



## Online Help

Websense Content Gateway

**v7.6**

## **Websense Content Gateway Online Help**

**April, 2011**

R033011760

Copyright © 1996-2011 Yahoo, Inc., and Websense, Inc. All rights reserved.

This document contains proprietary and confidential information of Yahoo, Inc and Websense, Inc. The contents of this document may not be disclosed to third parties, copied, or duplicated in any form, in whole or in part, without prior written permission of Websense, Inc.

Websense, the Websense Logo, ThreatSeeker and the YES! Logo are registered trademarks of Websense, Inc. in the United States and/or other countries. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., and Yahoo, Inc. make no warranties with respect to this documentation and disclaim any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Traffic Server is a trademark or registered trademark of Yahoo! Inc. in the United States and other countries.

Red Hat is a registered trademark of Red Hat Software, Inc.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, Windows NT, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and in other countries.

UNIX is a registered trademark of AT&T.

All other trademarks are property of their respective owners.

### **RESTRICTED RIGHTS LEGEND**

Use, duplication, or disclosure of the technical data contained in this document by the Government is subject to restrictions as set forth in subdivision (c) (1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 52.227-7013 and/or in similar or successor clauses in the FAR, or in the DOD or NASA FAR Supplement. Unpublished rights reserved under the Copyright Laws of the United States. Contractor/manufacturer is Websense, Inc, 10240 Sorrento Valley Parkway, San Diego, CA 92121.

Portions of Websense Content Gateway include third-party technology used under license. Notices and attribution are included elsewhere in this manual.

# Contents

<b>Topic 1</b>	<b>Overview</b>	<b>1</b>
	TRITON Unified Security Center	2
	Deployment options	3
	As a Web proxy cache	3
	In a cache hierarchy	3
	In a managed cluster	3
	As an SSL server	4
	As a DNS proxy cache	4
	Components	5
	Cache	5
	RAM cache	5
	Adaptive Redirection Module	5
	Host database	5
	DNS resolver	6
	Processes	6
	Administration tools	7
	Proxy traffic analysis features	7
	Online Help	8
	Technical Support	8
<b>Topic 2</b>	<b>Getting Started</b>	<b>11</b>
	Starting Content Gateway Manager	11
	Entering your subscription key	12
	Providing system information	13
	Verifying that the proxy is processing Internet requests	14
	Using the command-line interface	14
	Starting and stopping Content Gateway on the Command Line	15
<b>Topic 3</b>	<b>Web Proxy Caching</b>	<b>17</b>
	Cache requests	17
	Ensuring cached object freshness	18
	HTTP object freshness	18
	FTP object freshness	22
	Scheduling updates to local cache content	22
	Configuring the Scheduled Update option	23
	Forcing an immediate update	24
	Pinning content in the cache	24
	Setting cache pinning rules	25
	Enabling cache pinning	25
	To cache or not to cache?	25

	Caching HTTP objects .....	25
	Client directives .....	26
	Origin server directives .....	27
	Configuration directives .....	29
	Forcing object caching .....	31
	Caching HTTP alternates .....	31
	Configuring how Content Gateway caches alternates. ....	31
	Limiting the number of alternates for an object .....	32
	Caching FTP objects. ....	32
	Disabling FTP over HTTP caching. ....	33
<b>Topic 4</b>	<b>Explicit Proxy Caching .....</b>	<b>35</b>
	Manual browser configuration .....	35
	Using a PAC file. ....	36
	Sample PAC file .....	37
	Using WPAD .....	38
	Configuring FTP clients in an explicit proxy environment .....	39
<b>Topic 5</b>	<b>Transparent Proxy and ARM .....</b>	<b>43</b>
	Enabling the ARM .....	44
	Transparent interception strategies .....	45
	Transparent interception with a Layer 4 switch .....	45
	Transparent interception with WCCP v2 devices .....	46
	Transparent interception and multicast mode .....	59
	Transparent interception with policy-based routing .....	60
	Transparent interception with software-based routing .....	60
	Interception bypass .....	61
	Dynamic bypass rules .....	62
	Static bypass rules .....	63
	Viewing the current set of bypass rules .....	64
	Connection load shedding .....	64
	Reducing DNS lookups .....	65
	IP spoofing .....	66
	IP spoofing and the flow of traffic .....	66
	Enabling IP spoofing: .....	68
<b>Topic 6</b>	<b>Clusters.....</b>	<b>69</b>
	Management clustering .....	70
	SSL Manager clustering .....	70
	Configuring SSL Manager clustering: .....	71
	Changing clustering configuration .....	72
	Adding nodes to a cluster .....	72
	Deleting nodes from a cluster .....	74

	Virtual IP failover . . . . .	74
	What are virtual IP addresses? . . . . .	75
	Enabling and disabling virtual IP addressing . . . . .	75
	Adding and editing virtual IP addresses . . . . .	76
<b>Topic 7</b>	<b>Hierarchical Caching . . . . .</b>	<b>77</b>
	HTTP cache hierarchies . . . . .	77
	Parent failover . . . . .	78
	Configuring Content Gateway to use an HTTP parent cache . . . . .	78
<b>Topic 8</b>	<b>Configuring the Cache . . . . .</b>	<b>81</b>
	Adding a cache disk after installation . . . . .	82
	Changing cache capacity . . . . .	83
	Querying cache size . . . . .	83
	Increasing cache capacity . . . . .	83
	Reducing cache capacity . . . . .	84
	Partitioning the cache . . . . .	85
	Creating cache partitions for specific protocols . . . . .	85
	Making changes to partition sizes and protocols . . . . .	85
	Partitioning the cache according to origin server or domain . . . . .	86
	Configuring cache object size limit . . . . .	87
	Clearing the cache . . . . .	87
	Changing the size of the RAM cache . . . . .	88
<b>Topic 9</b>	<b>DNS Proxy Caching . . . . .</b>	<b>91</b>
	Configuring DNS proxy caching . . . . .	92
<b>Topic 10</b>	<b>Configuring the System . . . . .</b>	<b>95</b>
	Content Gateway Manager . . . . .	95
	Starting Configure mode . . . . .	95
	Using Configure mode . . . . .	96
	Command-line interface . . . . .	99
	Configuration files . . . . .	100
	Saving and restoring configurations . . . . .	101
	Taking configuration snapshots . . . . .	101
	Restoring configuration snapshots . . . . .	102
	Deleting configuration snapshots . . . . .	102
<b>Topic 11</b>	<b>Monitoring Traffic . . . . .</b>	<b>103</b>
	Viewing statistics . . . . .	103
	Starting Monitor mode . . . . .	103
	Using Monitor mode . . . . .	104
	Viewing statistics from the command line . . . . .	106
	Working with alarms . . . . .	107

	Clearing alarms . . . . .	108
	Configuring Content Gateway to email alarms. . . . .	108
	Using a script file for alarms. . . . .	108
	Using Performance graphs . . . . .	109
	Creating reports with SSL Manager. . . . .	110
	Certificate Authorities. . . . .	110
	Incidents . . . . .	111
<b>Topic 12</b>	<b>Working With Websense Data Security . . . . .</b>	<b>113</b>
	Registering and configuring on-box Data Security . . . . .	115
	Unregistering on-box Data Security. . . . .	116
	Stopping and starting Data Security processes. . . . .	117
	Configuring the ICAP client. . . . .	117
	ICAP failover and load balancing. . . . .	118
<b>Topic 13</b>	<b>Working With Encrypted Data . . . . .</b>	<b>121</b>
	Running in explicit proxy mode. . . . .	123
	Enabling SSL Manager. . . . .	124
	Tasks. . . . .	125
	Certificates . . . . .	126
	Internal Root CA . . . . .	126
	Importing your Root CA . . . . .	127
	Creating your new Root CA . . . . .	127
	Creating a subordinate CA . . . . .	128
	Backing up your internal Root CA. . . . .	133
	Managing certificates . . . . .	134
	View a certificate . . . . .	134
	Delete a certificate. . . . .	134
	Change the allow/deny status of a certificate . . . . .	135
	Adding new certificate authorities . . . . .	135
	Backing up certificates . . . . .	136
	Restoring certificates. . . . .	136
	Decryption and Encryption. . . . .	136
	Configuring SSL Manager for inbound traffic . . . . .	136
	Configuring SSL Manager for outbound traffic . . . . .	137
	Validating certificates. . . . .	138
	Configuring validation . . . . .	139
	Bypassing verification . . . . .	141
	Keeping revocation information up to date . . . . .	141
	Certificate revocation lists. . . . .	142
	Online certification status protocol (OCSP) . . . . .	142
	Managing Web HTTPS site access . . . . .	143

---

Viewing incidents . . . . .	143
Changing the status of an incident . . . . .	145
Deleting an incident . . . . .	145
Changing the text of a message. . . . .	145
Viewing incident details . . . . .	145
Adding Web sites to the incident list . . . . .	146
Client certificates . . . . .	146
When a client certificate is requested . . . . .	146
Importing client certificates . . . . .	147
When a client certificate is always required: the hostlist . . . . .	147
Deleting client certificates. . . . .	147
Configuring SSL Manager logging . . . . .	148
How long should SSL log files be kept? . . . . .	149
How big can SSL log files grow? . . . . .	149
What fields should appear in the SSL access log files? . . . . .	149
Customizing SSL connection failure messages . . . . .	150
Certificate validation failed. . . . .	151
SSL connection failure . . . . .	151
<b>Topic 14 Security . . . . .</b>	<b>153</b>
Controlling client access to the proxy . . . . .	153
Controlling access to Content Gateway Manager . . . . .	154
Setting the administrator ID and password . . . . .	154
Creating a list of user accounts . . . . .	155
Controlling host access to Content Gateway Manager . . . . .	155
Using SSL for secure administration . . . . .	156
Filtering Rules . . . . .	156
Creating filtering rules . . . . .	157
Configuring SOCKS firewall integration. . . . .	159
Configuring the proxy to use a SOCKS firewall. . . . .	159
Setting SOCKS proxy options . . . . .	160
Setting authentication. . . . .	160
Setting SOCKS server bypass . . . . .	161
Example. . . . .	161
Using the Split DNS option . . . . .	161
Proxy user authentication. . . . .	162
Browser limitations . . . . .	164
Transparent proxy authentication settings . . . . .	165
Integrated Windows Authentication . . . . .	166
Legacy NTLM authentication. . . . .	171
LDAP authentication. . . . .	173
RADIUS authentication . . . . .	176

	Multiple realm authentication . . . . .	179
<b>Topic 15</b>	<b>Working With Log Files. . . . .</b>	<b>195</b>
	Event log files . . . . .	196
	Managing event log files . . . . .	197
	Choosing the logging directory . . . . .	197
	Controlling logging space . . . . .	197
	Event log file formats . . . . .	198
	Using standard formats . . . . .	199
	Custom format . . . . .	199
	Choosing binary or ASCII . . . . .	202
	Using logcat to convert binary logs to ASCII . . . . .	203
	Rolling event log files . . . . .	204
	Rolled log filename format . . . . .	205
	Rolling intervals . . . . .	206
	Setting log file rolling options . . . . .	206
	Splitting event log files . . . . .	207
	HTTP host log splitting . . . . .	207
	Setting log splitting options . . . . .	208
	Collating event log files . . . . .	209
	Configuring Content Gateway to be a collation server . . . . .	210
	Configuring Content Gateway to be a collation client . . . . .	210
	Using a stand-alone collator . . . . .	211
	Viewing logging statistics . . . . .	212
	Viewing log files . . . . .	213
	Example event log file entries . . . . .	214
	Squid format . . . . .	215
	Netscape examples . . . . .	216
<b>Appendix A</b>	<b>Statistics. . . . .</b>	<b>219</b>
	My Proxy . . . . .	219
	Summary . . . . .	219
	Node . . . . .	221
	Graphs . . . . .	222
	Alarms . . . . .	222
	Protocols . . . . .	222
	HTTP . . . . .	223
	FTP . . . . .	225
	Security . . . . .	225
	Integrated Windows Authentication . . . . .	226
	LDAP . . . . .	227
	Legacy NTLM . . . . .	228
	SOCKS . . . . .	228



	Data Security . . . . .	228
	Subsystems . . . . .	229
	Cache . . . . .	229
	Clustering . . . . .	230
	Logging . . . . .	231
	Networking . . . . .	231
	System . . . . .	231
	ARM . . . . .	232
	ICAP . . . . .	233
	WCCP . . . . .	233
	DNS Proxy . . . . .	235
	DNS Resolver . . . . .	235
	Virtual IP . . . . .	235
	Performance . . . . .	235
	SSL . . . . .	238
	SSL Key Data . . . . .	238
	CRL Statistics . . . . .	239
	Reports . . . . .	239
<b>Appendix B</b>	<b>Commands and Variables . . . . .</b>	<b>241</b>
	Websense Content Gateway commands . . . . .	241
	Websense Content Gateway variables . . . . .	242
	Statistics . . . . .	242
<b>Appendix C</b>	<b>Configuration Options . . . . .</b>	<b>247</b>
	My Proxy . . . . .	247
	Basic . . . . .	248
	Subscription . . . . .	252
	UI Setup . . . . .	252
	Snapshots . . . . .	255
	Logs . . . . .	256
	Protocols . . . . .	257
	HTTP . . . . .	258
	HTTP Responses . . . . .	266
	HTTP Scheduled Update . . . . .	267
	HTTPS . . . . .	268
	FTP . . . . .	269
	Content Routing . . . . .	270
	Hierarchies . . . . .	270
	Mapping and Redirection . . . . .	273
	Browser Auto-Config . . . . .	274
	Security . . . . .	275
	Connection Control . . . . .	275

	Data Security . . . . .	276
	Access Control . . . . .	276
	SOCKS . . . . .	287
	Subsystems . . . . .	289
	Cache . . . . .	289
	Logging . . . . .	291
	Networking . . . . .	294
	Connection Management . . . . .	294
	ARM . . . . .	295
	WCCP . . . . .	299
	DNS Proxy . . . . .	302
	DNS Resolver . . . . .	303
	ICAP . . . . .	304
	Virtual IP . . . . .	306
	SSL . . . . .	306
<b>Appendix D</b>	<b>Event Logging Formats . . . . .</b>	<b>309</b>
	Custom logging fields . . . . .	309
	Logging format cross-reference . . . . .	312
	Squid logging formats . . . . .	312
	Netscape Common logging formats . . . . .	313
	Netscape Extended logging formats . . . . .	313
	Netscape Extended-2 logging formats . . . . .	314
<b>Appendix E</b>	<b>Configuration Files . . . . .</b>	<b>317</b>
	Specifying URL regular expressions (url_regex) . . . . .	317
	Examples . . . . .	318
	auth.config . . . . .	319
	Format . . . . .	319
	Examples . . . . .	321
	bypass.config . . . . .	322
	Format . . . . .	323
	Dynamic deny bypass rules . . . . .	323
	Examples . . . . .	324
	cache.config . . . . .	324
	Format . . . . .	325
	Examples . . . . .	326
	filter.config . . . . .	327
	Format . . . . .	328
	Examples . . . . .	329
	hosting.config . . . . .	330
	Format . . . . .	330
	Examples . . . . .	331

ip_allow.config	332
Format	332
Examples	332
ipnat.conf	333
Format	333
Examples	333
log_hosts.config	334
Format	334
Examples	334
logs_xml.config	335
Format	335
Examples	340
WELF (WebTrends Enhanced Log Format)	342
mgmt_allow.config	342
Format	342
Examples	343
parent.config	343
Format	343
Examples	345
partition.config	346
Format	346
Examples	347
records.config	347
Format	347
Examples	347
Configuration variables	348
System variables	349
Local manager	351
Process manager	354
Virtual IP manager	354
Alarm configuration	354
ARM (transparency configuration)	355
Load shedding configuration (ARM)	358
Authentication basic realm	358
LDAP	359
RADIUS authentication	360
NTLM	362
Integrated Windows Authentication	364
Transparent authentication	365
HTTP engine	366
Parent proxy configuration	369
HTTP connection timeouts (secs)	370

Origin server connection attempts. . . . .	371
Negative response caching . . . . .	373
Proxy users variables. . . . .	373
Security . . . . .	375
Cache control. . . . .	375
Heuristic expiration. . . . .	377
Dynamic content and content negotiation. . . . .	378
Anonymous FTP password . . . . .	378
Cached FTP document lifetime. . . . .	378
FTP transfer mode. . . . .	379
Customizable user response pages . . . . .	379
FTP engine . . . . .	380
SOCKS processor . . . . .	384
Net subsystem . . . . .	384
Cluster subsystem . . . . .	385
Cache. . . . .	385
DNS. . . . .	386
DNS proxy . . . . .	387
HostDB . . . . .	387
Logging configuration. . . . .	388
URL remap rules. . . . .	393
Scheduled update configuration . . . . .	394
WCCP configuration. . . . .	394
SSL Decryption. . . . .	395
ICAP . . . . .	396
Data Security. . . . .	398
Connectivity, analysis, and boundary conditions . . . . .	398
remap.config . . . . .	401
Format . . . . .	401
Examples . . . . .	402
socks.config . . . . .	402
Format . . . . .	402
Examples . . . . .	403
splitdns.config . . . . .	404
Format . . . . .	404
Examples . . . . .	405
storage.config . . . . .	406
Format . . . . .	406
update.config . . . . .	406
Format . . . . .	407
Examples . . . . .	408
wccp.config . . . . .	408

<b>Appendix F</b>	<b>Error Messages . . . . .</b>	<b>411</b>
	Websense Content Gateway error messages . . . . .	411
	Process fatal errors . . . . .	411
	Warnings . . . . .	412
	Alarm messages . . . . .	413
	HTML messages sent to clients . . . . .	416
	Standard HTTP response messages . . . . .	419
<b>Appendix G</b>	<b>The req_ca.cnf File . . . . .</b>	<b>421</b>
<b>Appendix H</b>	<b>FAQs and Troubleshooting Tips . . . . .</b>	<b>423</b>
	Frequently Asked Questions (FAQs) . . . . .	423
	How do disk I/O errors affect the cache and what does Content Gateway do when a cache disk fails? . . . . .	423
	If a client disconnects during the time that Content Gateway is downloading a large object, is any of the object saved in the cache? . . . . .	424
	Can Content Gateway cache Java applets, JavaScript programs, or other application files like VBScript? . . . . .	424
	How do you access Content Gateway Manager if you forget the master administrator password? . . . . .	424
	How do you apply changes to the logs_xml.config file to all nodes in a cluster? . . . . .	425
	In Squid- and Netscape-format log files, what do the cache result codes mean? . . . . .	425
	What does the cqtx field record in a custom log file? . . . . .	427
	Does Content Gateway refresh entries in its host database after a certain period of time if they have not been used? . . . . .	427
	Can you improve the look of your custom response pages by using images, animated gifs, and Java applets? . . . . .	427
	How do you configure Content Gateway to serve only transparent requests? . . . . .	428
	Troubleshooting tips . . . . .	429
	The throughput statistic is inaccurate in Content Gateway Manager . . . . .	429
	You are unable to execute Content Gateway commands . . . . .	429
	You observe inconsistent behavior when one node obtains an object from another node in the cluster . . . . .	430
	Web browsers may display an error document with a data missing message . . . . .	430
	Content Gateway does not resolve any Web sites. . . . .	431
	Maximum document size exceeded message in the system log file . . . . .	431
	DrainIncomingChannel message in the system log file . . . . .	431
	No cop file message in the system log file . . . . .	432
	Warning in system log file when editing vaddrs.config (Linux) . . . . .	432
	Non transparent requests fail after enabling always_query_destination . . . . .	433
	Content Gateway is running but no log files are created . . . . .	433

	Content Gateway error indicates too many network connections . . .	434
	Low memory symptoms . . . . .	434
	Connection timeouts with the origin server . . . . .	435
	IBM Web servers do not work with Content Gateway . . . . .	435
	Content Gateway does not start (or stop) . . . . .	435
<b>Appendix I</b>	<b>Glossary . . . . .</b>	<b>437</b>
<b>Appendix J</b>	<b>Copyrights . . . . .</b>	<b>443</b>
<b>Index</b>	<b>. . . . .</b>	<b>447</b>

# 1

## Overview

Websense® Content Gateway is the Web proxy component of the Websense Web Security Gateway and Websense Web Security Gateway Anywhere solutions.

Content Gateway is a configurable, high-performance Web proxy that works in combination with Websense Web Security to protect users and networks from malicious and unwanted content by performing advanced content analysis precisely when it is needed—as the content flows through the proxy—using the results of analysis to apply appropriate Web Security policy. This on-demand analysis protects users and networks at the same time that it makes dynamic, Web 2.0 sites safe for your organization and users.

The precise application of content analysis is configured by the administrator for each Web Security Gateway deployment.

**Web proxy cache:** Content Gateway can also be configured to function as a high-performance Web proxy cache that improves network efficiency and performance by caching frequently accessed information at the edge of the network. This brings content physically closer to end users for faster delivery and reduced bandwidth usage.

**Content Gateway can be deployed:**

- ◆ *As a Web proxy cache*
- ◆ *In a cache hierarchy*
- ◆ *In a managed cluster*
- ◆ *As an SSL server*
- ◆ *As a DNS proxy cache*

In addition, Content Gateway can be configured to perform several security functions:

- ◆ Control client access to the proxy cache.
- ◆ Use different DNS servers, depending on whether it needs to resolve host names located inside or outside a firewall. This enables you to keep your internal network configuration secure while providing transparent access to external sites on the Internet.
- ◆ Ensure that clients are authenticated before they access content. Content Gateway supports Integrated Windows Authentication, legacy NTLM (NTLMSSP), LDAP, and RADIUS.

- ◆ Use the on-box Data Security policy engine or the ICAP interface to enable sites using Websense Data Security to examine outbound material such as Web postings, and either block or allow the posting based on company policy. See [Working With Websense Data Security, page 113](#).
- ◆ Control access to the Content Gateway Manager using:
  - SSL (Secure Sockets Layer) protection for encrypted, authenticated access
  - User accounts that define which users can access Content Gateway Manager and which activities they can perform (for example, view statistics only or view statistics and configure Content Gateway).
- ◆ Integrate into your firewall and control traffic through a SOCKS server.

See [Security, page 153](#).

Related topics:

[TRITON Unified Security Center, page 2](#)

[Deployment options, page 3](#)

[Components, page 5](#)

[Proxy traffic analysis features, page 7](#)

[Online Help, page 8](#)

[Technical Support, page 8](#)

---

## TRITON Unified Security Center

The **TRITON Unified Security Center** is the central configuration and management console for the TRITON Web security, Data security, and Email security modules. It also provides access to registered V-Series appliances.

At installation, the **TRITON Unified Security Center** is configured to allow full access to all TRITON modules and TRITON settings to a single administrator account: **admin**. The password for this account is set during installation.

The **TRITON - Web Security** section is used to configure Web filtering behavior, monitor Internet usage, generate Internet usage reports, and manage settings for Websense Web Security. The **Settings > Content Gateway Access** screen can be used to register instances of Content Gateway. Registered instances have an indicator of system health and provide a link to the Content Gateway Manager log on portal.

For a complete description of the **TRITON Unified Security Center**, open the **TRITON Unified Security Center** and access the embedded Help system.



---

## Deployment options

---

### As a Web proxy cache

When Content Gateway is deployed as a Web proxy cache, user requests for Web content pass through Content Gateway on their way to the destination Web server (origin server). If the Content Gateway cache contains the requested content, Content Gateway serves the content directly. If the Content Gateway cache does not have the requested content, Content Gateway acts as a proxy, fetching the content from the origin server on the user's behalf, while keeping a copy to satisfy future requests.

Content Gateway provides the following proxy caching options:

- ◆ *Explicit proxy caching*, where the user's client software must be configured to send requests directly to Content Gateway. See [Explicit Proxy Caching, page 35](#).
- ◆ *Transparent proxy caching*, where user requests are invisibly routed through the Content Gateway cache on their way to the destination server. Users request Internet content as usual, without any browser configuration, and Content Gateway serves their requests. The user's client software (typically a browser) is unaware that it is communicating with a proxy. See [Transparent Proxy and ARM, page 43](#).

### In a cache hierarchy

Websense Content Gateway can participate in flexible cache hierarchies, where Internet requests not fulfilled in one cache can be routed to other regional caches, taking advantage of their contents and proximity. In a hierarchy of proxy servers, Content Gateway can act either as a parent or child cache, either to other Content Gateway systems or to other caching products. See [Hierarchical Caching, page 77](#).

### In a managed cluster

Websense Content Gateway scales from a single node to multiple nodes, forming a managed cluster that improves system capacity, performance, and reliability.

- ◆ A managed cluster detects the addition and removal of nodes.
- ◆ Cluster nodes automatically share configuration information, allowing members of the cluster to all be administered at the same time.
- ◆ When SSL Manager is enabled, SSL configuration information is also propagated around the cluster. However, the mechanism used to synchronize information is different from that used by other information.

If the virtual IP failover option is enabled, Content Gateway maintains a pool of virtual IP addresses that it assigns to the nodes of the cluster. Content Gateway can detect hard node failures (such as power supply or CPU failures) and reassign IP addresses of the failed node to the operational nodes. See [Virtual IP failover, page 74](#), for details.

If Content Gateway is configured as a transparent proxy with WCCP, failover is handled by WCCP and virtual IP failover should not be used. See [WCCP load distribution](#), page 48.

For complete information, see [Clusters](#), page 69.

## As an SSL server

If SSL Manager is enabled, HTTPS data is decrypted, inspected, and then re-encrypted as it travels to and from the client and origin server.

Content Gateway does not cache HTTPS data.

SSL Manager includes a complete set of certificate-handling capabilities. See [Working With Encrypted Data](#), page 121.



### Important

Even when SSL Manager is **not** enabled and HTTPS is not decrypted, Content Gateway performs HTTPS URL filtering. This means that for every HTTPS request, a URL lookup is performed and policy is applied.

In explicit proxy mode, when SSL is turned off, Content Gateway performs URL filtering based on the Host name in the request. If the site is blocked, Content Gateway serves a block page. Note that some browsers do not support display of the block page. To disable this feature, configure clients to not send HTTPS requests to the proxy.

In transparent proxy mode, when SSL is turned off, Content Gateway performs URL filtering based on the common name present in the certificate from the origin server. If the site is blocked, the connection with the client is dropped; no block page is served. To disable this feature when used with WCCP, do not create a service group for HTTPS.

---

## As a DNS proxy cache

As a DNS proxy cache, Content Gateway can resolve DNS requests for clients. This offloads remote DNS servers and reduces response times for DNS lookups. See [DNS Proxy Caching](#), page 91.

