.

Creating a Configuration File using a Text File

If you create a configuration file using a text editor, assign the file the extension `.txt`. Note the following Blue Coat ProxySG configuration file rules:

- Only one command (and any associated parameters) is permitted, per line.
- Comments must begin with a semicolon (;) or a pound sign (#).
- Comments can begin in any column; however, all characters from the beginning of the comment to the end of the line are considered part of the comment and, therefore, are ignored.

For examples of various types of WCCP configurations, see "Examples" on page 802.

To Create a Configuration File using a Text Editor and Load the File on a ProxySG:

1. Open a text editor.
2. Using the commands described in "Syntax to create a customized configuration file:" on page 798, enter the arguments you need.
3. Copy the configuration file to an HTTP server so that it can be downloaded to the ProxySG.
4. Enable WCCP and download the WCCP configuration file using the following syntax:

wccp {enable | disable | no} [path config-file-url] | [version version-number]

where:

enable	Enables WCCP on the ProxySG.
disable	Disables WCCP on the ProxySG.
no	Indicates that you want to clear the current WCCP configuration settings.
config-file-url	Specifies the ProxySG WCCP configuration file or alternate configuration file.
version-number	Indicates the version of WCCP that your router is configured to use. If version-number is omitted, it is assumed to be 2.

For example:

```
SGOS#(config) wccp enable
SGOS#(config) wccp path http://205.66.255.10/files/wccp.txt
SGOS#(config) load wccp-settings
```

Examples

This section provides detailed examples of both the router and ProxySG configurations for:

- Standard HTTP redirection
- Standard HTTP redirection and a multicast address
- Standard HTTP redirection and a security password
- Standard transparent FTP
- A service group and alternate hashing

For information and examples about using WCCP, refer to
http://www.cisco.com/univercd/cc/td/doc/product/software/ios121/121cgcr/fun_r/frpt3/frd3005.htm

Displaying the Router's Known Caches

Use the router `show` command to display information about the ProxySG Appliances that are known to the router.

```
Router# show ip wccp web-caches
WCCP Web-Cache information:
IP Address:192.168.51.102
Protocol Version:0.3
State:Usable
Initial Hash
Info:FFFFFFFFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFFFFFFFF
Assigned Hash:
Info:FFFFFFFFFFFFFFFFFFFFFFFF
FFFFFFFFFFFFFFFFFFFF
Hash Allotment:256 (100.00%)
Packets Redirected:0
Connect Time:00:00:31
Router# exit
```

Standard HTTP Redirection

The web-cache service group enables HTTP traffic redirection on port 80.

Router Configuration

The following example enables standard HTTP traffic redirection on a WCCP version 2-capable Cisco router.

```
Router(config)# ip wccp web-cache
Router(config)# interface ethernet 0/0
```

```
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# end
```

ProxySG Configuration

To enable the web-cache service group within the ProxySG, the following configuration file could be loaded.

```
# Enable WCCP to allow WCCP protocol communication between
# the ProxySG Appliance and the home router.
wccp enable
# By default, the WCCP version 2 protocol is assumed. An
# explicit "wccp version 2" command could be specified here.
service-group web-cache
# Specify the address for the router.
home-router 90.0.0.90
# Network interface 0 will participate.
interface 0
end
```

Standard HTTP Redirection and a Multicast Address

Configuring a multicast address on a WCCP-capable router provides reduced WCCP protocol traffic and the ability to easily add and remove caches and routers from a service group without having to reconfigure all service group members.

Router Configuration

The following example enables the standard HTTP traffic redirection on a WCCP version 2-capable Cisco router. In this case, WCCP protocol traffic is directed to the multicast address 226.1.1.1.

```
Router(config)# ip wccp web-cache group-address 226.1.1.1
Router(config)# interface ethernet 0/0
Router(config-if)# ip wccp web-cache group-listen
Router(config-if)# ip wccp web-cache redirect out
Router(config-if)# end
```

ProxySG Configuration

To enable the standard web-cache service group within the ProxySG, the following configuration file should be loaded. Note that in this example, both network interfaces 0 and 1 will participate within the service group. Both interfaces send and receive WCCP protocol packets by way of the multicast address.

```
# Enable WCCP to allow WCCP protocol communication between
# the ProxySG Appliance and the home router.
wccp enable
# By default, the WCCP version 2 protocol is assumed. An
# explicit "wccp version 2" command could be specified here.
service-group web-cache
# Specify the multicast address.
home-router 224.1.1.1
# Network interface 0 will participate.
interface 0
```

```
# Network interface 1 will also participate.  
interface 1  
end
```

Standard HTTP Redirection Using a Security Password

A simple eight-character password is configured within the router. This password must match the password configured within the ProxySG.

Router Configuration

The following example enables standard HTTP traffic redirection on a WCCP version 2-capable Cisco router.

```
Router(config)# ip wccp web-cache password 29gy8c2  
Router(config)# interface ethernet 0/0  
Router(config-if)# ip wccp web-cache redirect out  
Router(config-if)# end
```

ProxySG Configuration

To enable the standard WCCP version 2 service group within the ProxySG, the following configuration file could be loaded.

```
# Enable WCCP to allow WCCP protocol communication between  
# the ProxySG Appliance and the home router.  
wccp enable  
# By default, the WCCP version 2 protocol is assumed. An  
# explicit "wccp version 2" command could be specified  
# here.  
service-group web-cache  
# Specify the address for the router.  
home-router 90.0.0.90  
# Network interface 0 will participate.  
interface 0  
password 29gy8c2  
end
```

Standard Transparent FTP

In WCCP version 1, only HTTP traffic on port 80 could be redirected. In WCCP version 2, you can create a numbered service group that redirects other protocols on other ports.

You set the service group on the router, and tell the ProxySG which ports should be redirected.

Router Configuration

In this configuration, you create a new service group that you are dedicating to FTP redirects.

```
# Enables the service group that redirects ports besides 80.  
Router(config)# ip wccp 10  
# Enables a service group that allows user-defined  
# ports to be redirected.
```

```
Router(config)# int e0
Router(config-if)# ip wccp 10 redirect out
```

ProxySG Configuration

In this configuration, you take the service group created by the router and assign the characteristics to the group.

```
SGOS#(config) inline wccp eof
wccp enable
service-group 10
interface 0
home-router 10.1.1.1
protocol 6
priority 1
service-flags ports-defined
service-flags destination-port-hash
ports 20 21 80 80 80 80 80 80
eof
```

Reverse Proxy Service Group

This service group redirects IP packets for TCP destination port 80 traffic by hashing the source IP address.

Router Configuration

The following example enables the special ProxySG service group on a WCCP-capable router.

```
Router(config)# ip wccp 99
Router(config)# interface ethernet 0/0
Router(config-if)# ip wccp 99 redirect out
Router(config-if)# end
```

ProxySG Configuration

To configure the special ProxySG service group on the appliance, a dynamic service group must be created as illustrated by the following example.

```
# Enable WCCP to allow WCCP protocol communication between
# the ProxySG Appliance and the home router.
wccp enable
# By default, the WCCP version 2 protocol is assumed. An
# explicit "wccp version 2" command could be specified here.
# Service Group 99 is specially identified within the router
# as representing the ProxySG Appliance service.
service-group 99
# Specify the address for the router.
home-router 90.0.0.90
# Network interface 0 will participate.
interface 0
# Specify the TCP protocol.
protocol 6
# The hash should be based on the source IP address.
```

```
service-flags source-ip-hash
end
```

Service Group with Alternate Hashing

You can create a special service group on a WCCP-capable router that uses alternate hashing when hot spots are detected. This service group redirects IP packets by hashing the source IP address.

Router Configuration

In this configuration, you create a new service group that you are dedicating to website hot spots.

```
Router(config)# ip wccp 5
Router(config)# interface ethernet 0/0
Router(config-if)# ip wccp 5 redirect out
Router(config-if)# end
```

ProxySG Configuration

To configure this special service group on the ProxySG, a dynamic service group must be created.

```
# Enable WCCP to allow WCCP protocol communication between
# the ProxySG Appliance and the home router.
wccp enable
# By default, the WCCP version 2 protocol is assumed. An
# explicit "wccp version 2" command could be specified here.
# Service Group 5 will be created to redirect standard HTTP
# traffic and use an alternate hash function based on the
# source IP address, if necessary.
service-group 5
# Specify the address for router 1.
home-router 90.0.0.90
# Specify the address for router 2.
home-router 90.0.1.5
# Network interface 0 will participate.
interface 0
# Specify the TCP protocol.
protocol 6
# The following two flags specify that a hash function based
# on the destination IP address should be applied first. If
# a hot-spot is detected, then an alternate hash
# function using the source IP address should be used.
service-flags destination-ip-hash
service-flags source-ip-alternate-hash
end
```

Troubleshooting: Home Router

If you install WCCP settings and then later upgrade the Cisco IOS software or change network configuration by adding a device with a higher IP address, the change might result in a different home router IP assignment. WCCP might or might not work under these conditions, and performance might decrease. If you upgrade the router software or change the network configuration, verify that the actual home router IP address and home router IP address in the WCCP configuration match.

To Verify the Home Router IP Address Matches the Home Router IP Address Listed in the WCCP Configuration:

- From the router CLI, view the WCCP configuration:

```
Router#(config) show ip wccp
```

The home router information appears, similar to the example below:

```
Global WCCP information:  
Router information:  
Home router Identifier:195.200.10.230  
Protocol Version:2.0
```

- From the Blue Coat ProxySG, verify that the home router IP address specified in the ProxySG WCCP configuration file is the same as the actual home router IP address discovered through the router CLI command. The following is a ProxySG WCCP configuration file showing the same home router IP as in the example above:

```
SGOS# show wccp config  
;WCCP Settings  
;Version 1.3  
wccp enable  
wccp version 2  
service-group web-cache  
interface 1  
home-router 195.200.10.230  
end
```

In this case, the two home router identifiers match.

Identifying a Home Router/Router ID Mismatch

The following is some helpful information for resolving a home-router/Router ID mis-match that results in the router crashing the ProxySG. This situation can occur when the router interface is set to a higher IP address than the home-router and WCCP messages show w/bad rcv_id.

Note that WCCP version 1 does not care what home router the cache had configured. So if you upgrade from WCCP version 1 to WCCP version 2, the router might pick a different IP address than was configured as a home router in the cache.

This means that a mismatch can occur after an upgrade.

ProxySG Configuration

Use the `show wccp statistics` command to identify the configured home router and the highest router IP.

```
SGOS#(config) show wccp statistics  
Service Group ident.      :512,1,9, 1,6,18, 1755,554,20,21,80,80,80,80  
  Home Routers      :10.2.3.224 <=====Configured Home Router IP  
  Hotspots announced   :0  
  Assignment state     :idle  
  Designated Cache    :10.2.3.228 <=====Blue Coat IP  
  Announcement key #  :2  
  Cache view change # :13 <==== # times cache view changed
```

```
Router View Changed      :0
Recent hit count        :0
Primary hit count       :0
Alternate hit count     :0
Instance IP address :10.2.3.228      <=====Blue Coat IP
Sequence info           :10.2.3.231,636
Query response info:
Active                  :1
Primary hash weight     :0
Hotspot information     :0,0,0,0
Total assign weight     :0
Router IP address :10.2.3.231 <=====Router ID/Highest IP on Router
Receive #               :636
Change #                :4
Activation time          :Wed, Jan 30 2002 00:17:58 UTC
Last I-See-You time      :Wed, Jan 30 2002 01:08:58 UTC
Active caches            :10.2.3.228
Assignment key           :10.2.3.228,2
Router state             :active
Cache                   :10.2.3.228,L,D
Active                  :1
```

Notice that .231 is highest IP on router and is automatically selected as the home router, even though .224 is the configured home router IP.

You can also use the `show wccp configuration` command if you already know the highest IP and just want to know what the Security Gateway identifies as the home-router.

```
SGOS# (config) show wccp configuration
;WCCP Settings
;Version 1.3
wccp enable
wccp version 2
service-group 9
interface 0
home-router 10.2.3.224
protocol 6
priority 1
service-flags ports-defined
service-flags destination-ip-hash
ports 1755 554 20 21 80 80 80 80
```

Router Configuration

The configuration below reveals that two interfaces are active on the router, and that one of the IP addresses is higher than the home router configured in the ProxySG configuration file. The higher IP address takes over duties as the home router, causing a mismatch between the router and the ProxySG.

```
Router# show conf
Using 689 out of 129016 bytes
version 12.1
service timestamps debug uptime
service timestamps log uptime
no service password-encryption
```

```

hostname NachoL3
enable secret 5 $1$r6nJ$dr58AZ.ZDg6RKA6MYeGRb.
enable password nacho

ip subnet-zero
no ip routing
ip wccp 9

interface FastEthernet0/0
  ip address 10.2.3.224 255.255.255.0
  ip wccp 9 redirect out
  no ip route-cache
  no ip mroute-cache
  speed 100
  half-duplex
!
interface FastEthernet0/1
  ip address 10.2.3.231 255.255.255.0
  no ip route-cache
  no ip mroute-cache
  speed 100
  half-duplex

```

Correcting a Home Router Mismatch

The home router must have the same IP address on both the router and the ProxySG. Every time a higher IP address is introduced to the router, the higher address becomes the home router.

To Set the Correct Home Router IP Address on the Router:

Run the following command from the router's (config) prompt.

```
Router(config)# home-router [ip-address | domain-name]
```

To Set the Correct Home Router IP Address on the ProxySG:

You cannot edit a WCCP configuration file created by the SGOS inline commands. You must recreate the configuration file. For more information on creating a WCCP configuration file using CLI commands on a ProxySG, see "Creating a Configuration File using CLI Inline Commands" on page 800.

If you created a text file and downloaded it, you can edit the file and then download it again to the ProxySG. For more information for editing the WCCP text file and downloading it, see "Creating a Configuration File using a Text File" on page 801.

Tips

- If you use IP spoofing with WCCP, do the following for best results:
The `ip wccp redirect exclude` command should be applied to the interface to which the ProxySG is attached.
- For L2 forwarding, the ProxySG should be directly connected to the router interface.

Appendix D: RIP Commands

You can place any of the commands below into a Routing Information Protocol (RIP) configuration text file. Note that you cannot edit a RIP file through the command line. You can overwrite a RIP file using the `inline rip-settings` command.

Once the file is complete, place it on an HTTP or FTP server accessible to the ProxySG and use the following commands to install the file on the ProxySG:

At the (config) command prompt:

```
SGOS#(config) rip path url  
SGOS#(config) load rip-settings
```

For more information on installing the RIP configuration file, see "Using RIP" on page 79.

net

```
net Nname[/mask] gateway Gname metric Value {passive | active | external}
```

Syntax

Parameters:	Description
<i>Nname</i>	Name of the destination network. It can be a symbolic network name, or an Internet address specified in dot notation.
<i>/mask</i>	Optional number between 1 and 32 indicating the netmask associated with <i>Nname</i> .
<i>Gname</i>	Name or address of the gateway to which RIP responses should be forwarded.
<i>Value</i>	The hop count to the destination host or network. A net <i>Nname</i> /32 specification is equivalent to the host <i>Hname</i> command.
<i>passive active external</i>	Indicates whether the gateway should be treated as passive or active, or whether the gateway is external to the scope of the RIP protocol.

host

```
host Hname gateway Gname metric Value {passive | active | external}
```

Syntax

Parameters:	Description
<i>Hname</i>	Name of the destination network. It can be a symbolic network name, or an Internet address specified in dot notation.

<i>Gname</i>	Name or address of the gateway to which RIP responses should be forwarded. It can be a symbolic network name, or an Internet address specified in dot notation.
<i>Value</i>	The hop count to the destination host or network. A net Nname/32 specification is equivalent to the host Hname command.
<i>passive active external</i>	Indicates whether the gateway should be treated as passive or active, or whether the gateway is external to the scope of the RIP protocol.

RIP Parameters

Lines that do not start with net or host commands must consist of one or more of the following parameter settings, separated by commas or blank spaces:

Parameters:	Description
<i>if=[0 1 2 3]</i>	Indicates that the other parameters on the line apply to the interface numbered 0,1,2, or 3 in SGOS terms.
<i>passwd=XXX</i>	Specifies an RIPv2 password that will be included on all RIPv2 responses sent and checked on all RIPv2 responses received. The password must not contain any blanks, tab characters, commas or '#' characters.
<i>no_ag</i>	Turns off aggregation of subnets in RIPv1 and RIPv2 responses.
<i>no_super_ag</i>	Turns off aggregation of networks into supernets in RIPv2 responses.
<i>passive</i>	Marks the interface to not be advertised in updates sent via other interfaces, and turns off all RIP and router discovery through the interface.
<i>no_rip</i>	Disables all RIP processing on the specified interface.
<i>no_ripv1_in</i>	Causes RIPv1 received responses to be ignored.
<i>no_ripv2_in</i>	Causes RIPv2 received responses to be ignored.
<i>ripv2_out</i>	Turns off RIPv1 output and causes RIPv2 advertisements to be multicast when possible.
<i>ripv2</i>	Is equivalent to <i>no_ripv1_in</i> and <i>no_ripv1_out</i> . This parameter is set by default.
<i>no_rdsc</i>	Disables the Internet Router Discovery Protocol. This parameter is set by default.
<i>no_solicit</i>	Disables the transmission of Router Discovery Solicitations.
<i>send_solicit</i>	Specifies that Router Discovery solicitations should be sent, even on point-to-point links, which by default only listen to Router Discovery messages.
<i>no_rdsc_adv</i>	Disables the transmission of Router Discovery Advertisements.