---

## Components

---

### Cache

The *cache* consists of a high-speed object database called the object store. The object store indexes objects according to URLs and associated headers. The object store can cache alternate versions of the same object, varying on spoken language or encoding type, and can store small and large documents, minimizing wasted space. When the cache is full, the proxy removes stale data, ensuring that frequently requested objects are fresh.

Content Gateway tolerates disk failure on any cache disk. If the disk fails completely, Content Gateway marks the disk as corrupt and continues using the remaining disks. If all cache disks fail, Content Gateway goes into proxy-only mode.

You can partition the cache to reserve disk space for storing data for specific protocols and origin servers. See [Configuring the Cache](#), page 81.

### RAM cache

Content Gateway maintains a small RAM memory cache of extremely popular objects. This RAM cache serves the most popular objects quickly and reduces load on disks, especially during traffic peaks. You can configure the RAM cache size. See [Changing the size of the RAM cache](#), page 88.

### Adaptive Redirection Module

The Adaptive Redirection Module (ARM) is used in transparent proxy caching to redirect user requests destined for an origin server to the proxy. Before the traffic is redirected by the ARM, it is intercepted by a Layer 4 switch or router.

To redirect user requests to the proxy, the ARM changes an incoming packet's address. The packet's destination IP address is changed to the IP address of the proxy, and the packet's destination port is changed according to the protocol used. For example, for HTTP, the packet's destination port is changed to the proxy's HTTP port (usually 8080).

The ARM supports automatic bypass of sites that do not function properly with proxy caches.

The ARM also prevents client request overloads. When there are more client connections than the specified limit, the ARM forwards incoming requests directly to the origin server. See [Connection load shedding](#), page 64.

### Host database

The host database stores the Domain Name Server (DNS) entries of origin servers to which the proxy connects. Among other information, the host database tracks:

- ◆ DNS information (for fast conversion of host names to IP addresses)
- ◆ The HTTP version of each host (so advanced protocol features can be used with hosts running modern servers)
- ◆ Host reliability and availability information (to avoid waits for non-functional servers)

## DNS resolver

For transparent proxy deployments, the proxy includes an asynchronous DNS resolver to streamline conversion of host names to IP addresses. Content Gateway implements the DNS resolver natively, directly issuing DNS command packets, rather than relying on resolver libraries. Many DNS queries can be issued in parallel and a fast DNS cache maintains popular bindings in memory, reducing DNS traffic.



### Important

Should the Linux system DNS server configuration change (/etc/resolv.conf), you must restart Content Gateway.

## Processes

Content Gateway has 5 primary processes:

Process name	Description
content_gateway	Accepts connections, processes protocol requests, and serves documents from the cache or origin server.
content_manager	<p>Launches, monitors, and reconfigures the <b>content_gateway</b> process.</p> <p>The <b>content_manager</b> process is also responsible for the Content Gateway Manager user interface, the proxy auto-configuration port, the statistics interface, cluster administration, and virtual IP failover.</p> <p>If the <b>content_manager</b> process detects a <b>content_gateway</b> process failure, it restarts the process and also maintains a connection queue of all incoming requests. Incoming connections that arrive in the several seconds before server restart are saved in the connection queue and processed in sequence. This connection queueing shields users from server restart downtime.</p>
content_cop	<p>Monitors the health of <b>content_gateway</b> and <b>content_manager</b>.</p> <p>The <b>content_cop</b> process periodically (several times each minute) queries <b>content_gateway</b> and <b>content_manager</b> by issuing heartbeat requests to fetch synthetic Web pages. If no response is received within the timeout interval or if an incorrect response is received, <b>content_cop</b> restarts <b>content_manager</b> and <b>content_gateway</b>.</p>

Process name	Description
analytics_server	Manages the requests made and processes spawned for Content Classification Analytics.
download_service	Periodically runs to check the Websense Database Download Service for updates.

## Administration tools

Related topics:

[Content Gateway Manager, page 95](#)

[Command-line interface, page 99](#)

[Configuration files, page 100](#)

Websense Content Gateway provides 3 modes of administration:

- ◆ *Content Gateway Manager* is a Web-based interface accessible through a browser. Content Gateway Manager provides graphs and statistical displays for monitoring Content Gateway performance and network traffic, and options for configuring and fine-tuning the proxy. Content Gateway Manager offers password-protected, SSL-encrypted, single-point administration for an entire Content Gateway cluster. This is the recommended administration mode.
- ◆ A *command-line interface* enables you to monitor Content Gateway performance and network traffic, and configure the proxy. You can execute individual commands or script a series of commands in a shell.
- ◆ *Configuration files* allow administration through a file-editing and signal-handling interface. You can change configuration options by editing configuration files instead of using Content Gateway Manager or the command-line interface. Any changes you make through Content Gateway Manager or the command-line interface are automatically made to the configuration files.

## Proxy traffic analysis features

Content Gateway provides options for network traffic analysis and monitoring:

- ◆ *Manager statistics and graphs* show network traffic information. View graphs and statistics from Content Gateway Manager, or collect and process statistics using the command-line interface.
- ◆ A variety of *Performance* graphs show historical information about virtual memory usage, client connections, document hit rates, and so on. View *Performance* graphs in the Content Gateway Manager.
- ◆ *Manager alarms* are presented in Content Gateway Manager. Content Gateway signals an alarm for any detected failure condition. You can configure Content Gateway to send email or page support personnel when an alarm occurs.

Content Gateway also sends select alarms to TRITON - Web Security, where they are referred to as **alerts**. Summary alert messages are displayed on the TRITON - Web Security **Status > Today** page. The full alert message is displayed on the **Alerts** page. TRITON - Web Security administrators can configure which Content Gateway conditions cause alert messages to be sent, and which methods (email, pop-up, or SNMP) are used to send the alert.

- ◆ *Transaction logging* lets you record information in a log file about every request the proxy receives and every error it detects. Use the logs to determine how many people use the proxy, how much information each person requested, and which pages are most popular. You can see why a transaction was in error and see the state of the proxy cache at a particular time. For example, you can see that Content Gateway was restarted or that cluster communication timed out.

Content Gateway supports several standard log file formats, such as Squid and Netscape, and its own custom format. You can analyze the standard format log files with off-the-shelf analysis packages. To help with log file analysis, separate log files so that they contain information specific to protocol or hosts.

For traffic analysis options, see [Monitoring Traffic, page 103](#). For logging options, see [Working With Log Files, page 195](#).

## Online Help ---

Click on **Get Help!** on any page in Content Gateway Manager to get detailed information about using the product.



### Important

Default Microsoft Internet Explorer settings may block operation of the Help system. If a security alert appears, select **Allow Blocked Content** to display Help.

If your organization's security standards permit, you can permanently disable the warning message on the Advanced tab of the **Tools > Internet Options** interface. (Check **Allow active content to run in files on My Computer** under Security options.)

To access a PDF version of online help, or to access [Release Notes](#), installation and deployment information, FAQs, tips, and other technical information, go to the [Websense Technical Library](#).

## Technical Support ---

Technical information about Websense products is available 24 hours a day at:

<http://support.websense.com>

In the Support site you will find:

- ◆ tips
- ◆ Customer Forums
- ◆ latest release information
- ◆ searchable Websense Knowledge Base
- ◆ latest hotfixes and patches
- ◆ Show-Me tutorials and videos
- ◆ product documents
- ◆ Technical Library
- ◆ answers to frequently asked questions
- ◆ in-depth technical papers
- ◆ Monthly Support Webinars
- ◆ Technical Alerts
- ◆ Most Popular Solutions

The Websense Support site offers access to all technical resources, including opening a case through the Service Request portal.





# 2

## Getting Started

After you have installed Content Gateway on your system or all of the nodes in your cluster, the proxy is ready for use.

Refer to the following procedures to get started:

- ◆ [Starting Content Gateway Manager, page 11](#)
- ◆ [Entering your subscription key, page 12](#)
- ◆ [Verifying that the proxy is processing Internet requests, page 14](#)
- ◆ [Using the command-line interface, page 14](#)
- ◆ [Starting and stopping Content Gateway on the Command Line, page 15](#)

### Starting Content Gateway Manager

---

Content Gateway Manager is the management user interface to Websense Content Gateway.

Content Gateway Manager is supported on Microsoft Internet Explorer 7 and greater, and on Firefox 3 and greater. Use of other browsers and versions may result in unexpected behavior. Java and JavaScript must be enabled in your browser. See your browser documentation for information on enabling Java and JavaScript.

There are 3 ways to access Content Gateway Manager:

- ◆ From the Content Gateway button in TRITON - Web Security
- ◆ By entering the IP address and port of the Content Gateway host system in your browser
- ◆ When Content Gateway is a module on a V-Series appliance, by opening the V-Series Logon portal and clicking the Content Gateway button.

#### **To access Content Gateway Manager directly:**

1. Open your Web browser.
2. Enter the following location in your browser:

`https://nodename:adminport`

where *nodename* is the IP address and *adminport* is the number assigned to the Content Gateway Manager port (default: 8081).

For more information on using HTTPS to start Content Gateway Manager, see [Using SSL for secure administration](#), page 156.

3. Log on to Content Gateway Manager with the administrator ID (default: admin) and password, or your user account.

The Content Gateway Manager password is set during installation.

You can change the ID and password, as well as create and modify user accounts. See [Controlling access to Content Gateway Manager](#), page 154.

Content Gateway Manager opens to the **Monitor > My Proxy > Summary** page. This page provides information on the features of your subscription and details of your Content Gateway system. See [Viewing statistics](#), page 103, for additional information on the Monitor tab and [Configuring the System](#), page 95 for information on the configuration options in Content Gateway Manager.

#### **Installing the content\_gateway\_ca.cer certificate:**

If you receive a message indicating that Content Gateway Manager is finding an unrecognized or invalid certificate, install the **content\_gateway\_ca.cer** certificate provided by Websense. It is located in the **/home/Websense** directory.

Use the **Configure > SSL > Certificates > Add Root CA** page to import this certificate.

1. Browse to **/home/Websense**, and select **content\_gateway\_ca.cer**.
2. Click **Open**.
3. Click **Add Certificate Authority**.

## Entering your subscription key

---

Related topic:

[Providing system information](#), page 13

When Content Gateway is deployed with Web Security Gateway or Web Security Gateway Anywhere, there is no need to enter your subscription key in Content

Gateway Manager. The key is shared automatically when it is specified in TRITON – Web Security.

**Note**

The TRITON - Web Security instance that is used is determined by the Policy Server that is configured. The configured Policy Server IP address is shown in Content Gateway Manager on the **Monitor > My Proxy > Summary** page when the **More Details** view is selected.

To configure Policy Server:

- ◆ On a V-Series appliance, in Appliance Manager go to **Configuration > Web Security Components**.
- ◆ On a software install, edit `/opt/WCG/websense.ini` and set the value of **PolicyServerIP**. Then stop and start Content Gateway processes:

```
/opt/WCG/WCGAdmin stop
```

```
/opt/WCG/WCGAdmin start
```

When Content Gateway is deployed with only Websense Data Security you must enter your subscription key in Content Gateway Manager.

1. On the **Configure > My Proxy > Subscription > Subscription Management** tab, enter the subscription key that Websense provided to you.
2. Click **Apply**.
3. Click **Restart** on **Configure > My Proxy > Basic > General** page.

---

## Providing system information

If Content Gateway is the proxy integration for Websense Web security (Web Security Gateway or Web Security Gateway Anywhere), the IP address and port to the Policy Server and Filtering Service were specified during installation.

1. Select the **Configure > My Proxy > Subscription > Scanning** tab. Notice the IP address and port for the Filtering Service. This is the information that you entered when you installed the filtering product.

**Note**

The Scanning tab appears only if you have subscribed to Web Security Gateway or Web Security Gateway Anywhere.

2. Select the appropriate check box to permit or block traffic if communication with Policy Server or Filtering Service fails.

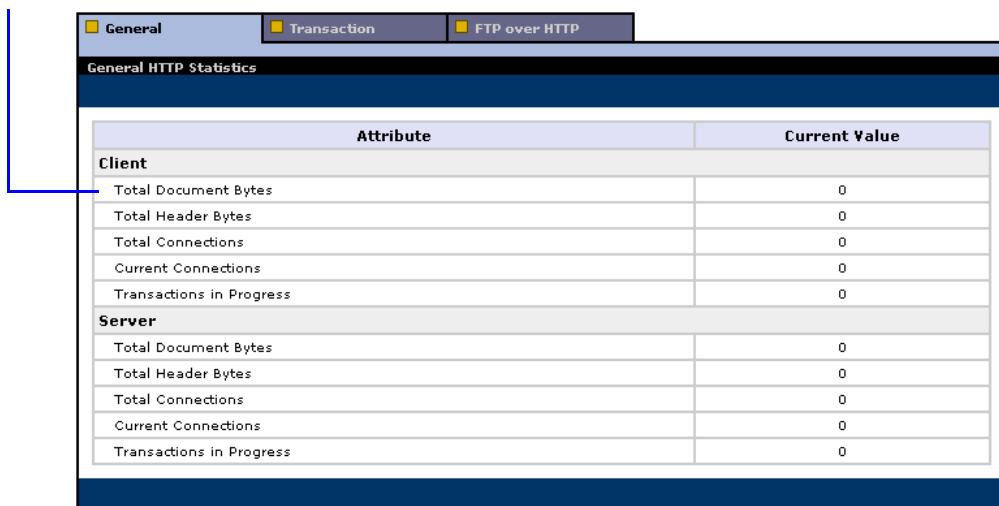
3. Click **Apply**.

## Verifying that the proxy is processing Internet requests

After you have installed the proxy, verify that it is processing requests for Web content.

1. Open Content Gateway Manager. See [Starting Content Gateway Manager](#), page 11.
2. Navigate to the **Monitor > My Proxy > Summary** page to view subscription detail, scanning data file status, and node details, including the number of objects served, the hit rate, and other basic proxy service information.
3. Navigate to **Monitor > Protocol > HTTP > General** to display the General HTTP Statistics table.
4. Note the current **Total Document Bytes** statistic in the **Client** section of the table.

Check the value of this statistic.



General HTTP Statistics		
Attribute		
		Current Value
<b>Client</b>		
Total Document Bytes		0
Total Header Bytes		0
Total Connections		0
Current Connections		0
Transactions in Progress		0
<b>Server</b>		
Total Document Bytes		0
Total Header Bytes		0
Total Connections		0
Current Connections		0
Transactions in Progress		0

4. Set your browser to the proxy port.
5. Browse the Internet.
6. Recheck the **Total Document Bytes** statistic.

This value increases as the proxy processes HTTP requests.

## Using the command-line interface

The command-line interface provides a quick way to view proxy statistics and configure Content Gateway if you do not have access to a browser or if you prefer to use a UNIX shell-like command interface.

You can execute individual commands or script multiple commands in a shell. See [Websense Content Gateway commands](#), page 241.

1. Become root:

```
su
```

2. Change to the Content Gateway **bin** directory (/opt/WCG/bin). Run Content Gateway commands from this directory.

Commands take the form:

```
content_line -command argument
```

3. For a list of **content\_line** commands, enter:

```
content_line -h
```

**Note**

If the Content Gateway **bin** directory is not in your path, prepend the command with: `./`

For example:

```
./content_line -h
```

---

## Starting and stopping Content Gateway on the Command Line

---

To stop or start Content Gateway from the command line:

1. Become root:

```
su
```

2. Change to the Content Gateway installation directory (/opt/WCG).

To start the proxy:

```
./WCGAdmin start
```

To stop the proxy

```
./WCGAdmin stop
```

To restart the proxy

```
./WCGAdmin restart
```

To see what Content Gateway services are running:

```
./WCGAdmin status
```

**Note**

Always use the `./WCGAdmin stop` command to stop Content Gateway from the command line.

---

After you have installed Content Gateway, open Content Gateway Manager (the management interface) to verify that the proxy is running. See [Starting Content Gateway Manager](#), page 11 and [Verifying that the proxy is processing Internet requests](#), page 14.

# 3

## Web Proxy Caching

Web proxy caching stores copies of frequently accessed Web objects (such as documents, images, and articles) close to users and serves this information to them. Internet users get their information faster, and Internet bandwidth is freed for other tasks.

Internet users direct their requests to Web servers all over the Internet. For a caching server to serve these requests, it must act as a Web proxy server. A Web proxy server receives user requests for Web objects and either serves the requests or forwards them to the *origin server* (the Web server that contains the original copy of the requested information).

Content Gateway supports both *transparent proxy caching*, where the user's client software (typically a browser) is unaware that it is communicating with a proxy, and *explicit proxy caching*, where the user's client software must be configured to send requests directly to the proxy.

### Cache requests

---

#### Related topics:

[Ensuring cached object freshness, page 18](#)  
[Scheduling updates to local cache content, page 22](#)  
[Pinning content in the cache, page 24](#)  
[To cache or not to cache?, page 25](#)  
[Caching HTTP objects, page 25](#)  
[Forcing object caching, page 31](#)  
[Caching HTTP alternates, page 31](#)  
[Caching FTP objects, page 32](#)

The following overview illustrates how Content Gateway serves a user request.

1. Content Gateway receives a user request for a document, image, news article, or other Web object.
2. Using the object address, the proxy tries to locate the requested object in its object database (cache).

3. If the object is in the cache, the proxy checks to see if the object is fresh enough to serve (see [Ensuring cached object freshness](#), page 18). If the object is fresh, the proxy serves it to the user as a *cache hit*.
4. If the data in the cache is stale, the proxy connects to the origin server and asks if the object is still fresh (a revalidation). If the object is still fresh, the proxy sends the cached copy to the user immediately.
5. If the object is not in the cache (a cache miss) or the server indicates that the cached copy is no longer valid, the proxy obtains the object from the origin server, simultaneously streaming it to the user and the cache. Subsequent requests for the object will be served faster because the object will come directly from the cache.

## Ensuring cached object freshness

---

When Content Gateway receives a request for a Web object, it tries to locate the requested object in its cache. If the object is in the cache, the proxy checks to see if the object is fresh enough to serve.

The protocol determines how the proxy handles object freshness in the cache:

- ◆ HTTP objects support author-specified expiration dates. The proxy adheres to these expiration dates; otherwise, it picks an expiration date based on how frequently the object is changing and on administrator-chosen freshness guidelines. In addition, objects can be revalidated, checking with the origin server if an object is still fresh. See [HTTP object freshness](#), page 18.
- ◆ FTP objects stay in the cache for a specified time period. See [FTP object freshness](#), page 22.

## HTTP object freshness

Content Gateway determines whether an HTTP object in the cache is fresh by:

- ◆ Checking the **Expires** or **max-age** header  
Some HTTP objects contain **Expires** headers or **max-age** headers that define how long the object can be cached. Comparing the current time with the expiration time tells the proxy whether or not the object is fresh.
- ◆ Checking the **Last-Modified** / **Date** headers

If an HTTP object has no **Expires** header or **max-age** header, the proxy can calculate a freshness limit using the following formula:

$$\text{freshness\_limit} = (\text{date} - \text{last\_modified}) * 0.10$$

where *date* is the date in the object's server response header, and *last\_modified* is the date in the **Last-Modified** header. If there is no **Last-Modified** header, the proxy uses the date that the object was written to cache. You can increase or reduce the value 0.10 (10 percent). See [Modifying the aging factor for freshness computations](#), page 19.

The computed freshness limit is bound by minimum and maximum boundaries. See [Setting an absolute freshness limit](#), page 19.



- ◆ Checking the absolute freshness limit  
For HTTP objects that do not have **Expires** headers or do not have both **Last-Modified** and **Date** headers, the proxy uses a maximum and minimum freshness limit. See [Setting an absolute freshness limit](#), page 19.
- ◆ Checking revalidate rules in the **cache.config** file  
Revalidate rules apply freshness limits to specific HTTP objects. You can set freshness limits for objects originating from particular domains or IP addresses, objects with URLs that contain specified regular expressions, and objects requested by particular clients, for example. See [cache.config](#), page 324.

## Modifying the aging factor for freshness computations

If an object does not contain any expiration information, Content Gateway can estimate its freshness from the **Last-Modified** and **Date** headers. By default, the proxy stores an object for 10% of the time that elapsed since it last changed. You can increase or reduce the percentage.

1. Open the **records.config** file located in the Content Gateway **config** directory.
2. Edit the following variable:

Variable	Description
<code>proxy.config.http.cache.heuristic_lm_factor</code>	Specify the aging factor for freshness computations. The default value is 0.10 (10 percent).

3. Save and close the file.
4. To apply the changes, run the following command from the Content Gateway **bin** directory:

```
content_line -x
```

## Setting an absolute freshness limit

Some objects do not have **Expires** headers or do not have both **Last-Modified** and **Date** headers. You can control how long these objects are considered fresh in the cache by specifying an absolute freshness limit. A longer lifetime means objects are kept in the cache longer. Performance can improve if pages are taken from the cache rather than going out to the network.

1. Navigate to the **Configure > Protocols > HTTP > Cacheability** tab.
2. In the **Minimum Heuristic Lifetime** area of the **Freshness** section, specify the minimum amount of time that HTTP objects without an expiration date can remain fresh in the cache before being considered stale. The default value is 3600 seconds (1 hour).

3. In the **Maximum Heuristic Lifetime** field, specify the maximum amount of time that HTTP objects without an expiration date can remain fresh in the cache before being considered stale. The default value is 86400 seconds (1 day).
4. Click **Apply**.

## Specifying header requirements

To ensure freshness of the objects in the cache, configure Content Gateway to cache only objects with specific headers.



### Warning

By default, the proxy caches all objects (including objects with no headers). Websense recommends that you change the default setting only for specialized proxy situations. If you configure the proxy to cache only HTTP objects with **Expires** or **max-age** headers, the cache hit rate will be seriously reduced (very few objects have explicit expiration information).

1. Navigate to the **Configure > Protocols > HTTP > Cacheability** tab.
2. In the **Required Headers** area of the **Behavior** section, select one of the following:
  - **An Explicit Lifetime Header** to cache only HTTP objects with **Expires** or **Cache-Control** headers.
  - **A Last-Modified Header** to cache only HTTP objects with **Expires** or **Last-Modified** headers.
  - **No Required Headers** to cache all HTTP objects (no specific headers are required). This is the default.
3. Click **Apply**.

## Cache-Control headers

Even though an object might be fresh in the cache, clients or servers might have constraints that prevent them from retrieving the object from the cache. For example, a client might request that a object not come from a cache, or if it does, it cannot have been cached for more than 10 minutes.

Content Gateway bases the servability of a cached object on **Cache-Control** headers. **Cache-Control** headers can appear in both client requests and server responses.

The following **Cache-Control** headers affect whether objects are served from the cache:

- ◆ The **no-cache** header, sent by clients, tells the proxy to serve *no* objects directly from the cache; always obtain the object from the origin server. You can configure the proxy to ignore client **no-cache** headers (see [Configuring the proxy to ignore client no-cache headers](#), page 26).

- ◆ The **max-age** header, sent by servers, is compared to the object age; if the age is less than **max-age**, the object is fresh and can be served.
- ◆ The **min-fresh** header, sent by clients, is an *acceptable freshness tolerance*. The client wants the object to be at least this fresh. If a cached object does not remain fresh at least this long in the future, it is revalidated.
- ◆ The **max-stale** header, sent by clients, permits the proxy to serve stale objects provided they are not too old. Some browsers might be willing to take slightly old objects in exchange for improved performance, especially during periods of poor Internet availability.

The proxy applies Cache-Control servability criteria *after* HTTP freshness criteria. For example, an object might be considered fresh, but if its age is greater than its *max-age*, it is not served.

## Revalidating HTTP objects

When a client requests an HTTP object that is stale in the cache, Content Gateway revalidates the object, querying the origin server to check if the object is unchanged. Revalidation results in one of the following:

- ◆ If the object is still fresh, the proxy resets its freshness limit and serves the object.
- ◆ If a new copy of the object is available, the proxy caches the new object, replacing the stale copy, and serves the object to the user simultaneously.
- ◆ If the object no longer exists on the origin server, the proxy does not serve the cached copy.
- ◆ If the origin server does not respond to the revalidation query, the proxy does not perform any validation; it serves the stale object from the cache.

By default, the proxy revalidates a requested HTTP object in the cache if it considers the object to be stale. The proxy evaluates object freshness as described in [HTTP object freshness](#), page 18. You can configure how often you want the proxy to revalidate an HTTP object.

1. Navigate to the **Configure > Protocols > HTTP > Cacheability** tab.
2. In the **When to Revalidate** area of the **Behavior** section, select:
  - **Never Revalidate** to never verify the freshness of a requested HTTP object with the origin server.
  - **Always Revalidate** to always verify the freshness of a requested HTTP object with the origin server.
  - **Revalidate if Heuristic Expiration** to verify the freshness of a requested HTTP object with the origin server if the object contains no **Expires** or **Cache-Control** headers. Content Gateway considers all HTTP objects without **Expires** or **Cache-Control** headers to be stale.
  - **Use Cache Directive or Heuristic** to verify the freshness of a requested HTTP object with the origin server when Content Gateway considers the object in the cache to be stale. This is the default.

3. Click **Apply**.

**Note**

You can also set specific revalidation rules in the **cache.config** file. See [cache.config](#), page 324.

## FTP object freshness

FTP objects carry no time stamp or date information and remain fresh in the cache for the period of time you specify (from 15 minutes to 2 weeks), after which they are considered stale.

FTP objects can be requested from either an HTTP client (such as a browser) or an FTP client (such as WS\_FTP). Content Gateway caches only the FTP objects requested from HTTP clients.

### FTP objects requested by HTTP clients

You can set an absolute freshness limit for FTP objects requested by HTTP clients (FTP over HTTP objects).

**Note**

In addition to setting an absolute freshness limit for all FTP objects requested by HTTP clients, you can set freshness rules for specific FTP objects in the **cache.config** file (see [cache.config](#), page 324).

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. In the **FTP Document Lifetime** area of the **Freshness** section, enter the amount of time that FTP objects requested by HTTP clients can remain fresh in the cache before being considered stale. The default value is 259200 seconds (3 days).
3. Click **Apply**.

## Scheduling updates to local cache content

---

To further increase performance and to ensure that HTTP and FTP objects (requested from HTTP clients) are fresh in the cache, you can use the Scheduled Update option to configure the proxy to load specific objects into the cache at scheduled times.

To use the Scheduled Update option:

- ◆ Specify the list of URLs that contain the objects you want to schedule for update, the time the update should take place, and the recursion depth for the URL.
- ◆ Enable the Scheduled Update option and configure optional retry settings.

See [Configuring the Scheduled Update option](#), page 23 for more information.