<code>rdisc_adv</code>	Specifies that Router Discovery Advertisements should be sent, even on point-to-point links, which by default only listen to Router Discovery messages.
<code>bcast_rdisc</code>	Specifies that Router Discovery packets should be broadcast instead of multicast.
<code>rdisc_pref=N</code>	Sets the preference in Router Discovery Advertisements to the integer N.
<code>rdisc_interval=N</code>	Sets the nominal interval with which Router Discovery Advertisements are transmitted to N seconds and their lifetime to 3*N.
<code>trust_gateway=rname</code>	Causes RIP packets from that router and other routers named in other <code>trust_gateway</code> keywords to be accepted, and packets from other routers to be ignored.
<code>redirect_ok</code>	Causes RIP to allow ICMP Redirect messages when the system is acting as a router and forwarding packets. Otherwise, ICMP Redirect messages are overridden.

ProxySG-Specific RIP Parameters

The following RIP parameters are unique to ProxySG configuration:

Parameters:	Description
<code>supply_routing_info</code> -or- <code>advertise_routes</code>	-s option: Supplying this option forces routers to supply routing information whether it is acting as an internetwork router or not. This is the default if multiple network interfaces are present or if a point-to-point link is in use.
<code>no_supply_routing_info</code>	-q option: opposite of -s.
<code>default_gateway</code>	-g option: This flag is used on internetwork routers to offer a route to the `default' destination. This is typically used on a gateway to the Internet, or on a gateway that uses another routing protocol whose routes are not reported to other local routers.
<code>suppress_extra_host_routes</code> -or- <code>advertise_host_route</code>	-h option: This flag causes host or point-to-point routes to not be advertised, provided there is a network route going the same direction. This option is useful on gateways to ethernet networks that have other gateway machines connected with point-to-point links.
<code>advertise_host_route</code>	-m option: This flag causes the machine to advertise a host or point-to-point route to its primary interface. The option is useful on multi-homed machines.
<code>Ignore_authentication</code>	-A option: This option is required for conformance with RFC 1723.

no_rip_out	Disables the transmission of all RIP packets. This setting is the default.
no_ripv1_out	Disables the transmission of RIPv1 packets.
no_ripv2_out	Disables the transmission of RIPv2 packets.
rip_out	Enables the transmission of RIPv1 packets.
ripv1_out	Enables the transmission of RIPv1 packets.
rdisc	Enables the transmission of Router Discovery Advertisements.
ripv1	Causes RIPv1 packets to be sent.
ripv1_in	Causes RIPv1 received responses to be handled.

Using Passwords with RIP

The first password specified for an interface is used for output. All passwords pertaining to an interface are accepted on input. For example, with the following settings:

```
if=0 passwd=aaa
if=1 passwd=bbb
passwd=ccc
```

Interface 0 accepts passwords `aaa` and `ccc`, and transmits using password `aaa`. Interface 1 accepts passwords `bbb` and `ccc`, and transmits using password `bbb`. The other interfaces accept and transmit the password `ccc`.

Appendix E: Using Regular Expressions

Regular expressions can be used for complex pattern matching. The ProxySG supports regular expressions as arguments for some conditions and actions in policy files, and as values for some CLI commands.

Note: Avoid using a regular expression when a non-regular expression alternative is available. Regular expressions are almost always less effective and more error prone than non-regular expressions. For instance, instead of using the regular expression "`^[:^:]*://.*\bluecoat\.com/.*$`" you should write "url.domain=bluecoat.com".

The following Content Policy Language (CPL) conditions use regular-expression arguments:

- All triggers with the `.regex` qualifier (for example, `url.regex=`, `url.host.regex=`, `im.text.message.regex=`)
- Request and response header triggers (for example, `request.header.NAME=`, `request.x.header_NAME=`, `response.header.NAME=`, `response.x_header.NAME=`)

The following CPL actions include regular-expression arguments (refer to the *Blue Coat Content Policy Language Guide* for more information):

- `delete_matching()`
- `redirect()`
- `replace()`

ProxySG Appliance commands that make use of regular expressions include:

- `(config) content delete regex`
- `(config) content priority regex`
- `(config) content revalidate regex`

Regular expressions were also used in CacheOS version 4.x filter files, to match URLs. If a CacheOS version 4.x filter file is being compiled, a filter line is considered to be a regular expression if it contains one or more regular expression metacharacters from the following set:

`\ ^ \$ [| (? * + {`

The regular expression support in the ProxySG described in this appendix is based on the Perl-compatible regular expression libraries (PCRE) by Philip Hazel. The text of this appendix is based on the PCRE documentation.

A *regular expression* (or RE) is a pattern that is matched against a subject string from left to right. Most characters stand for themselves in a pattern, and match the corresponding characters in the subject. The power of regular expressions comes from the ability to include alternatives and repetitions in the pattern. These are encoded in the pattern by the use of metacharacters, which do not stand for themselves, but instead are interpreted in some special way. For details of the theory and implementation of regular expressions, consult Jeffrey Friedl's *Mastering Regular Expressions*, published by O'Reilly (ISBN 0-596-00289-0).

The ProxySG uses a Regular Expression Engine (RE ENGINE) to evaluate regular expressions.

This appendix covers the following subjects:

- Syntax and semantics, including a table of metacharacters
- Differences between the RE ENGINE and Perl

Regular Expression Syntax

Regular expressions can contain both special and ordinary characters. Most ordinary characters, like 'A', 'a', or '3', are the simplest regular expressions; they simply match themselves. You can concatenate ordinary characters, so 'last' matches the characters 'last'. (In the rest of this section, regular expressions are written in a `courier` font, usually without quotes, and strings to be matched are 'in single quotes'.)

Some characters, like | or (), are special. Special characters, called *metacharacters*, either stand for classes of ordinary characters, or affect how the regular expressions around them are interpreted. The metacharacters are described in the following table.

Table E.1: Metacharacters Used in Regular Expressions

Metacharacter	Description
(?i)	Evaluate the expression following this metacharacter in a case-insensitive manner.
.	(Dot) In the default mode, this matches any character except a newline. (Note that newlines should not be detected when using regular expressions in CPL.)
^	(Circumflex or caret) Matches the start of the string.
\$	Matches the end of the string.
*	Causes the resulting RE to match zero (0) or more repetitions of the preceding RE, as many repetitions as are possible. ab* will match 'a', 'ab', or 'a' followed by any number of 'b's.
+	Causes the resulting RE to match one (1) or more repetitions of the preceding RE. ab+ will match 'a' followed by any non-zero number of 'b's; it will not match just 'a'.
?	Causes the resulting RE to match 0 or 1 repetitions of the preceding RE. ab? will match either 'a' or 'ab'.
*?, +?, ??	The *, +, and ? qualifiers are all greedy; they match as much text as possible. Sometimes this behavior isn't desired. If the RE /page1/.*/ is matched against /page1/heading/images/, it will match the entire string, and not just /page1/heading/. Adding ? after the qualifier makes it perform the match in non-greedy or minimal fashion; matching as few characters as possible. Using .*? in the previous expression will match only /page1/heading/.
{m, n}	Causes the resulting RE to match from m to n repetitions of the preceding RE, attempting to match as many repetitions as possible. For example, a{3,5} will match from 3 to 5 'a' characters.
{m, n}?	Causes the resulting RE to match from m to n repetitions of the preceding RE, attempting to match as few repetitions as possible. This is the non-greedy version of the previous qualifier. For example, on the 6-character string 'aaaaaa', a{3,5} will match 5 'a' characters, while a{3,5}?? will only match 3 characters.
\	Either escapes special characters (permitting you to match characters like '*?+&\$'), or signals a special sequence; special sequences are discussed below.

Table E.1: Metacharacters Used in Regular Expressions (Continued)

Metacharacter	Description
[]	Used to indicate a set of characters. Characters can be listed individually, or a range of characters can be indicated by giving two characters and separating them by a '-'. Special characters are not active inside sets. For example, [akm\$] will match any of the characters 'a', 'k', 'm', or '\$'; [a-z] will match any lowercase letter and [a-zA-Z0-9] matches any letter or digit. Character classes such as \w or \S (defined below) are also acceptable inside a range. If you want to include a] or a - inside a set, precede it with a backslash. Characters not within a range can be matched by including a ^ as the first character of the set; ^ elsewhere will simply match the '^' character.
	A B, where A and B can be arbitrary REs, creates a regular expression that will match either A or B. This can be used inside groups (see below) as well. To match a literal ' ', use \ , or enclose it inside a character class, like [].
(. . .)	Matches whatever regular expression is inside the parentheses, and indicates the start and end of a group; the contents of a group can be retrieved after a match has been performed, and can be matched later in the string with the \number special sequence, described below. To match the literals '(' or ')', use \(or \), or enclose them inside a character class: [()].

Regular Expression Details

This section describes the syntax and semantics of the regular expressions supported. Regular expressions are also described in most Perl documentation and in a number of other books, some of which have copious examples. Jeffrey Friedl's *Mastering Regular Expressions*, published by O'Reilly (ISBN 0-596-00289-0), covers them in great detail. The description here is intended as reference documentation.

There are two different sets of metacharacters: those that are recognized anywhere in the pattern except within square brackets, and those that are recognized in square brackets. Outside square brackets, the metacharacters are:

Table E.2: Metacharacters Used Outside Square Brackets

Metacharacter	Description
\	general escape character with several uses
^	assert start of subject (or line, in multiline mode)
\$	assert end of subject (or line, in multiline mode)
.	match any character except newline (by default)
[start character class definition
	start of alternative branch
(start subpattern
)	end subpattern
?	extends the meaning of "(" also 0 or 1 quantifier also quantifier minimizer
*	0 or more quantifier
+	1 or more quantifier
{	start min/max quantifier

The part of a pattern that is in square brackets is called a “character class.” In a character class the only metacharacters are:

Table E.3: Metacharacters Used in Square Brackets (Character Class)

Metacharacter	Description
\	general escape character
^	negate the class, but only if the first character
-	indicates character range
]	terminates the character class

The following sections describe the use of each of the metacharacters.

Backslash

The backslash character has several uses. If it is followed by a non-alphanumeric character, it takes away any special meaning that character might have. This use of backslash as an escape character applies both inside and outside character classes.

For example, if you want to match a “*” character, you write “*” in the pattern. This applies whether or not the following character would otherwise be interpreted as a metacharacter, so it is always safe to precede a non-alphanumeric with “\” to specify that it stands for itself. In particular, if you want to match a backslash, you write “\\”.

An escaping backslash can be used to include a white space or “#” character as part of the pattern.

A second use of backslash provides a way of encoding non-printing characters in patterns in a visible manner. There is no restriction on the appearance of non-printing characters, apart from the binary zero that terminates a pattern; but when a pattern is being prepared by text editing, it is usually easier to use one of the following escape sequences than the binary character it represents. For example, \a represents “alarm”, the BEL character (hex 07).

The handling of a backslash followed by a digit other than 0 is complicated. Outside a character class, RE ENGINE reads it and any following digits as a decimal number. If the number is less than 10, or if there have been at least that many previous capturing left parentheses in the expression, the entire sequence is taken as a *back reference*. A description of how this works is given later, following the discussion of parenthesized subpatterns.

Inside a character class, or if the decimal number is greater than 9 and there have not been that many capturing subpatterns, RE ENGINE re-reads up to three octal digits following the backslash, and generates a single byte from the least significant 8 bits of the value. Any subsequent digits stand for themselves. For example, \040 is another way of writing a space

Note that octal values of 100 or greater must not be introduced by a leading zero, because no more than three octal digits are ever read. All the sequences that define a single byte value can be used both inside and outside character classes. In addition, inside a character class, the sequence “\b” is interpreted as the backspace character (hex 08). Outside a character class it has a different meaning (see below).

The third use of backslash is for specifying generic character types:

- \d Any decimal digit
- \D Any character that is not a decimal digit

- \s Any white space character
- \S Any character that is not a white space character
- \w Any *word* character
- \W Any *non-word* character

Each pair of escape sequences partitions the complete set of characters into two disjoint sets. Any given character matches one, and only one, of each pair.

A “word” character is any letter or digit or the underscore character; that is, any character that can be part of a Perl “word.”

These character-type sequences can appear both inside and outside character classes. They each match one character of the appropriate type. If the current matching point is at the end of the subject string, all of them fail, since there is no character to match.

The fourth use of backslash is for certain simple assertions. An assertion specifies a condition that has to be met at a particular point in a match, without consuming any characters from the subject string. The use of subpatterns for more complicated assertions is described below. The back slashed assertions are

- \b Word boundary
- \B Not a word boundary
- \A Start of subject (independent of multiline mode)
- \Z End of subject or newline at end (independent of multiline mode)
- \z End of subject (independent of multiline mode)

These assertions might not appear in character classes (but note that “\b” has a different meaning, namely the backspace character, inside a character class).

A word boundary is a position in the subject string where the current character and the previous character do not both match \w or \W (i.e. one matches \w and the other matches \W), or the start or end of the string if the first or last character matches \w, respectively.

The \A, \Z, and \z assertions differ from the traditional circumflex and dollar (described below) in that they only ever match at the very start and end of the subject string, whatever options are set. The difference between \Z and \z is that \Z matches before a newline that is the last character of the string as well as at the end of the string, whereas \z matches only at the end. (Note that newlines should not be detected when using regular expressions in CPL.)

Circumflex and Dollar

Regular expressions are anchored in the CPL actions `redirect()`, `replace()`, and `rewrite()`, and unanchored in all other CPL and command uses of regular-expression patterns. In a regular expression that is by default unanchored, use the circumflex and dollar (^ and \$) to anchor the match at the beginning and end.

Circumflex need not be the first character of the pattern if a number of alternatives are involved, but it should be the first thing in each alternative in which it appears if the pattern is ever to match that branch. If all possible alternatives start with a circumflex, that is, if the pattern is constrained to match only at the start of the subject, it is said to be an “anchored” pattern. (There are also other constructs that can cause a pattern to be anchored.)

A dollar character is an assertion that is true only if the current matching point is at the end of the subject string, or immediately before a newline character that is the last character in the string (by default). Dollar need not be the last character of the pattern if a number of alternatives are involved, but it should be the last item in any branch in which it appears. Dollar has no special meaning in a character class.

Period (Dot)

Outside a character class, a dot in the pattern matches any one character in the subject, including a non-printing character, but not (by default) newline. (Note that newlines should not be detected when using regular expressions in CPL.) The handling of dot is entirely independent of the handling of circumflex and dollar, the only relationship being that they both involve newline characters. Dot has no special meaning in a character class.

Square Brackets

An opening square bracket introduces a character class, terminated by a closing square bracket. A closing square bracket on its own is not special. If a closing square bracket is required as a member of the class, it should be the first data character in the class (after an initial circumflex, if present) or escaped with a backslash.

A character class matches a single character in the subject; the character must be in the set of characters defined by the class, unless the first character in the class is a circumflex, in which case the subject character must not be in the set defined by the class. If a circumflex is actually required as a member of the class, ensure it is not the first character, or escape it with a backslash.

For example, the character class [aeiou] matches any lowercase vowel, while [^aeiou] matches any character that is not a lowercase vowel. Note that a circumflex is just a convenient notation for specifying the characters, which are in the class by enumerating those that are not. It is not an assertion: it still consumes a character from the subject string, and fails if the current pointer is at the end of the string.

When caseless matching is set, any letters in a class represent both their uppercase and lowercase versions; for example, a caseless [aeiou] matches “A” as well as “a”, and a caseless [^aeiou] does not match “A”, whereas a careful version would.

A class such as [^a] will always match a newline. (Note that newlines should not be detected when using regular expressions in CPL.)

The minus (hyphen) character can be used to specify a range of characters in a character class. For example, [d-m] matches any letter between d and m, inclusive. If a minus character is required in a class, it must be escaped with a backslash or appear in a position where it cannot be interpreted as indicating a range, typically as the first or last character in the class. It is not possible to have the character "]" as the end character of a range, since a sequence such as [w-] is interpreted as a class of two characters. The octal or hexadecimal representation of "]" can, however, be used to end a range.

Ranges operate in ASCII collating sequence. They can also be used for characters specified numerically, for example [\000-\037]. If a range that includes letters is used when caseless matching is set, it matches the letters in either case. For example, [W-c] is equivalent to [][\^_`wxyzabc], matched caselessly.

The character types \d, \D, \s, \S, \w, and \W might also appear in a character class, and add the characters that they match to the class. For example, [\dABCDEF] matches any hexadecimal digit. A circumflex can conveniently be used with the upper case character types to specify a more restricted set of characters than the matching lower case type. For example, the class [^\W_] matches any letter or digit, but not underscore.

All non-alphanumeric characters other than \, -, ^ (at the start) and the terminating] are non-special in character classes, but it does no harm if they are escaped.