Content Gateway uses the information you specify to determine the URLs for which it is responsible and, for each URL, derives all recursive URLs if applicable. It then generates a unique URL list. Using this list, the proxy initiates an HTTP **GET** for each unaccessed URL, ensuring that it remains within the user-defined limits for HTTP concurrency at any given time.



#### Note

The system logs the completion of all HTTP **GET** operations, enabling you to monitor the performance of this feature.

The Force Immediate Update option that enables you to update URLs without waiting for the specified update time to occur. You can use this option to test your scheduled update configuration. See [Forcing an immediate update](#), page 24.

## Configuring the Scheduled Update option

1. Navigate to **Configure > Protocols > HTTP Scheduled Update > Update URLs**.
2. In the **Scheduled Object Update** area, click **Edit File** to open the configuration file editor for the **update.config** file.
3. Enter the following information:
  - In the **URL** field, enter the URL you want to schedule for update.
  - *Optional.* In the **Request Headers** field, enter the semicolon-separated list of headers passed in each **GET** request. You can define any request header that conforms to the HTTP specification.
  - In the **Offset Hour** field, enter the base hour used to derive the update periods. You can specify a value in the range 00 to 23.
  - In the **Interval** field, enter the interval (in seconds) at which updates occur, starting at the offset hour.
  - In the **Recursion Depth** field, enter the depth to which referenced URLs are recursively updated, starting at the given URL. For example, a recursion depth of 1 updates the given URL, as well as all URLs immediately referenced by links from the original URL.
4. Click **Add**, and then click **Apply**.
5. Click **Close**.
6. Click the **General** tab.
7. Enable **Scheduled Update**.
8. In the **Maximum Concurrent Updates** field, enter the maximum number of simultaneous update requests allowed at any time to prevent the scheduled update process from overburdening the host. The default is 100.

9. In the **Count** field of the **Retry on Update Error** section, enter the number of times you want to retry the scheduled update of a URL in the event of failure. The default value is 10.
10. In the **Interval** field of the **Retry on Update Error** section, enter the delay in seconds between each scheduled update retry for a URL in the event of failure. The default value is 2.
11. Click **Apply**.

## Forcing an immediate update

The Force Immediate Update option lets you verify the URLs listed in the **update.config** file immediately. This option disregards the offset hour and interval set in the **update.config** file and updates the URLs listed.



### Important

When you enable the Force Immediate Update option, the proxy continually updates the URLs specified in the **update.config** file until you disable the option.

---

1. Navigate to **Configure > Protocols > HTTP Scheduled Update > General**.
2. Ensure that **Scheduled Update** is enabled.
3. Click the **Update URLs** tab.
4. Enable **Force Immediate Update**.
5. Click **Apply**.

## Pinning content in the cache

---

The cache pinning option configures Content Gateway to keep certain HTTP objects (and FTP objects requested from HTTP clients) in the cache for a specified time. Use this option to ensure that the most popular objects are in the cache when needed and that the proxy does not delete important objects from the cache.



### Note

The proxy observes Cache-Control headers and pins an object in the cache only if it is cacheable.

---

To use cache pinning, perform the following tasks:

- ◆ Set cache pinning rules in the **cache.config** file. See [Setting cache pinning rules, page 25](#).
- ◆ Enable the cache pinning option. See [Enabling cache pinning, page 25](#).

## Setting cache pinning rules

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. Click **Edit File** at the end of the page to display the configuration file editor for the **cache.config** file.
3. In the fields provided, supply the following information:
  - From the **Rule Type** drop-down box, select **pin-in-cache**.
  - From the **Primary Destination Type** drop-down box, select **url\_regex**.
  - In the **Primary Destination Value** field, specify the URL you want to pin in the cache.
  - In the **Time Period** field, specify the amount of time that the proxy pins the object in the cache.

In addition, you can add secondary specifiers (such as **Prefix** and **Suffix**) to the rule. All the fields are described under [HTTP](#), page 258.
4. Click **Add** to add the rule to the list, and then click **Apply**.
5. Click **Close**.

## Enabling cache pinning

1. On **Configure > Subsystems > Cache > General**, enable **Allow Pinning**.
2. Click **Apply**.

## To cache or not to cache?

---

When Content Gateway receives a request for a Web object that is not in the cache, it retrieves the object from the origin server and serves it to the client. At the same time, the proxy checks if the object is cacheable before storing it in its cache to serve future requests.

Content Gateway determines if an object is cacheable based on protocol:

- ◆ For HTTP objects, the proxy responds to caching directives from clients and origin servers. In addition, you can configure the proxy not to cache certain objects. See [Caching HTTP objects](#), page 25.
- ◆ For FTP objects, the proxy responds to caching directives you specify through configuration options and files. See [Caching FTP objects](#), page 32.

## Caching HTTP objects

---

Content Gateway responds to caching directives from clients and origin servers, as well as directives you specify through configuration options and files.

This section discusses the following topics:

- ◆ [Client directives](#), page 26
- ◆ [Origin server directives](#), page 27
- ◆ [Configuration directives](#), page 29

## Client directives

By default, Content Gateway does *not* cache objects with the following request headers:

- ◆ **Cache-Control: no-store**
- ◆ **Cache-Control: no-cache**



### Note

You can configure the proxy to ignore the **Cache-Control: no-cache** header. See [Configuring the proxy to ignore client no-cache headers](#), page 26.

---

- ◆ **Cookie:** (for text objects)

By default, the proxy caches objects served in response to requests that contain cookies unless the object is text. You can configure the proxy to *not* cache cooked content of any type, cache all cooked content, or cache cooked content that is of image type only. See [Caching cooked objects](#), page 30.

- ◆ **Authorization:**



### Note

FTP objects requested from HTTP clients can also contain **Cache-Control: no-store**, **Cache-Control: no-cache**, or **Authorization** headers. If an FTP object requested from an HTTP client contains such a header, the proxy does not cache it unless explicitly configured to do so.

---

## Configuring the proxy to ignore client no-cache headers

By default, Content Gateway observes client **Cache Control:no-cache** directives. If a requested object contains a **no-cache** header, the proxy forwards the request to the origin server even if it has a fresh copy in the cache.



You can configure the proxy to ignore client **no-cache** directives. In this case, the proxy ignores **no-cache** headers from client requests and serves the object from its cache.

**Important**

The default behavior of observing **no-cache** directives is appropriate in most cases. Configure Content Gateway to ignore client **no-cache** directives only if you are knowledgeable about HTTP 1.1.

---

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. In the **Behavior** section, enable the **Ignore “no-cache” in Client Requests** option.
3. Click **Apply**.

**Note**

Certain versions of Microsoft Internet Explorer do not request cache reloads from transparent caches when the user presses the browser **Refresh** button. This can prevent content from being loaded directly from the origin server. You can configure Content Gateway to treat Microsoft Internet Explorer requests more conservatively, providing fresher content at the cost of serving fewer documents from the cache. You can configure the proxy to add **no-cache** headers to requests from Microsoft Internet Explorer in Content Gateway Manager (in the **Behavior** section **Configure > Protocols > HTTP > Cacheability** tab).

---

## Origin server directives

By default, Content Gateway does not cache objects with the following response headers:

- ◆ **Cache-Control: no-store**
- ◆ **Cache-Control: private**
- ◆ **WWW-Authenticate:**

**Note**

You can configure the proxy to ignore **WWW-Authenticate** headers. See [Configuring the proxy to ignore WWW-Authenticate headers](#), page 29.

---

- ◆ **Set-Cookie:**

- ◆ **Cache-Control: no-cache**

**Note**

You can configure the proxy to ignore **no-cache** headers. See [Configuring the proxy to ignore server no-cache headers](#), page 28.

- ◆ **Expires:** header with value of 0 (zero) or a past date

## Configuring the proxy to ignore server no-cache headers

By default, Content Gateway observes **Cache-Control:no-cache** directives. A response from an origin server with a **no-cache** header is not stored in the cache, and any previous copy of the object in the cache is removed.

**Important**

If you configure the proxy to ignore **no-cache** headers, it also ignores **no-store** headers.

**Important**

The default behavior of observing **no-cache** directives is appropriate in most cases. Configure the proxy to ignore origin server **no-cache** headers only if you are knowledgeable about HTTP 1.1.

You can configure the proxy to ignore origin server **no-cache** headers.

1. Open the **records.config** file located in the Content Gateway **config** directory.
2. Edit the following variable:

Variable	Description
<code>proxy.config.http.cache.ignore_server_no_cache</code>	Set to 1 to ignore server directives to bypass the cache.

3. Save and close the file.
4. To apply the changes, run the following command from the Content Gateway **bin** directory:

```
content_line -x
```

## Configuring the proxy to ignore WWW-Authenticate headers

By default, Content Gateway does not cache objects that contain **WWW-Authenticate** response headers. The **WWW-Authenticate** header contains authentication parameters that the client uses when preparing the authentication challenge response to an origin server.



### Important

The default behavior of not caching objects with **WWW-Authenticate** headers is appropriate in most cases. Configure the proxy to ignore server **WWW-Authenticate** headers only if you are knowledgeable about HTTP 1.1.

You can configure the proxy to ignore origin server **WWW-Authenticate** headers, in which case, objects with **WWW-Authenticate** headers are stored in the cache for future requests.

1. Open the **records.config** file located in the Content Gateway **config** directory.
2. Edit the following variable:

Variable	Description
<code>proxy.config.http.cache.ignore_authentication</code>	Set to 1 to cache objects with <b>WWW-Authenticate</b> headers.

3. Save and close the file.
4. To apply the changes, run the following command from the Content Gateway **bin** directory:

```
content_line -x
```

## Configuration directives

In addition to client and origin server directives, Content Gateway responds to directives you specify through configuration options and files.

You can configure the proxy to:

- ◆ *Not* cache any HTTP objects. See [Disabling HTTP object caching](#), page 30.
- ◆ Cache dynamic content (objects with URLs that contain a question mark (?), a semicolon (;), or cgi, or that end in .asp). See [Caching dynamic content](#), page 30.
- ◆ Cache objects served in response to the **Cookie:** header. See [Caching cookie objects](#), page 30.
- ◆ Observe never-cache rules in the **cache.config** file. See [cache.config](#), page 324.

## Disabling HTTP object caching

By default, Content Gateway caches all HTTP objects except those for which you have set never cache rules in the **cache.config** file. You can disable HTTP object caching so that all HTTP objects are served from the origin server and never cached.

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. Disable **HTTP Caching**.
3. Click **Apply**.

## Caching dynamic content

A URL is considered dynamic if it contains a question mark (?), a semicolon (;), or cgi, or if it ends in .asp. By default, Content Gateway does *not* cache dynamic content. However, you can configure the proxy to cache this content.



### Warning

It is recommended that you configure the proxy to cache dynamic content for specialized proxy situations only.

---

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. In the **Dynamic Caching** section, enable **Caching Documents with Dynamic URLs**.
3. Click **Apply**.

## Caching cookieed objects

By default, Content Gateway caches objects served in response to requests that contain cookies *unless* the object is text. The proxy does not cache cookieed text content, because object headers are stored as well as the object, and personalized cookie header values could be saved with the object.

With non-text objects, personalized headers are unlikely to be delivered or used.

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. In the **Caching Response to Cookies** area of the **Dynamic Caching** section, select a caching option:
  - Select **Cache All but Text** to cache all cookieed content except content that is text (this is the default setting).
  - Select **Cache Only Image Types** to cache cookieed content that is an image.
  - Select **Cache Any Content Type** to cache cookieed content of all types.
  - Select **No Cache on Cookies** to *not* cache cookieed content of any type.
3. Click **Apply**.

## Forcing object caching

You can force Content Gateway to cache specific URLs (including dynamic URLs) for a specified duration regardless of **Cache-Control** response headers.

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. Click **Edit File** at the end of the page to display the configuration file editor for the **cache.config** file.
3. In the fields provided, supply the following information:
  - From the **Rule Type** drop-down box, select **ttd-in-cache**.
  - From the **Primary Destination Type** drop-down box, select **url\_regex**.
  - In the **Primary Destination Value** field, specify the URL you want to force cache.
  - In the **Time Period** field, specify the amount of time that the proxy can serve the URL from the cache.

In addition, you can add secondary specifiers (such as **Prefix** and **Suffix**) to the rule. All the fields are described in [HTTP](#), page 258.
4. Click **Add**, and then click **Apply**.
5. Click **Close**.

## Caching HTTP alternates

Some origin servers answer requests to the same URL with a variety of objects. The content of these objects can vary, according to whether a server delivers content for different languages, targets different browsers with different presentation styles, or provides different document formats (HTML, PDF). Different versions of the same object are termed *alternates* and are cached by Content Gateway based on **Vary** response headers.

## Configuring how Content Gateway caches alternates

You can specify additional request and response headers for specific content types that the proxy will identify as alternates for caching.

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. In the **Vary Based on Content Type** section, click **Enabled** to cache alternate versions of HTTP documents that do not contain the **Vary** header.
3. Specify additional request and response headers for the proxy server to identify:
  - In the **Vary by Default on Text** field, enter the HTTP header field on which you want to vary if the request is for text (for example, an HTML document).
  - In the **Vary by Default on Images** field, enter the HTTP header field on which you want to vary if the request is for images (for example, a **.gif** file).

- In the **Vary by Default on Other Document Types** field, enter the HTTP header field on which you want to vary if the request is for anything other than text or images.

**Note**

If you specify **Cookie** as the header field on which to vary in the above fields, make sure that the appropriate option is enabled in the **Caching Response to Cookies** area of the **Dynamic Caching** section. For example, if you enable the **Cache Only Image Types** option in the **Caching Response to Cookies** area and you enable the **Vary by Default on Text** option in the **Vary Based on Content Type** section, alternates by cookie will not apply to text.

4. Click **Apply**.

## Limiting the number of alternates for an object

You can limit the number of alternates Content Gateway can cache per object. The default number of alternates is 3.

**Note**

Large numbers of alternates can affect proxy performance because all alternates have the same URL. Although Content Gateway can look up the URL in the index very quickly, it must scan sequentially through available alternates in the object store.

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. In the **Maximum Alternates** field, enter the maximum number of alternate versions of an object you want the proxy to cache. The default value is 3.
3. Click **Apply**.

## Caching FTP objects

---

FTP objects can be requested from either an HTTP client (such as a browser) or an FTP client (such as WS\_FTP).

For FTP objects requested from HTTP clients (FTP over HTTP), perform the following configuration to determine what the proxy stores in the cache:

- ◆ Disable FTP over HTTP caching so that the proxy does not cache any FTP objects requested from HTTP clients (see [Disabling FTP over HTTP caching, page 33](#)).
- ◆ Set never cache rules in the **cache.config** file (see [cache.config, page 324](#)).

- ◆ Configure the proxy to ignore client **Cache-Control: no-store** or **Cache-Control: no-cache** headers (see [Configuring the proxy to ignore client no-cache headers](#), page 26).

Caching is not supported for FTP objects requested from FTP clients.

## Disabling FTP over HTTP caching

You can configure Content Gateway not to cache any FTP objects that are requested from HTTP clients by disabling the FTP over HTTP option. The proxy processes the requests by forwarding them to the FTP server but does not cache any requested objects.

1. Navigate to **Configure > Protocols > HTTP > Cacheability**.
2. In the **Caching** section, disable **FTP over HTTP Caching**.
3. Click **Apply**.





# 4

## Explicit Proxy Caching

If Internet requests are not transparently routed to Content Gateway via a Layer 4 switch or router (see [Transparent Proxy and ARM, page 43](#)), traffic must be **explicitly** routed to Content Gateway by configuring the client's Internet browser. (This is sometimes referred to as an *explicit proxy deployment*.)

Clients can configure their Web browsers in 1 of 3 ways:

- ◆ By configuring their browsers to send requests directly to the proxy. See [Manual browser configuration, page 35](#).
- ◆ By configuring their browsers to download proxy configuration instructions from a PAC (Proxy Auto-Config) file. See [Using a PAC file, page 36](#).
- ◆ By using WPAD (Web Proxy Auto-Discovery Protocol) to download proxy configuration instructions from a WPAD server (Microsoft Internet Explorer only). See [Using WPAD, page 38](#).

In addition, if Content Gateway is configured to proxy FTP traffic, FTP client applications, such as FileZilla or WS\_FTP, must be configured to explicitly send requests to the proxy. See [Configuring FTP clients in an explicit proxy environment, page 39](#).

### Manual browser configuration

---

To configure a browser to send requests to Content Gateway, clients must provide the following information for each protocol they want the proxy to serve to their browsers:

- ◆ The proxy's hostname or IP address.



#### Important

If Integrated Windows Authentication is configured for user authentication, the Fully Qualified Domain Name must be used. Specifying the IP address will result in authentication failure. See [Integrated Windows Authentication, page 166](#).

- ◆ The proxy server port. The Content Gateway default proxy server port is 8080.



---

**Important**

Do not set up the IP address of the Content Gateway proxy to be a virtual IP address.

Although Content Gateway Manager does not prohibit the entry of a virtual IP address, the proxy does not function properly if a VIP is used.

---

In addition, clients can specify not to use the proxy for certain sites. Requests to the listed sites go directly to the origin server.

For Microsoft Internet Explorer version 7.0 and later, proxy configuration settings are in **Tools > Internet Options > Connections > LAN Settings**. By default, Microsoft Internet Explorer sets all protocols to the same proxy server. To configure each protocol separately, click **Advanced** in the **LAN Settings** section. See the browser documentation for complete proxy configuration instructions.

For Mozilla Firefox 2.0 and later, proxy configuration settings are in **Tools > Options > Advanced > Network > Settings > Connection Settings > Manual Proxy Configuration**. By default, you must configure each protocol separately. However, you can set all protocols to the same proxy server by selecting **Use this proxy server for all protocols**.

You do not have to set configuration options on the proxy to accept requests from manually configured browsers.

---

## Using a PAC file

---

A PAC file is a JavaScript function definition that a browser calls to determine how requests are handled. Clients must specify in their browser settings the URL from which the PAC file is loaded.

You can store a PAC file on the proxy and provide the URL for this file to your clients. If you have a **proxy.pac** file, copy it into the Content Gateway **config** directory.



---

**Note**

The PAC file can reside on any server in your network.

If you are using SSL Manager, refer to [Running in explicit proxy mode, page 123](#), for information on a PAC file to use with HTTPS traffic.

---

1. If you have an existing **wpad.dat** file, replace the **wpad.dat** file located in the Content Gateway **config** directory with your existing file.

2. Navigate to the **Configure > Content Routing > Browser Auto-Config > PAC** tab.
3. In the **Auto-Configuration Port** field, specify the port that Content Gateway uses to serve the PAC file. The default port is 8083.
4. The PAC Settings area displays the **proxy.pac** file:
  - If you copied an existing PAC file into the Content Gateway **config** directory, the **proxy.pac** file contains your proxy configuration settings. Check the settings and make changes if necessary.
  - If you did not copy an existing PAC file into the Content Gateway **config** directory, the PAC Settings area is empty. Enter the script that provides the proxy server configuration settings. A sample script is provided in [Sample PAC file](#), page 37. See, also, the [Websense Technical Library](#).
5. Click **Apply**.
6. Click **Restart** on **Configure > My Proxy > Basic > General**.
7. Inform your users to set their browsers to point to this PAC file.

For example, if the PAC file is located on the proxy server with the hostname **proxy1** and Content Gateway uses the default port 8083 to serve the file, users must specify the following URL in the proxy configuration settings:

```
http://proxy1.company.com:8083/proxy.pac
```

The procedures for specifying the PAC file location vary among browsers. For example, for Microsoft Internet Explorer, you set the location of the PAC file in the **Use automatic configuration script** field under **Tools > Internet Options > Connections > LAN Settings**. For Mozilla Firefox, proxy configuration settings are in **Tools > Options > Advanced > Network > Settings > Connection Settings > Automatic proxy configuration URL**. See the documentation for your browser for details.

## Sample PAC file

The following sample PAC file instructs browsers to connect directly to all hosts without a fully qualified domain name and to all hosts in the local domain. All other requests go to the proxy server called **myproxy.company.com**.

```
function FindProxyForURL(url, host)
{
  if (isPlainHostName(host) || dnsDomainIs(host,
    ".company.com"))
    return "DIRECT";
  else
    return "PROXY myproxy.company.com:8080; DIRECT";
}
```

## Using WPAD

---

WPAD allows Internet Explorer version 7 and later to automatically detect a server that will supply it with proxy server configuration settings. Clients do not have to configure their browsers to send requests to a proxy server: a single server provides the settings to all clients on the network.

**Note**

WPAD is incompatible with transparent proxy deployments.

When an Internet Explorer version 7 or later browser starts up, it searches for a WPAD server that will supply it with proxy server configuration settings. It prepends the hostname WPAD to the current fully qualified domain name. For example, a client in **x.y.company.com** searches for a WPAD server at **wpad.x.y.company.com**. If unsuccessful, the browser removes the bottommost domain and tries again; for example, it tries **wpad.y.company.com**. The browser stops searching when it detects a WPAD server or reaches the third-level domain, **wpad.company.com**. The algorithm stops at the third level so that the browser does not search outside the current network.

**Note**

By default, Microsoft Internet Explorer version 7 and later are set to automatically detect WPAD servers. However, browser users can disable this setting.

You can configure Content Gateway to be a WPAD server:

1. If you have an existing **wpad.dat** file, replace the **wpad.dat** file located in the Content Gateway **config** directory with your existing file.
2. Navigate to **Configure > My Proxy > Basic > General**.
3. In the **Features** table, ensure that **ARM** is **On** (the default) in the **Networking** section.
4. Navigate to **Configure > Content Routing > Browser Auto-Config > WPAD** to display the **wpad.dat** file.
5. The WPAD Settings area displays the **wpad.dat** file:
  - If you copied an existing **wpad.dat** file into the Content Gateway **config** directory, the file contains your proxy configuration settings. Check the settings and make changes if necessary.
  - If you did not copy an existing **wpad.dat** file into the Content Gateway **config** directory (/opt/WCG/config), the WPAD Settings area is empty. Enter a script that will provide the proxy server configuration settings. A sample script is provided in [Sample PAC file](#), page 37 (a **wpad.dat** file can contain the same script as a **proxy.pac** file).
6. Click **Apply**.

7. Navigate to **Configure > Networking > ARM**.
8. In the **Network Address Translation (NAT)** section, click **Edit File** to add a special remap rule to the **ipnat.conf** file.
9. Enter information in the fields provided, and then click **Add**:
  - In the **Ethernet Interface** field, enter the network interface that receives browser WPAD requests (for example hme0 or eth0).
  - From the **Connection Type** drop-down list, select **tcp**.
  - In the **Destination IP** field, enter the IP address of the Content Gateway server that will be resolved to the WPAD server name by the local name servers followed by /32; for example: 123.456.7.8/32.
  - In the **Destination Port** field, enter **80**.
  - In the **Redirected Destination IP** field enter the same IP address you entered in the **Destination IP** field but omit /32.
  - In the **Redirected Destination Port** field, enter **8083**.
10. Click **Add**.
11. Use the arrow keys on the left side to move the new rule to the first line in the file.
12. Click **Apply**, and then click **Close**.
13. Click **Restart** on the **Configure > My Proxy > Basic > General**.

## Configuring FTP clients in an explicit proxy environment

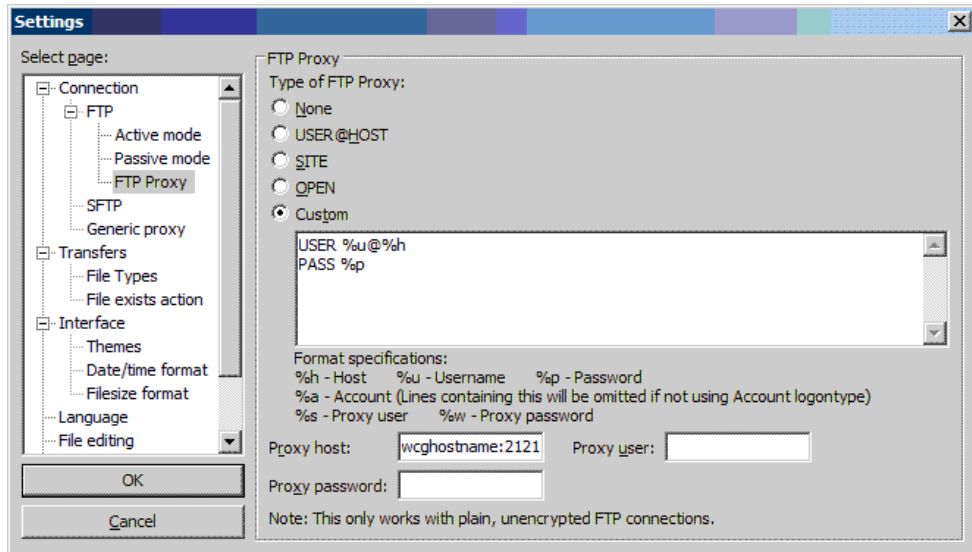
When Content Gateway is configured to proxy FTP traffic (see [FTP, page 269](#)), FTP client applications, such as FileZilla or WS\_FTP, should be configured to send FTP requests to the proxy. When so configured, the user works with the FTP client application as if no proxy were present.

To connect to an FTP server, 4 pieces of information are usually needed. These pieces of information are mapped as follows:

From:	To:
FTP server hostname	FTP <i>proxy</i> hostname
FTP server port number	FTP <i>proxy</i> port number (default is 2121)
FTP server username	FTP_server_username@FTP_server_hostname For example: anon@ftp.abc.com
FTP server password	FTP server password

Some FTP client applications have a configuration page for specifying FTP proxy information. Update those settings to point to the Content Gateway FTP proxy. See your FTP client application documentation.

Here is an example configuration using a recent version of FileZilla.



In the **FTP Proxy** area:

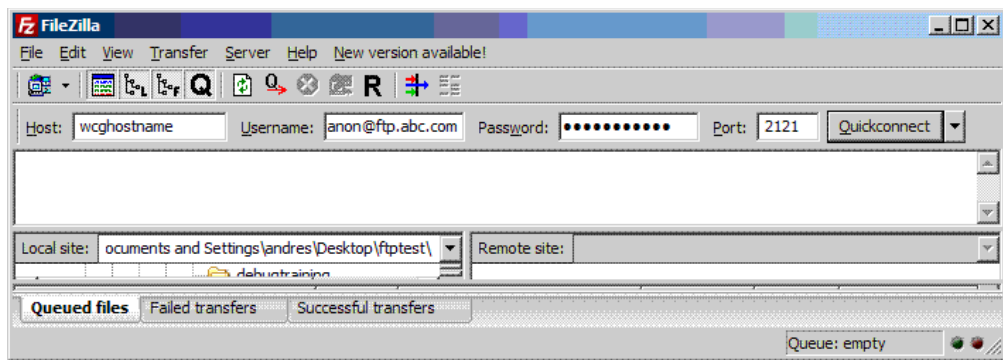
1. Set **FTP Proxy** to **Custom** and define **USER** and **PASS** as shown.
2. Set **Proxy host** to the Content Gateway FTP proxy hostname and port number.
3. Accept the settings by clicking **OK**.