Vertical Bar

Vertical bar characters are used to separate alternative patterns. For example, the pattern

```
gilbert|sullivan
```

matches either "gilbert" or "sullivan." Any number of alternatives might appear, and an empty alternative is permitted (matching the empty string). The matching process tries each alternative in turn, from left to right, and the first one that succeeds is used. If the alternatives are within a subpattern (defined below), "succeeds" means matching the rest of the main pattern as well as the alternative in the subpattern.

Lowercase-Sensitivity

By default, CPL conditions that take regular-expression arguments perform a case-insensitive match. In all other places where the ProxySG performs a regular-expression match, the match is case sensitive.

Note: In CPL, use the ".case+sensitive" condition modifier for case sensitivity, rather than relying on Perl syntax.

Override the default for case sensitivity by using the following syntax:

- (?i) Sets case-insensitive matching mode.
- (?-i) Sets case-sensitive matching mode.

The scope of a mode setting depends on where in the pattern the setting occurs. For settings that are outside any subpattern (see the next section), the effect is the same as if the options were set or unset at the start of matching. The following patterns all behave in exactly the same way:

```
(?i)abc  
a(?i)bc  
ab(?i)c  
abc(?i)
```

In other words, such “top level” settings apply to the whole pattern (unless there are other changes inside subpatterns). If there is more than one setting of the same option at the top level, the rightmost setting is used.

If an option change occurs inside a subpattern, the effect is different. This is a change of behavior in Perl 5.005. An option change inside a subpattern affects only that part of the subpattern that follows it, so `(a (?i)b)c` matches `abc` and `aBc` and no other strings (assuming the default is case sensitive). By this means, options can be made to have different settings in different parts of the pattern. Any changes made in one alternative do carry on into subsequent branches within the same subpattern. For example `(a (?i)b|c)` matches “ab”, “aB”, “c”, and “C”, even though when matching “C” the first branch is abandoned before the option setting. This is because the effects of option settings happen at compile time. This avoids some strange side-effects.

Subpatterns

Subpatterns are delimited by parentheses (round brackets), which can be nested. Marking part of a pattern as a subpattern does two things:

- It localizes a set of alternatives.

For example, the pattern `cat(aract|erpillar|)` matches one of the words “cat”, “cataract”, or “caterpillar”. Without the parentheses, it would match “cataract”, “erpillar” or the empty string.

- It sets up the subpattern as a capturing subpattern (as defined above). When the whole pattern matches, that portion of the subject string that matched the subpattern is passed back to the caller via the *ovecotor* argument of *RE Engine_exec()*. Opening parentheses are counted from left to right (starting from 1) to obtain the numbers of the capturing subpatterns.

For example, if the string “the red king” is matched against the pattern `the ((red|white) (king|queen))` the captured substrings are “red king”, “red”, and “king”, and are numbered 1, 2, and 3.

The fact that plain parentheses fulfill two functions is not always helpful. There are times when a grouping subpattern is required without a capturing requirement. If an opening parenthesis is followed by “?:”, the subpattern does not do any capturing, and is not counted when computing the number of any subsequent capturing subpatterns. For example, if the string “the white queen” is matched against the pattern `((?:red|white) (king|queen))` the captured substrings are “white queen” and “queen,” and are numbered 1 and 2. The maximum number of captured substrings is 99, and the maximum number of all subpatterns, both capturing and non-capturing, is 200.

As a convenient shorthand, if any option settings are required at the start of a non-capturing subpattern, the option letters might appear between the "?" and the ":". Thus the two patterns `(?i:saturday|sunday)` and `(:(?i)saturday | sunday)` match exactly the same set of strings. Because alternative branches are tried from left to right, and options are not reset until the end of the subpattern is reached, an option setting in one branch does affect subsequent branches, so the above patterns match "SUNDAY" as well as "Saturday".

Repetition

Repetition is specified by quantifiers, which can follow any of the following items:

- A single character, possibly escaped by the `.` metacharacter
- A character class
- A back reference (see next section)
- A parenthesized subpattern (unless it is an assertion - see below)

The general repetition quantifier specifies a minimum and maximum number of permitted matches, by giving the two numbers in curly brackets (braces), separated by a comma. The numbers must be less than 65536, and the first must be less than or equal to the second. For example, `z{2,4}` matches "zz", "zzz", or "zzzz." A closing brace on its own is not a special character. If the second number is omitted, but the comma is present, there is no upper limit; if the second number and the comma are both omitted, the quantifier specifies an exact number of required matches. Thus `[aeiou]{3,}` matches at least 3 successive vowels, but might match many more, while `\d{8}` matches exactly 8 digits. An opening curly bracket that appears in a position where a quantifier is not allowed, or one that does not match the syntax of a quantifier, is taken as a literal character. For example, `{,6}` is not a quantifier, but a literal string of four characters.

The quantifier `{0}` is permitted, causing the expression to behave as if the previous item and the quantifier were not present. For convenience (and historical compatibility) the three most common quantifiers have single-character abbreviations:

- * Equivalent to `{0,}`
- + Equivalent to `{1,}`
- ? Equivalent to `{0,1}`

It is possible to construct infinite loops by following a subpattern that can match no characters with a quantifier that has no upper limit, for example `(a?)^*`

Earlier versions of Perl gave an error at compile time for such patterns. However, because there are cases where this can be useful, such patterns are now accepted, but if any repetition of the subpattern does in fact match no characters, the loop is forcibly broken.

By default, the quantifiers are “greedy,” that is, they match as much as possible (up to the maximum number of permitted times) without causing the rest of the pattern to fail. The classic example of where this gives problems is in trying to match comments in C programs. These appear between the sequences /* and */ and within the sequence, individual * and / characters might appear. An attempt to match C comments by applying the following pattern fails because it matches the entire string due to the greediness of the .* item.

```
/\*.*\*/
```

to the string

```
/* first command */ not comment /* second comment */
```

However, if a quantifier is followed by a question mark, then it ceases to be greedy, and instead matches the minimum number of times possible, so the following pattern does the right thing with the C comments.

```
/\*.*?\*/
```

The meaning of the various quantifiers is not otherwise changed, just the preferred number of matches. Do not confuse this use of question mark with its use as a quantifier in its own right. Because it has two uses, it can sometimes appear doubled, as below, which matches one digit by preference, but can match two if that is the only way the rest of the pattern matches.

```
\d??\d
```

When a parenthesized subpattern is quantified with a minimum repeat count that is greater than 1 or with a limited maximum, more store is required for the compiled pattern, in proportion to the size of the minimum or maximum.

If a pattern starts with .* then it is implicitly anchored, since whatever follows will be tried against every character position in the subject string. RE ENGINE treats this as though it were preceded by \A.

When a capturing subpattern is repeated, the value captured is the substring that matched the final iteration. For example, after the following expression has matched “tweedledum tweedledee” the value of the captured substring is “tweedledee”.

```
(tweedle [dume] {3}\s*)+
```

However, if there are nested capturing subpatterns, the corresponding captured values might have been set in previous iterations. For example, after

```
/ (a | (b ))+ /
```

matches “aba” the value of the second captured substring is “b”.

Back References

Outside a character class, a backslash followed by a digit greater than 0 (and possibly further digits) is a back reference to a capturing subpattern earlier (i.e., to its left) in the pattern, provided there have been that many previous capturing left parentheses.

However, if the decimal number following the backslash is less than 10, it is always taken as a back reference, and causes an error only if there are not that many capturing left parentheses in the entire pattern. In other words, the parentheses that are referenced need not be to the left of the reference for numbers less than 10. See the section entitled “Backslash” above for further details of the handling of digits following a backslash.

A back reference matches whatever actually matched the capturing subpattern in the current subject string, rather than anything matching the subpattern itself. So the following pattern matches “sense and sensibility” and “response and responsibility,” but not “sense and responsibility.”

```
(sens|respons)e and \1ibility
```

If caseful matching is in force at the time of the back reference, then the case of letters is relevant. For example, the following expression matches “rah rah” and “RAH RAH”, but not “RAH rah”, even though the original capturing subpattern is matched caselessly.

```
((?i)rah)\s+\1
```

There might be more than one back reference to the same subpattern. If a subpattern has not actually been used in a particular match, then any back references to it always fail. For example, the following pattern always fails if it starts to match “a” rather than “bc.” Because there might be up to 99 back references, all digits following the backslash are taken as part of a potential back reference number. If the pattern continues with a digit character, then some delimiter must be used to terminate the back reference.

```
(a|(bc))\2
```

A back reference that occurs inside the parentheses to which it refers fails when the subpattern is first used, so, for example, (a\1) never matches. However, such references can be useful inside repeated subpatterns. For example, the following pattern matches any number of “a”s and also “aba”, “ababaa” etc. At each iteration of the subpattern, the back reference matches the character string corresponding to the previous iteration. In order for this to work, the pattern must be such that the first iteration does not need to match the back reference. This can be done using alternation, as in the example above, or by a quantifier with a minimum of zero.

```
(a|b\1)+
```

Assertions

An assertion is a test on the characters following or preceding the current matching point that does not actually consume any characters. The simple assertions coded as \b, \B, \A, \Z, \z, ^ and \$ are described above. More complicated assertions are coded as subpatterns. There are two kinds: those that look ahead of the current position in the subject string, and those that look behind it.

An assertion subpattern is matched in the normal way, except that it does not cause the current matching position to be changed. Lookahead assertions start with (?= for positive assertions and (?! for negative assertions. For example, the following expression matches a word followed by a semicolon, but does not include the semicolon in the match.

```
\w+ (?=; )
```

The following expression matches any occurrence of “example” that is not followed by “bar”.

```
example(?!bar)
```

Note that the apparently similar pattern that follows does not find an occurrence of “bar” that is preceded by something other than “example”; it finds any occurrence of “bar” whatsoever, because the assertion (?example) is always true when the next three characters are “bar”. A lookbehind assertion is needed to achieve this effect.

```
(?!example)bar
```

Lookbehind assertions start with (?<= for positive assertions and (?<! for negative assertions. For example, the following expression does find an occurrence of “bar” that is not preceded by “example”. The contents of a lookbehind assertion are restricted such that all the strings it matches must have a fixed length.

```
(?<!example)bar
```

However, if there are several alternatives, they do not all have to have the same fixed length. Thus (?<=bullock|donkey) is permitted, but (?<!dogs?|cats?) causes an error at compile time. Branches that match different length strings are permitted only at the top level of a lookbehind assertion. This is an extension compared with Perl 5.005, which requires all branches to match the same length of string. An assertion such as (?<=ab(c|de)) is not permitted, because its single branch can match two different lengths, but it is acceptable if rewritten to use two branches:

```
(?<=abc|abde)
```

The implementation of lookbehind assertions is, for each alternative, to temporarily move the current position back by the fixed width and then try to match. If there are insufficient characters before the current position, the match is deemed to fail.

Assertions can be nested in any combination. For example, the following expression matches an occurrence of “baz” that is preceded by “bar” which in turn is not preceded by “example”.

```
(?<=(?<!example)bar)baz
```

Assertion subpatterns are not capturing subpatterns, and might not be repeated, because it makes no sense to assert the same thing several times. If an assertion contains capturing subpatterns within it, these are always counted for the purposes of numbering the capturing subpatterns in the whole pattern. Substring capturing is carried out for positive assertions, but it does not make sense for negative assertions.

Assertions count towards the maximum of 200 parenthesized subpatterns.

Once-Only Subpatterns

With both maximizing and minimizing repetition, failure of what follows normally causes the repeated item to be re-evaluated to see if a different number of repeats allows the rest of the pattern to match. Sometimes it is useful to prevent this, either to change the nature of the match, or to cause it fail earlier than it otherwise might, when the author of the pattern knows there is no point in carrying on.

Consider, for example, the pattern `\d+example` when applied to the subject line

```
123456bar
```

After matching all 6 digits and then failing to match “example,” the normal action of the matcher is to try again with only 5 digits matching the `\d+` item, and then with 4, and so on, before ultimately failing. Once-only subpatterns provide the means for specifying that once a portion of the pattern has matched, it is not to be re-evaluated in this way, so the matcher would give up immediately on failing to match “example” the first time. The notation is another kind of special parenthesis, starting with `(?>` as in this example:

```
(?>\d+)bar
```

This kind of parenthesis “locks up” the part of the pattern it contains once it has matched, and a failure further into the pattern is prevented from backtracking into it. Backtracking past it to previous items, however, works as normal.

An alternative description is that a subpattern of this type matches the string of characters that an identical standalone pattern would match, if anchored at the current point in the subject string.

Once-only subpatterns are not capturing subpatterns. Simple cases such as the above example can be thought of as a maximizing repeat that must swallow everything it can. So, while both `\d+` and `\d+?` are prepared to adjust the number of digits they match in order to make the rest of the pattern match, `(?>\d+)` can only match an entire sequence of digits.

This construction can of course contain arbitrarily complicated subpatterns, and it can be nested.

Conditional Subpatterns

It is possible to cause the matching process to obey a subpattern conditionally or to choose between two alternative subpatterns, depending on the result of an assertion, or whether a previous capturing subpattern matched or not. The two possible forms of conditional subpattern are

```
(? (condition) yes-pattern)
(?) (condition) yes-pattern|no-pattern)
```

If the condition is satisfied, the yes-pattern is used; otherwise the no-pattern (if present) is used. If there are more than two alternatives in the subpattern, a compile-time error occurs.

There are two kinds of condition. If the text between the parentheses consists of a sequence of digits, then the condition is satisfied if the capturing subpattern of that number has previously matched. Consider the following pattern, which contains non-significant white space to make it more readable and to divide it into three parts for ease of discussion:

```
( \ ( )?      [^()]+      (?(1) \) )
```

The first part matches an optional opening parenthesis, and if that character is present, sets it as the first captured substring. The second part matches one or more characters that are not parentheses. The third part is a conditional subpattern that tests whether the first set of parentheses matched or not. If they did, that is, if subject started with an opening parenthesis, the condition is true, and so the yes-pattern is executed and a closing parenthesis is required. Otherwise, since no-pattern is not present, the subpattern matches nothing. In other words, this pattern matches a sequence of non-parentheses, optionally enclosed in parentheses.

If the condition is not a sequence of digits, it must be an assertion. This might be a positive or negative lookahead or lookbehind assertion. Consider this pattern, again containing non-significant white space, and with the two alternatives on the second line:

```
(? (?:[^a-z]*[a-z])  
 \d{2} [a-z]{3}-\d{2} |\d{2}-\d{2}-\d{2} )
```

The condition is a positive lookahead assertion that matches an optional sequence of non-letters followed by a letter. In other words, it tests for the presence of at least one letter in the subject. If a letter is found, the subject is matched against the first alternative; otherwise it is matched against the second. This pattern matches strings in one of the two forms dd-aaa-dd or dd-dd-dd, where aaa are letters and dd are digits.

Comments

The sequence `?#` marks the start of a comment which continues up to the next closing parenthesis. Nested parentheses are not permitted. The characters that make up a comment play no part in the pattern matching at all.

Performance

Certain items that might appear in patterns are more efficient than others. It is more efficient to use a character class like `[aeiou]` than a set of alternatives such as `(a|e|i|o|u)`. In general, the simplest construction that provides the required behavior is usually the most efficient. Remember that non-regular expressions are simpler constructions than regular expressions, and are thus more efficient in general. Refer to the *Blue Coat Content Policy Language Guide* for more information about non-regular expression alternatives.

Regular Expression Engine Differences From Perl

This section describes differences between the RE ENGINE and Perl 5.005.

- Normally “space” matches space, formfeed, newline, carriage return, horizontal tab, and vertical tab. Perl 5 no longer includes vertical tab in its set of white-space characters. The `\v` escape that was in the Perl documentation for a long time was never in fact recognized. However, the character itself was treated as white space at least up to 5.002. In 5.004 and 5.005 it does not match `\s`.
- RE ENGINE does not allow repeat quantifiers on lookahead assertions. Perl permits them, but they do not mean what you might think. For example, `(?!a){3}` does not assert that the next three characters are not “a”. It just asserts that the next character is not “a” three times.

- Capturing subpatterns that occur inside negative lookahead assertions are counted, but their entries in the offsets vector are never set. Perl sets its numerical variables from any such patterns that are matched before the assertion fails to match something (thereby succeeding), but only if the negative lookahead assertion contains just one branch.
- Though binary zero characters are supported in the subject string, they are not allowed in a pattern string because it is passed as a normal C string, terminated by zero. The escape sequence "\0" can be used in the pattern to represent a binary zero.
- The following Perl escape sequences are not supported: \l, \u, \L, \U, \E, \Q. In fact these are implemented by Perl's general string handling and are not part of its pattern-matching engine.
- The Perl \G assertion is not supported as it is not relevant to single pattern matches.
- RE ENGINE does not support the (?{code}) construction.
- There are at the time of writing some oddities in Perl 5.005_02 concerned with the settings of captured strings when part of a pattern is repeated. For example, matching "aba" against the pattern `/^(a(b)?) +$/` sets \$2 to the value "b", but matching "aabbaa" against `/^(aa(bb)?) +$/` leaves \$2 unset. However, if the pattern is changed to `/^(aa(b(b))?) +$/` then \$2 (and \$3) get set. In Perl 5.004 \$2 is set in both cases, and that is also true of RE ENGINE.
- Another as yet unresolved discrepancy is that in Perl 5.005_02 the pattern `/^(a)?(?(1)a|b)+$/` matches the string "a", whereas in RE ENGINE it does not. However, in both Perl and RE ENGINE `/^(a)?a/` matched against "a" leaves \$1 unset.
- RE ENGINE provides some extensions to the Perl regular expression facilities: Although lookbehind assertions must match fixed length strings, each alternative branch of a lookbehind assertion can match a different length of string. Perl 5.005 requires them all to have the same length.

Note: When regular expressions are used to match a URL, a space character matches a %20 in the request URL. However, a %20 in the regular-expression pattern will not match anything in any request URL, because "%20" is normalized to " " in the subject string before the regex match is performed.

Appendix F: Diagnostics

Blue Coat Systems has a number of resources to provide diagnostic information:

- Heartbeats: Enabled by default, Heartbeats (statistics) are a primary diagnostic tool used by Blue Coat, allowing them to proactively monitor the health of ProxySG appliances.
- Core images: Created when there is an unexpected system restarted. This stores the system state at the time of the restart, enhancing the ability for Blue Coat to determine the root cause of the restart.
- SysInfo (System Information): SysInfo provides a snapshot of statistics and events on the ProxySG.
- PCAP: An onboard packet capture utility that captures packets of Ethernet frames going in or out of a ProxySG.
- Policy trace: A policy trace can provide debugging information on policy transactions. This is helpful, even when policy is not the issue. For information on using policy tracing, refer to Appendix B: "Troubleshooting" in the *Blue Coat Content Policy Language Guide*.
- Event Logging: The event log files contain messages generated by software or hardware events encountered by the ProxySG. For information on configuring event logging, see "Event Logging and Notification" on page 698.
- Access Logging: Access logs allow for analysis of Quality of Service, content retrieved, and other troubleshooting. For information on Access Logging, see "Access Logging" on page 641.

To test connectivity, use the following commands from the enable prompt:

- `ping`: Verifies that a particular IP address exists and is responding to requests.
- `traceroute`: Traces the route from the current host to the specified destination host.
- `test http get path_to_URL`: Makes a request through the same code paths as a proxied client.
- `display path_to_URL`: Makes a direct request (bypassing the cache device).
- `show services`: Verifies the port of the Management Console configuration.
- `show policy`: Verifies if policy is controlling the Management Console.

For information on using these commands, refer to Chapter 2: "Standard and Privileged Mode Commands" in the *ProxySG Command Line Interface Reference Guide*.

Note: If you cannot access the Management Console at all, be sure that you are using HTTPS (`https://ProxySG_IP_address:8082`). This more secure option was added in SGOS 3.x. If you want to use HTTP, you must explicitly enable it before you can access the Management Console.

This appendix discusses the following topics:

- "Service Information" on page 832. This includes taking snapshots of the system.
- "Packet Capturing (the PCAP Utility)" on page 839.

- "Core Image Restart Options" on page 845.
- "Diagnostic Reporting (Heartbeats)" on page 846.

If the ProxySG does not appear to work correctly and you are unable to diagnose the problem, contact Blue Coat Technical Support.

Service Information

The service information options allow you to send service information to Blue Coat using either the Management Console or the CLI. You can select the information to send, send the information, view the status of current transactions, and cancel current transactions. You can also send service information automatically in case of a crash.

Important: You must specify a service-request number before you can send service information. See Blue Coat Technical Support at: <http://www.bluecoat.com/support/index.html> for details on opening a service request ticket.

The following list details information that you can send:

- Packet Capture
- Event Log
- Memory Core
- SYSInfo
- Access Logs (can specify multiple)
- Snapshots (can specify multiple)
- Contexts (can specify multiple)

Sending Information

To Send Information through the Management Console:

1. Select Maintenance>Service Information>Send Information.

The Send Service Information tab displays.

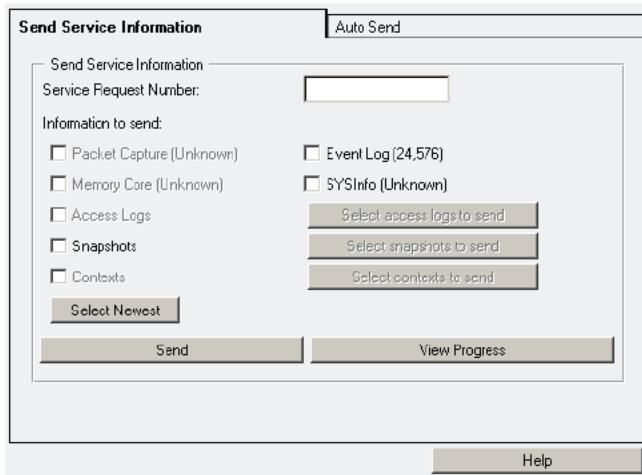


Figure F-1: Send Service Information Tab

2. Enter the service-request number that you received from a Technical Support representative (the service-request number is in the form xx-xxxxxxx or x-xxxxxxx).
3. Select the appropriate checkboxes (as indicated by a Technical Support representative) in the Information to send field.

Note: Options for items that you do not have on your system will be grayed out and you will not be able to select that checkbox.

4. (Optional) If you select Access Logs, Snapshots, or Contexts checkbox, you must also click Select access logs to send, Select snapshots to send, or Select contexts to send and complete the following steps in the corresponding dialog that appears:

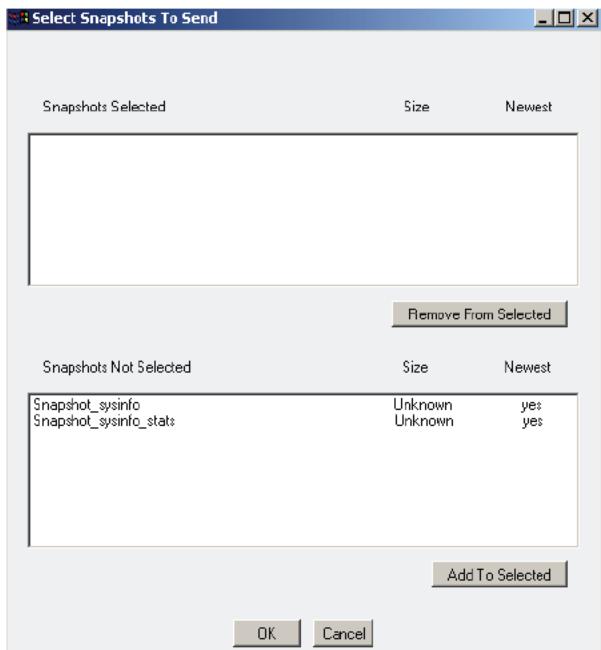


Figure F-2: Select Snapshots to Send Dialog

- To select information to send, highlight the appropriate selection in the Access Logs/Snapshots/Contexts Not Selected field and click Add to Selected.
 - To remove information from the Access Logs/Snapshots/Contexts Selected field, highlight the appropriate selection and click Remove from Selected.
 - Click Ok.
5. Click Send.
 6. Click Ok in the Information upload started dialog that appears.

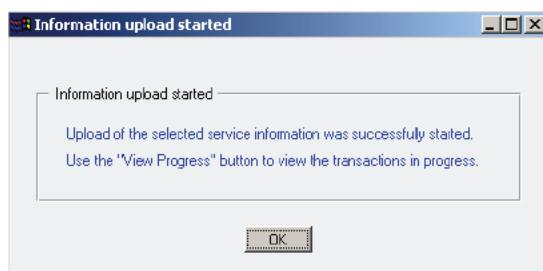


Figure F-3: Information Upload Started Dialog

7. (Optional) Click View Progress to open a window displaying the current transactions in progress; click Ok to close the window.

To Send Information through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) diagnostics
SGOS#(config diagnostics) service-info
SGOS#(config service-info) view available
SGOS#(config service-info) send sr_number one_or_more_commands_from_view_available
SGOS#(config service-info) view status
SGOS#(config service-info) cancel all | one_or_more_from_view_status
SGOS#(config service-info) exit
```

where:

cancel	all	Cancels all service information being sent to Blue Coat.
	<i>one_or_more_from_view_status</i>	Cancels certain service information items being sent to Blue Coat. These items can be chosen from the list provided by the view status command.
send	<i>sr_number</i> <i>one_or_more_commands_from_view_available</i>	Sends a specific service request and one or more commands (chosen from the list provided by the view available command) to Blue Coat.
view	available	Shows the list of service information than can be sent to Blue Coat.
	status	Shows the transfer status of service information to Blue Coat.
exit		Exits configure diagnostics service-info mode and returns to configure diagnostics mode.

Example:

```
SGOS#(config) diagnostics
SGOS#(config diagnostics) service-info
SGOS#(diagnostics service-info) view available
Service information that can be sent to Blue Coat

Name                                     Approx Size (bytes)
Event_log                                188,416
System_information                         Unknown
Snapshot_sysinfo                          Unknown
Snapshot_sysinfo_stats                    Unknown
SGOS#(diagnostics service-info) send 1-4974446 event_log system_information
snapshot_sysinfo
Sending the following reports
Event_log
System_information
Snapshot_sysinfo
SGOS#(diagnostics service-info) view status
Name                                     Transferred    Total Size    % Done
Event_log                                Transferred successfully
Snapshot_sysinfo                          Transferred successfully
Event_log                                Transferred successfully
System_information                        Transferred successfully
```

```
SGOS#(diagnostics service-info) exit
SGOS#(config diagnostics) exit
SGOS#(config)
```

Sending Service Information Automatically

Enabling automatic service information allows you to enable the transfer of relevant service information automatically whenever a crash occurs. This saves you from initiating the transfer, and increases the amount of service information that Blue Coat can use to solve the problem.

Important: A core image can contain sensitive information—for example, parts of an HTTP request or response. The transfer to Blue Coat is encrypted, and therefore secure; however, if you do not want potentially sensitive core image information to be sent to Blue Coat automatically, do not enable the automatic service information feature.

To Send Service Information Automatically through the Management Console:

1. Select Maintenance>Service Information>Send Information>Auto Send.

The Auto Send tab displays.

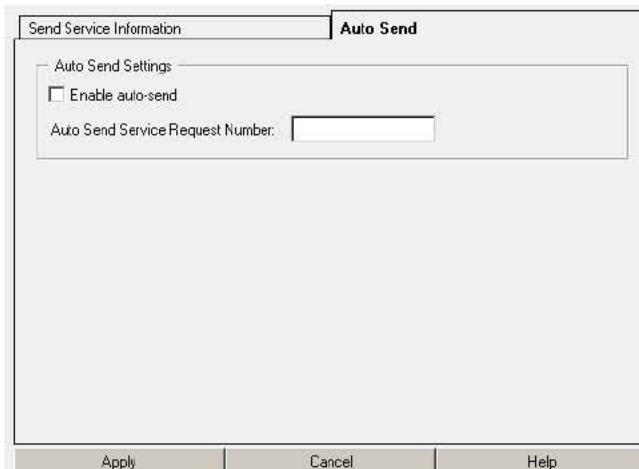


Figure F-4: Auto Send Information Tab

2. To send core image service information to Blue Coat automatically, select **Enable auto-send**.
3. Enter the service-request number for the automatic service information feature into the **Auto Send Service Request Number**.
4. Click **Apply**.

Note: To clear the service-request number, clear the **Auto Send Service Request Number** field and click **Apply**.

To Send Information Automatically through the CLI:

To enable (or disable) the automatic service information feature, enter the following commands at the (config) command prompt:

```
SGOS#(config) diagnostics
SGOS#(config diagnostics) service-info
SGOS#(diagnostics service-info) auto {enable | disable}
SGOS#(diagnostics service-info) auto sr-number sr_number
```

where:

enable	Enables the automatic service information feature.
disable	Disables the automatic service information feature.
sr-number	Sets the service-request number for the automatic service information feature.

Note: To clear the service-request number, enter the following command:

```
SGOS#(diagnostics service-info) auto no sr-number
```

Creating and Editing Snapshot Jobs

To Create a New Snapshot Job through the Management Console:

1. Select Maintenance>Service Information>Snapshots.

The Snapshots tab displays.

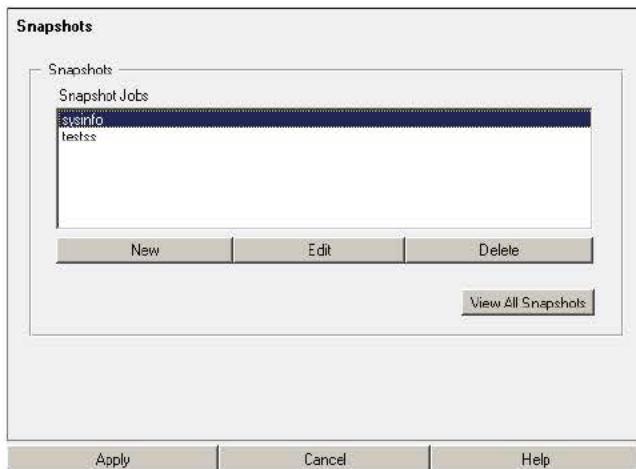


Figure F-5: Snapshots Tab

2. Click New.
3. Enter a snapshot job into the Add list item dialog that displays; click Ok.
4. Click Apply.
5. (Optional) To view snapshot job information, click View All Snapshots. Close the window that opens when you are finished viewing.

To Create a New Snapshot Job through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) diagnostics
SGOS#(config diagnostics) snapshot create snapshot_name
```

To Edit an Existing Snapshot job through the Management Console:

1. Select Maintenance>Service Information>Snapshots.

The Snapshots tab displays.

2. Select the snapshot job you want to edit (highlight it).
3. Click Edit.

The Edit Snapshot dialog displays.

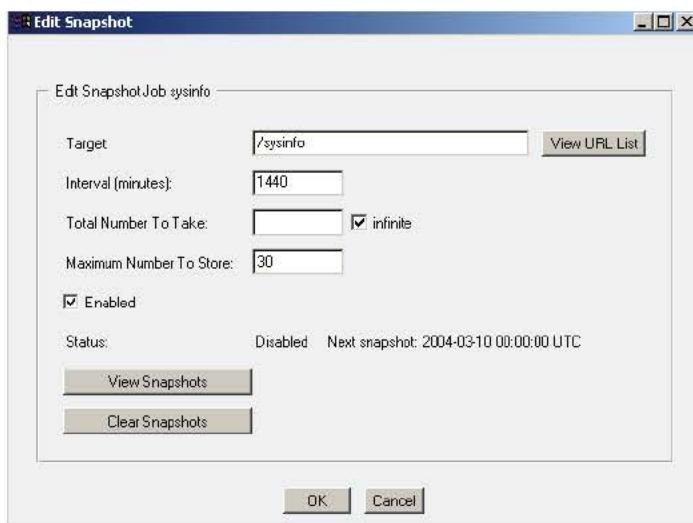


Figure F-6: Edit Snapshot Dialog

4. Enter the following information into the Edit Snapshot fields:
 - **Target:** Enter the object to snapshot.
 - **Interval (minutes):** Enter the interval between snapshot reports.
 - **Total Number To Take:** Enter the total number of snapshots to take or select the Infinite checkbox to take an infinite number of snapshots.
 - **Maximum Number To Store:** Enter the maximum number of snapshots to store.
 - **Enabled:** Check this box to enable this snapshot job or uncheck it to disable this snapshot job.
5. (Optional) Click View URL List to open a window displaying a list of URLs; close the window when you are finished viewing.
6. (Optional) Click View Snapshots to open a window displaying snapshot information; close the window when you are finished viewing.
7. (Optional) Click Clear Snapshots to clear all stored snapshot reports.

To Edit an Existing Snapshot Job through the CLI:

At the (config) command prompt, enter the following commands:

```
SGOS#(config) diagnostics
SGOS#(config diagnostics) snapshot edit snapshot_name
SGOS#(config snapshot snapshot_name) clear-reports
SGOS#(config snapshot snapshot_name) disable
SGOS#(config snapshot snapshot_name) enable
SGOS#(config snapshot snapshot_name) exit
SGOS#(config snapshot snapshot_name) interval minutes
SGOS#(config snapshot snapshot_name) keep number_to_keep (from 1 - 100)
SGOS#(config snapshot snapshot_name) take infinite | number_to_take
SGOS#(config snapshot snapshot_name) target object_to_fetch
SGOS#(config snapshot snapshot_name) view
```

where:

clear-reports	Clears all stored snapshots reports.	
disable	Disables this snapshot job.	
enable	Enables this snapshot job.	
exit	Exits configure diagnostics snapshot name mode and returns to configure diagnostics service-info mode.	
interval minutes	Specifies the interval between snapshots reports in minutes.	
keep number_to_keep (from 1 - 100)	Specifies the number of snapshot reports to keep.	
take infinite number_to_take	Specifies the number of snapshot reports to take.	
target object_to_fetch	Specifies the object to snapshot.	
view	Displays snapshot status and configuration.	