The user then enters FTP connection information in the usual way, as if no proxy were present. For example:

```
Host:      ftp.abc.com
Username:  anon
Password:  123abc
```

If the FTP client application is **not** configured, the user must enter FTP requests as shown below.

```
Host:      Content Gateway proxy hostname
Username:  anon@ftp.abc.com
Password:  123acb
Port:      2121
```







# 5

## Transparent Proxy and ARM

The transparent proxy option enables Content Gateway to respond to client Internet requests without requiring users to reconfigure their browsers. It does this by redirecting the request flow into the proxy after the traffic has been intercepted, typically by a Layer 4 (L4) switch or router.

In a transparent proxy deployment:

1. The proxy intercepts client requests to origin servers via a switch or router. See [Transparent interception strategies, page 45](#).
2. The Adaptive Redirection Module (ARM) changes the destination IP address of an incoming packet to the proxy's IP address and the destination port to the proxy port, if different. (The ARM is enabled by default. See [Enabling the ARM, page 44](#).)
3. The proxy receives and begins processing the intercepted client requests. If a request is a cache hit, the proxy serves the requested object. If a request is a miss, the proxy retrieves the object from the origin server and serves it to the client.
4. On the way back to the client, the ARM changes the source IP address to the origin server IP address and the source port to the origin server port.



---

### Note

For transparent proxy configurations with multiple interfaces or gateways, Content Gateway must have proper routes to clients and the Internet in the operating system's routing table.

---

For HTTP, the proxy can identify problem clients and servers, and the ARM can disable interception for those clients and servers, passing their traffic directly to the

origin server. You can create static rules to exempt clients and servers from being redirected to the proxy. See [Interception bypass](#), page 61.

Related topics:

[Transparent interception strategies](#), page 45

[Interception bypass](#), page 61

[Connection load shedding](#), page 64

[Reducing DNS lookups](#), page 65

[IP spoofing](#), page 66

---

## Enabling the ARM

---

The Content Gateway ARM inspects incoming packets before the IP layer sees them and readdresses the packets to Content Gateway for processing.

The ARM can make two changes to an incoming packet's address. It can change its destination IP address and its destination port. For example, the destination IP address of an HTTP packet is readdressed to the IP address of the proxy and the destination HTTP port is readdressed to the Content Gateway HTTP proxy port (usually port 8080).

On the way back to the client, the ARM changes the source IP address to the origin server IP address and the source port to the origin server port.

The ARM component consists of several files and a kernel module, which are installed during product installation. The installation program also creates redirection rules to readdress packets using the IP address of the proxy machine and default port assignments. The ARM is enabled by default when Content Gateway is installed.

For the proxy to serve HTTP, HTTPS, FTP, or DNS requests transparently, you must check the redirection rules in the **ipnat.conf** file and edit them if necessary. If you are using WCCP for transparent interception, there must be a redirection rule for every port in every active service group. Rules for standard ports are included by default. To view and work with ARM redirection rules, follow these steps.

1. Check that the ARM has been enabled by logging into the Content Gateway Manager and looking at the **Configure > My Proxy > Basic > General** tab. If it is not already selected, click **ARM On**, and click **Apply**.
2. Navigate to the **Configure > Networking > ARM > General** tab.

The **Network Address Translation (NAT)** section displays the redirection rules in the **ipnat.conf** file. Check the redirection rules and make any needed changes.

- a. To change a redirection rule, click **Edit File** to open the configuration file editor for the **ipnat.conf** file.
- b. Select the rule you want to edit and modify the appropriate fields. Click **Set** and then click **Apply** to apply your changes. Click **Close** to exit the configuration file editor.

All fields are described in [ARM, page 295](#).

3. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Transparent interception strategies

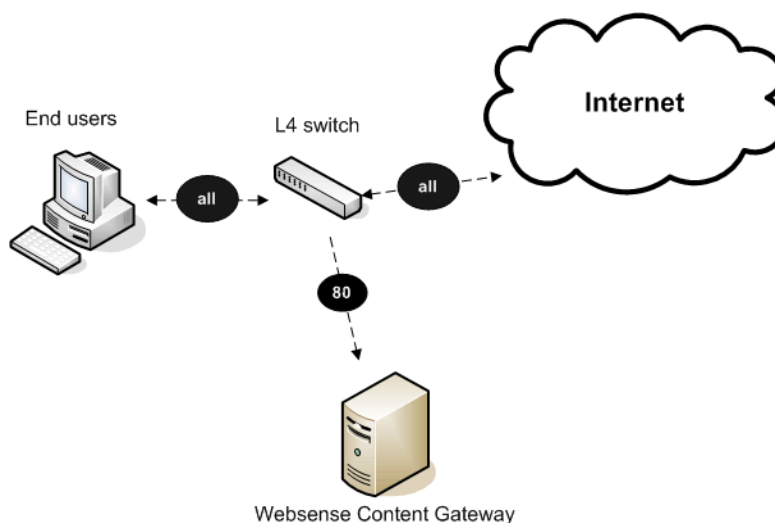
Websense Content Gateway supports the following transparent interception solutions:

- ◆ A Layer 4 switch. See [Transparent interception with a Layer 4 switch, page 45](#).
- ◆ A router or switch that supports WCCP v2. Cisco IOS-based routers are the most common. See [Transparent interception with WCCP v2 devices, page 46](#).
- ◆ Policy-based routing. See [Transparent interception and multicast mode, page 59](#).
- ◆ Software routing. See [Transparent interception with software-based routing, page 60](#).

Exactly how client requests reach the proxy depends on network topology. In a complex network, you must decide which clients are to be served transparently and make sure that network devices and the proxy are positioned to intercept their requests. Content Gateway, or routers or switches feeding Content Gateway, are often deployed at a major artery or aggregation pipe to the Internet.

### Transparent interception with a Layer 4 switch

Layer 4 switches can redirect supported protocols to the proxy, while passing all other Internet traffic directly to its destination, as shown below for HTTP.



Layer 4 switches offer the following features, depending on the particular switch:

- ◆ A Layer 4 switch that can sense downed hosts on the network and redirect traffic adds reliability.
- ◆ If a single Layer 4 switch feeds several proxy servers, the switch handles load balancing among the Content Gateway nodes. Different switches might use

different load-balancing methods, such as round-robin or hashing. If a node becomes unavailable, the switch redistributes the load. When the node returns to service, some switches return the node to its previous workload, so that the node cache need not be repopulated; this feature is called *cache affinity*.

**Note**

It is recommended that you do *not* enable Content Gateway virtual IP failover when a switch is providing load balancing in a cluster configuration.

## Transparent interception with WCCP v2 devices

Related topics:

[WCCP load distribution](#), page 48

[Configuring WCCP v2 routers](#), page 50

[Enabling WCCP v2 in Content Gateway](#), page 53

[ARM bypass and WCCP](#), page 48

Content Gateway supports transparent interception with WCCP v2-enabled routers and switches.

HTTP, HTTPS, FTP, and DNS protocols are supported. Default ARM redirection rules are included for these protocols communicating on standard ports.

A list of [WCCP v2 supported features](#) follows the setup outline.

**Important**

The network clients, Content Gateway proxy servers, and destination Web servers (default gateway) must reside on separate subnets.

Following is a WCCP v2 setup outline.

1. Install and configure your WCCP v2 devices.

On the WCCP v2 device:

- Program the service groups.
- Configure password security, if needed.
- Configure multicast communication, if needed.

See [Configuring WCCP v2 routers](#), page 50.

2. Configure Content Gateway to work with your WCCP devices.

- Define matching service groups.

In addition to protocols, ports, authentication (if used), and multicast communication (if used), also configure:

- The IP addresses of the WCCP v2 devices.
- The Packet Forward Method and Packet Return Method.
- If Content Gateway is deployed in a cluster, *assignment method* load distribution, if desired.

- Create ARM NAT rules for non-standard ports.

See [Enabling WCCP v2 in Content Gateway, page 53](#) and [Enabling the ARM, page 44](#).

3. Validate the configuration with test traffic.

## WCCP v2 supported features

Content Gateway supports the following WCCP v2 features:

- ◆ Multiple routers in a proxy cluster
- ◆ Multiple ports per service group
- ◆ Multiple service groups per protocol. Sometimes it is necessary or convenient to have different service groups for different WCCP devices. For example, for Cisco ASA firewall, different service groups are required for each WCCP device in the network.
- ◆ Dynamic load distribution in a proxy cluster through *assignment method* HASH or MASK, and *weight*. See [WCCP load distribution, page 48](#).
- ◆ Packet Return Method and Packet Forward Method negotiation
- ◆ MD5 password security per service group
- ◆ Multicast mode

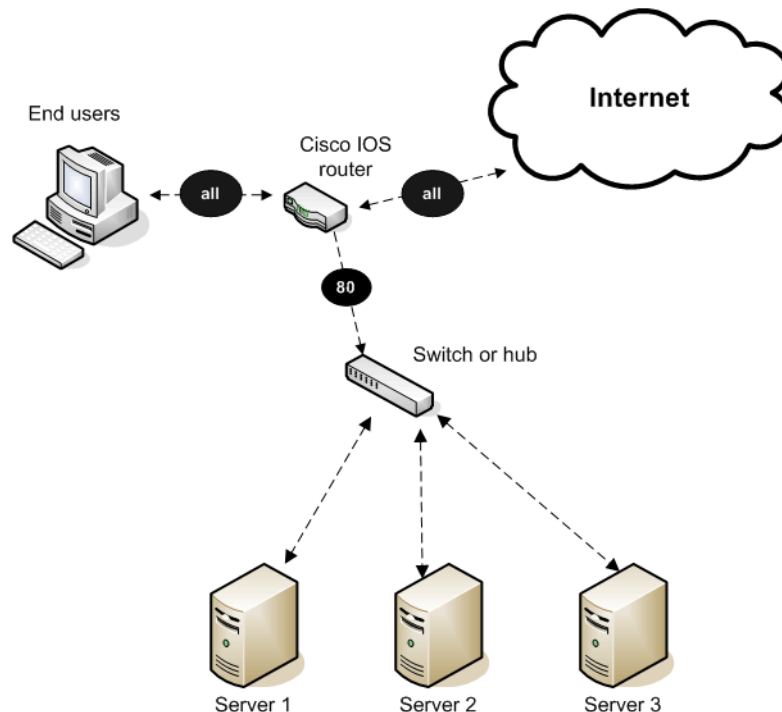
In a Content Gateway cluster, it is recommended that you **not** enable virtual IP failover in WCCP environments. WCCP v2 and the Content Gateway configuration handles node failures and restarts. (See [WCCP load distribution, page 48](#) and [Virtual IP failover, page 74](#).)

Content Gateway also supports cache affinity. If a node becomes unavailable and then recovers, the node's cache does not need to be repopulated.

## How WCCP v2 interception works:

1. WCCP v2 devices send HTTP, HTTPS, FTP, and DNS traffic, per the configuration of the service group, to the proxy server or cluster of servers.
2. The ARM readdresses traffic. For example, HTTP traffic on port 80 is readdressed to Content Gateway port 8080.
3. The proxy processes the request as usual, sending the response back to the client.

4. The ARM readdresses the proxy port in the response header to port 80 (undoing the readdressing it did on the way to the proxy). As a result, the user sees the response as if it had been sent directly from the origin server.



## ARM bypass and WCCP

If Content Gateway has an ARM bypass rule (discussed in [Interception bypass](#), page 61), Content Gateway forwards particular client requests directly to the origin server, bypassing the proxy.

Bypassed requests are unchanged by the ARM; they retain their client source IP address.

With WCCP v2, you can exclude certain router interfaces from redirection.

Content Gateway bypass rules can work if you exclude the router interface on which Content Gateway is connected from using WCCP. You can do this by setting the router configuration command **ip wccp redirect exclude**.

## WCCP load distribution

The WCCP protocol provides the **assignment method** for dynamic symmetric and asymmetric load distribution in a cluster. WCCP detects node failures and performs redistribution based on the configuration communicated to it by Content Gateway.

- ◆ Load distribution is configured in Content Gateway Manager and is pushed to the WCCP devices.
- ◆ Load distribution is configured **per service group**.

For each service group:

- Participating cluster members must be registered to the service group. (The WCCP device makes no decisions about load balancing.)
- The HASH or MASK assignment method is selected. HASH is typically used with the GRE forward/return method, and MASK with the L2 forward/return method.



### Important

MASK was developed specifically for the Cisco Catalyst series switches, and is one of the key characteristics that enable WCCP interception to be performed completely in hardware on these platforms. It should be used only with devices for which there is documented support.

- One or more **distribution attributes** are selected. Typically the destination IP address is used.
- If load is to be distributed to different cluster members in different proportions, a **weight** value is set on each cluster member. These values determine the proportion of requests each will receive relative to other members of the cluster.

Asymmetric load distribution using the **weight** value is helpful when:

- There are multiple Content Gateway servers with different performance capabilities, for example a V-Series V10000 and a V10000 G2.
- The Internet traffic profile doesn't lend itself to even distribution due to preferences for specific origin servers (and therefore destination IP addresses).

### How dynamic redistribution works:

Dynamic redistribution is accomplished when the WCCP device detects that a cluster member is offline. It then automatically redistributes the load to the remaining cluster members based on the load distribution configuration. When a cluster member returns to service and is detected by the WCCP device, load distribution is, again, automatically adjusted based on the configuration.

For configuration steps, see [Configuring service groups in Content Gateway Manager, page 55](#).

### How the weight value supports asymmetric load distribution:

The weight value, if used, must be set on every node in the cluster. The weight value is unique to each service group and node. The weight value does not propagate around the cluster.

The value of weight, relative to the settings on other cluster members, determines the proportion of traffic that WCCP directs to the node.

By default, weight is set to 0, which results in equal distribution to all cluster members.

To achieve asymmetric distribution, weight is set relative to other members of the cluster. For example, assume a cluster of 3 nodes:

Node	Weight value	Load distribution
Node1	50	50%
Node2	25	25%
Node3	25	25%

If Node1 goes offline, Node2 and Node3 will get an equal amount of traffic. If Node3 goes offline, Node1 will get two thirds of the traffic and Node2 will get one third of the traffic.

Because the weight value is relative to the settings on other cluster nodes, the same distribution as above can be achieved with weight values of 10, 5, 5. (The valid range of weight is 0-255.)

If weight is changed from its default value of 0, it should be configured on all nodes in the cluster.

## Configuring WCCP v2 routers

It is strongly recommended that you consult the documentation and the manufacturer's support site for information regarding optimal configuration and performance of your WCCP v2 device. Most devices should be configured to take best advantage of hardware-based redirection. With Cisco devices, the most recent version of IOS is usually the best.

To prepare WCCP v2 devices for use with the proxy:

1. Configure one or more service groups for the protocols you intend to use. A service group can handle one or multiple protocols. See *Configuring service groups on the WCCP device*, page 51.
2. Configure the router to enable WCCP processing for these service groups. See *Enabling WCCP processing for a service group*, page 51.
3. Optionally, enable router security. Router security must also be enabled for the service group in Content Gateway. See *Enabling WCCP v2 security on the router*, page 53.



### Note

For instructions on configuring your specific router, please refer to the documentation provided by your hardware vendor. For Cisco routers, see <http://www.cisco.com/univerd/cc/td/doc/product/core/> and search for your IOS and device version, for example, IOS 12.4.

---



- When you are done configuring the router, you must also enable WCCP processing in Content Gateway Manager. See [Enabling WCCP in Content Gateway Manager](#), page 54.

## Configuring service groups on the WCCP device

WCCP uses **service groups** to specify the traffic that is redirected to Content Gateway (and other devices).

A service group can intercept:

- one or more protocols
- on one or more ports

Service groups are assigned a unique integer identifier (ID) from 0 to 255. Service groups IDs are user defined; they do not have a default port or traffic type. The following table illustrates a set of service group ID definitions that are often found in networks. If you are configuring for IP spoofing, see the table in [IP spoofing](#), page 66 for common reverse service groups IDs.

Service ID	Port	Traffic Type
0	80	HTTP
5	21	FTP
70	443	HTTPS (requires SSL Manager)

Service groups must be configured on the router and in Content Gateway. The best practice is to configure the router(s) first and Content Gateway second.

Follow the instructions in your router documentation for specifics, but in general:

- To see what has been configured on the router for WCCP, enter:  
`show running-config | include wccp`
- To enable WCCP v2, enter:  
`ip wccp version 2`
- If you used another proxy cache with your router prior to Content Gateway, disable the service ID that was previously used. For example, if you have a Cisco router, disable the service ID **web-cache** by issuing this command:  
`no ip wccp web-cache`
- Specify the service group IDs you will use with Content Gateway. For the specific commands to use, see your router documentation.  
  
You must configure each service group supported by the router individually. You cannot configure a router globally.

## Enabling WCCP processing for a service group

For each WCCP v2 service group that you configure, you must enable WCCP processing. WCCP v2 routers contain multiple network interfaces, including:

- ◆ an interface dedicated to outbound traffic that is aimed at the Internet
- ◆ one or more interfaces connected to Content Gateway
- ◆ one or more interfaces that receive inbound client traffic

Following are some guidelines for enabling WCCP processing for a service group on a router. Consult the procedures in your router documentation for specific details.

1. Turn on the WCCP feature:

```
ip wccp <service group ID> password [0-7] <passwd>
```

2. On the router or switch interface, enable redirection for incoming packets or outgoing packets. **Be sure to substitute the service group IDs that you have established on your router(s).**

**For *incoming* packets:**

```
ip wccp <service group ID> redirect in
```

For example, to turn on redirection of HTTP destination port traffic, enter:

```
ip wccp 0 redirect in
```

To turn on redirection of HTTP source port traffic, which is required for IP spoofing, enter:

```
ip wccp 20 redirect in
```

To turn on redirection of HTTPS destination port traffic:

```
ip wccp 70 redirect in
```

To turn on redirection of FTP destination port traffic enter:

```
ip wccp 5 redirect in
```

Run the command above for each protocol you want to support, but *only for the interface dedicated to inbound traffic*.

**For *outgoing* packets:**

```
ip wccp <service group ID> redirect out
```

For example, to turn on redirection for HTTP, enter:

```
ip wccp 0 redirect out
```

To turn on redirection for HTTPS:

```
ip wccp 70 redirect out
```

To turn on redirection for FTP enter:

```
ip wccp 5 redirect out
```

Run the command above for each protocol you want to support, but *only for the interface dedicated to outbound traffic*.

3. When dynamic or static bypass is enabled, turn off redirection for packets received on the proxy interface:

```
ip wccp redirect exclude in
```

With bypass enabled, the proxy redirects bypassed traffic to the Internet. This command prevents looping back of packets by stopping the router from redirecting this same bypassed traffic back to Content Gateway. Run the command above for each interface connected to the proxy.

## Disabling WCCP processing for a service group

If you need to disable WCCP processing for any reason, issue this command to turn off the WCCP feature:

```
no ip wccp <service group ID> password [0-7] <passwd>
```

## Enabling WCCP v2 security on the router

If you are running WCCP v2, you can enable security on the Content Gateway node so that the proxy and your routers can authenticate each other. You must individually enable security for each service group that the router supports. You cannot configure a router globally as you would Content Gateway.

You enable the security option and provide the authentication password in Content Gateway Manager.

The authentication password you specify must match the authentication password configured on the router for each service group being intercepted. The following procedure provides an example of how to set an authentication password for different service groups.

1. Telnet to the router and switch to Enable mode.
2. At the prompt, enter the following command to configure the router from the terminal:  

```
configure terminal
```
3. If you defined a password when you enabled WCCP on the router, skip to step 4. Otherwise, enter the following command for each service group that the router intercepts:

```
hostname(config)# ip wccp service_group password password
```

where *hostname* is the host name of the router you are configuring, *service\_group* is the service group ID (for example, 0 for HTTP), and *password* is the password you want to use to authenticate Content Gateway. This password must match the password you specify in the Content Gateway configuration for this service group.

4. Exit and save the router configuration.

## Enabling WCCP v2 in Content Gateway

Related topics:

[Configuring WCCP v2 routers, page 50](#)

[Configuring service groups on the WCCP device](#)

[Enabling WCCP processing for a service group](#)

[Enabling WCCP v2 security on the router, page 53](#)

After you have configured your WCCP v2 routers, these steps remain:

1. *Enabling WCCP in Content Gateway Manager*
2. *Specifying the WCCP network interface*
3. *Configuring service groups in Content Gateway Manager*
4. Restarting Content Gateway



#### **Important**

Before you restart Content Gateway, make sure that your configuration meets the following requirements:

- ◆ Cisco IOS devices are running a very recent version of IOS with all appropriate patches applied.
  - ◆ WCCP routers are programmed with the correct service groups and other features.
  - ◆ ARM is enabled on all Content Gateway cluster nodes (the default configuration).
- 

## **Enabling WCCP in Content Gateway Manager**

1. Go to **Configure > My Proxy > Basic > General**.
2. In the **Networking** section of the **Features** table, locate **WCCP**, click **On**, and click **Apply**. Do **not** restart Content Gateway.

## **Specifying the WCCP network interface**

1. Go to **Configure > Networking > WCCP > General**.
2. In the **WCCP Network Interface** section, enter the network interface to use to communicate with the WCCP routers.
  - **This interface is used by all service groups.**
  - **The interface value must be set on each node in the cluster.** The value is **not** propagated around the cluster.

## Configuring service groups in Content Gateway Manager

Every WCCP service group that redirects traffic to a Content Gateway server must have a corresponding service group defined for it in the Content Gateway server or cluster.



### Important

With the exception of the service group **enabled/disabled** state, and the **weight**, all other service group attributes are propagated to all cluster members.

This means:

- ◆ Service groups need only be configured once within the cluster.
- ◆ *Except* the **enabled/disabled** setting and the **weight**, if used, which must be set on each node.

This supports the ability to specifically exclude service group activity on a given node. And also, by excluding weight, make proportional load distribution possible (see [WCCP load distribution](#)).

- ◆ To define service groups, go to **Configure > Networking > WCCP > General**. The **Service Groups** table displays a list of configured service groups and a subset of their configuration settings.  
Entries are stored in the **wccp.config** file.  
The **Refresh** button rereads **wccp.config** and refreshes the table.
- ◆ To add, modify, delete, or reorder service groups, click **Edit File**.

### Configuring a service group (editing wccp.config)

1. On **Configure > Networking > WCCP > General**, click **Edit File** to open **wccp.config** in the editor.  
Defined service groups are summarized at the top of the page.  
Click an entry in the list to view its complete details, modify, or reposition it.  
When an entry is selected, the down and up arrows to the left of the list reposition the entry in the list.  
Click “X” to delete a selected entry.
2. **Service Group Information**
  - a. **Service Group Status:** To enable a service group, select **Enabled**. A service group can be defined but not active. The **enabled/disabled** status is not propagated around the cluster.
  - b. **Service Group Name:** Specify a unique service group name. The service group name is an aid to administration.

- c. **Service Group ID:** Specify a WCCP service group identification number from 0-255. This ID must match a corresponding service group ID configured on the router. See [Configuring service groups on the WCCP device](#).
- d. **Protocol:** Specify the network protocol applicable to the service group, either TCP or UDP.
- e. **Ports:** Specify the ports that this service group handles. You can specify up to 8 ports in a comma-separated list. The ports must match the list in the corresponding service group on the router.

**Important**

Every port in the service group must have a corresponding ARM NAT rule to redirect the traffic to Content Gateway. See [Enabling the ARM](#).

---

**3. Router Information**

- a. **Security:** To use optional WCCP authentication, select **Enabled** and enter the same password used for service group authentication on the router. See [Enabling WCCP v2 security on the router](#), page 53.
- b. **Multicast:** To run in multicast mode, select **Enabled** and enter the multicast IP address. The multicast IP address must match the multicast IP address specified on the router. See [Transparent interception and multicast mode](#), page 59.
- c. **WCCP Routers:** Specify up to 10 WCCP router IP addresses in a comma-separated list. These routers must be configured with a corresponding service group.

**Note**

If the WCCP router is configured with multiple IP addresses, as for example when the router is configured to support multiple VLANs, the IP address reported in **Monitor > Networking > WCCP** statistics, and in packet captures, may differ from the IP address configured here. This is because the router always reports traffic on the highest active IP address.

One way to get the router to always report the same IP address is to set the router's loopback address to a value higher than the router's highest IP address, then the loopback address is always reported as the router's IP address. This is the recommended configuration.

---

**4. Mode Negotiation**

The mode should be selected to match the capabilities and position of the router or switch.

- a. **Packet Forward Method:** Select L2 or GRE.

- b. **Packet Return Method:** Select L2 or GRE.

The **Packet Forward Method** determines how intercepted traffic is transmitted from the WCCP router to the proxy.

The **Packet Return Method** specifies the method used to return intercepted traffic back to the WCCP router.

Typically the router supports only one method.

Typically, the forward and return methods match.



### Important

Selecting L2 requires that the router or switch be Layer 2-adjacent (in the same subnet) as Content Gateway.

**The proxy always adjusts to use a method that the router supports.** If the WCCP router supports more than one method, Content Gateway negotiates to use the method specified here.

## 5. Advanced Settings

- a. **Assignment Method:** Specify the parameters used to distribute intercepted traffic among multiple nodes in a cluster. It can be used in combination with **Weight** to provide dynamic load distribution. For a description of the WCCP load distribution feature, see [WCCP load distribution](#), page 48.

**HASH** applies a hash operation to the selected distribution attributes.

- With HASH, more than one distribution attribute can be selected.
- The result of the hash operation determines the cluster member that receives the traffic.

**MASK** applies a mask operation to the selected distribution attribute.

- Only one distribution attribute can be selected, typically the destination IP address.
- The result of the mask operation determines the cluster member that receives the traffic.

The following distribution attributes can be selected:

- Destination IP address
- Destination Port
- Source IP address
- Source Port

The MASK value is applied up to 6 significant bits (in a cluster, a total of 64 buckets are created). See your WCCP documentation for more information about assignment method HASH and MASK operations. Use the value recommended in the manufacturer's documentation for your device.

- b. **Weight:** For proportional load distribution, specify a value from 0-255. This value determines the proportional distribution of load among servers in a cluster.

All cluster members have a value of 0 by default, which results in a balanced distribution of traffic. If weight is set to 1 or higher, the value guides proportional distribution among the nodes. For example, if there are 3 nodes

in a cluster and proxy 1 has a weight of 20, proxy 2 has a weight of 10, and proxy 3 has a weight of 10, proxy 1 will get one half of the traffic, proxy 2 will get one-quarter of the traffic, and proxy 3 will get one-quarter of the traffic.

**Note**

When the value of **weight** is greater than 0 on any member of the cluster, any member of the cluster with a weight of 0 receives **no** traffic. If you plan to use weight, be sure to set the weight on every member of the cluster.

---

**Note**

Because the value of weight determines the proportional distribution relative to the value set on other cluster members, the value of weight is not propagated around the cluster.

---

For more information about load distribution, see [WCCP load distribution, page 48](#).

- c. **Reverse Service Group ID:** Allows you to specify a reserve service group ID.

When IP spoofing is enabled, you must define a reverse service group for each HTTP and HTTPS (if enabled) forward service group.

**Note**

Only HTTP and HTTPS are supported for IP Spoofing.

---

Using the specified ID, Content Gateway creates a reverse service group that is a mirror of the forward service group. For example, if the forward service group has assignment method based on destination IP address, the reverse service has an assignment method based on the source IP address.

**Note**

IP spoofing is not supported with service groups that use a hashing assignment method with both destination and source attributes. If IP spoofing is enabled on such a service group, an alarm is raised and IP spoofing is disabled.

---

6. Click **Add** to an entry, or click **Set** to save changes to an existing entry.
7. Click **Close** to close the editor.
8. On the **Configure > Networking > WCCP > General** page, click **Apply** to apply changes. Navigating away from the page before clicking **Apply** results in the loss of all changes.



9. To restart the proxy to cause the changes to take effect, go to **Configure > My Proxy > Basic > General** and click **Restart**.



#### Note

To check that the router is sending traffic to the proxy, examine the statistics in the Content Gateway Manager **Monitor** pane. For example, check that the **Objects Served** statistic in the **My Proxy > Summary** section increases.



#### Note

It may take up to a minute for the router to report that a new proxy server has joined a service group.

## Transparent interception and multicast mode

To configure Content Gateway to run in multicast mode, you must enable multicast mode and specify the multicast IP address in Content Gateway Manager.

In addition, you must set the multicast address on your routers for each service group being intercepted (HTTP, FTP, DNS, and SOCKS). The following procedure provides an example of how to set the multicast address for different service groups on a WCCP v2-enabled router.

1. Telnet to the router and switch to Enable mode.
2. At the prompt, enter the following command to configure the router from the terminal:  

```
configure terminal
```
3. At the prompt, enter the following command for each service group that the router intercepts:  

```
hostname(config)# ip wccp service_group group-address multicast_address
```

where *hostname* is the host name of the router you are configuring, *service\_group* is the service group ID (for example, 0 for HTTP), and *multicast\_address* is the IP multicast address.
4. At the prompt, enter the following command to configure the network interface:  

```
interface interface_name
```

where *interface\_name* is the network interface on the router that is being intercepted and redirected.
5. At the prompt, enter the following command for each service group that the router intercepts:  

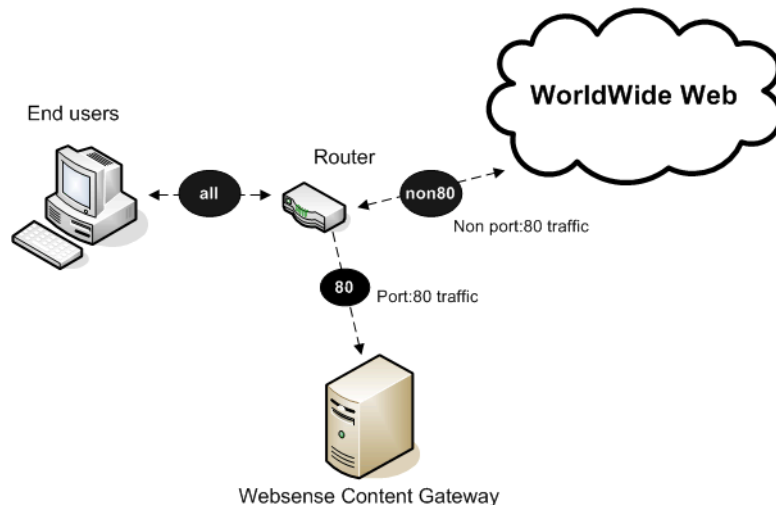
```
hostname(config-if)# ip wccp service_group group-listen
```
6. Exit and save the router configuration.

## Transparent interception with policy-based routing

Instead of the WCCP protocol, you can use the policy routing capabilities of a router to send traffic to Content Gateway. WCCP or a Layer 4 switch are generally preferable to this configuration because policy-based routing has a performance impact on the router, and policy-based routing does not support load balancing or heartbeat messaging.

- ◆ All client Internet traffic is sent to a router that feeds Content Gateway.
- ◆ The router sends port 80 (HTTP) traffic to the proxy and sends the remaining traffic to the next hop router.
- ◆ The ARM translates intercepted requests into Content Gateway requests.
- ◆ Translated requests are sent to the proxy.
- ◆ Web objects to be served transparently are readdressed by the ARM on the return path to the client, so that the documents appear to have come from the origin server.

A Content Gateway cluster with virtual IP failover adds reliability; if one node fails, another node can take up its transparency requests. See [Virtual IP failover](#), page 74.



## Transparent interception with software-based routing

You can deploy Content Gateway without adding routers or switches by using routing software on the Content Gateway node. In this case, Content Gateway is a software router and directs all traffic through the proxy machine. This solution can be useful in low-traffic situations, where the performance cost of using the proxy machine as a router is not high.

On Linux systems, you can use the **routed** and **gated** daemons as a software-based routing solution. The **routed** daemon is a bundled part of all normal Linux distributions. The **gated** daemon is an extensible commercial software package from the Merit GateD Consortium.

When you use routing software with Content Gateway:

- ◆ All Internet traffic goes through Content Gateway from machines behind it in the network.
- ◆ The routing software routes all non-transparent requests to the Internet; it routes port 80 HTTP requests to the proxy cache.
- ◆ The ARM translates intercepted requests into proxy requests.
- ◆ Translated requests are sent to the proxy.
- ◆ Web objects to be served transparently are readdressed by the ARM on the return path to the client, so that the objects appear to have come from the origin server.

**Note**

Although Content Gateway machines can function as routers, they are not expressly designed to be routers. For reliability, you can use a Content Gateway cluster with the virtual IP failover option. If one node fails, another cluster node takes over. See [Virtual IP failover, page 74](#).) The Content Gateway cluster failover mechanism is similar to the Hot Standby Router Protocol (HSRP).

---

## Interception bypass

---

A small number of clients and servers do not work correctly with Web proxies. Some reasons include:

- ◆ Client software irregularities (customized, non-commercial browsers).
- ◆ Server software irregularities.
- ◆ Applications that send non-HTTP traffic over HTTP ports as a way of defeating security restrictions.
- ◆ Server IP address authentication (the origin server limits access to a few client IP addresses, but the Content Gateway IP address is different, so it cannot get access). This is not in frequent use because many ISPs dynamically allocate client IP dial-up addresses, and more secure cryptographic protocols are now more often used.

Web proxies are very common in corporate and Internet use, so interoperability problems are rare. However, Content Gateway contains an adaptive learning module that recognizes interoperability problems caused by transparent proxy processing and automatically bypasses the traffic around the proxy server without operator intervention.

Content Gateway follows 2 types of bypass rules:

- ◆ *Dynamic* (also called adaptive) bypass rules are generated dynamically if you configure Content Gateway to bypass the cache when it detects non-HTTP traffic

on port 80 or when it encounters certain HTTP errors. See [Dynamic bypass rules](#), page 62.

- ◆ *Static* bypass rules must be manually configured in the **bypass.config** file. See [Static bypass rules](#), page 63.



#### Note

Do not confuse bypass rules with client access control lists. Bypass rules are generated in response to interoperability problems. Client access control is simply restriction of the client IP addresses that can access the proxy cache, as described in [Controlling client access to the proxy](#), page 153.

## Dynamic bypass rules

Related topics:

[Setting dynamic bypass rules](#), page 63

[Viewing dynamic bypass statistics](#), page 63

When configured to do so, the proxy watches for protocol interoperability errors. As it detects errors, it configures the ARM to bypass the proxy for those clients and servers causing the errors.

In this way, the small number of clients or servers that do not operate correctly through proxies are auto-detected and routed around the proxy caching server so that they can continue to function (but without caching).

You can configure the proxy to dynamically bypass the cache for any of the following errors:

Error code	Description
N/A	Non-HTTP traffic on port 80
400	Bad Request
401	Unauthorized
403	Forbidden (authentication failed)
405	Method Not Allowed
406	Not Acceptable (access)
408	Request Timeout
500	Internal Server Error

For example, when Content Gateway is configured to bypass on authentication failure (**403 Forbidden**), if any request to an origin server returns a 403 error, Content

Gateway generates a destination bypass rule for the origin server's IP address. All requests to that origin server are bypassed until you restart the proxy.

In another example, if the ARM detects that a client is sending a non-HTTP request on port 80 to a particular origin server, Content Gateway generates a source/destination rule. All requests from that particular client to the origin server are bypassed; requests from other clients are not bypassed.

Bypass rules that are generated dynamically are purged after a Content Gateway restart. If you want to preserve dynamically generated rules, you can save a snapshot of the current set of bypass rules. See [Viewing the current set of bypass rules](#), page 64.

To prevent Content Gateway from bypassing certain IP addresses dynamically, you can set dynamic deny bypass rules in the **bypass.config** file. Deny bypass rules can prevent the proxy from bypassing itself. For information about setting dynamic deny bypass rules, see [bypass.config](#), page 322.

## Setting dynamic bypass rules

By default, Content Gateway is not configured to bypass the cache when it encounters HTTP errors or non-HTTP traffic on port 80. You must enable dynamic bypass rules by setting the appropriate options.

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the **Features** table, make sure that **ARM** is **On** in the **Networking** section.
3. Navigate to **Configure > Networking > ARM > Dynamic Bypass**.
4. Enable the **Dynamic Bypass** option.
5. In the **Behavior** section, select the dynamic bypass rules you want to use.
6. Click **Apply**.
7. Click **Restart** on the **Configure > My Proxy > Basic > General** tab.

## Viewing dynamic bypass statistics

Content Gateway tallies bypassed requests for each type of dynamic bypass trigger. For example, Content Gateway counts all requests that are bypassed in response to a 401 error.

- Navigate to **Monitor > Networking > ARM**.

The statistics are displayed in the **HTTP Bypass Statistics** section of the table.

## Static bypass rules

You can configure bypass rules to direct requests from certain clients or to particular origin servers around the proxy. Unlike dynamic bypass rules that are purged when you restart the proxy, these static bypass rules are saved in a configuration file.

You can configure 3 types of static bypass rules:

- ◆ Source bypass, in which Content Gateway bypasses a particular source IP address or range of IP addresses. For example, you can use this solution to bypass clients who want to opt out of a caching solution.
- ◆ Destination bypass, in which Content Gateway bypasses a particular destination IP address or range of IP addresses. For example, these could be origin servers that use IP authentication based on the client's real IP address. Destination bypass rules prevent Content Gateway from caching an entire site. You will experience hit rate impacts if the site you bypass is popular.
- ◆ Source/destination pair bypass, in which Content Gateway bypasses requests that originate from the specified source to the specified destination. For example, you could route around specific client-server pairs that experience broken IP authentication or out of band HTTP traffic problems when cached.  
  
Source/destination bypass rules might be preferable to destination rules because they block a destination server only for those particular users that experience problems.

To configure static bypass rules, edit the **bypass.config** file (See [bypass.config](#), page 322).

## Viewing the current set of bypass rules

The ARM has a supporting utility called **print\_bypass** that allows you to view the current dynamic and static bypass rules.

To view all current dynamic and static bypass rules:

1. Log on to a Content Gateway node as the Content Gateway administrator, and then change to the Content Gateway **bin** directory (`/opt/WCG/bin`).
2. Enter the following command at the prompt and press **Return**:

```
./print_bypass
```

All current static and dynamic bypass rules are displayed on screen. The rules are sorted by IP address. You can direct the output of **print\_bypass** to a file and save it.

## Connection load shedding

---

The load shedding feature prevents client request overloads. When there are more client connections than the specified limit, the ARM forwards incoming requests directly to the origin server. The default client connection limit is 1 million connections.

1. Navigate to **Configure > Networking > Connection Management > Load Shedding**.
2. In the **Maximum Connections** field, specify the maximum number of client connections allowed before the ARM starts forwarding requests directly to the origin server.

3. Click **Apply**.
4. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Reducing DNS lookups

If you are running Content Gateway in transparent proxy mode, you can enable the *Always Query Destination* option to reduce the number of DNS lookups and improve response time. When enabled, the Always Query Destination option configures the proxy to always obtain the original destination IP address of incoming requests from the ARM. Content Gateway then uses that IP address to determine the origin server instead of doing a DNS lookup on the hostname of the request. Because the client already performed a DNS lookup, Content Gateway does not have to.



### Note

It is recommended that you do not enable the Always Query Destination option if Content Gateway is running in both explicit and transparent proxy mode. See [How do you configure Content Gateway to serve only transparent requests?](#), page 428, for information about running Content Gateway in transparent proxy mode only. In explicit proxy mode, the client does not perform a DNS lookup on the hostname of the origin server, so the proxy must perform a DNS lookup. Also, the category lookup is performed based on the IP address, which is not always as accurate as a URL-based lookup.

In addition, do not enable the Always Query Destination option if you want domain names, rather than IP addresses, to be captured in the log server.

To enable the Always Query Destination option:

1. Open the **records.config** file in the Content Gateway **config** directory (/opt/WCG/config).
2. Edit the following variable:

Variable	Description
<code>proxy.config.arm.always_query_dest</code>	<p>Set to 0 to disable the Always Query Destination option. Domain names are captured.</p> <p>Set to 1 to enable the Always Query Destination option. IP addresses are captured; domain names are not.</p>

3. Save and close the file.

4. To apply the changes, run the following command from the Content Gateway **bin** directory:

```
content_line -x
```

## IP spoofing

---

IP spoofing configures the proxy to use the IP address of the client when communicating with the origin server, instead of the proxy's own IP address. As a result, requests appear to come from the client rather than the proxy.

- ◆ IP spoofing is supported for HTTP and HTTPS traffic only.
- ◆ When IP spoofing is enabled, it is applied to both HTTP and HTTPS. It cannot be configured to apply to only one protocol.
- ◆ IP spoofing is supported for transparent traffic only.

Use of the ARM is required with IP spoofing. Before IP spoofing can be enabled, ARM must be enabled. (ARM translates the IP addresses of outgoing requests and incoming responses.) Do not disable ARM when IP spoofing is enabled.



### Warning

Deploying IP spoofing requires precise control of the routing paths on your network, overriding the normal routing process for traffic running on TCP port 80 and 443.

With IP spoofing enabled, traditional debugging tools such as **traceroute** and **ping** have limited utility.



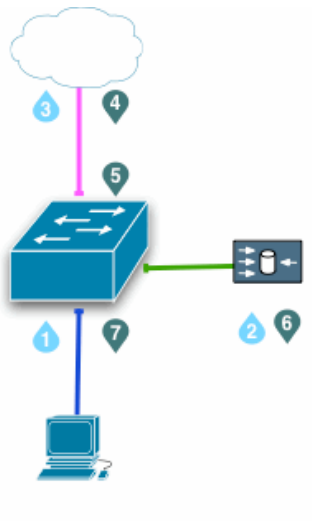
### Important

For a discussion of how the proxy kernel routing table impacts transparent proxy deployment, see the Solution Center article titled, “Web sites in the Static or Dynamic bypass list fail to connect”.

## IP spoofing and the flow of traffic

The following describes the flow of HTTP and HTTPS traffic when IP spoofing is used with WCCP. Policy-based routing can be implemented to achieve the same results. The numbers in the diagram correspond to the actions described in the numbered list.





1. A client request arrives at a routed port or Switched Virtual Interface (SVI) looking for traffic with a destination port of HTTP (80) or HTTPS (443).
2. The switch redirects the client request to Content Gateway (the proxy), and Content Gateway internally routes the traffic to port 8080 (HTTP) or 8070 (HTTPS) of its own IP address.  
If needed, the proxy creates a connection to the Web origin server using the original client IP address.
3. The request is sent to the Web origin server through the switch, NAT and/or firewall.
4. When the origin server response is returned, the IP packet has the client IP address as the destination.
5. The origin server response arrives at a routed port or Switched Virtual Interface (SVI) looking for traffic with a source port of HTTP (80) or HTTPS (443). See the note below.
6. The switch redirects the origin server response to the proxy, completing the proxy-to-Web server TCP connection.
7. A proxy response to the client is generated and returned to the client on the proxy-to-client TCP connection.



#### Note

When IP spoofing is enabled, the proxy advertises a reverse service group for each enabled WCCP service. The reverse service group must be applied along the return path of the proxy.

WCCP service group IDs are user defined and must be programmed on the WCCP device(s) and in Content Gateway (see [Configuring service groups on the WCCP device](#) and [Configuring service groups in Content Gateway Manager](#)).

Following is a set of suggested definitions.

Service ID	Port	Traffic Type
0	destination port 80	HTTP
20	source port 80	HTTP
70	destination port 443	HTTPS (requires SSL Manager)
90	source port 443	HTTPS

**Policy-based routing** (PBR) uses access control lists (ACL) to identify and redirect flows. In a PBR deployment, all of the configuration is done on the router and there is no corresponding Content Gateway configuration. PBR deployments have to redirect traffic returning from origin servers from port 80 and 443 to Content Gateway.

## Enabling IP spoofing:

1. Navigate to **Configure > Networking > ARM > General**.  
(If ARM is not a choice, go to **Configure > My Proxy > Basic > General** and ensure that ARM is **On**.)
2. Select **IP Spoofing**.
3. Click **Apply**.
4. Click **Restart** on **Configure > My Proxy > Basic > General**.



### Warning

Do not disable ARM while IP spoofing is enabled. If it is, client requests receive a cannot display Web page error; an error message is also recorded in /var/log/message.

---

For information about configuring WCCP routers, see [Configuring WCCP v2 routers](#), page 50.

# 6

## Clusters

### Related topics:

[SSL Manager clustering, page 70](#)

[Changing clustering configuration, page 72](#)

[Adding nodes to a cluster, page 72](#)

[Deleting nodes from a cluster, page 74](#)

[Virtual IP failover, page 74](#)

Websense Content Gateway scales from a single node to a cluster of up to 8 nodes, allowing you to increase capacity and improve system performance and reliability.

- ◆ Content Gateway detects the addition and deletion of nodes in the cluster and can detect when a node is down.
- ◆ You can add or delete a node from a cluster at any time.
- ◆ When you remove a node from the cluster, Content Gateway removes all references to the missing node.
- ◆ Restarting a node in the cluster causes all nodes in the cluster to restart.
- ◆ When the [Virtual IP failover](#) feature is enabled, the live nodes in a cluster can assume a failed node's traffic.
- ◆ Nodes in a cluster automatically share configuration information.



### Note

Filtering Service and Policy Service IP addresses are not propagated around the cluster.

In transparent proxy deployments with WCCP, the service group Enabled/Disabled state and Weight settings are not propagated. See [Transparent interception with WCCP v2 devices, page 46](#).

Content Gateway uses a proprietary protocol for clustering, which is multicast for node discovery and heartbeat, and unicast for all data exchange within the cluster.



---

**Important**

It is recommended that a dedicated network interface be used for Content Gateway cluster communication, **except** when the host is a V-Series appliance, in which case the P1 (eth0) interface is recommended.

---



---

**Important**

In a proxy hierarchy, the nodes in the cluster cannot be a mixture of HTTP parents and children; you must configure each node in a Content Gateway cluster as a single node in the hierarchy because they share a common configuration.

---

## Management clustering

---

In management clustering mode, you can administer all Content Gateway nodes at the same time because cluster nodes share configuration information.



---

**Note**

Cluster size is limited to 8 nodes.

---

Content Gateway uses a multicast management protocol to provide a single system image of your Content Gateway cluster. Information about cluster membership, configuration, and exceptions is shared across all nodes, and the **content\_manager** process automatically propagates configuration changes to all nodes.

When SSL Manager is enabled, SSL configuration information is propagated around the cluster, however it uses a separate mechanism. See the following section.

## SSL Manager clustering

---

When SSL Manager is enabled in a cluster, SSL configuration information can also be propagated around the cluster, however it uses a different mechanism that requires separate configuration.

To configure SSL Manager to propagate configuration information around the cluster, one node must be selected as the **primary** node on which all SSL configuration changes are made. The primary is known as the **SSL Manager Configuration Server**. All other nodes are **secondaries**.

- ◆ Settings made on the primary are propagated to the secondaries.
- ◆ Secondaries periodically poll the primary to see if changes are pending. If changes are pending, each secondary pulls them down.
- ◆ If configuration changes are made on a secondary, they are overwritten when the master configuration is pulled from the primary.
- ◆ Should the primary go down, an alarm is generated and the secondaries continue to operate with their current configuration until the primary returns to service or a new primary is configured.

When SSL Manager clustering is configured, the following configuration settings are propagated:

- ◆ The IP address of the primary
- ◆ Configure > SSL > Certificates > Certificate Authorities
- ◆ Configure > SSL > Certificates > Add Root CA
- ◆ Configure > SSL > Certificates > Restore Certificates
- ◆ Configure > SSL > Decryption / Encryption: all settings
- ◆ Configure > SSL > Validation: all settings
- ◆ Configure > SSL > Client Certificates: all settings
- ◆ Configure > SSL > Logging: all settings
- ◆ Configure > SSL > Internal Root CA > Import Root CA
- ◆ Configure > SSL > Internal Root CA > Create Root CA
- ◆ Dynamically generated certificates and incidents

## Configuring SSL Manager clustering:

1. Configure and start Management Clustering. See [Changing clustering configuration](#).
2. On any node in the cluster, log on to Content Gateway Manager.
3. Go to the **Configure > My Proxy > Basic > Clustering** tab.
4. In the **SSL Manager Configuration Server** field, enter the IP address of the SSL Manager Configuration Server (the primary). (If the field is not editable, the system is not a member of a cluster.)
5. Click **Apply** and restart Content Gateway. Note that all Content Gateway nodes are restarted. The restart identifies the primary to all cluster members and activates SSL clustering.

The configuration can be confirmed on the **Monitor > My Proxy > Summary** page, at the bottom of the **Node Details** section. If the **SSL Manager Configuration Server** IP address is a link, the server is another node in the cluster. Click the link to log onto the **SSL Manager Configuration Server**.

## Changing clustering configuration

---

Clustering is usually configured when you install the proxy. You can, however, configure clustering afterward, or at any time, in Content Gateway Manager.

1. In Content Gateway Manager, go to the **Configure > My Proxy > Basic > Clustering** tab.
2. In the **Cluster Type** area, select the clustering mode:
  - Select **Management Clustering** to include this proxy in a cluster.
  - Select **Single Node** if this node is not part of a cluster.
3. In the **Cluster Interface** area, enter the name of the network interface. This is the interface used by Content Gateway to communicate with other nodes in the cluster, for example: eth0.

It is recommended that you use a dedicated secondary interface.

Node configuration information is multicast, in plain text, to other Content Gateway nodes on the same subnet. Therefore, Websense recommends that clients be located on a separate subnet from Content Gateway nodes (multicast communications for clustering are not routed).

On V-Series appliances, P1 (eth0) is the recommended interface. However, you may also use P2 (eth1) if you want to isolate cluster management traffic.

4. In the **Cluster Multicast Group Address** area, enter the multicast group address that all members of the cluster share.
5. If you are using **SSL Manager** and want SSL configuration information to propagate around the cluster, enter the IP address of the SSL Manager Configuration Server. In a cluster, SSL configuration information is managed via a separate mechanism. You must be familiar with the mechanism to effectively use this feature. See [SSL Manager clustering](#).
6. Click **Apply**.
7. Click **Restart** on **Configure > My Proxy > Basic > General**.



### Important

Content Gateway does not apply the clustering mode change to all of the nodes in the cluster. You must change the clustering mode on each node individually.

---

## Adding nodes to a cluster

---

Content Gateway detects new Content Gateway nodes on your network and adds them to the cluster, propagating the latest configuration information to the newcomer. This provides a convenient way to bootstrap new machines.

To connect a node to a Content Gateway cluster, you need only install Content Gateway software on the new node, making sure during the process that the cluster name and port assignments are the same as those of the existing cluster. In this way, Content Gateway automatically recognizes the new node.



### Important

The nodes in a cluster must be homogeneous; each node must be on the same hardware platform, each must be on the same operating system version, and Content Gateway must be installed in the same directory (/opt/WCG).

1. Install the appropriate hardware and connect it to your network. (Consult your hardware documentation for hardware installation instructions.)
2. Install the Content Gateway software using the appropriate procedure for installing a cluster node. See the *Content Gateway Installation Guide*. During the installation procedure, make sure that the following is true:
  - The cluster name that you assign to the new node is the same as the cluster name for the existing cluster.
  - The port assignments for the new node are the same as the port assignments used by the other nodes in the cluster.
  - You have added multicast addresses and multicast route settings.
3. Restart Content Gateway. See [Starting and stopping Content Gateway on the Command Line](#), page 15.

If you have an existing Content Gateway installation and you want to add that server to the cluster, you do not have to reinstall Content Gateway on the node. Instead, you can edit configuration variables on the existing Content Gateway node.

1. On the node you want to add to the cluster, open the **records.config** file located in **/opt/WCG/config**.
2. Edit the following variables:

Variable	Description
<code>proxy.local.cluster.type</code>	Specify the clustering mode: 2 = management mode 3 = no clustering
<code>proxy.config.proxy_name</code>	Specify the name of the Content Gateway cluster. All nodes in a cluster must use the same name.
<code>proxy.config.cluster.mc_group_addr</code>	Specify the multicast address for cluster communications. All nodes in a cluster must use the same multicast address.

Variable	Description
<code>proxy.config.cluster.rsport</code>	Specify the reliable service port. The reliable service port is used to send data between the nodes in the cluster. All nodes in a cluster must use the same reliable service port. The default value is 8087.
<code>proxy.config.cluster.mcport</code>	Specify the multicast port. The multicast port is used for node identification. All nodes in a cluster must use the same multicast port. The default port number is 8088.
<code>proxy.config.cluster.ethernet_interface</code>	Specify the network interface for cluster traffic. All nodes in a cluster must use the same network interface.