Packet Capturing (the PCAP Utility)

You can capture packets of Ethernet frames going into or leaving a ProxySG. Packet capturing allows filtering on various attributes of the frame to limit the amount of data collected. The maximum PCAP size allowed is 100MB. Any packet filters must be defined before a capture is initiated, and the current packet filter can only be modified if no capture is in progress.

The `pcap` utility captures all received packets that are either directly addressed to the ProxySG via an interface's MAC address or via an interface's broadcast address. The utility also captures transmitted packets that are sent from the ProxySG. The collected data can then be transferred to the desktop or to Blue Coat for analysis.

Note: Packet capturing increases the amount of processor usage performed in TCP/IP.

To analyze captured packet data, you must have a tool that reads Packet Sniffer Pro 1.1 files (for example, Ethereal or Packet Sniffer Pro 3.0).

PCAP File Name Format

The name of a downloaded packet capture file has the format:

`bluecoat_date_filter-expression.cap`, revealing the date and time (UTC) of the packet capture as well as any filter expressions used. Because the filter expression can contain characters that are not supported by a file system, a translation can occur. The following characters are not translated:

- Alphanumeric characters (a-z, A-Z, 0-9)
- Periods (.)

Characters that are translated are:

- Space (replaced by an underscore)
- All other characters (including the underscore and dash) are replaced by a dash followed by the ASCII equivalent; for example, a dash is translated to -2D and an ampersand (&) to -26.

Common PCAP Filter Expressions

Packet capturing allows filtering on various attributes of the frame to limit the amount of data collected. PCAP filter expressions can be defined in the Management Console or the CLI. Below are examples of filter expressions; for PCAP configuration instructions, see "Configuring Packet Capturing" on page 841.

Some common filter expressions for the Management Console and CLI are listed below. The filter uses the Berkeley Packet Filter format (BPF), which is also used by the `tcpdump` program. A few simple examples are provided below. If filters with greater complexity are required, you can find many resources on the Internet and in books that describe the BPF filter syntax.

Note: Some qualifiers must be escaped with a backslash because their identifiers are also keywords within the filter expression parser.

`ip proto protocol` where `protocol` is a number or name (icmp, udp, tcp).
`ether proto protocol` where `protocol` can be a number or name (ip, arp, rarp).

Table F.1: Common Filter Expressions

Filter Expression	Packets Captured
<code>ip host 10.25.36.47</code>	Captures packets from a specific host with IP address 10.25.36.47.
<code>not ip host 10.25.36.47</code>	Captures packets from all IP addresses except 10.25.36.47.
<code>ip host 10.25.36.47 and ip host 10.25.36.48</code>	Captures packets from two IP addresses: 10.25.36.47 and 10.25.36.48.
<code>ether host 00:e0:81:01:f8:fc</code>	Captures packets from MAC address 00:e0:81:01:f8:fc::.
<code>port 80</code>	Captures packets to port 80.
<code>ip src bluecoat.com</code>	Captures all packets that came from the host <code>bluecoat.com</code> to the ProxySG.
<code>Host example.com and tcp</code>	Captures all TCP packets sent between the host <code>example.com</code> and the ProxySG.

Using Filter Expressions in the CLI

To add a filter to the CLI, use the command:

```
SGOS#pcap filter expr parameters
```

To remove a filter, use the command:

```
SGOS#pcap filter <enter>
```

Important: Define CLI filter `expr` parameters with double-quotes to avoid confusion with special characters. For example, a space is interpreted by the CLI as an additional parameter, but the CLI accepts only one parameter for the filter expression. Enclosing the entire filter expression in quotations allows multiple spaces in the filter expression.

Configuring Packet Capturing

Use the following procedures to configure packet capturing. If a download of the captured packets is requested, packet capturing is implicitly stopped. In addition to starting and stopping packet capture, a filter expression can be configured to control which packets are captured. For information on configuring a PCAP filter, see "Common PCAP Filter Expressions" above.

Note: Requesting a packet capture download stops packet capturing.

To analyze captured packet data, you must have a tool that reads Packet Sniffer Pro 1.1 files (for example, Ethereal or Packet Sniffer Pro 3.0).

To Enable, Stop, and Download Packet Captures through the Management Console:

1. Select Maintenance>Service Information>Packet Captures.

The Packet Captures tab displays.

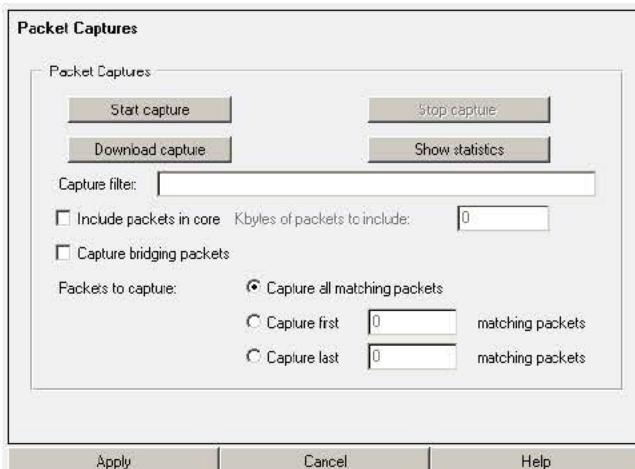


Figure F-7: Packet Captures Tab

2. To configure packet capturing, complete the following steps:

- To define or change the PCAP filter, enter the filter information into the Capture filter field. (See "Common PCAP Filter Expressions" on page 840 for information about PCAP filter expressions for this field.) To remove the filter, clear this field.
 - To specify the number of kilobytes to capture, check the Include packets in core checkbox and enter a number. You can capture packets and include them along with a core image. This is extremely useful if a certain pattern of packets causes the unit to restart unexpectedly.
 - To capture all packets, even those that are bridged, check the Capture bridging packets checkbox. Normally, the packets that are bridged from one interface to another (see "Software and Hardware Bridges" on page 68) are not included in the packet capture.
3. Choose one of the following three radio buttons:
 - Capture all matching packets
 - Capture first *n* matching packets. Enter the number of matching packets (*n*) to capture. If the number of packets reaches this limit, packet capturing stops automatically.
 - Capture last *n* matching packets. Enter the number of matching packets (*n*) to capture. Any packet received after the memory limit is reached results in the discarding of the oldest saved packet prior to saving the new packet. The saved packets in memory are written to disk when the capture is stopped.
 4. Click Apply.
 5. To start the capture, click the Start capture button. This button will be grayed out if a packet capture is already started.
 6. To stop the capture, click the Stop capture button. This button will be grayed out if a packet capture is already stopped.
 7. To download the capture, click the Download capture button. This button will be grayed out if no file is available for downloading.

To Define Packet Capturing Settings through the CLI:

1. To define PCAP filter parameters, enter the following command at the enable command prompt:

```
SGOS#pcap filter parameters
```

This captures packets according to the parameters set. If no parameters are set, all packets are captured until the `pcap stop` command is issued. See "Using Filter Expressions in the CLI" on page 841 for information about CLI filter parameters.

2. To begin capturing packets, enter the following command at the enable command prompt:

```
SGOS#pcap start {first number | last number | capsiz number (kilobytes) | trunc number}
```

where:

`first number` allows you to enter the number of matching packets (*number*) to capture. Any packet received after the memory limit is reached results in the discarding of the oldest saved packet prior to saving the new packet. The saved packets in memory are written to disk when the capture is stopped.

last *number* allows you to enter the number of matching packets (*number*) to capture. Any packet received after the memory limit is reached results in the discarding of the oldest saved packet prior to saving the new packet. The saved packets in memory are written to disk when the capture is stopped. The **last** and **first** options supersede each other.

capsize *number (kilobytes)* allows you to stop the collection after *number* kilobytes (up to 100 MB) of packets have been captured. This command prevents packet capturing from taking up too much memory and degrading performance. If no parameter is specified, the default is to capture packets until the stop directive is issued.

trunc *number* allows collecting, at most, *number* of packets from each frame.

To Enable, Stop, and Download Packet Captures through a Browser:

1. Start your Web browser.
2. Enter the URL: `https://ProxySG_IP_address:8082/PCAP/Statistics` and log on to the ProxySG as needed.

The Packet Capture Web page opens.

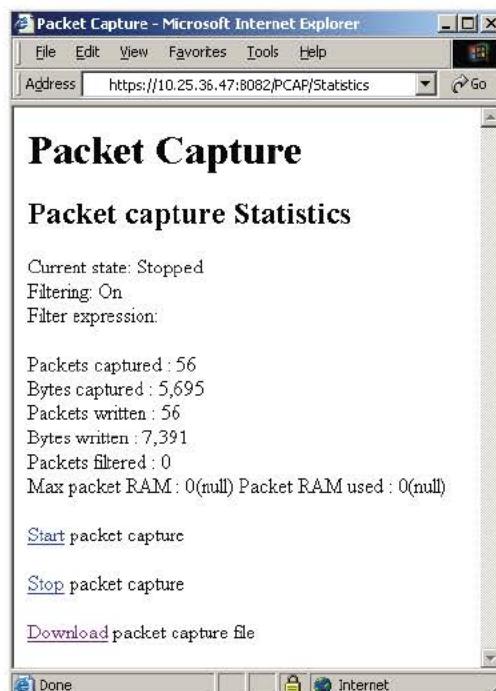


Figure F-8: Packet Capture Web Page

3. Select the desired action: Start packet capture, Stop packet capture, Download packet capture file.

You can also use the following URLs to configure these individually:

- To enable packet capturing, use this URL:
`https://ProxySG_IP_address:8082/PCAP/start`
- To stop packet capturing, use this URL:
`https://ProxySG_IP_address:8082/PCAP/stop`

- To download packet capturing data, use this URL:
`https://ProxySG_IP_address:8082/PCAP/bluecoat.cap`

Viewing Current Packet Capture Data

Use the following procedures to display current capture information from the ProxySG.

To View Current Packet Capture Data through the Management Console:

1. Select Maintenance>Service Information>Packet Captures.

The Packet Captures tab displays.

2. To view the packet capture statistics, click the Show statistics button.

A window opens displaying the statistics on the current packet capture settings. Close the window when you are finished viewing the statistics.

To View Current Packet Capture Data through the CLI:

At the enable command prompt, enter the following command:

```
SGOS#pcap info
packet capture information:
Packets captured:          12
Bytes captured:            1879
Packets written:           12
Bytes written:              2343
Max packet ram:            16384
Packet ram used:           2167
Packets filtered:          405
Bridge capture all:        Disabled
Current state:              Stopped
Filtering:                  On
Filter expression:           iface out expr ""
```

Uploading Packet Capture Data

Use the following steps to transfer packet capture data from the ProxySG to an FTP site through the CLI. You cannot use the Management Console. After uploading is complete, you can analyze the packet capture data.

To Upload Packet Captures to a Server through the CLI:

At the enable command prompt, enter the following command:

```
SGOS#pcap transfer ftp://url/path/filename.cap username password
```

Specify a username and password, if the FTP server requires these. The username and password must be recognized by the FTP server.

Core Image Restart Options

This option specifies how much detail is logged to disk when a system is restarted. Although this information is not visible to the ProxySG user, Blue Coat Technical Support uses it in resolving system problems. The more detail logged, the longer it takes the ProxySG to restart. There are three options:

- None—no system state information is logged. Not recommended.
- Context only—the state of active processes is logged to disk. This is the default.
- Full—A complete dump is logged to disk. Use only when asked to do so by Blue Coat Technical Support.

The default setting of Context only is the optimum balance between restart speed and the information needs of Blue Coat Technical Support in helping to resolve a system problem.

You can also select the number of core images that will be retained. The default value is 2; the range is between 1 and 10.

To Configure Core Image Restart Options through the Management Console:

1. Select Maintenance>Core Images.

The Core Images tab displays.

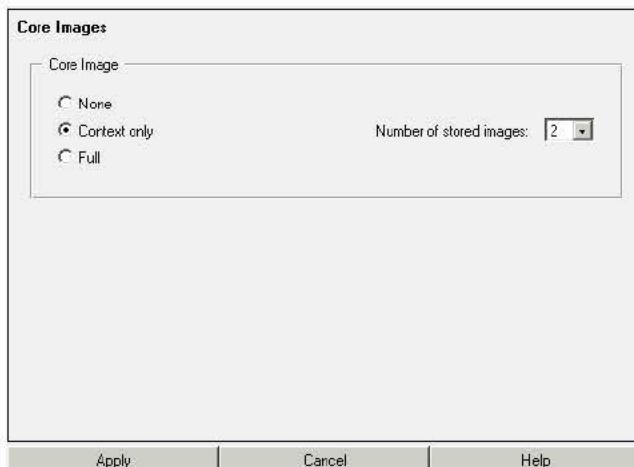


Figure F-9: Configuring Core Image Restart Options

2. Select a core image restart option.
3. (Optional) Select the number of core images that will be retained from the Number of stored images drop-down list.
4. Click Apply.

To Configure Core Image Restart Options through the CLI:

1. At the (config) command prompt, enter the following command:

```
SGOS#(config) restart core-image {context | full | none}
```

2. (Optional) To select the number of core images that will be retained, enter the following command:

```
SGOS# (config) restart core-image keep number
```

Diagnostic Reporting (Heartbeats)

The Maintenance>Heartbeats tab allows you to control whether Daily Heartbeats and/or Blue Coat Monitoring are enabled or disabled.

Heartbeats are messages that are sent once every 24 hours and contain ProxySG statistical data. Besides telling the recipient that the device is alive, heartbeats also are an indicator of the ProxySG Appliance's health. Heartbeats are commonly sent to system administrators and to Blue Coat. Heartbeats do not contain any private information; they have only aggregate statistics that can be useful for preemptively diagnosing support issues.

Blue Coat Monitoring enables Blue Coat to gather heartbeat messages to track ProxySG health in the field. These heartbeats are used by Blue Coat to fix system issues preemptively. The default setting enables the sending of emergency heartbeat messages to Blue Coat through HTTPS. If disabled, Blue Coat does not receive emergency heartbeat messages. However, even when Blue Coat Monitoring is disabled, Blue Coat can still receive heartbeat messages sent using the CLI command, send-heartbeat.

Blue Coat receives emergency heartbeats whenever a ProxySG is rebooted. Emergency heartbeats contain core dump and restart flags, in addition to daily heartbeat information.

To Change Daily Heartbeats and/or Blue Coat Monitoring through the Management Console:

1. Select Maintenance>Heartbeats.

The Heartbeats tab displays.

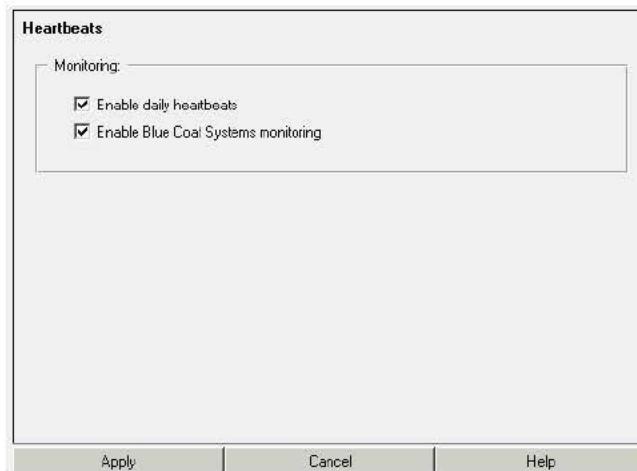


Figure F-10: Maintenance Heartbeats Tab

2. Select or deselect the Enable daily heartbeats or Enable Blue Coat monitoring.
3. Click Apply.

To Set Daily Heartbeats through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) diagnostics
SGOS# (config diagnostics) heartbeat enable
```

To Set Blue Coat Monitoring through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) diagnostics
SGOS# (config diagnostics) monitor enable
```

To Send an Immediate Heartbeat Message through the CLI:

At the (config) command prompt, enter the following command:

```
SGOS# (config) diagnostics
SGOS# (config diagnostics) send-heartbeat
```

Note: This option is not available through the Management Console.

Appendix G: Using Blue Coat Director to Manage Multiple Appliances

If you are managing multiple ProxySG Appliances, you might find it easier to use Blue Coat Systems standalone product, Blue Coat Director, than to configure and control the appliances individually.

Director allows you to configure a ProxySG and then push that configuration out to as many ProxySG Appliances as you need. Director also allows you to delegate network and content control to multiple administrators and distribute user and content policy across a Content Delivery Network (CDN). With Director, you can:

- Reduce management costs by centrally managing all Blue Coat ProxySG Appliances.
- Eliminate the need to configure each remote ProxySG manually.
- Recover from system problems with configuration snapshots and recovery.

Configuration management specifically includes:

- Configure groups of ProxySG Appliances based on locations, applications, or other factors
- Delegate ProxySG administration by access level, group, or policy
- Rapidly deploy standardized configurations using profiles
- Manage the scheduling of policy and configuration changes
- Easily schedule incremental changes to one or more ProxySG Appliances
- Create and distribute policy across a system of ProxySG Appliances
- Automatically back up configuration snapshots
- Back up ProxySG backup files
- Compare backup files from different ProxySG Appliances
- Restore configuration backups to multiple ProxySG Appliances
- Automatically distribute software licenses
- Quickly monitor ProxySG status, statistics, and configurations
- Upgrade an entire content-smart network at once

How Director Works with ProxySG

Director consists of a management node (a *domain*) and the ProxySG Appliances that you want to manage. The appliances can be added to the domain through either Director's CLI or Management Console.