3. Save and close the file.
4. Restart Content Gateway (**/opt/WCG/WCGAdmin restart**).

To change from Management mode to Single node or vice versa:

1. Access Content Gateway Manager.
2. Navigate to **Configure > My Proxy > Basic > Clustering**.
3. In the **Cluster Type** area, select the appropriate type (**Single** or **Management**).
4. Click **Apply**.
5. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Deleting nodes from a cluster

---

On the node you want to remove from the cluster:

1. Navigate to **Configure > My Proxy > Basic > Clustering**.
2. In the **Cluster Type** area, select **Single Node**.
3. Click **Apply**.
4. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Virtual IP failover

---

Through the virtual IP failover feature, Content Gateway maintains a pool of virtual IP addresses that it assigns to the nodes in the cluster as necessary. These addresses are virtual only in the sense that they are not tied to a specific machine; Content Gateway can assign them to any of its nodes. To the outside world, these virtual IP addresses are the addresses of Content Gateway servers.



Virtual IP failover assures that if a node in the cluster fails, other nodes can assume the failed node's responsibilities. Content Gateway handles virtual IP failover in the following ways:

- ◆ The **content\_manager** process maintains cluster communication. Nodes automatically exchange statistics and configuration information through multicast communication. If multicast heartbeats are not received from one of the cluster nodes, the other nodes recognize it as unavailable.
- ◆ The **content\_manager** process reassigns the IP addresses of the failed node to the remaining operational nodes within approximately 30 seconds, so that service can continue without interruption.
- ◆ The IP addresses are assigned to new network interfaces, and the new assignment is broadcast to the local network. The IP reassignment is done through a process called *ARP rebinding*.

## What are virtual IP addresses?

Related topics:

[Enabling and disabling virtual IP addressing, page 75](#)

[Adding and editing virtual IP addresses, page 76](#)

Virtual IP addresses are IP addresses that are not tethered to particular machines. Thus, they can rotate among nodes in a Content Gateway cluster.

It is common for a single machine to represent multiple IP addresses on the same subnet. This machine would have a primary or real IP address bound to its interface card and also serve many more virtual addresses.

You can set up your user base to use a DNS round-robin pointing at virtual IP addresses, as opposed to using the real IP addresses of the Content Gateway machines.

Because virtual IP addresses are not bound to machines, a Content Gateway cluster can take addresses from inactive nodes and distribute those addresses among the remaining live nodes.

Using a proprietary management protocol, Content Gateway nodes communicate their status with their peers. If a node fails, its peers notice the failure and negotiate which of the remaining nodes will mask the fault by taking over the failed node's virtual interface.

## Enabling and disabling virtual IP addressing

1. Navigate to **Configure > My Proxy > Basic > General**.
2. Under the Networking section in the Features table, select **On** or **Off** for **Virtual IP** to enable or disable Virtual IP addressing.
3. Click **Apply**.

4. Click **Restart** on **Configure > My Proxy > Basic > General** to restart Content Gateway on all the nodes in the cluster.

## Adding and editing virtual IP addresses

Virtual IP addresses must be pre-reserved like all IP addresses before they can be assigned to Content Gateway.



---

### Warning

Incorrect IP addressing can disable your system. Make sure you understand how virtual IP addresses work before changing them.

---

1. Navigate to **Configure > Networking > Virtual IP**.

The **Virtual IP Addresses** area displays the virtual IP addresses managed by Content Gateway.



---

### Note

The Virtual IP button is displayed only if you have enabled the Virtual IP option in the Features table on **Configure > My Proxy > Basic > General**.

---

2. Click **Edit File** to add new or edit existing virtual IP addresses.
3. To edit a virtual IP address, select it from the table at the top of the page, edit the fields provided, and then click **Set**.  
To delete the selected IP address, click **Clear Fields**.  
To add a virtual IP address, specify the virtual IP address, the Ethernet interface, and the Subinterface in the fields provided, and then click **Add**.
4. Click **Apply**, and then click **Close**.
5. Click **Restart** on **Configure > My Proxy > Basic > General**.

# 7

## Hierarchical Caching

Websense Content Gateway can participate in [HTTP cache hierarchies](#), [page 77](#), in which requests not fulfilled in one cache can be routed to other regional caches, taking advantage of the contents and proximity of nearby caches.

A cache hierarchy consists of levels of caches that communicate with each other. Content Gateway supports several types of cache hierarchies. All cache hierarchies recognize the concept of *parent* and *child*. A parent cache is a cache higher up in the hierarchy, to which the proxy can forward requests. A child cache is a cache for which the proxy is a parent.

### HTTP cache hierarchies

---

In an HTTP cache hierarchy, if a Content Gateway node cannot find a requested object in its cache, it can search a parent cache—which itself can search other caches—before resorting to retrieving the object from the origin server.

You can configure a Content Gateway node to use one or more HTTP parent caches, so that if one parent is unavailable, another parent can service requests. This is called parent failover and is described in [Parent failover, page 78](#).

**Note**

If you do not want all requests to go to the parent cache, you can configure the proxy to route certain requests directly to the origin server (for example, requests that contain specific URLs) by setting parent proxy rules in the **parent.config** configuration file (described in [parent.config, page 343](#)).

**Note**

If the request is a cache miss on the parent, the parent retrieves the content from the origin server (or from another cache, depending on the parent's configuration). The parent caches the content and then sends a copy to the proxy (its child), where it is cached and served to the client.

## Parent failover

When you configure the proxy to use more than one parent cache, the proxy detects when a parent is not available and sends missed requests to another parent cache. If you specify more than two parent caches, the order in which the parent caches are queried depends upon the parent proxy rules configured in the parent configuration file described in [parent.config, page 343](#). By default, the parent caches are queried in the order in which they are listed in the configuration file.

## Configuring Content Gateway to use an HTTP parent cache

1. On the **Configure > Content Routing > Hierarchies > Parenting** page, enable **Parent Proxy**.
2. Click **Edit File** to open the configuration file editor for the [parent.config](#) file.
3. Enter information in the fields provided, and then click **Add**. All the fields are described in [Hierarchies, page 270](#).
4. Click **Apply**, and then click **Close**.
5. On the **Parenting** tab, click **Apply** to save your configuration.

**Important**

Perform this procedure on the *child* proxy. Do not make any changes on the parent.





# 8

## Configuring the Cache

The cache consists of a high-speed object database called the **object store**. The object store indexes objects according to URLs and associated headers, enabling Websense Content Gateway to store, retrieve, and serve Web pages, and also parts of Web pages, providing optimum bandwidth savings. Using object management, the object store can cache alternate versions of the same object, varying on spoken language or encoding type, and can store small and large documents, minimizing wasted space. When the cache is full, Content Gateway removes stale data.

Content Gateway can tolerate disk failures on any cache disk. If the disk fails, Content Gateway marks the disk as corrupt and continues using the remaining disks. An alarm is sent to Content Gateway Manager, indicating which disk failed. If all cache disks fail, Content Gateway goes into proxy-only mode.

You can perform the following cache configuration tasks:

- ◆ Add a cache disk after installation. See [Adding a cache disk after installation](#), page 82.
- ◆ Change the total amount of disk space allocated to the cache. See [Changing cache capacity](#), page 83.
- ◆ Partition the cache by reserving cache disk space for specific protocols and origin servers and domains. See [Partitioning the cache](#), page 85.
- ◆ Specify a size limit for objects allowed in the cache. See [Configuring cache object size limit](#), page 87.
- ◆ Delete all data in the cache. See [Clearing the cache](#), page 87.
- ◆ Change the size of the RAM cache. See [Changing the size of the RAM cache](#), page 88.

### RAM cache

Content Gateway maintains a small RAM cache of popular objects. This RAM cache serves the most popular objects as fast as possible and reduces load on disks, especially during temporary traffic peaks. You can configure the RAM cache size. See [Changing the size of the RAM cache](#), page 88.

## Adding a cache disk after installation

---

To add a cache disk, you need to have:

- ◆ An unformatted physical disk device (created by OS install). Note the size in bytes.
- ◆ A raw character device (created with `mknod`)

Adding the device includes mapping the physical disk to the raw character device.

Most of the examples below show commands for an HP DL360 and its RAID controller. (All disks are RAID 0.)

1. Set up the raw device and modify the permissions:

```
mknod /etc/udev/devices/raw c 162 0
chmod 600 /etc/udev/devices/raw
```

2. Identify the cache disk physical device name and note the size in bytes (used later):

```
fdisk -l | grep "^Disk"
Disk /dev/cciss/c0d1: 146.7 GB, 146778685440 bytes
```

3. Create a node, change the owner of the node, and map that raw node to a physical disk. Note that the final argument increments by 1 for each disk added:

```
mknod /etc/udev/devices/raw_c0d1 c 162 1 You can change
the device name to the name that is returned from the
fdisk -l command.

chown Websense /etc/udev/devices/raw_c0d1 Use the device
name you used in the mknod statement.

/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
Use the device name you used in the mknod statement.
```

4. To make the changes effective on reboot, add the same `/usr/bin/raw` commands to `/etc/init.d/content_gateway` at line 6:

```
...
case "$1" in
'start')

/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
Use the device name you used in the mknod statement.

...
```

5. Add the devices to `/opt/WCG/config/storage.conf` using the raw node and the size in blocks returned by `fdisk -l`:

```
/etc/udev/devices/raw_c0d1 146778685440
Use the device name you used in the mknod statement.
```

6. Verify that caching is enabled. If the installation didn't set up any cache disks, caching will be disabled:



- a. In Content Manager, go to **Configure > Protocols > HTTP** and click the **Cacheability** tab.
- b. Under **HTTP Caching**, select **Enabled**.
- c. Click **Apply** and restart Content Gateway.

## Changing cache capacity

The maximum aggregate disk cache size is limited to 147 GB. This size makes best use of system resources, while also providing an excellent end-user experience.

The minimum disk cache size is 2 GB.

Related topics:

[Querying cache size, page 83](#)

[Increasing cache capacity, page 83](#)

[Reducing cache capacity, page 84](#)

## Querying cache size

To view the configured aggregate cache size, open the Content Manager and go to **Monitor > Subsystems > Cache**. The cache size is displayed, in bytes, in the **Current Value** column of the **Cache Size** field.

Alternatively, display the cache size with the following command, executed from the Content Gateway **bin** directory (**/opt/WCG/bin**).

```
content_line -r proxy.process.cache.bytes_total
```

## Increasing cache capacity

To increase the total disk space allocated to the cache on existing disks, or to add new disks to a Content Gateway node:

1. Stop Content Gateway. See [Starting and stopping Content Gateway on the Command Line, page 15](#).
2. Add hardware, if necessary.
  - a. Set up the raw device and modify the permissions. For example:
 

```
mknod /etc/udev/devices/raw c 162 0
chmod 600 /etc/udev/devices/raw
```
  - b. Identify the physical device name and note the size in bytes (used later). For example:
 

```
fdisk -l | grep "^Disk"
```

Disk /dev/cciss/c0d1: 146.7 GB, 146778685440 bytes

- c. For each real disk, create a node, change the owner of the node, and map that raw node to a physical disk. Note that the final argument increments by 1 for each disk added.

To create a node:

```
mknod /etc/udev/devices/raw_c0d1 c 162 1
```

You can change the device name to the name that is returned from the **fdisk -l** command in step b.

To change the owner:

```
chown Websense /etc/udev/devices/raw_c0d1
```

The owner is the installation user (default is Websense). Use the device name used in the mknod statement.

To map the raw node to a physical disk:

```
/usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
```

Use the device name used in the mknod statement.

- d. Add the same **/usr/bin/raw** commands to the **/etc/init.d/content\_gateway** file to make the changes effective on reboot. For example, at line 6 add:

```
...
case "$1" in
'start')
    /usr/bin/raw /etc/udev/devices/raw_c0d1 /dev/cciss/c0d1
```

3. Edit the **storage.config** file in the Content Gateway **config** directory (**/opt/WCG/config**) to increase the amount of disk space allocated to the cache on existing disks or add the new disk devices. See [storage.config](#), page 406.
4. Restart Content Gateway.

## Reducing cache capacity

You can reduce the total amount of disk space allocated to the cache on an existing disk or remove disks from a Content Gateway node.

1. Stop Content Gateway.
2. Remove hardware, if necessary.
3. Edit the **storage.config** file to reduce the amount of disk space allocated to the cache on existing disks or to delete the reference to the hardware you are removing. See [storage.config](#), page 406.
4. If you remove a disk, you must edit the **/etc/rc.d/init.d/content\_gateway** file to remove the raw disk binding for the disk.

5. Restart Content Gateway.

**Important**

In the **storage.config** file, a formatted or raw disk must be at least 2 GB.

---

## Partitioning the cache

---

You can manage your cache space more efficiently and restrict disk usage by creating cache partitions of different sizes for specific protocols. You can further configure these partitions to store data from specific origin servers and domains.

**Important**

HTTP is the only protocol supported at this time.

**Important**

The partition configuration must be the same on all nodes in a cluster.

---

## Creating cache partitions for specific protocols

You can create separate partitions for your cache that vary in size to store content according to protocol. This configuration ensures that a certain amount of disk space is always available for a particular protocol.

**Important**

HTTP is the only protocol supported at this time.

In the Content Gateway Manager:

1. Go to the **Configure > Subsystems > Cache > Partition** tab.
2. In the **Cache Partition** area, click **Edit File** to open the configuration file editor for the **partition.config** file.
3. Enter information in the fields provided, and then click **Add**. All the fields are described in [Cache, page 289](#).
4. Click **Apply** to save the information, and then click **Close**.

---

## Making changes to partition sizes and protocols

After you have configured your cache partitions based on protocol, you can make changes to the configuration at any time. Before making changes, note the following:

- ◆ You must stop Content Gateway before you change the cache partition size and protocol assignment.
- ◆ When you increase the size of a partition, the contents of the partition are **not** deleted. However, when you reduce the size of a partition, the contents of the partition **are** deleted.
- ◆ When you change the partition number, the partition is deleted and then re-created, even if the size and protocol type remain the same.
- ◆ When you add new disks to your Content Gateway node, the partition sizes specified in percentages increase proportionately.
- ◆ A lot of changes to the partition sizes might result in disk fragmentation, which affects performance and hit rate. It is recommended that you clear the cache (see [Clearing the cache](#), page 87) before making many changes to cache partition sizes.

## Partitioning the cache according to origin server or domain

After you have partitioned the cache according to size and protocol, you can assign the partitions you created to specific origin servers and domains.

You can assign a partition to a single origin server or multiple origin servers. However, if a partition is assigned to multiple origin servers, there is no guarantee on the space available in the partition for each origin server. Content is stored in the partition according to popularity.

In addition to assigning partitions to specific origin servers and domains, you must assign a generic partition to store content from all origin servers and domains that are not listed. This generic partition is also used if the partitions for a particular origin server or domain become corrupt.



### Important

If you do not assign a generic partition, Content Gateway runs in proxy-only mode.

---



### Note

You do **not** need to stop Content Gateway before you assign partitions to particular hosts or domains. However, this type of configuration can cause a spike in memory usage and is time consuming. It is recommended that you configure partition assignment during periods of low traffic.

---

You can partition the cache according to host name and domain in Content Gateway Manager.

In Content Gateway Manager:

1. Configure the cache partitions according to size and protocol, as described in [partition.config](#), page 346.

You should create a separate partition based on protocol (HTTP only) for each host and domain, and an additional generic partition to use for content that does not belong to these origin servers or domains. For example, if you want to separate content from two different origin servers, you must have at least three separate partitions: one HTTP-based partition for each origin server and a generic partition for all other origin servers not listed (the partitions do not have to be the same size).

2. On the **Configure** tab, click **Subsystems**, and then click **Cache**.
3. Click the **Hosting** tab and in the **Cache Hosting** area, click **Edit File** to open the configuration file editor for the **hosting.config** file.
4. Enter information in the fields provided, and then click **Add**. All the fields are described in [Cache](#), page 289.
5. Click **Apply**, and then click **Close**.

## Configuring cache object size limit

---

By default, Content Gateway allows objects of any size in the cache. You can change the default behavior and specify a size limit for objects in the cache.

1. Select **Configure > Subsystems > Cache > General**.
2. In the **Maximum Object Size** field, enter the maximum size allowed (in bytes) for objects in the cache. Enter 0 (zero) if you do not want to have a size limit.
3. Click **Apply**.

## Clearing the cache

---

When you clear the cache, you remove all data from the entire cache, which includes the data in the host database. Clear the cache before performing certain cache configuration tasks, such as partitioning.



### Note

You cannot clear the cache when Content Gateway is running.

---

1. Stop Content Gateway. See [Starting and stopping Content Gateway on the Command Line](#), page 15.
2. Enter the following command to clear the cache:

```
content_gateway -Cclear
```



---

**Warning**

The **clear** command deletes all data in the object store and the host database. Content Gateway does **not** prompt you to confirm the deletion.

---

3. Restart Content Gateway.

## Changing the size of the RAM cache

---

Content Gateway provides a dedicated RAM cache for fast retrieval of popular small objects. The default RAM cache size is calculated based on the number and size of the cache partitions you have configured. You can increase the RAM cache size for better cache hit performance.



---

**Warning**

If you increase the size of the RAM cache and observe a decrease in Content Gateway performance (such as increased latencies), the operating system might require more memory for network resources. Return the RAM cache size to its previous value.

---



---

**Note**

If you have partitioned your cache according to protocol or hosts, the size of the RAM cache for each partition is proportional to the size of that partition.

---

1. Select **Configure > Subsystems > Cache > General**.
2. In the **Ram Cache Size** field, enter the amount of space (in megabytes) you want to allocate to the RAM cache. Although the user interface will accept larger values, **do not exceed 512 MB**.

The default size is 104857600 (100 MB).



---

**Note**

A value of “-1” directs Content Gateway to automatically size the RAM cache to be approximately 1 MB per 1 GB of disk cache.

---

3. Click **Apply**.
4. Click **Restart** on **Configure > My Proxy > Basic > General**.







# 9

## DNS Proxy Caching

Typically, clients send DNS requests to a DNS server to resolve host names. However, DNS servers are frequently overloaded or not located close to the client; therefore DNS lookups can be slow and can be a bottleneck to fulfilling requests.

The DNS proxy caching option allows Content Gateway to resolve DNS requests on behalf of clients. This option off-loads remote DNS servers and reduces response time for DNS lookups.



### Important

You can use the DNS proxy caching option only with a layer 4 switch or a Cisco router running WCCP v2.

The following overview illustrates how Content Gateway serves a DNS request.

1. A client sends a DNS request. The request is intercepted by a router or L4 switch that is configured to redirect all DNS traffic on port 53 to Content Gateway.
2. The ARM examines the DNS packet. If the DNS request is **type A** (answer), the ARM forwards the request to Content Gateway. The ARM forwards all DNS requests that are not **type A** to the DNS server.
3. Content Gateway checks its DNS cache to see if it has the host name to IP address mapping for the DNS request. If the mapping is in the DNS cache, Content Gateway sends the IP address to the client. If the mapping is not in the cache, Content Gateway contacts the DNS server to resolve the host name. When Content Gateway receives the response from the DNS server, it caches the host name to IP address mapping and sends the IP address to the client. If round-robin is used, Content Gateway sends the entire list of IP address mappings to the client and the round-robin order is strictly followed.



### Note

If the host name to IP address mapping is not in the DNS cache, Content Gateway contacts the DNS server specified in the `/etc/resolv.conf` file. This might not be the same DNS server for which the DNS request was originally intended.

The DNS cache is held in memory and backed up on disk. Content Gateway updates the data on disk every 60 seconds. The TTL (time-to-live) is strictly followed with every host name to IP address mapping.

## Configuring DNS proxy caching

---

To configure Content Gateway as a DNS proxy cache:

- ◆ Add a remap rule in the **ipnat.conf** file.
- ◆ Enable the DNS proxy option and specify the port that Content Gateway will use for DNS proxy traffic.



### Important

You can use the DNS proxy caching option only with a layer 4 switch or a Cisco router running WCCP v2.

In Content Gateway Manager:

1. Go to the **Configure > Networking > ARM > General** tab.
2. In the **Network Address Translation (NAT)** section, click **Edit File** to open the file editor for the **ipnat.conf** file.
3. Enter information in the fields provided:
  - In the **Ethernet Interface** field, enter the Content Gateway ethernet interface to which client DNS requests are routed. For example, eth0.
  - In the **Connection Type** drop-down list, select **udp**.
  - In the **Original Destination IP** field, enter **0.0.0.0** to accept DNS requests from all clients.
  - In the **Original Destination CIDR field** (optional), enter the CIDR mask value. If you have specified 0.0.0.0 in the Original Destination IP field, enter '0' here.
  - In the **Original Destination Port** field, enter the port on which DNS requests are sent to Content Gateway. The default port is 53.
  - In the **Local Client IP** field, enter the IP address of Content Gateway.
  - In the **Local Client Port** field, enter the port that Content Gateway uses to communicate with the DNS server. The default port is 5353.
  - In the **User Protocol** drop-down list, select **dns**.
4. Click **Add**, then click **Apply**, and then click **Close**.
5. Go to **My Proxy > Basic** and in the **Features** table, enable **DNS Proxy** in the **Networking** section and click **Apply**.
6. Go to **Networking > DNS Proxy**.
7. In the **DNS Proxy Port** field, enter the DNS proxy port. The default port is 5353.
8. Click **Apply** and restart Content Gateway.





# 10

## Configuring the System

Websense Content Gateway provides several options for configuring the system:

- ◆ [Content Gateway Manager](#), page 95
- ◆ [Command-line interface](#), page 99
- ◆ [Configuration files](#), page 100
- ◆ [Saving and restoring configurations](#), page 101

You should restart Content Gateway any time a configuration change is made.

### Content Gateway Manager

---

Use Configure mode to view and change your Content Gateway configuration.



#### Note

Certain options can be changed only by editing configuration variables either in the **records.config** file or from the command-line interface. See [Command-line interface](#), page 99 and [Configuration files](#), page 100.

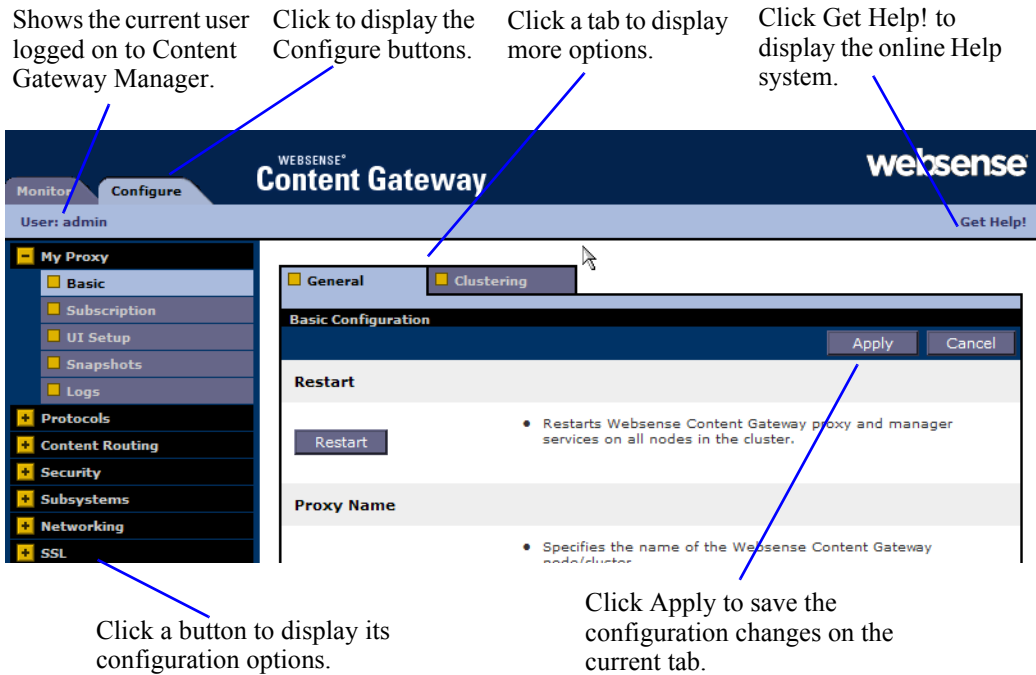
### Starting Configure mode

1. Open your Web browser.  
Content Gateway Manager requires Java and JavaScript; be sure to enable Java and JavaScript in your browser.
2. Enter the following location in your browser:  
`https://nodename:adminport`  
where **nodename** is the name of the node and **adminport** is the number assigned to the Content Gateway Manager port (8081 by default).

3. If necessary, log on to Content Gateway Manager with the administrator ID and password, or use your user account. The administrator ID and password are set during product installation. You can change the ID and password, as well as create and modify user accounts. For more information, refer to [Controlling access to Content Gateway Manager](#), page 154.

Content Gateway Manager starts by default in Monitor mode.

4. Click the **Configure** tab to display the Configure mode buttons.



## Using Configure mode

In Configure mode, Content Gateway Manager displays a series of buttons. Each button represents a group of configuration options.

All the configuration options available in Configure mode are described in [Configuration Options](#).

### My Proxy

- ◆ Click **Basic** to restart the proxy and manager services (you need to restart after changing certain configuration options), identify the name of the Content Gateway node, set alarm email, and enable or disable features (such as FTP processing, proxy user authentication, ARM, WCCP, cluster options, and so on).
- ◆ Click **Subscription** to view your subscription key. See the Web Security Manager Help system for information on subscription keys and scanning options. If Content Gateway is integrated with only Data Security Suite, enter your Data Security subscription key in the entry field.

- ◆ Click **UI Setup** to identify and change the port on which browsers connect to Content Gateway Manager, enable SSL connections to Content Gateway Manager, specify how often Content Gateway Manager refreshes the statistics on the Monitor tab, and configure access control lists, administrator accounts, and user accounts to secure Content Gateway Manager access.
- ◆ Click **Snapshots** to take and restore configuration snapshots.
- ◆ Click **Logs** to display, delete, or copy a selected log file to the local filesystem.

## Protocols

- ◆ Click **HTTP** to configure HTTP caching and tune HTTP timeouts.
- ◆ Click **HTTP Responses** to specify which HTTP responses are sent to clients when the proxy detects an HTTP problem with a client transaction (such as unavailable origin servers, authentication requirements, and protocol errors).
- ◆ Click **HTTP Scheduled Update** to configure the proxy to load specific objects into the cache at scheduled times.
- ◆ Click **FTP** to configure FTP options and tune FTP timeouts.