Note: Do not mix ProxySG versions within a domain; errors might result if you try to push the same configuration to machines that are running different versions of SGOS.

When a ProxySG is added to the domain, you provide connection information about the ProxySG: name (meaningful to you), IP address or full hostname, username/password, authentication method and credentials, and, optionally, a description.

Only the appliances added to the domain can be managed by the domain. Multiple domains can be created.

Once added to the domain, you can manage the ProxySG either individually, through the Quick View/Edit module, or you can manage multiple appliances through the Configuration Management module.

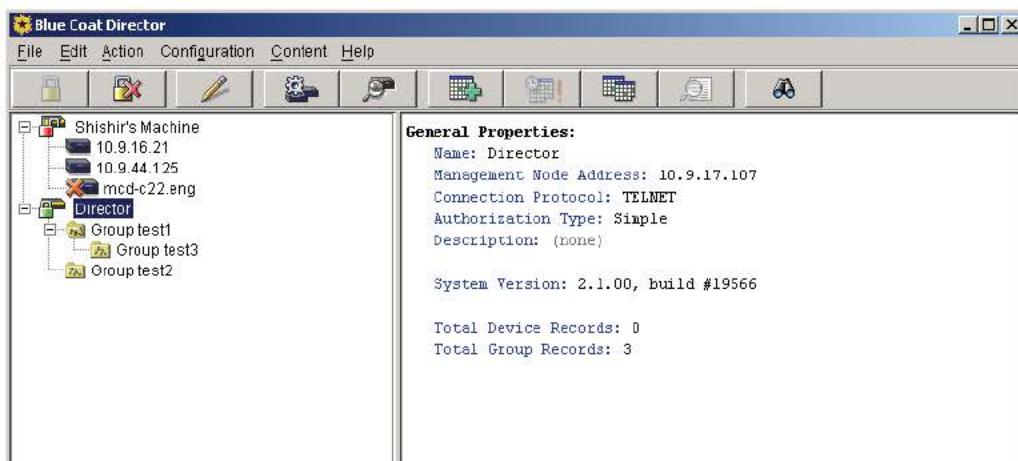


Figure G-1: Director Management Console

Communication Between Director and the ProxySG

Director and the ProxySG use SSHv2 as the default communication mode. To use SSHv1 or Telnet, you must do additional configuration on the ProxySG.

For Director to successfully manage multiple ProxySG Appliances, it must be able to communicate with a ProxySG using SSH/RSA and the Director's public key must be put on each ProxySG that Director manages. This creates a *golden profile*, meaning that the ProxySG is fully authenticated and can be used to push configurations to multiple ProxySGs using the same version of the software.

At initial set up of the ProxySG on Director, Director connects to the device using the authentication method established on the device: Telnet, SSH with simple authentication, or SSH/RSA. SSH/RSA is preferred, and must also be set up on Director before connecting to the ProxySG.

Note: You cannot connect to a ProxySG using Telnet without first enabling the Telnet-Console on the ProxySG.

Director can create an RSA keypair for a ProxySG to allow connections. However, for full functionality, Director's public key must be put on each ProxySG. You can put the key on the ProxySG two ways:

- Use Director to create and push the key.
- Use the `import-director-client-key` CLI command from the ProxySG.

Using Director to create and push client keys is the recommended method. The CLI command is provided for reference.

Complete the following steps to put Director's public key on the ProxySG using the CLI of the ProxySG. You must complete this procedure from the CLI. The Management Console is not available.

Note: For information on creating and pushing a SSH keypair on Director, refer to the *Blue Coat Director Installation Manual*.

Login to the ProxySG you want to manage from Director.

Using SGOS 2.x, Complete the Following Steps:

1. From the (config) prompt, enter SSH mode.

```
SGOS#(config) ssh
```

The prompt changes to SGOS#(config sshd)

2. Import Director's key that was previously created on Director and copied to the clipboard.

Important: You must add the Director identification at the end of the client key. The example shows the username, IP address, and MAC address of Director. "Director" (without quotes) must be the username, allowing you access to passwords in clear text.

```
SGOS#(config sshd) import director-client-key
Paste client key here, end with "..." (three periods)
1024 35
12999972424841580015120232422276923944398398687186826236351866926327873980944361
40021875567656584396224129186767257689612899184491932211183030490667098587892725
82600126521236261900215886326073496821771264041863915228768515743204386905918354
144183861502464586257447115649145443553588115604955636343894596239631
director@10.25.36.47-2.00e0.8105.d46b
...
ok
```

Using SGOS 3.x, Complete the Following Steps:

1. From the (config) prompt, enter the services>ssh-console submode:

```
SGOS#(config) services
SGOS#(config services) ssh-console
SGOS#(config services ssh-console)
```

2. Import Director's key that was previously created on Director and copied to the clipboard.

Important: You must add the Director identification at the end of the client key. The example shows the username, IP address, and MAC address of Director. "Director" (without quotes) must be the username, allowing you access to passwords in clear text.

```
SGOS#(config services ssh-console) import director-client-key
Paste client key here, end with "..." (three periods)
ssh-rsa
AAAAB3NzaC1yc2EAAAABIwAAAIEAvJIXt1ZausE9qrcXem2IK/mC4dY8Cxxo1/B8th4KvedFY33OByO
/pvwcuchPZz+b1LETTY/zc3SL7jdVffq00KBN/ir4zu7L2XT68ML20Rwa9tXFedNmK1/iagI3/QZJ8T
8zQM6o7WnBzTvMC/ZElMZZddAE3yPCv9+s2TR/Ipk=director@10.25.36.47-2.00e0.8105.d46b
...
ok
```

To View the Fingerprint of the Key:

```
SGOS#(config sshd) view director-client-key clientID
jsmith@granite.example.com 83:C0:0D:57:CC:24:36:09:C3:42:B7:86:35:AC:D6:47
```

To Delete a Key:

```
SGOS#(config sshd) delete director-client-key clientID
```

Importing VPM Policy

If you have your VPM policy stored locally and want to install it on a ProxySG, you can use SGOS inline commands to install them directly on the system. Note that VPM policy is stored in two files, vpm-cpl and vpm-xml. You must install both of them. (For more information on using VPM, see Chapter 13: “The Visual Policy Manager” on page 377.)

Note: VPM files are generally pulled from a specified ProxySG (reference device) and distributed to other ProxySG Appliances through the Director Management Console, and this is the recommended method. The procedure below is provided for reference.

For information on using VPM files with Director, refer to the *Blue Coat Director User Guide*.

Before you begin, copy the policy you are installing to the clipboard.

From the `(config)` prompt, enter the following commands:

```
SGOS#(config) inline policy vpm-cpl eof
<Proxy>
  Deny url_domain="restricted"; Rule 1 eof
ok
```

where `eof` is the string you use to indicate to the system that you are beginning or ending. It can be any string of letters, but it should not be a string you type as part of the policy.

```
SGOS#(config) inline policy vpm-xml eof
<vpmapp>
<conditionObjects>
  destination-url name="URL1" port="-1" single="true" url="restricted" />
</conditionObjects>
<layers>
  <layer layertype="com.bluecoat.sgos.vpm.WebAccessPolicyTable">
    <name>Web Access Policy (1)</name>
    <numRows>1</numRows>
    <rowItem enabled="true" num="0">
      <colItem col="0" value="1" />
      <colItem col="1" name="Any" type="String" />
```

```
<colItem col="2" name="URL1" negate="false" type="Condition" />
<colItem col="3" name="Any" type="String" />
<colItem col="4" name="Deny" type="String" />
<colItem col="5" name="Any" type="String" />
<colItem col="6" name="" type="String" />
</rowItem>
</layer>
</layers>
</vpmapp>
eof
ok
```

Director Documentation

The following documentation is available:

- *Blue Coat Director Installation Manual*
- *Blue Coat Director User Guide*
- *Blue Coat Director Content Sync Module Guide*
- *Blue Coat Director Request Management Guide*

Blue Coat Director documentation can be found at www.bluecoat.com.

Index

A

‐Admin‐ layer
 actions 216
 conditions 213
 example 216
 properties 215
access control list
 creating through the CLI 211
 creating through the Management Console 210
 restricting access with 210
access lists
 cache bypass, associating with service group 792
 cache bypass, creating 791
 creating 790
 redirection, associating with service group 791
 redirection, creating 791
 syntax 790
access logging 647, 649
 CLI default-logging command 653
 commands, facility format 645
 continuous uploading 655
 creating log file through the CLI 648
 creating/editing log formats 642
 creating/editing through Management Console 646
 custom client port number 668
 custom client, configuring through Management Console 668
 custom client, editing through CLI 668
 custom format, creating/editing 644
 custom log formats 751
 deleting log formats through CLI 646
 ELFF format, creating/editing 644
 ELFF log formats 751
 file compression, discussed 655
 filename formats 756
 FTP upload client port number 660
 FTP upload client, editing 659
 ftp-client CLI commands 661
 global settings 654
 global settings commands 655
 HTTP upload client port number 664
 HTTP upload client, configuring through CLI 665
 HTTP upload client, configuring through

Management Console 664
HTTPS upload client CLI commands 666
ICAP 342
instant messaging format 643
log file
 creating through Management Console 646
 deleting 651
 edit commands 650
 editing 648
log size, viewing statistics 678
log tail, viewing through Management Console 678
logging
 add 682
 disable 682
maximum bandwidth, setting 658
maximum log size, setting 654
NCSA common log formats 755
NCSA/common format 643
new features 26
overview 641
PASV, configuring for FTP client 661
policy, using with 682
protocol association, configuring through CLI 653
protocol association, configuring through Management Console 652
protocols, using with 652
resetting 682
scheduled uploading 655
SQUID format 643, 754
statistics
 viewing 678
 viewing through CLI 681
status statistics, viewing 679
streaming format 643
SurfControl client, configuring through Management Console 669
SurfControl client, editing through CLI 670
tail options 678
testing upload 676
upload behavior 654
upload client commands 658
upload client, configuring 655
upload client, configuring through Management

Console 656
upload client, configuring through the CLI 658
upload compression 657
upload filename, configuring through the Management Console 661, 665
upload schedule, configuring 673
upload schedule, configuring through CLI 675
upload schedule, configuring through Management Console 673
W3C format for Windows Media 520
Websense client port number 672
Websense client, editing through CLI 672
Websense upload client, editing through Management Console 671
Windows Media 520

access logging, overriding 682
access restrictions
 access control list for 210
 configuring 210
active client connections 719
active content
 and HTTPS tunneled connection 474
 definition of 474
 embed tags 476
 JavaScript 475
 object tags 476
 script tags 475
 stripping 474
 types 475
 types that can be removed or replaced 475
active content, stripping 474
Administration Access policy
 Visual Policy Manager reference 389
Administration Authentication policy
 Visual Policy Manager reference 389
administrator
 defining policies 212
 read-only and read-write access 39
 security levels 207
advanced forwarding, *see* forwarding
alternate hash table, creating 797
alternate hashing
 ProxySG example 806
 router example 806
AOL port service, creating 129
ASX rewrite
 command syntax 515
 rules 515
 setting up for Windows Media 514

attack-detection
client
 block-action, explained 89
 connection-limit, explained 89
 creating and editing 88
 failure-limit, explained 89
 global defaults 86
 global defaults, changing 87
 unblock-time, explained 89
 warning-limit, explained 89
configuration, viewing 89
mode, entering 86
overview 86
server
 add or remove server from group 91
 configuration, viewing 91
 configuring 90
 creating 90
 editing 91
 hostname, explained 91
 request-limit, explained 91
authenticate.mode
 NTLM, setting for 219
Authenticate-401 122
authentication
 configuring transparent proxy authentication 220
 definition 203
 definition of 175, 203, 233
 LDAP 242
 policies 175, 203, 233
 setting options for transparent proxy
 authentication using the CLI 222
 setting options for transparent proxy
 authentication using the Management Console 220

authentication realm
 definition of 233
 in Visual Policy Manager 398
 typical configuration 233

authorization
 definition of 175, 203, 233
 LDAP 242
 policies 175, 203, 233

B

bandwidth
 access logging, setting for 658
 statistics 715

bandwidth, refresh
 CLI, setting through 149
 discussed 148
 Management Console, setting through 148
 base DN for a group
 in Visual Policy Manager 399
BCAAA
 event messages 745
 troubleshooting 745
 viewing the event log 743
 viewing the services 744
 WIDMS, configuring for 294
 blocking pop-up windows 473
 blocking Web content 545
 Blue Coat monitoring 846
 Blue Coat Web Filter
 automatic download through CLI 558
 automatic download through Management Console 558
 configuring through Management Console 555
 dynamic real-time rating, configuring 559
 dynamic real-time rating, overview 554
 selecting dynamic real-time rating settings 561
 bridging
 about 68
 configuring
 failover 71
 failover 71
 pass-through card 68
 bridging, transparent proxy, setting up 169
 bridging
 configuring
 software bridge 69
 browser
 accessing the Management Console with 41
 proxy, configuring for 139
 setting for explicit proxies 139
 viewing policy files with 373
 browser, troubleshooting 692
 bypass list
 central 96
 central, understanding 96
 local
 installing through CLI 99
 understanding 91
 policy based, understanding 99
 bytes served 719, 731

C
CAASNT. *See BCAA*
CA-Certificates
 certificate signing request, creating through CLI 189
 creating certificate signing request 188
 error message 188
 lists, creating through Management Console 193
 lists, creating through the CLI 194
 managing 188
 troubleshooting 188
 cache bypass list, associating with service group 792
 cache bypass list, creating 791
 cached objects by size 733
 CacheOS 4.x, logs, retrieving 736
 caching
 clearing the system cache 692
 efficiency statistics 729
 freshness statistics 716
 purging the DNS cache 691
 restarting the ProxySG 687
 capturing packets. *See packet capturing*
 central bypass list 96
Central policy file
 automatic installation 371
 automatic installation, configuring the Management Console 371
 automatic installation, configuring through the CLI 371
 email notification 372
 email notification, configuring through the CLI 372
 email notification, configuring through the Management Console 372
 managing 371
 obtaining from Blue Coat Systems 367
 update interval for 372
 update interval, configuring 372
 updated, checking for 373
certificate realm
 defining properties 278
 how it works 276
 LDAP authorization, adding 278
 local authorization, adding 278
 overview 276
 policies, creating 282
 requirements 276
 results, viewing 281
 certificate signing request, creating 188

certificates
 chaining, about 183
 challenge 183, 190
 CLI, importing through 185
 commands, create certificate 189
 commands, importing certificate 185
 common name 183, 190
 country code 183, 190
 creating 180
 CSA 174
 CSA commands 192
 CSA, deleting through CLI 193
 CSA, importing 190
 deleting through CLI 188
 encryption, using for 175
 explained 174
 external, using 175
 importing 184
 importing through Management Console 185
 self-signed 174
 self-signed, creating through CLI 182
 self-signed, creating through Management Console 181
 troubleshooting 195
 wildcard, using 175
 X.509, using externally 175
challenge type, explained 217
cipher suites
 CLI, changing through 199
 SGOS, supported by 175
 working with International Step-Up 176
 working with Server Gated Cryptography 176
cipher suites shipped with ProxySG 175
CLI
 accessing 40
 changing username and passwords in 44
 configuring forwarding 598
 configuring host affinity 606
 configuring load balancing 604
 creating a default sequence 607
 creating hosts/host groups 598
 editing a host 601
 SSH client keypairs, importing in 51
 SSH, configuring host keypairs in 48
CLI configuration file, creating for ProxySG 800
client map. *see* SSL client.
commands
 access log file, creating 648
 access logging global settings 655
 access-log custom-client commands 668
 access-log format 645
 access-log ftp-client commands 661
 access-log https-client 666
 access-log upload commands 658
 access-log upload configuration 675
 access-log websense-client commands 672
 acquire-utc 56
 bypass-list local 99
 certificate realm create-realm 280
 certificate realm edit-realm 280
 certificate, importing 185
 create host-keypair 48
 create keyring 179
 create ssl-client 198
 dns alternate 83
 dns imputing 85
 dns server 83
 failover 107
 forwarding add 201
 forwarding for explicit TCP-Tunnel 134
 ftp 125
 hostname 54
 https= 201
 https-console 116, 118
 https-console, create 118
 import client-key 51
 inline policy, empty 370
 interface 140
 InterSafe content filtering, automatic downloads 566
 InterSafe content filtering, configuring 563
 ip-default-gateway 74
 keyring, import 180, 185
 keyring, view 180
 load policy 370
 load rip-settings 81
 load static-route-table 78
 load wccp-settings 102
 local database content filtering, automatic downloads 554
 local database content filtering, configuring 551
 log file, edit 650
 ntp 57
 policy 370
 policy notify 372
 policy poll-interval 372
 policy poll-now 373
 policy subscribe 371

policy trace 366
 Proventia content filtering, automatic downloads 570
 Proventia content filtering, configuring 568
 rip 81
 security allowed-access 211
 security enable-password 45
 security enforce-acl 211
 security front-panel-pin 45
 security hashed-enabled-password 45
 security hashed-front-panel 45
 security hashed-password 45
 security LDAP edit-realm 246
 security ldap realm_name membership-attribute 253
 security ldap realm_name membership-type 253
 security local view 273
 security management display-realm 45
 security management login-timeout 46
 security ntlm create-realm 237
 security ntlm edit-realm 237
 security password 45
 security radius create-realm 262
 security radius edit-realm 262
 security sequence create-realm 288
 security sequence edit realm 288
 security siteminder create-realm 294
 security siteminder edit-realm 294
 security transparent-proxy-auth 222
 security username 45
 services dns 123
 services http 127, 172
 services https 129
 services MMS 130
 services RTSP 130
 services socks-proxy 162
 services, tcp-tunnel 134
 show configuration 374
 show policy 374
 show socks-proxy 161
 SmartFilter content filtering, automatic downloads 578
 SmartFilter content filtering, configuring 575
 socks 132
 socks-proxy 161
 ssh-console 119
 ssl ccl list-name 195
 ssl ccl list-name cert-name 195
 ssl ccl list-name view 195

ssl create certificate 189
 ssl import ca-certificate 192
 ssl no ca-certificate 193
 ssl no certificate 186, 188
 ssl set cipher-suite ssl-client 199
 ssl view summary ca-certificate 195
 ssl-verify-server= 201
 static-routes 78
 SurfControl content filtering, automatic downloads 582
 SurfControl content filtering, configuring 580
 telnet-console 120
 view client-key 51
 view host-public-key 49
 virtual clear 104
 virtual ip-address 104
 virtual no address 104
 wccp 102
 Websense content filtering, automatic downloads 588
 Websense content filtering, configuring 585, 586
 common access log format 755
 community strings 706
 configuration
 archive running configuration 62
 sharing between systems 59
 configuration file
 creating with inline commands 800
 creating with text editor 801
 loading on ProxySG 801
 configuration mode, understanding 39
 CONNECT, using with origin-style redirection 220
 console account
 minimum security 207
 tab in Management Console 43
 console password, *see* password
 content filtering
 "category=" example 589
 blocking content 545
 Blue Coat Web Filter, automatic download 558
 Blue Coat Web Filter, automatic download through CLI 558
 Blue Coat Web Filter, configuring through Management Console 555
 definition of 545
 expired database, using 594
 expired license, downloading a database with 594
 InterSafe, automatic download 565, 566
 InterSafe, configuring through CLI 563

InterSafe, configuring through Management Console 561
local database, automatic download 553, 554
local database, configuring through CLI 551
local database, configuring through Management Console 550
policy with vendor categories 591
Proventia, automatic download 569, 570
Proventia, configuring through CLI 568
Proventia, configuring through Management Console 566
provider, selecting through CLI 547
provider, selecting through Management Console 546
SmartFilter, automatic download 577, 578
SmartFilter, configuring through CLI 575
SmartFilter, configuring through Management Console 572
SurfControl, automatic download 582
SurfControl, configuring through CLI 580
SurfControl, configuring through Management Console 579
Websense, automatic download 587, 588
Websense, configuring through CLI 585, 586
Websense, configuring through Management Console 583
content scanning
about 323
defined 21
ICAP service 325
policy for 324
CPL
 <Admin> layer actions 216
 <Admin> layer conditions 213
 <Admin> layer example 216
 <Admin> layer properties 215
 <Proxy> layer actions 231
 <Proxy> layer conditions 223
 <Proxy> layer properties 229
certificate realm, policies, creating 282
creating using the CLI 369
enabling ICP 636
generated by VPM 452
inline command 369
LDAP examples 257
local realm, creating policies 275
Netegrity SiteMinder policies, creating 304
NTLM policies, creating 240
policy overview 20

RADIUS policies, creating 264
unloading policy files 370
CPU utilization 715
custom client, configuring for access logging 668
custom format, creating/editing 644

D

data access pattern 731
data allocation 728
database
 creating through ProxySG 271
 local realm, setting up 268
 viewing all users 272
defaults, restoring system defaults 689
deleting a ProxySG system 698
deleting headers 476
deleting objects from the ProxySG 709
Director
 client-key importing 851
 communicating with 850
 inline commands, using 852
 ProxySG, using with 849
disk
 multi-disk ProxySG 709
 reinitialization 708
 resource use 726
 single-disk ProxySG 709
DNS
 adding alternate server through CLI 83
 adding alternate server through Management Console 83
 adding primary through Management Console 82
 cache, purging 691
 negative caching, disabling 85
 negative caching, enabling 86
 to origin content server 202
 understanding 81
DNS servers
 addresses, specifying 81
 changing name imputing order 85
 changing order 84
 changing order of 83
 name imputing 84
DNS-Proxy
 CLI, configuring through 123
 commands 123
 Management Console, configuring through 123
 overview 122

-
- resolving name list, explained 123
 - resource record, creating 124
 - document**
 - conventions 29
 - organization 27
 - domain name for a group
 - in Visual Policy Manager 399
 - domain name for a group in Visual Policy Manager 400
 - Do-Not-Fragment. See PMTU.
 - Drange multicast address, explained 106
 - dynamic bypass
 - troubleshooting 93
 - dynamic real-time rating
 - categorize dynamically in real-time 561
 - categorize dynamically in the background 561
 - configuring 559
 - do not categorize dynamically 561
 - overview 554

 - E**
 - ELFF
 - access log formats 751
 - creating/editing 644
 - embed tags 476
 - empty system 695
 - enable mode, understanding 39
 - error message, HTTPS Console 195
 - event log 734
 - configuration, viewing through CLI 703
 - contents, CLI, viewing through 703
 - event logging
 - event notification 700
 - log levels 699
 - log size 700
 - overview 698
 - event messages
 - BCAAA 745
 - exceptions
 - built-in 477
 - defining 477
 - definitions 480
 - hierarchy 481
 - installable list, about 482
 - installable list, install 484
 - user-defined 480
 - view 486

 - F**
 - failover
 - CLI, configuring through 107
 - configuring 105
 - configuring through Management Console 105
 - group secret 107
 - master 107
 - master, explained 105
 - multicast address, using 106
 - priority ranges 107
 - show failover configuration 108
 - statistics page, viewing 109, 735
 - statistics, viewing through CLI 108
 - VRRP, using with 105
 - filename formats, access logging 756
 - filtering, *see* content filtering
 - Finjan Vital Security scanning server 322
 - force-ntlm
 - enabling through CPL 157
 - enabling through VPM 157
 - forms-based authentication
 - CPL substitutions for 308
 - CPL, using with 314
 - creating through CLI 311
 - creating, tips 308
 - creating/downloading through the CLI 312
 - creating/editing form 308
 - creating/editing form through Management Console 308
 - credentials sent in cleartext 316
 - customizing through Proxy<\$emphasis 311
 - editing through CLI 312
 - installing from local file 310
 - installing from remote URL 309
 - required values 307
 - storage options, setting 313
 - storage options, setting through CLI 314
 - storage options, setting through Management

Console 313
tips/boundary conditions 315
understanding 306

forward proxy, definition 203

forwarding
configuring through the CLI 598
configuring host affinity 606
configuring load balancing 604
creating a default sequence 607
creating hosts/host groups 598
editing a host 601

hosts/host groups, creating 598

policy table 636

policy, managing with 636

using forwarding directives to create an installable list 609
fail open/closed 611
host timeout values 611

front panel password, creating 206

front panel PIN
clearing 206
creating 206

FTP
access logging, using with 652
and content scanning 323
ProxySG, configuration for 805
router configuration for 804
WCCP example 804

FTP clients, configuring 145

FTP port service
commands 125
creating 125
service defined 125

FTP proxy
configuring 140, 141
FTP clients, configuring 145

FTP upload client, editing through the Management Console 659

FTP upload client, troubleshooting 663

G

gateways
load balancing through CLI 74
load balancing through the Management Console 73
switching to secondary 73
understanding 72

gateways, using multiple default IP gateways 73

global configurations 53

global settings
syntax 789
using 789

graph scale 711

H

.htpasswd file
creating password realm database 270
loading 271
uploading 271

hash table. *see* redirection hash table

hashed passwords, *see* passwords

headers
request modification 324
response modification 324

Health check
creating forwarding 359
creating general 355
instant 359

heartbeats, configuring 846

home router
mismatch errors 807
ProxySG IP address 807
troubleshooting 806
version 1 usage 786
version 2 configuration 787
WCCP IP address 807

hot spot, working with 797

HTTP
access logging, using with 652
handoff, enabling 504
persistent timeout, setting 58
receive timeout, setting 58
scanning HTTP objects 323
timeout, configuring 58

HTTP Console
CLI, managing through 118
Management Console, managing through 117

HTTP port service
commands 127, 172
creating 126

HTTP proxy
configuring 147
profile differences table 154
profile, configuring through Management Console 154
profile, controlling 153
profile, switching through CLI 155
traffic, controlling 148

-
- HTTP redirection
 - multicast address example 803
 - multicast address router configuration 803
 - password example 804
 - ProxySG configuration 803
 - ProxySG multicast address configuration 803
 - ProxySG password example 804
 - router configuration example 802
 - router configuration for password 804
 - HTTP upload client, configuring 664
 - HTTPS
 - content filtering, using with 594
 - content scanning HTTP objects 323
 - origination 200
 - tolerant request parsing 153
 - tunneled connection 474
 - HTTPS Console
 - certificate error message 195
 - CLI, managing through 116
 - commands 116, 118
 - creating through CLI 115
 - enabling 115
 - IP address, selecting 115
 - keyring, selecting 114
 - Management Console, managing through 115
 - port service, creating 117
 - troubleshooting certificate problems 195
 - HTTPS port service
 - commands 129
 - creating 127, 200
 - HTTPS termination
 - certificates 174
 - client map 176
 - configuring 177
 - DNS resolution to origin content server 202
 - keyring, creating 178
 - offloading SSL processing 173
 - overview 25

 - I**
 - ICAP
 - access logging 342
 - configuring the ProxySG for 325
 - content scanning 323
 - definition of 322
 - Finjan Vital Security 322
 - installing 325
 - ISTags 323
 - patience pages 327, 329
 - persistent connections 323
 - sense settings 322
 - Symantec CarrierScan Server 322
 - Trend Micro InterScan VirusWall 322
 - WebWasher 322
 - ICAP server
 - defined 21
 - ICMP broadcast echo
 - configuring 110
 - ICMP Host Unreachable error message
 - error messages
 - ICMP Host Unreachable 111
 - ICMP timestamp echo
 - configuring 111
 - ICP
 - access logging, using with 652
 - creating an installable list for 629
 - enabling through CPL 636
 - hierarchy 628
 - icp_access_domain directive 631
 - icp_access_ip directive 631
 - installable list, creating through CLI 635
 - installing an ICP configuration 484
 - restricting access 631
 - identification (Ident) protocol 625
 - imputing
 - adding names through CLI 85
 - adding names through the Management Console 84
 - changing name order 85
 - changing suffix order 85
 - definition of 84
 - understanding *see also* DNS 84
 - inbound connections, rejecting 66
 - inline commands
 - creating policy with 366, 369
 - Director, using 852
 - using with forms-based authentication 312
 - installable list
 - ICP 629
 - SOCKS 622
 - instant messaging
 - access log format 643
 - access logging, using with 652
 - AOL Messenger client configuration 538
 - configuring clients 536
 - configuring proxies 534
 - creating 129

defined 22
MSN Messenger client configuration 538
protocol policies 527
proxy authentication 532
securing 527
statistics, im clients tab 542
statistics, im data tab 540
VPM 539
Yahoo Messenger client configuration 537
interface cards, CLI, configuring through 140
Internet Explorer 27
Internet Explorer, explicit proxy, using with 155
InterSafe
 automatic download 565, 566
 configuring through CLI 563
 configuring through Management Console 561
IP address, configuring with the CLI 65
IP forwarding, enabling 171

J

Java Runtime Environment 27
JavaScript 475
JRE 27

K

keyring
 commands, create 179
 commands, import 180, 185
 creating 178
 creating through CLI 179
 creating through the Management Console 178
 importing 184
 importing through the Management Console 184
 showable 179
 ssl client, associating 197
 view command 180

L

LDAP
 authentication and authorization overview 242
 authorization 251
 case-sensitive configuration 246, 256
 certificate realm, adding to 278
 configuring authentication and authorization 242
 CPL examples 257
 defining Base DNs using the CLI 250
 defining Base DNs using the Management Console 248
 defining realm authorization properties and

group information using the Management Console 251, 253
defining server properties using the CLI 239, 246, 256
defining server properties using the Management Console 244
edit-realm commands 246
group information 252
membership-attribute command 253
membership-type command 253
search boundaries 252
search user DN, boundary condition 254
searching multiple base DNs 248
SSL, enabling 246
v2/v3 support 242
virtual URL, setting up 256
licensing
 about 31
 components 31
 expiration 32
 installing 33
 trial period 32
 updating 37
 viewing 36

Lightweight Directory Access Protocol, *see* LDAP

link settings 67

load balancing

 assigning percentages 796
 gateways 73
 understanding 796
 using multiple default IP gateways 73

local database

 automatic download 553, 554
 clearing 552
 configuring through CLI 551
 configuring through Management Console 550

local realm

 certificate realm, adding to 278
 changing properties 266
 CPL, creating policies 275
 database group, creating 272
 database user, creating 272
 database users, viewing 272
 database, creating 269, 270
 database, creating through ProxySG 271
 database, populated 269
 database, setting up 268
 database, viewing user 272
 deleting groups 274

-
- deleting users 273, 274
 - groups, defined 270
 - groups, deleting 273, 274
 - hashed passwords 270
 - results, viewing 268
 - security local view 273
 - user account, enabling 272
 - user name, defined 270
 - user password, creating 272
 - users, deleting 274
 - virtual URL, setting up 267
 - local user list
 - security settings, changing 274
 - locking and unlocking ProxySG systems 697
 - log file
 - creating 646
 - deleting 651
 - editing 648
 - log format
 - troubleshooting 642
 - logging
 - event log 734
 - moving 682
 - see* access logging and event logging
 - SNMP 705
 - syslog event monitoring 702
 - login parameters 41
 - logs
 - CacheOS 4.x, retrieving 736
 - SGOS 2.x, retrieving 736
 - M**
 - maintenance diagnostics 846
 - management architecture, overview 20
 - Management Console
 - accessing 40
 - changing username and passwords in 42
 - configuring SSH 47
 - console account 43, 44
 - features 24
 - home page 41
 - HTTP Console 117
 - HTTPS Console 114
 - importing SSH client keypairs 50
 - logging in 41
 - logging out 42
 - managing 114, 121
 - SSH Console 118
 - Telnet Console 119
 - troubleshooting 692
 - menu bar in Visual Policy Manager 381
 - MIBs 705
 - Microsoft Internet Explorer 27
 - MMS
 - port service, creating 130
 - port services mms commands 130
 - modes, understanding 39
 - modifying headers 476
 - Mozilla 27
 - MSN port service, creating 129
 - multicast
 - D range address, explained 106
 - defined 491
 - failover, using with 106
 - unicast, converting by Windows Media 506
 - multicast address
 - configuring 790
 - ProxySG
 - configuration 803
 - router configuration 803
 - syntax 790
 - multicast packet reception, enabling 793
 - N**
 - name imputing, *see* imputing
 - name, configuring 53
 - NCSA, common access log format 643, 755
 - Negate option, using in Visual Policy Manager 384
 - negative caching
 - disabling for DNS responses 85
 - enabling for DNS responses 86
 - Netegrity SiteMinder
 - case-sensitive configuration 304
 - policies, creating 304
 - realm, creating through CLI 294
 - realm, creating through Management Console 293
 - Netegrity SiteMinder realm
 - agents, configuring 294
 - CLI, making general settings through 304
 - CLI, viewing through 300
 - creating 293
 - defining server properties using the CLI 302
 - display name, changing 304
 - protected resource, entering 301
 - server mode, configuring 301
 - servers, configuring 297
 - servers, editing 298

servers, editing through CLI 299
servers, editing through Management Console 297
SiteMinder agent, defining through CLI 296
SiteMinder agent, defining through Management Console 295
SSO-Only mode, enabling 301
Netscape Communicator 27
network adapter
 advanced configuration 66
 configuring with CLI 65
 link faults 68
 link settings 67
 rejecting inbound connections 66
Network Time Protocol server, *see* NTP
non-cacheable data 730
nsc file 510
NTLM
 authenticate.mode, setting 219
 authentication and authorization overview 235, 242, 258, 265, 276, 284
 configuring authentication and authorization 235, 242, 258, 265, 276, 284
 creating a realm using the CLI 237, 280
 defining realm server properties 235
 defining realm server properties using the Management Console 235, 243, 258, 265, 276, 284
 explicit proxy, using with Internet Explorer 155
 Internet Explorer, using with 155
 overview 235
 policies, creating 240
 realm sequence position 288
 single sign-on, configuring 240
 using with forms-based authentication 316
ntlm-force
 disabling 157
 enabling 157
NTP
 adding server through CLI 57
 adding server through Management Console 57
 server order, changing 58
 time server, definition of 55
 understanding 56