The FTP options affect requests that originate from FTP clients only. You can configure options that affect FTP requests originating from HTTP clients in the HTTP group. The FTP button appears only if you have enabled FTP processing in the **Features** table on **Configure > My Proxy > Basic > General**.
- ◆ Click **HTTPS** to specify port information for inbound and outbound HTTPS traffic.

## Content Routing

- ◆ Click **Hierarchies** to configure HTTP parent caching.
- ◆ Click **Mapping and Redirection** to set URL remapping rules and FTP remapping rules.
- ◆ Click **Browser Auto-Config** to identify the port used to download browser auto-configuration files, and to set PAC and WPAD options.

## Security

- ◆ Click **Access Control** to set filtering rules and set proxy authentication options (LDAP, RADIUS, and NTLM).
- ◆ Click **Data Security** to register with the Data Security Management Server and enable the local Data Security policy engine.
- ◆ Click **SOCKS** to configure Content Gateway to use a SOCKS firewall. The SOCKS button appears only if you have enabled SOCKS in the Features table on **Configure > My Proxy > Basic > General**.



### Note

To use SOCKS there must be a separate SOCKS server.

---

## Subsystems

- ◆ Click **Cache** to enable or disable cache pinning, configure the RAM cache size, specify the maximum size of objects allowed in the cache, and partition your cache according to protocol and origin servers.
- ◆ Click **Logging** to enable or disable event logging and set logging configuration options.

## Networking

- ◆ Click **Connection Management** to specify the maximum number of connections the proxy can accept. For transparent proxy caching, you can specify the maximum number of client connections allowed before the proxy starts forwarding incoming requests directly to the origin server.  
Ensure that the ARM is **On** (**Configure > My Proxy > Basic > General**) before setting redirection rules.
- ◆ Click **ARM** to set redirection rules that specify how incoming packets are readdressed in transparent mode. You can also set dynamic and static bypass rules. The ARM button appears only if ARM is enabled in the Features table on **Configure > My Proxy > Basic > General**.
- ◆ Click **WCCP** to set WCCP configuration settings. The WCCP button appears only if WCCP is enabled in the Features table under the **Configure > My Proxy > Basic > General** tab.
- ◆ Click **DNS Proxy** to specify the DNS proxy port. The DNS Proxy button appears only if you have enabled the DNS Proxy option in the Features table under the **Configure > My Proxy > Basic > General** tab.
- ◆ Click **DNS Resolver** to enable or disable local domain expansion, tune host database timeouts, and configure Split DNS options.
- ◆ Click **Virtual IP** to enable or disable virtual IP failover and specify the virtual IP addresses managed by the Content Gateway node. The Virtual IP button appears only if you have enabled Virtual IP in the Features table on **Configure > My Proxy > Basic > General**.

## SSL

- ◆ Click **Certificates** to view the certificate authority tree. Click any entry to view the details of that certificate.
- ◆ Click **Decryption/Encryption** to configure how SSL Manager handles inbound and outbound traffic. Inbound traffic travels from the browser to SSL Manager, where the content is decrypted and inspected. Outbound traffic travels from SSL Manager to the destination Web server. SSL Manager checks the revocation status of the site certificate before forwarding re-encrypted data to the site.
- ◆ Click **Validation** to configure certificate validation, specify what to do in the case that a certificate is invalid, set up verification bypass, and configure the handling of certificate revocation lists.



- ◆ Click **Incidents** to view a report of occurrences in which clients received an access denial message, and to identify URLs that you want to allow, blacklist, or tunnel.
- ◆ Click **Client Certificates** to configure how SSL Manager handles client certificate requests.
- ◆ Click **Logging** to select the SSL logging level, logging detail, log file names, and log file handling.
- ◆ Click **Customization** to customize the certificate validation failure message.
- ◆ Click **Internal Root CA** to import, create, or backup the internal Root Certificate Authority.

## Command-line interface

---

As an alternative to Content Gateway Manager, you can use the command-line interface to view and change your Websense Content Gateway configuration.

1. Log on to a Content Gateway node as the Content Gateway administrator, and then change directory ('cd') to the Content Gateway **bin** directory (/opt/WCG/bin).
2. To view a configuration setting, enter the following command:

```
content_line -r var
```

where *var* is the variable associated with the configuration option (for a list of the variables, refer to [Configuration variables](#), page 348).

3. To change the value of a configuration setting, enter the following command:

```
content_line -s var -v value
```

where *var* is the variable associated with the configuration option and *value* is the value you want to use.

For example, to change the FTP inactivity timeout option to 200 seconds, enter the following command at the prompt and press Return:

```
content_line -s  
proxy.config.ftp.control_connection_timeout -v 200
```



### Note

If the Content Gateway **bin** directory is not in your path, prepend the command with: `./`

For example:

```
./content_line -r variable
```

---

## Configuration files

You can change Content Gateway configuration options by editing specific variables in the **records.config** file, located in **/opt/WCG/config**. Open the file in a text editor (such as **vi** or **emacs**) and change the value of the variable.



### Note

After you modify the **records.config** file, Content Gateway must reread the configuration files; from the Content Gateway **bin** directory (**/opt/WCG/bin**), enter the command:

```
content_line -x
```

In some cases, you have to restart the proxy to apply the changes.

The figure below shows a sample portion of the **records.config** file:

```
##Id: records.config.v 1.617.2.27 2008/09/16 22:06:35 brilee Exp #
#
# Process Records Config File
#
# <RECORD-TYPE> <NAME> <TYPE> <VALUE (till end of line)>
#
#   RECORD-TYPE:   CONFIG, LOCAL
#   NAME:          name of variable
#   TYPE:          INT, STRING, FLOAT
#   VALUE:         Initial value for record
#
#####
# System Variables
#
#####
CONFIG proxy.config.proxy_name STRING ibid
CONFIG proxy.config.bin_path STRING bin
CONFIG proxy.config.proxy_binary STRING traffic_server
CONFIG proxy.config.proxy_binary_opts STRING -M
CONFIG proxy.config.manager_binary STRING traffic_manager
CONFIG proxy.config.cli_binary STRING traffic_line
CONFIG proxy.config.watch_script STRING traffic_cop
CONFIG proxy.config.env_prep STRING example_prep.sh
CONFIG proxy.config.config_dir STRING config
CONFIG proxy.config.temp_dir STRING /tmp
CONFIG proxy.config.alarm_email STRING inktomi
```

The variable name ——— The variable type: an integer (INT), a string (STRING), or a floating point (FLOAT)

————— The variable value that you can edit

Content Gateway provides other configuration files that are used to configure specific features. All the configuration files are described in [Configuration Files, page 317](#).

## Saving and restoring configurations

The configuration snapshot feature lets you save all current configuration settings and restore them if needed. Content Gateway can store configuration snapshots on the node where they are taken, on an FTP server, and on portable media. Content Gateway restores a configuration snapshot on all the nodes in the cluster.



### Note

It is recommended that you take a configuration snapshot before performing system maintenance or attempting to tune system performance. Taking a configuration snapshot takes only a few seconds.

This section describes how to perform the following tasks:

- ◆ Take a snapshot of the current configuration. See [Taking configuration snapshots](#), page 101.
- ◆ Restore previously taken configuration snapshots. See [Restoring configuration snapshots](#), page 102.
- ◆ Delete configuration snapshots stored on the Content Gateway node. See [Deleting configuration snapshots](#), page 102.

## Taking configuration snapshots

You can save all the current configuration settings on your Content Gateway system through Content Gateway Manager.

### To take a configuration snapshot and save it on the local system

1. Navigate to **Configure > Snapshots > File System**.
2. The **Change Snapshot Directory** field displays the name of the directory where Content Gateway saves configuration snapshots. The default location is the Content Gateway **config/snapshots** directory. To change the directory, enter the full path in the **Change Snapshot Directory** field. If you enter a relative path, Content Gateway assumes that the directory is located in its **config** directory.
3. In the **Save Snapshot** field, type the name you want to use for the current configuration.
4. Click **Apply**.

### To take a configuration snapshot and save it on an FTP server

1. Navigate to **Configure > Snapshots > FTP Server**.
2. In the fields provided, enter the FTP server name, the login and password, and the remote directory where the FTP server stores configuration snapshots.
3. Click **Apply**.

After you have successfully logged on to the FTP server, the **FTP Server** page displays additional fields.

4. In the **Save Snapshot to FTP Server** field, enter the name of the configuration snapshot you want to take.
5. Click **Apply**.

## Restoring configuration snapshots

If you are running a cluster of Content Gateway servers, the configuration is restored to all the nodes in the cluster.

### To restore a configuration snapshot stored on the local node

1. Navigate to the **Configure > Snapshots > File System** tab.
2. From the **Restore > Delete Snapshot** drop-down list, select the configuration snapshot that you want to restore.
3. Click the **Restore Snapshot from “*directory\_name*” Directory** box.
4. Click **Apply**.

The Content Gateway system or cluster uses the restored configuration.

### To restore a configuration snapshot from an FTP server

1. Navigate to **Configure > Snapshots > FTP Server**.
2. In the fields provided, enter the FTP server name, the login and password, and the remote directory in which the FTP server stores configuration snapshots.
3. Click **Apply**.

After you have successfully logged on to the FTP server, the **FTP Server** tab displays additional fields.

4. In the **Restore Snapshot** drop-down list, select the configuration snapshot that you want to restore.
5. Click **Apply**.

The Content Gateway system or cluster uses the restored configuration.

## Deleting configuration snapshots

1. Navigate to **Configure > Snapshots > File System**.
2. From the **Restore > Delete a Snapshot** drop-down list, select the configuration snapshot you want to delete.
3. Click the **Delete Snapshot from “*directory\_name*” directory** box.
4. Click **Apply**.

The configuration snapshot is deleted.

# 11

## Monitoring Traffic

Websense Content Gateway provides the following tools to monitor system performance and analyze network traffic:

- ◆ Statistics that show Content Gateway performance and network traffic information. See [Viewing statistics](#), page 103. The command-line interface provides an alternative method of viewing this information. See [Viewing statistics from the command line](#), page 106.
- ◆ Alarms that signal detected failure conditions. See [Working with alarms](#), page 107.
- ◆ Performance graphs that show historical Content Gateway performance and network traffic information. See [Using Performance graphs](#), page 109.
- ◆ Reports generated through SSL Manager to see the status of certificate authorities and incidents. See [Creating reports with SSL Manager](#), page 110.

### Viewing statistics

---

Use Content Gateway Manager to collect and interpret statistics about Content Gateway performance and Web traffic. View statistics using Monitor mode.

### Starting Monitor mode

1. Open your Web browser.  
Content Gateway Manager requires Java and JavaScript; be sure to enable Java and JavaScript in your browser.
2. Enter the following location in your browser:  
`https://nodename:adminport`  
where *nodename* is the name of the Content Gateway node and *adminport* is the number assigned to the Content Gateway Manager port.
3. If necessary, log on to Content Gateway Manager with the administrator ID and password, or use your user account. The administrator ID and password are set during installation. You can change the ID and password, as well as create and modify user accounts. For more information, see [Controlling access to Content Gateway Manager](#), page 154.

## Using Monitor mode

In Monitor mode, Content Gateway Manager displays a series of buttons on the left of the display. Click a button to view its statistics.

All statistics displayed in Monitor mode are described in detail in [Statistics, page 219](#).

### My Proxy

Click **My Proxy** to see statistics about Content Gateway.

- ◆ Click **Summary** to see a concise view of your Content Gateway system. The top portion of the page displays information about the features of your Websense Web Security Gateway subscription, including the expiration date. The middle portion of the page displays information about the scanning engines in use and their associated data files. The bottom portion of the page contains statistics on proxy nodes, displaying all cluster nodes by name and tracking essential statistics for each node. If you want to display detailed information about a particular node in a cluster, click the node's name in the Summary table, and then click one of the other buttons on the **Monitor** tab.
- ◆ Click **Node** to see information about the selected node. You can see if the node is active or inactive, the date and time that the **content\_gateway** process was started, cache performance information (document hit rate, bandwidth savings, and what percentage of the cache is currently free), the number of client and server connections currently open, and the number of transfers currently in progress. You can also see name resolution information, such as the host database hit rate and the number of DNS lookups per second.



#### Note

If the node is part of a cluster, two sets of statistics are shown: information about the single node and information showing an average value for all nodes in the cluster. Click the name of a statistic to display the information in graphical format.

---

- ◆ Click **Graphs** to view the same statistics displayed on the **Node** page (cache performance, current connections and transfers, network, and name resolution) in graphical format. You can display multiple statistics in one graph. To display a particular statistic in graphical format, click the box next to the name of the graph, and then click **Graph**. To display multiple statistics in one graph, click the box next to the name of each graph you want to display, and then click **Graph**.
- ◆ Click **Alarms** to view the alarms that Content Gateway has signaled. See [Working with alarms, page 107](#).

### Protocols

The Protocols button provides information about HTTP and FTP transactions.

- ◆ Click **HTTP** to see information about HTTP transactions and speeds (such as cache misses, cache hits, connection errors, aborted transactions) and client and server connection information. Also see information about FTP requests from HTTP clients, such as the number of open FTP server connections, the number of successful and unsuccessful PASV and PORT connections, and the number of cache lookups, hits, and misses.
- ◆ Click **FTP** to see information about FTP requests from FTP clients.



#### Note

The **FTP** button appears only if you have enabled FTP processing in the **Features** table under the **Configure > My Proxy > Basic** tab.

## Security

The Security button provides information about proxy authentication, and SOCKS server connections:

- ◆ Click **LDAP** to see the number of LDAP cache hits and misses, and the number of LDAP authentication server errors and unsuccessful authentication attempts. The LDAP button appears only if you have enabled the LDAP option in the Features table on the **Configure > My Proxy > Basic > General** tab.
- ◆ Click **NTLM** to see the number of NTLM cache hits and misses, and the number of NTLM authentication server errors and unsuccessful authentication attempts. The NTLM button appears only if you have enabled the NTLM option in the Features table on the **Configure > My Proxy > Basic > General** tab.
- ◆ Click **Integrated Windows Authentication (IWA)** to see the negotiated requests counters, the NTLM request counters and the Basic authentication request counters. The IWA tab appears only if you have enabled the IWA option in the Features table on the **Configure > My Proxy > Basic > General** tab.
- ◆ Click **SOCKS** to see the number of successful and unsuccessful connections to the SOCKS server and the number of connections currently in progress. The SOCKS button appears only if you have enabled the SOCKS option in the Features table on the **Configure > My Proxy > Basic > General** tab.

## Subsystems

The Subsystems button provides information about the proxy cache, clusters, and event logging:

- ◆ Click **Cache** to see information about the proxy cache. See how much space in the cache is currently being used, the total size of the cache in gigabytes, the total size of the RAM cache in bytes, the number of RAM cache hits and misses, and the number of cache lookups, object reads, writes, updates, and removes.
- ◆ Click **Clustering** to see the number of nodes in the cluster, the total number of cluster operations, the number of bytes read and written to all the nodes in the cluster, and the current number of open connections in the cluster.

- ◆ Click **Logging** to see the number of log files currently open, the amount of space currently being used for log files, the number of access events and error events logged, and the number of access events skipped.

## Networking

The Networking button provides information about system network configuration, the ARM, WCCP routers, DNS proxy, domain name resolution, and virtual IP addressing.

- ◆ Click **System** to see system network configuration, including the host name assigned to the proxy machine and the default gateway, search domain, and DNS servers that the proxy machine uses.
- ◆ Click **ARM** to see information about Network Address Translation and dynamic bypass. The ARM button appears only if you have enabled ARM in the Features table under the **Configure > My Proxy > Basic** tab.
- ◆ Click **WCCP** to see WCCP v2 fragmentation statistics and the configuration of every WCCP service group enabled on the Content Gateway node. The WCCP tab appears only if you have enabled WCCP in the Features table on the **Configure > My Proxy > Basic > General** tab.
- ◆ Click **DNS Proxy** to see the total number of DNS requests served by Content Gateway, and the number of cache hits and misses. The DNS Proxy button appears only if you have enabled the DNS Proxy option in the Features table on the **Configure > My Proxy > Basic > General** tab.
- ◆ Click **DNS Resolver** to see the total number of lookups and hits in the host database, and the average lookup time, the total number of lookups, and the number of successful lookups in the DNS server.
- ◆ Click **Virtual IP Address** to see the current virtual IP address mappings. The Virtual IP Address button appears only if you have enabled the Virtual IP option in the Features table on the **Configure > My Proxy > Basic > General** tab.

## Performance

The Performance button displays historical performance graphs. See [Using Performance graphs, page 109](#).

## Viewing statistics from the command line

You can use the command-line interface to view statistics about Content Gateway performance and Web traffic.

You can also configure, stop, and restart Content Gateway from the command line. See [Command-line interface, page 99](#), and [Websense Content Gateway variables, page 242](#).

To view specific information about a Content Gateway node or cluster, specify the variable that corresponds to the desired statistic.

1. Become root:

```
su
```



2. Log on to a node as the Content Gateway administrator.
3. From the Content Gateway **bin** directory (/opt/WCG/bin), enter the following command:

```
content_line -r variable
```

where *variable* is the variable that represents the information you want. For a list of the variables you can specify, see [Websense Content Gateway variables](#), page 242.

For example, the following command displays the document hit rate for the node:

```
content_line -r proxy.node.http.cache_hit_ratio
```



### Note

If the Content Gateway **bin** directory is not in your path, prepend the command with: `./`

For example:

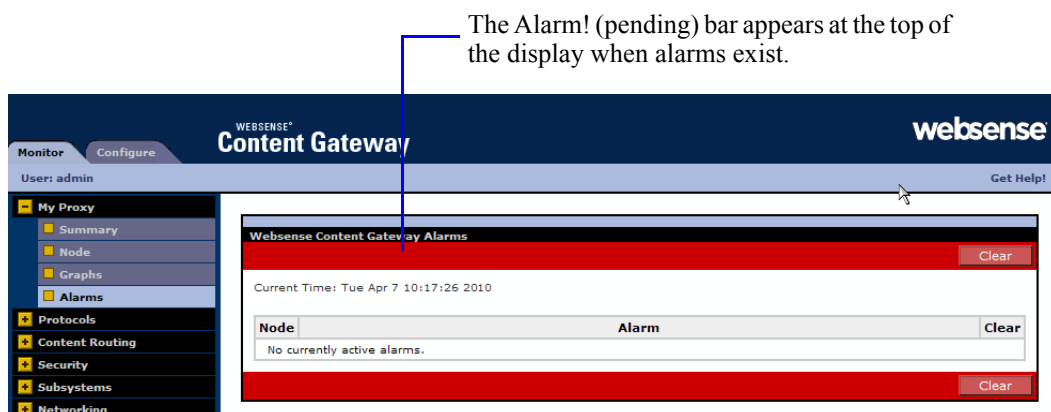
```
./content_line -r variable
```

## Working with alarms

Content Gateway signals an alarm when it detects a problem, for example if the space allocated to event logs is full, or if it cannot write to a configuration file.

Not all alarms are critical. Some alarms report transient conditions. For example, a **license download failed:4** alarm can be generated by a temporary disruption in internet connectivity.

Navigate to **Monitor > My Proxy > Alarms** to see a listing of current alarms, as shown below.



**Note**

Content Gateway also sends select alarms to TRITON - Web Security, where they are referred to as **alerts**. Summary alert messages are displayed on the TRITON - Web Security **Status > Today** page. Web Security administrators can configure which Content Gateway conditions cause alert messages to be sent, and which methods (email, pop-up, or SNMP) are used to send the alert, on the **Settings > Alerts** pages.

## Clearing alarms

After you have read an alarm message, you can click **Clear** in the alarm message window to dismiss the alarm. [Alarm messages](#), [page 413](#), provides a description of some of the alarm messages that Content Gateway generates.

**Important**

Clicking **Clear** only dismisses alarm messages; it does not resolve the cause of the alarms.

If the same alarm condition occurs a second time, it will not be logged if the first alarm has not been cleared.

## Configuring Content Gateway to email alarms

1. Navigate to the **Configure > My Proxy > Basic > General** tab.
2. In the **Alarm eMail** field, enter the email address to which you want to send alarms. Be sure to use the full mail address including @ notation, for example:  
receivername@example.com
3. Click **Apply**.

## Using a script file for alarms

Alarm messages are built into Content Gateway; you cannot change them. However, you can write a script file to execute certain actions when an alarm is signaled.

A sample script file named **example\_alarm\_bin.sh** is provided in **/opt/WCG/bin**. You can modify this file.

## Using Performance graphs

The Performance graphing tool (Multi Router Traffic Grapher) allows you to monitor Content Gateway performance and analyze network traffic. Performance graphs show information about virtual memory usage, client connections, cache hit and miss rates, and so on. The information provided is recorded from the time that Content Gateway was started. Statistics are gathered at 5-minute intervals.

Go to **Monitor > Performance** to access performance graphs.



### Important

To run Multi Router Traffic Grapher (the Performance graphing tool), you must have Perl version 5.005 or later installed on your Content Gateway system.

1. If your Content Gateway node is in a cluster, select the node whose statistics you want to view from the **Monitor > My Proxy > Summary** display.
2. On the **Monitor** tab, click **Performance**.
3. Click **Overview** to see a subset of available graphs.  
Click **Daily** to see statistics for the current day.  
Click **Weekly** to see statistics for the current week.  
Click **Monthly** to see statistics for the current month.  
Click **Yearly** to see statistics for the current year.
4. Wait at least 15 minutes after starting Content Gateway before looking at the graphs. It takes several 5-minute sample intervals for the tool to initialize statistics.

If Multi Router Traffic Grapher (MRTG) has not been configured, the system displays a message indicating that it is not available. To configure the tool:

1. Make sure Perl 5.005 is installed on your system.
2. At the command prompt, type  

```
perl ./pathfix.pl 'which perl'
```

  
to ensure that the perl binary is in your PATH.
3. Change to the Content Gateway **bin** directory (/opt/WCG/bin).
4. Modify the MRTG update interval by typing the following at the command prompt:  

```
./update_mrtg;sleep 5;./update_mrtg;sleep 5;
```

  
By default, an MRTG update interval is set to 15 minutes. This command sets the update to 5 minutes.
5. Start the MRTG cron updates:  

```
./mrtgcron start
```

6. Wait about 15 minutes before accessing the performance graphs from the Content Gateway Manager.

**Note**

To stop MRTG cron updates, type the command  
`./mrtgcron stop.`

---

## Creating reports with SSL Manager

---

You can request a report detailing the status of certificate authorities (see [Certificate Authorities](#), page 110) or listing incidents (see [Incidents](#), page 111). Reports can be either in HTML or comma-separated format. The comma-separated reports appear as Excel spreadsheets in SSL Manager.

### Certificate Authorities

1. Go to the **Monitor > SSL > Reports > Certificate Authorities** tab.
2. Select the format of the report.
  - a. HTML
  - b. Comma-separated values (CSV)  
If you select CVS, the report is created as an Excel spreadsheet.
3. Specify the time period the report will cover.
  - a. A number of days
  - b. A starting date spanning to the present
  - c. All records in the log
4. Indicate the sort order for the report.
  - a. List authorities by date
  - b. List OCSP good responses first
  - c. List OCSP bad responses first  
See [Keeping revocation information up to date](#), page 141.
5. Click **Generate Report** to generate the report.

HTML output looks like this:

Certificate Authorities

Incidents

Validation Reports

HTML Report of EVA - Certificate Authorities

Profile: default\_default

Certificate Authority	Count good	Percentage	Count bad	Percentage	Last Access Date
Class 3 Public Primary Certification Authority	167	13.47 %	0	0.00 %	2008-02-12 12:07:17
www.verisign.com/CPS Incomp.by Ref. LIABILITY LTD.(c)97 VeriSign	88	7.10 %	0	0.00 %	2008-02-12 12:07:17
VeriSign Class 3 Secure Server CA	75	6.05 %	0	0.00 %	2008-02-12 12:07:17
Equifax Secure Certificate Authority	535	43.15 %	0	0.00 %	2008-02-12 10:30:06
Microsoft Internet Authority	112	9.03 %	0	0.00 %	2008-02-11 19:41:58

The same report in comma-separated format appears as follows:

Certificate Authorities			Incidents				
Validation Reports							
A1		CSV Report of EVA - Certificate Authorities					
A	B	C	D	E	F	G	
CSV Report of EVA - Certificate Authorities							
2							
3	Profile: default_default						
4							
5	Certificate	Count good	Percentage	Count bad	Percentage	Last Access Date	
6	Class 3 Pu	167	13.47%	0	0.00%	#####	
7	www.verisi	88	7.10%	0	0.00%	#####	
8	VeriSign C	75	6.05%	0	0.00%	#####	
9	Equifax Se	535	43.15%	0	0.00%	#####	
10	Microsoft I	112	9.03%	0	0.00%	#####	



### Note

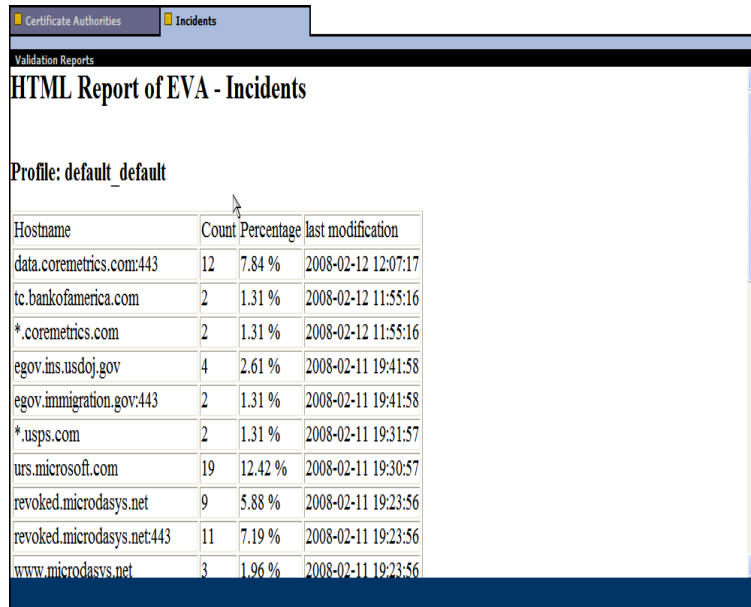
To delete the collected SSL log data, click **Reset all collected data**.