O

object tags 476
objects
 deleting from the ProxySG 709
 in Visual Policy Manager 386

served 718
served by size 733
optional negation syntax, using 798
origination, HTTPS 200
origin-style authentication
 origin 217
 origin-cookie 217
 origin-cookie-redirect 217
 origin-ip 217
 origin-ip-redirect 217

P

<Proxy> layer
 actions 231
 conditions 223
 properties 229
PAC file, defined 139
packet capturing
 about 839
 capturing 841
 uploading data 844
 viewing current data 844
packet redirection
 enabling 792
 excluding 793
password
 changing through CLI 44
 changing through Management Console 42
 default for 43
 hashed, encrypted 206
 HTTP redirection example 804
 security, understanding 206
 see also privileged-mode password
 with RIP 814
patience pages
 displaying 327, 329
 troubleshooting 483
PMTU
 enabled by default 111
 overview 111
policy
 bypass list 99
 changing in Visual Policy Manager 456
 configuring policy evaluation order 365
 configuring the default policy proxy setting 365
 content scanning 324
 creating using the CLI 369
 disabling 370
 disabling in Visual Policy Manager 456

-
- editing 366
 - enabling in Visual Policy Manager 456
 - example, limit access to certain Web sites 591
 - example, limit access to specified time of day 592
 - files loading 366
 - files, loading through the CLI 370
 - for maximum security 208
 - for moderate security 208
 - inline command 369
 - inline commands, using 366
 - layers in 454
 - loading in Visual Policy Manager 455
 - overview 20
 - policy editor 377
 - saving in Visual Policy Manager 455
 - source, viewing 374
 - source, viewing through CLI 374
 - statistics 375
 - statistics, viewing 375
 - tabs for in Visual Policy Manager 382
 - tracing 366
 - tracing information 375
 - unloading 370
 - unloading/disabling files through the CLI 370
 - using the CLI 369
 - vendor categories, using with 591
 - viewing through CLI 374
 - viewing with browser 373
 - Visual Policy Manager 377
 - policy evaluation order
 - configuring using the Management Console 365
 - pop-up ads, blocking 473
 - port services
 - AOL, Yahoo, MSN, creating 129
 - attributes 122
 - attributes supported 122
 - creating/editing 121
 - FTP, creating 125
 - FTP, defined 125
 - HTTP, creating 126
 - HTTPS Console, creating 115, 117
 - HTTPS, creating 127, 200
 - instant messaging protocols 129
 - MMS port services commands 130
 - MMS, creating 130
 - RTSP port services commands 130
 - RTSP, creating 130
 - SOCKS, creating 131
 - SSH Console, creating 118
 - supported 121
 - TCP-Tunnel, creating 133
 - Telnet Console
 - creating 119
 - explained 119
 - privilege (enabled) mode, understanding 39
 - privileged-mode password
 - changing through CLI 44
 - changing through Management Console 42
 - default for 43
 - prompt, Telnet, customizing for 165
 - Proventia
 - automatic download 569, 570
 - configuring through CLI 568
 - configuring through Management Console 566
 - proxies
 - CLI, setting policies through 151
 - configuring default settings using the Management Console 365
 - definition 137, 203
 - explicit, browser settings 139
 - explicit, creating 139
 - FTP, configuring 140
 - FTP, spoofing 141
 - HTTP, configuring 147
 - interface settings 140
 - Management Console, setting policies 150
 - setting up 137
 - SOCKS, configuring through CLI 161
 - SOCKS, configuring through Management Console 160
 - understanding 138
 - proxy gateway, defined 22
 - proxy server, using the ProxySG as 139
 - ProxySG
 - accessing 40
 - alternate hashing example 806
 - browsers supported 27
 - configuration file quick start 788
 - configuration file syntax 798
 - configuration file, creating 797
 - configuration file, creating with text editor 801
 - configuration file, loading 801
 - configuration file, using CLI 800
 - configuring serial number 54
 - configuring time 55
 - deleting a system 698
 - deleting a system from 698
 - deleting objects from 709

DNS server 81
enhanced security features 24
enhanced services 25
features 19
FTP example 805
home router IP address, verifying 807
HTTP configuration example 803
HTTP redirection multicast address example 803
HTTP redirection with password example 804
ICAP service configuration 325
instant messaging, AOL Messenger client configuration 538
instant messaging, configuring clients 536
instant messaging, configuring proxies 534
instant messaging, im clients tab statistics 542
instant messaging, im data tab statistics 540
instant messaging, MSN Messenger client configuration 538
instant messaging, protocol policies 527
instant messaging, proxy authentication 532
instant messaging, securing 527
instant messaging, VPM 539
instant messaging, Yahoo Messenger client configuration 537
IP address for 65
load balancing 796
locking and unlocking a system 697
managing 695
multi-disk 709
new features 22
optional negation syntax, using 798
protocols supported 26
read-only and read-write access 39, 207
realm name, changing through CLI 45
realm name, changing through Management Console 45, 46
replacing a system 695, 698
restarting 687
reverse proxy example 805
setting the default system to boot 697
single-disk 709
subnet mask for 65
system defaults 689
timeout, changing through CLI 46
upgrading 692
viewing details 695
WCCP configuration, creating 795
WCCP versions supported 785
WCCP-known caches, displaying 802

proxy-support header
disabling through CPL 157
disabling through VPM 156
Internet Explorer, using with 155
purging the DNS cache 691

Q

quick start
ProxySG, creating a configuration file 788
WCCP configuration 787
QuickTime, access logging, using with 652

R

RADIUS
case-sensitive usernames, setting 261
creating a realm using the CLI 262
defining realm server properties using the Management Console 259
policies, creating 264
read-only access in ProxySG 39, 207
read-write access in ProxySG 39, 207
real proxy 26
realm
name, changing 45
timeout, changing 46
realm banner, Telnet, customizing for 165
realm sequence
CLI, managing through 288
creating 285
Management Console, managing through 287
NTLM realm position 288
promote/demote member realms 287
results, viewing through CLI 288
virtual URL 288
RealMedia
access logging, using with 652
proxy authentication 496
realms
definition 203
promote/demote for sequence realms 287
sequence, troubleshooting 284
understanding 233
rebooting, *see* restarting 687
redirection access list, creating 791
redirection hash table
alternate, creating 797
assigning percentages 796
hot spot 797
understanding 796

-
- refresh bandwidth statistics 717
 - regular expressions
 - assertions 825
 - back references 825
 - backslash character 818
 - circumflex character 819
 - comments 828
 - definition of 815
 - details 817
 - dollar character 819
 - dot character 820
 - lowercase-sensitivity 821
 - performance 828
 - Regular Expression Engine differences 828
 - repetition 823
 - square brackets 820
 - subpatterns 822, 827
 - syntax 816
 - vertical bar character 821
 - remote max file size 647, 649
 - replacing a ProxySG system 698
 - reporting
 - event logging 698
 - syslog event monitoring 702
 - request modification 324
 - resolving name list, explained 123
 - resource use
 - disk 726
 - memory 726
 - response modification 324
 - restarting the ProxySG
 - restart options 687
 - setting the default system to boot 697
 - restoring system defaults 689
 - restricting access 210
 - reverse proxy
 - definition 203
 - ProxySG
 - configuration for 805
 - router configuration for 805
 - WCCP example 805
 - RFC-1323
 - configuring 110
 - RIP
 - configuring 78
 - definition of 78
 - installing configuration file through CLI 81
 - installing configuration file through Management Console 79
 - parameters 812
 - ProxySG-specific rip parameters 813
 - using passwords with 814
 - routing
 - bypass list 91
 - central bypass list 96
 - policy-based bypass list 99
 - static routes 74
 - routing information protocol, *see* RIP
 - RTSP
 - overview of changes 26
 - port service creating 130
 - port services commands 130
 - rules in policies
 - deleting in Visual Policy Manager 456
 - in Visual Policy Manager user interface 382
 - option menus for in Visual Policy Manager 383
 - ordering in Visual Policy Manager 452

S

- script tags 475
- security
 - console account 207
 - local user list settings, changing 274
 - policies for 208, 212
- sequences, troubleshooting 284
- serial console, defined 204
- serial console, definition 204
- serial number, configuring 54
- serial port
 - password, creating 206
- set_aut.pl script, using with .htpasswd file 271
- setup console
 - defined 204
 - password, creating 206
- SGOS 2.x, logs, retrieving 736
- shell lproxies
 - \$substitutions, using 163
- shell proxies
 - boundary conditions for 164
 - CLI commands, using 167
 - policy settings, customizing 163
 - Telnet 164
 - understanding 162
- Simple Network Management Protocol, *see* SNMP
- simultaneous connections to ProxySG, viewing 90
- SiteMinder. *See* Netegrity SiteMinder
- SmartFilter
 - automatic download 577, 578

configuring through CLI 575
configuring through Management Console 572

SNMP
community strings 706
enabling 705
MIB variables 705
MIBs 705
traps 707

SOCKS
access logging, using with 652
commands 132
creating an installable list for 622
enabling 162
gateway configuration 619
port service, creating 131
port services commands 162

SOCKS gateway
HTTP, using with SOCKS 628

SOCKS gateways
default sequence, creating 621

SOCKS proxy
bind timeout on accept value 161
CLI, configuring through 161
commands 161
connection timeout values 161
Management Console, configuring through 160
max-connection values 161
max-idle-timeout value 161
min-idle-timeout 161
show socks-proxy 161

SQUID access log format 643, 754

SSH
client, managing 49
configuring through Management Console 47
host connection, configuring 47
host keypair CLI commands 48
host keypairs, configuring through CLI 48
importing client keypairs through Management Console 50
password authentication 207
setting up 47
view client-key 51
view host-public-key 49

SSH Console
port service commands 119
port services, creating 118

SSH with RSA authentication, not controlled by policy 212

SSL
authentication/authorization services, using with 222
caching behavior, SSL client 177
caching behavior, SSL server 177
definition 203
LDAP, enabling 246
SSL certificates. *see certificates.*

ssl client
cipher suite, changing 199
CLI commands 198
explained 176
keyring, associating 197
managing 196

static routes 74
explained 74
loading 78
table, installing through CLI 78
table, installing through Management Console 75

statistics
access logging log size 678
access logging, status 679
access logging, viewing through CLI 681
active client connections 719
bandwidth gain 715
bytes served 719, 731
cache efficiency 729
cache freshness 716
cached objects by size 733
CPU utilization 715
data access pattern 731
data allocation 728
event log 734
failover page 109, 735
graph scale 711
non-cacheable data 730
objects served 718
objects served by size 733
policies 375
policy 375
refresh bandwidth 717
resource use 726
system summary 711

streaming media
access log format 643
delivery type 490
live content defined 491
multicast defined 491
prepopulating content, description 498
unicast defined 491

-
- streaming protocols, managing 130
 stripping active content 474
 subnet mask, configuring with the Management Console 65
- SurfControl**
 automatic download 582
 configuring for access logging 669
 configuring through CLI 580
 configuring through Management Console 579
 Reporter, using with SGOS3.x 581
- surrogate credentials, defined 217
- Symantec CarrierScan Server** 322
- syslog event monitoring 702
- system cache
 clearing 692
 troubleshooting 692
- system defaults, restoring 689
- system summary 711
- system time, *see* time 55
- T**
- TCP NewReno
 configuring 110
- TCP-IP
 configuration, showing 112
 ICMP broadcast echo 110
 ICMP timestamp echo 111
 overview 109
 PMTU, configuring 111
 RFC-1323 110
 TCP NewReno 110
- TCP-Tunnel
 access logging, using with 652
 commands 134
 commands, explicit 134
 explicit 133
 overview 132
 port services, creating 133
- Telnet
 banner settings, configuring through CLI 167
 banner settings, configuring through Management Console 165
 boundary conditions for Telnet shell proxy 168
 settings customizing 165
 shell proxy, creating service 165
 shell proxy, understanding 164
- Telnet Console
 commands 120
 error message 119
- port service, creating 119
 port service, explained 119
 troubleshooting 119
- time, configuring in the ProxySG 55
- timeout
 HTTP, configuring 58
 timeout, realm, changing 46
 tolerant request parsing, setting through CLI 153
 transforming active content tags 474
- transparent proxy
 CLI commands 222
 definition 203
 hardware, configuring 169
 IP forwarding 171
 IP forwarding, enabling through CLI 171
 Layer-4 switch, using with 170
 overview 138
 pass-through card, setting up 169
 service, creating 171
 software bridging, setting up 169
- transparent proxy authentication
 configuring 220
 setting options for using the CLI 222
 setting options for using the Management Console 220
- transparent redirection, using WCCP 785
- traps 707
- Trend Micro InterScan VirusWall 322
- troubleshooting
 BCAAA service 745
 browsers 692
 CA-Certificates 188
 CONNECT method 220
 explicit proxy and Internet Explorer 155
 forms-based authentication 315
 FTP upload client, upload-now command 663
 HTTPS and content filtering 594
 HTTPS Console 195
 ICMP Host Unreachable error message 111
 LDAP search user DN 254
 log format 642
 patience pages 483
 TCP_DENIED 218
 Telnet Console 119
 virtual IPs 104
 WCCP, home router mismatch 809
 XFTP users not prompted for proxy authentication 317

U

unicast
 defined 491
 handling video on demand 491
multicast, converting from by Windows Media
 506
Universal Time Coordinates, *see* UTC
UNIX
 creating a realm using the CLI 266, 277, 285
 creating a realm using the Management Console
 266
upgrade enhancements 27
upgrading
 overview 692
 system image from PC 693
 through the CLI 694
 through the Management Console 693
upload client, configuring through Management
 Console 656
username
 changing through CLI 44
 changing through Management Console 42
 default for 43
UTC time 55

V

viewing changes 794
virtual IPs
 CLI, creating through 104
 flags 108
 Management Console, creating through 103
 show virtual 104
 understanding 103
virtual URL
 LDAP set up 256
 realm sequence 288
virus scanning
 advanced configurations 341
 managing 341
 policies for in Visual Policy Manager 393
 replacing the ICAP server 342
virus, preventing 86
Visual Policy Manager
 Administration Access policy reference 389
 Administration Authentication policy reference
 389
 changing policies 456
 command reference 381
 deleting a policy 456

Director, using inline commands 852
disabling a policy 456
downloading files for 456
enabling a policy 456
files for 456
generated CPL 452
loading policies 455
menu bar 381
objects 386
overview 25, 377
policy layers 454
policy-layer tabs 382
rule options in the user interface 383
rule order in 452
rules in the user interface 382
saving policies 455
Web Access policy example 465
Web access policy reference 389, 391
Web Authentication policy example 461
Web Content policy reference 393
VRRP, failover, using with 105

W

W3C Extended Log File Format, *see* ELFF 751
WCCP
 access lists, creating 790
 alternate hash table, using 797
 alternate hashing example 806
 changes, viewing 794
 definition of 785
 examples 802
 global settings, using 789
 home router mismatch, troubleshooting 809
 home router troubleshooting 806
 hot spot, working with 797
 HTTP redirection example 802
 installing settings through CLI 102
 installing settings through Management Console
 96, 100
 interface commands, syntax 792
 interface commands, using 792
 known caches, displaying 802
 load balancing, understanding 796
 multicast address, configuring 790
 multicast packet reception, enabling 793
 optional negation syntax, explained 798
 overview 785
 packet redirection, enabling 792
 packet redirection, excluding 793

-
- ProxySG configuration for 795
 - quick start 787
 - router configuration, initial 788
 - saving changes 794
 - service group, naming 790
 - service group, setting up 789
 - settings 99
 - settings, understanding 99
 - transparent redirection, using with 785
 - version 1 overview 785
 - version 1 rules 786
 - version 2 overview 786
 - version 2 router, configuring 788
 - version 2, enabling 790
 - Web access policy
 - example in Visual Policy Manager 465
 - Visual Policy Manager reference 389, 391
 - Web access, content filtering 545
 - Web Authentication policy
 - example in Visual Policy Manager 461
 - Web Cache Control Protocol, *see* WCCP
 - Web Identity Management Systems. *See* WIDMS
 - Web interface, definition of 40
 - Websense
 - automatic download 587, 588
 - configuring through CLI 585, 586
 - configuring through Management Console 583
 - upload client, configuring 671
 - upload client, editing through CLI 672
 - WebWasher scanning server 322
 - welcome banner, Telnet, customizing for 165
 - WIDMS, overview 290
 - wildcard certificates, using 175
 - Windows Media
 - .ASX-rewrite rules 515
 - .nsc file 510
 - access logging format 520
 - access logging, using with 652
 - ASX rewrite and NTLM incompatibility 516
 - authentication limitations 495
 - HTTP handoff enabling 504
 - multicast station monitoring 510
 - multicast to unicast 506
 - Player 6.4 compatibility 514
 - prepopulating content description 498
 - setting up ASX rewrite 514
- X**
- X.509 certificates
 - using for encryption 175
 - wildcards, using with 175
 - XFTP users, not prompted for proxy authentication 317
- Y**
- Yahoo port service, creating 129