## Incidents

1. Navigate to the **Monitor > SSL > Reports > Incidents** tab.
2. Select HTML or comma-separated (CSV) format. If you select comma-separated, the report is created in an Excel spreadsheet.
3. Specify the time period the report should cover. You can specify
  - a. a number of days
  - b. a date range
  - c. the period since SSL Manager was deployed
4. Indicate the sort order for the report.
  - a. Listing incidents by date
  - b. Listing incidents by URL

- c. Listing the number of times each incident occurred  
See [Managing Web HTTPS site access](#), page 143.
5. Click **Generate Report** to generate the report.

TML output looks like this:



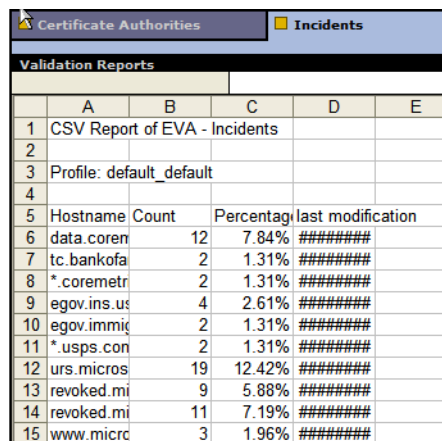
Validation Reports

### HTML Report of EVA - Incidents

Profile: default\_default

Hostname	Count	Percentage	last modification
data.coremetrics.com:443	12	7.84 %	2008-02-12 12:07:17
tc.bankofamerica.com	2	1.31 %	2008-02-12 11:55:16
*.coremetrics.com	2	1.31 %	2008-02-12 11:55:16
egov.ins.usdoj.gov	4	2.61 %	2008-02-11 19:41:58
egov.immigration.gov:443	2	1.31 %	2008-02-11 19:41:58
*.usps.com	2	1.31 %	2008-02-11 19:31:57
urs.microsoft.com	19	12.42 %	2008-02-11 19:30:57
revoked.microdasys.net	9	5.88 %	2008-02-11 19:23:56
revoked.microdasys.net:443	11	7.19 %	2008-02-11 19:23:56
www.microdasys.net	3	1.96 %	2008-02-11 19:23:56

The same report in comma-separated format appears as follows:



Validation Reports

### CSV Report of EVA - Incidents

Profile: default\_default

	A	B	C	D	E
1	Hostname	Count	Percentage	last modification	
6	data.coreme	12	7.84%	#####	
7	tc.bankofa	2	1.31%	#####	
8	*.coremetr	2	1.31%	#####	
9	egov.ins.us	4	2.61%	#####	
10	egov.immig	2	1.31%	#####	
11	*.usps.con	2	1.31%	#####	
12	urs.micros	19	12.42%	#####	
13	revoked.mi	9	5.88%	#####	
14	revoked.mi	11	7.19%	#####	
15	www.micrc	3	1.96%	#####	



#### Note

To delete the collected SSL log data, click **Reset all collected data**.

# 12

## Working With Websense Data Security

### Related topics:

*Registering and configuring on-box Data Security*, page 115

*Unregistering on-box Data Security*, page 116

*Stopping and starting Data Security processes*, page 117

*Configuring the ICAP client*, page 117

Websense Content Gateway can be deployed together with Websense Data Security to provide data loss prevention (DLP) over Web channels such as HTTP, HTTPS, FTP, and FTP over HTTP. A full data security deployment can extend DLP to include channels such as mobile devices, removable media, and printers. For a complete description of Websense Data Security, please visit the Data Security product page at [www.websense.com](http://www.websense.com).

Web data loss prevention, as well as other data security configurations, require separate installation of the Data Security Manager and other Data Security components. Before configuring Content Gateway to work with Websense data security, please see the deployment and installation information hosted in the [Websense Technical Library](#).

Content Gateway supports 2 methods of working with Websense Data Security:

- ◆ Using the Data Security policy engine located on-box with Content Gateway
- ◆ Over ICAP using a Data Security policy engine located on a separate computer (intended for use with Data Security Suite versions 7.1 and earlier)

Only one method can be used at a time. When one is configured the other is unavailable.

### How it works:

1. The proxy intercepts outbound content and provides that content to Data Security.
2. Data Security analyzes the content to determine if the Web posting or FTP upload is allowed or blocked.
  - The determination is based on the Data Security policy.
  - The disposition is communicated to the proxy.
  - Data Security logs the transaction.

3. The proxy acts on the Data Security determination.
  - a. If the content is blocked, it is not transmitted to the remote host, and Data Security returns a block page to the sender.
  - b. If the content is allowed, it is forwarded to its destination.

**Note**

When a request is blocked and the DLP server sends a block page in response:

- ◆ Content Gateway forwards the block page to the sender in a 403 Forbidden message.
- ◆ The block page must be larger than 512 bytes or some user agents (e.g., Internet Explorer) will substitute a generic error message.

Transactions over HTTP, HTTPS, FTP, and FTP over HTTP can be examined.

Transaction details are logged by Data Security per its configuration.

**Data Security policy engine on-box with Content Gateway**

When Content Gateway is installed, a Data Security policy engine is also installed, although it is disabled until registered with the Data Security Management Server (see [Registering and configuring on-box Data Security, page 115](#)).

After Data Security policies have been created and Content Gateway has registered with Data Security, Content Gateway sends content, such as postings and uploads, to the Data Security for analysis and policy enforcement.

When the on-box policy engine is used, Content Gateway collects and displays Data Security transaction statistics, such as the total number of posts, the total number of posts analyzed, the number of FTP uploads analyzed, the number of blocked requests, and more. These statistics can be viewed in the Content Gateway Manager by navigating to **Monitor > Security > Data Security**. For a complete list of statistics, see [Data Security, page 228](#).

**Data Security over ICAP**

When the Data Security policy engine is located on a different computer, Content Gateway can communicate with Data Security over ICAP v1.0. For configuration details, see [Configuring the ICAP client, page 117](#).



## Registering and configuring on-box Data Security

Related topics:

[Unregistering on-box Data Security, page 116](#)

[Stopping and starting Data Security processes, page 117](#)

For an introduction to Data Security, see [Working With Websense Data Security, page 113](#).

To complete Data Security registration, you need to know the IP address of the Data Security Management Server. The Data Security Management Server must be version 7.6. Registering Content Gateway with Data Security adds the Content Gateway module to the Data Security Manager.



### Important

If Content Gateway is **not** located on a V-Series appliance, registration **requires** that the Content Gateway host system have an IPv4 address assigned to the eth0 network interface. After registration, the IP address may move to another network interface on the system; however, that IP address is used for data security configuration deployment and must be available as long as the two modules are registered.

To enable the on-box Data Security policy engine:

1. Ensure that the Content Gateway and Data Security Management Server systems are running and accessible, and that their system clocks are synchronized within a few minutes.
2. Log on to Content Gateway Manager and select **Configure > Basic > General**.
3. In the list of **Features**, under **Networking** locate **Data Security**, select **On**, and then select **Integrated on-box**. A registration status link displays.
4. Click the **Not registered** link. This opens the **Configure > Security > Data Security** registration screen.
5. Enter the IP address of the **Data Security Management Server**.
6. Enter a user name and password for logging onto the Data Security Manager. This is the management interface in which Data Security policy is configured. The user must be a Data Security administrator with Deploy Settings privileges.
7. Click **Register**. If registration is successful, a message confirms the result and prompts you to restart Content Gateway.

If registration fails, an error message indicates the cause of failure. Correct the problem and perform the registration process again.

8. Before restarting Content Gateway, set the following configuration options:

- a. **Analyze FTP Uploads:** Select this option to send FTP uploads to Data Security for analysis and policy enforcement.
- b. **Analyze HTTPS Content:** Select this option to send decrypted HTTPS posts to Data Security for analysis and policy enforcement. SSL Manager must be enabled on Content Gateway. See [Working With Encrypted Data](#), page 121.

**Note**

In order for these options to have any effect, Content Gateway must be configured to proxy FTP and HTTPS traffic. Go to **Configuration > MyProxy > Basic**.

---

These options can be accessed whenever Data Security is registered by going to the **Configure > Security > Data Security > General** page.

9. Click **Apply** to save your settings and then go to **Configure > Basic** and click **Restart** to restart Content Gateway.
10. Log on to the Data Security Manager to configure Content Gateway module. See the section titled “Deploying the Content Gateway module” in the *Websense Web Security Gateway Anywhere Getting Started* guide.

Data Security and Content Gateway communicate over ports 5820, 8888, 8889, 8892, 9080, and 9443. If IPTables are configured on the Content Gateway host system, these ports must be open in IPTables. See the *Content Gateway Installation Guide*, or the Technical Library article titled “Configuring IPTables for Websense Content Gateway”.

**Note**

A Content Gateway Manager alarm is generated if:

- ◆ On-box Data Security is enabled but not registered
  - ◆ On-box Data Security is enabled and registered, but not configured in the Data Security Manager
- 

## Unregistering on-box Data Security

---

To disable the integration with the on-box Data Security policy engine:

1. Log on to Content Gateway Manager and navigate to **Configure > Security > Data Security > General**. This page should indicate that the **Registration status** is **Registered**.
2. Click the **Unregister** button and confirm the action by clicking **OK** in the confirmation dialog box. When the action is complete, the **Registration status** will read **Unregistered**.
3. Go to **Configure > Basic** and click **Restart** to restart Content Gateway.

## Stopping and starting Data Security processes

---

When Content Gateway is registered with Data Security Management Server and the on-box policy engine is running, 3 daemon processes are active on the Content Gateway machine:

- ◆ **PolicyEngine** handles transaction and data analysis.
- ◆ **PAFPREP** manages the Data Security fingerprint repository.
- ◆ **mgmtd** handles configuration storage and replication.

These processes start automatically whenever the computer is started.

You must have root privileges to stop or start the processes.

To stop or start **all** policy engine processes, on the command line enter:

```
/opt/websense/PolicyEngine/managePolicyEngine -command  
[stop|start]
```

To stop or start individual processes, on the command line enter:

```
service [service_name] [start|stop|restart]
```

## Configuring the ICAP client

---

ICAP can be used with any version of Websense Data Security, however the direct interface is recommended when the policy engine is on-box with Content Gateway. See [Registering and configuring on-box Data Security, page 115](#).

ICAP **must** be used for inter-operation with Data Security Suite versions 7.1 and earlier.



### Note

A secondary ICAP server can be specified as a failover server should the primary server fail.

The primary and secondary can also be configured to perform load balancing.

See [ICAP failover and load balancing](#), below.

---

To configure integration with ICAP, log on to Content Gateway Manager and go to **Configure > My Proxy > Basic > General** page.

1. In the **Networking** section of the Features table, select Data Security **On**.
2. Click **Apply**, and then click **Restart**.
3. Navigate to **Configure > Networking > ICAP > General**.

4. In the **ICAP Service URI** field, enter the Uniform Resource Identifier (URI) for the primary ICAP service, followed by a comma (no space) and the URI of the secondary ICAP service. A secondary ICAP service is optional.

A URI is similar to a URL, but the URI ends with a directory, rather than a page. Obtain the identifier from your Websense Data Security Suite administrator. Enter the URI in the following format:

```
icap://hostname:port/path
```

For *hostname*, enter the IP address or hostname of the Websense Data Security Suite Protector appliance.

The default ICAP port is 1344.

*Path* is the path of the ICAP service on the host machine.

For example:

```
icap://ICAP_machine:1344/REQMOD
```

You do not need to specify the port if you are using the default ICAP port 1344.

For example, the above URI can also be entered without the default port:

```
icap://ICAP_machine/REQMOD
```

5. Under **Analyze HTTPS Content**, indicate if decrypted traffic should be sent to Websense Data Security Suite for analysis or sent directly to the destination. You must be running SSL Manager to send traffic to Websense Data Security Suite. See [Working With Encrypted Data](#), page 121.
6. Under **Analyze FTP Uploads**, select whether to send FTP upload requests to Websense Data Security Suite for analysis. The FTP proxy feature must be enabled to send FTP traffic to Websense Data Security Suite. See [FTP](#), page 269.
7. Under **Action for Communication Errors**, select whether to permit traffic or send a block page if Content Gateway encounters an error while communicating with Websense Data Security Suite.
8. Under **Action for Large Files**, select whether to permit traffic or send a block page if a file larger than the size limit specified in Websense Data Security Suite is sent. The default size limit for Data Security Suite version 7.0 and later is 12 MB.
9. Click **Apply**.

**Note**

If you change the URI, you must restart Content Gateway. Other changes do not require a restart.

---

## ICAP failover and load balancing

Content Gateway can be configured to failover to a backup ICAP server if the active ICAP server fails. The proxy detects the failure condition and sends traffic to the secondary server. If the secondary becomes unresponsive, the proxy uses the primary. If no ICAP servers are available, the proxy fails open.

Load balancing between 2 ICAP servers is also an option.

### **Time to failover**

Content Gateway may experience temporary request-processing latency between the time the real failure occurs and the time the proxy marks the failed server as down. After the failed server is marked down, all new requests are sent to the second ICAP server. The time to failover is primarily limited by the connection timeout configuration.

### **Failure conditions leading to failover**

- ◆ ICAP request failed due to layer-3 failure (twice for the same request)
- ◆ Failure to connect to a port within a given timeout
- ◆ Failure to send request (server resetting connection, and similar)

### **Excluded failure conditions**

Content Gateway does not consider missing, invalid, or slow responses as failures.

However, Content Gateway does verify that the ICAP server is valid at startup by verifying the response to the ICAP OPTIONS request.

### **Recovery Conditions**

After the failed server is marked down, new requests are sent to the second server. No new ICAP requests are sent to the failed server until that server is detected to be active again, based on the recovery conditions below.

Content Gateway tests for recovery conditions for each down ICAP server at a specified interval. If load balancing is disabled, requests continue to be sent to a secondary ICAP server until the primary comes back online. If load balancing is enabled, Content Gateway starts sending requests to a server (round-robin) as soon as it is marked up.

- ◆ TCP connection success
- ◆ Successfully sent OPTIONS request
- ◆ Successfully received valid response to OPTIONS request

### **Recovery actions**

Upon server recovery (server comes back online and is marked as up)

- ◆ Load balancing ON: Requests start being distributed to the newly up server (round-robin)
- ◆ Load balancing OFF: If the primary server recovers, all requests start being sent to the primary. If the secondary server recovers, traffic continues to be sent to the primary, until the primary goes down.

## Fail open

If all ICAP servers are down, a configuration option allows fail open or fail closed behavior. When all ICAP servers are down, the background thread continuously attempts to reestablish a new connection with each server.

## Configuration settings

These ICAP failover parameters are set in the *records.config* file (defaults shown):

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.icap.ICAPUri</code>	STRING	(empty)	A comma-separated list of ICAP URIs. For example: icap://1.2.3.4:1344/reqmod, icap://4.3.2.1:1344/reqmod
<code>proxy.config.icap.ActiveTimeout</code>	INT	5	The read/response timeout in seconds. The activity is considered a failure if the timeout is exceeded.
<code>proxy.config.icap.RetryTime</code>	INT	5	The recovery interval, in seconds, to test whether a down server is back up.
<code>proxy.config.icap.FailOpen</code>	INT	1	Set to: <ul style="list-style-type: none"> <li>• 1 to allow traffic when the ICAP servers are down</li> <li>• 0 to send a block page if the ICAP servers are down</li> </ul>
<code>proxy.config.icap.LoadBalance</code>	INT	1	Set to: <ul style="list-style-type: none"> <li>• 1 to distribute requests to all available servers</li> <li>• 0 to distribute requests to only the primary server.</li> </ul>

# 13

## Working With Encrypted Data

### Related topics:

[Running in explicit proxy mode](#), page 123

[Tasks](#), page 125

[Enabling SSL Manager](#), page 124

[Certificates](#), page 126

[Internal Root CA](#), page 126

[Managing certificates](#), page 134

[Configuring SSL Manager for inbound traffic](#), page 136

[Configuring SSL Manager for outbound traffic](#), page 137

[Validating certificates](#), page 138

[Managing Web HTTPS site access](#), page 143

[Client certificates](#), page 146

[Configuring SSL Manager logging](#), page 148

[Customizing SSL connection failure messages](#), page 150

SSL (Secure Sockets Layer) is the industry standard for transmitting secure data over the Internet. It is based on encrypted content and a system of trusted certificates issued by certificate authorities and recognized by servers.

Content Gateway does not cache HTTPS content.

When SSL Manager is enabled, SSL-encrypted traffic is decrypted, inspected, and then re-encrypted before it is sent to its destination.



### Important

Even when SSL Manager is **not** enabled and HTTPS is not decrypted, Content Gateway performs HTTPS URL filtering. This means that for every HTTPS request, a URL lookup is performed and policy is applied.

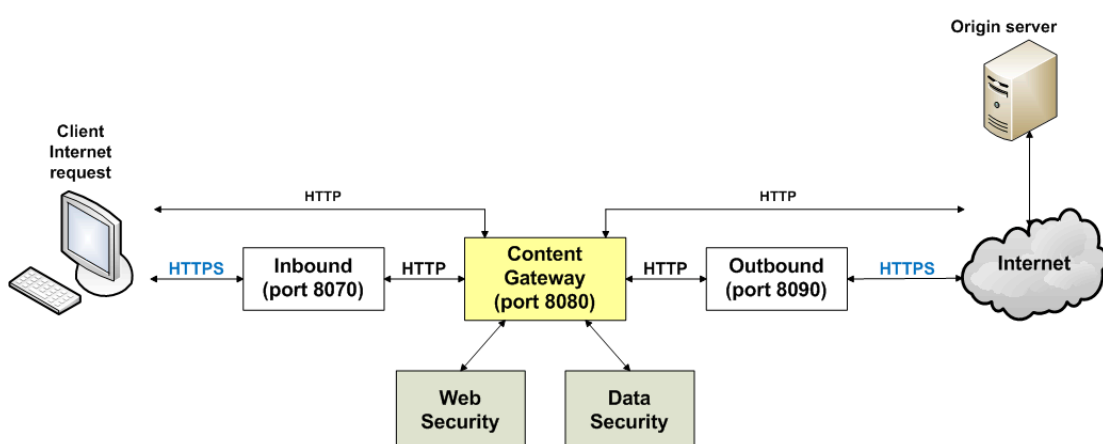
In explicit proxy mode, when SSL is turned off, Content Gateway performs URL filtering based on the Host name in the request. If the site is blocked, Content Gateway serves a block page. Note that some browsers do not support display of the block page. To disable this feature, configure clients to not send HTTPS requests to the proxy.

In transparent proxy mode, when SSL is turned off, Content Gateway performs URL filtering based on the common name present in the certificate from the origin server. If the site is blocked, the connection with the client is dropped; no block page is served. To disable this feature when used with WCCP, do not create a service group for HTTPS.

Each SSL-based request consists of two separate sessions:

- ◆ From the client browser to SSL Manager. This is considered *inbound* SSL traffic.
- ◆ From SSL Manager to the Web server that will receive the secure data. This is considered *outbound* SSL traffic.

Different certificates are required for these sessions.



For additional information on SSL and certificates, search the Internet or consult any of the commercially available books on SSL.



For information on preparing your system, see the deployment and installation material in the [Websense Technical Library](#).

## Running in explicit proxy mode

If you have an existing PAC file, replace the **proxy.pac** file located in the Content Gateway **config** directory (default location is **/opt/WCG/config**) with the existing file. If you do not have a PAC file already, see [Step 4](#) below for a script you can copy.

1. On the **Configure > My Proxy > Basic > General** tab, ensure that both ARM and HTTPS are enabled.  
For ARM, check the Networking section; for HTTPS check the Protocols section. If they are disabled, set them to **On**. Then click **Apply**, followed by **Restart**.
2. Navigate to **Configure > Content Routing > Browser Auto-Config > PAC**.
3. In the **Auto-Configuration Port** field, specify the port that the proxy uses to serve the PAC file. The default port is 8083.
4. The PAC Settings area displays the **proxy.pac** file:
  - If you copied an existing PAC file into the Content Gateway **config** directory, the **proxy.pac** file contains your proxy configuration settings. Check the settings and make changes if necessary.
  - If you did not copy an existing PAC file into the Content Gateway **config** directory, the **proxy.pac** file is empty. Copy and paste the following script for your PAC settings. You must provide the proxy domain name or IP address.

```
function FindProxyForURL(url, host)
{
    url = url.toLowerCase();
    host = host.toLowerCase();
    if(url.substring(0, 5) == "http:") {
        return "PROXY WCG_DOMAIN_NAME_or_IP_Address:8080";
    }
    else if(url.substring(0, 4) == "ftp:") {
        return "PROXY WCG_DOMAIN_NAME_or_IP_Address:2121";
    }
    else if(url.substring(0, 6) == "https:") {
        return "PROXY WCG_DOMAIN_NAME_or_IP_Address:8080";
    }
    else {
        return "DIRECT";
    }
}
```
5. Click **Apply**.
6. Click **Restart** on **Configure > My Proxy > Basic > General**.

Once the new PAC information is in place, you must inform your users to set their browsers to point to the PAC file. For example, if the PAC file is located on the proxy server with the hostname **proxy1** and Content Gateway uses the default port 8083 to

serve the file, users must specify the following URL in the proxy configuration settings:

```
http://proxy1.company.com:8083/proxy.pac
```

The procedures for specifying the PAC file location vary among browsers.

For Microsoft Internet Explorer version 7.0 and later:

1. Navigate to **Tools > Internet Options > Connections > LAN Settings**.
2. Select **Use automatic configuration script** field, and enter  
`http://WCG_Domain_Name_or_IP_Address:8083/proxy.pac`  
in the **Address** field.
3. Click **OK**.

For Mozilla Firefox 2.0 and later:

1. Navigate to **Tools > Options > Advanced > Network > Connection > Settings**.
2. Select **Automatic proxy configuration URL** field, and enter  
`http://WCG_Domain_Name_or_IP_Address:8083/proxy.pac`
3. Click **Reload**, and then click **OK**.

See your browser documentation for details.

## Enabling SSL Manager

---

1. On **Configure > My Proxy > Basic > General**, click **HTTPS On**.



### Note

If you are running with other Websense products that inspect HTTPS traffic, such as Websense Data Security Suite, you must enable HTTPS.

2. Click **Apply** and then click **Restart**.
3. On **Configure > My Proxy > UI Setup > General**, specify the port for the SSL Manager interface. The default is 8071. This must be a different port than the Content Gateway Manager interface (default 8081).
4. Enter the name of the SSL certificate file. See [Creating a subordinate CA](#), page 128.

Use the **Configure > Protocols > HTTPS** page to provide port information and enable Skype tunneling.

1. In the **HTTPS Proxy Server Port** field, enter the port for inbound (client to SSL Manager) HTTPS traffic. The default is 8070.

2. In the **SSL Outbound Port** field, enter the port SSL Manager will use for outbound HTTPS traffic from SSL Manager to the destination server. The default is 8090.
3. If Content Gateway is an **explicit proxy** and you want to allow Skype traffic, enable the **Tunnel Skype** option. This option is necessary because, although Skype presents an SSL handshake, Skype data flow does not conform to the SSL standard. Unless the traffic is tunneled, the connection is dropped.

**To complete the configuration**, you must ensure that all users who are allowed to use Skype have a Filtering policy that allows **uncategorized** and **internet telephony**. This is required regardless of whether Skype is used with SSL enabled or not.

Also, if not prevented, after the initial handshake Skype will route traffic over a non-HTTP port. To force Skype traffic to go through Content Gateway, a GPO should be used, as described in the [Skype IT Administrators Guide](#).

**Note**

There is no need to set this option if SSL Manager is not enabled.

This option is not valid and has no effect when Content Gateway is a transparent proxy.

---

## Tasks

---

For inbound (client to SSL Manager) traffic, perform these steps in preparation to deploying SSL Manager:

1. Create an internal root CA (certificate authority). In order to sign SSL traffic, SSL Manager requires an internal SSL Certificate Authority that has the ability to sign SSL certificates. This is for traffic between the browser and SSL Manager. See [Internal Root CA](#), page 126.
2. Add this CA to the certificate tree. Servers, such as destination servers, check this tree to ensure that they can trust users because they have certificates from an authority listed here. The certificates listed on the certificate tree are certificate authorities you empower (trust) to verify the validity of individual Web sites. Any Web site signed by a certificate authority in the certificate tree with the “allow” status is allowed through SSL Manager. See [Managing certificates](#), page 134
3. Customize pages that browser users will see. See [Customizing SSL connection failure messages](#), page 150. Among the pages that can be customized are a connect failure and certificate verification failure page.

## Certificates

---

Security revolves around certificates. One role SSL Manager plays is to ensure that certificates are valid. A certificate must meet three criteria:

- ◆ It must be current (has not expired or been revoked). See [Validating certificates](#), page 138.
- ◆ It must be issued by a trusted CA (certificate authority). See [Managing certificates](#), page 134
- ◆ The URL and the certificate owner match. See [Configuring validation](#), page 139.

Traffic from the client browser to SSL Manager requires a certificate issued by an internal root certificate authority. See [Internal Root CA](#), page 126.

Traffic from SSL Manager to the destination server requires a certificate issued by one of the authorities listed on the Certificate Authority Tree on the **Configure > SSL > Certificates > Certificate Authorities** tab. See [Managing certificates](#), page 134.

## Internal Root CA

---

The internal Root CA dynamically generates all certificates used between the client browser and SSL Manager.

- ◆ You must have an internal Root CA to pass inbound traffic to SSL Manager.
- ◆ You can either import or create the CA.
- ◆ The internal Root CA is stored in `/opt/WCG/sxsuite/conf/CA_default/PCA`.
- ◆ The name of the CA is **PCAcert.pem**



### Important

Back up the existing internal Root CA before importing or creating a new one. This enables you to return to an earlier version of the certificate, if necessary. See [Backing up your internal Root CA](#), page 133 for details.

Only one internal Root CA can be active at any time.

---



### Important

The default internal Root CA included with SSL Manager is not unique and should not be used in a production environment.

Replace the default Root CA with your organization's existing Root CA or create a new one. See the sections that follow.

---

There are three options for creating an internal Root CA:

- ◆ Leverage an existing corporate CA and import it into SSL Manager. See [Importing your Root CA, page 127](#).
- ◆ Create a new CA for proxies and make that CA available to browsers. See [Creating your new Root CA, page 127](#).
- ◆ Create a subordinate CA. This leverages a corporate CA, but can also be revoked by the corporate CA. See [Creating a subordinate CA, page 128](#).

## Importing your Root CA

If your organization already has a root certificate authority, you can import it. This certificate must be trusted by all browsers in your organization. Be sure to back up any new internal Root CAs that you import. See [Backing up your internal Root CA, page 133](#) for details.

1. Navigate to **Configure > SSL > Internal Root CA > Import Root CA**.
2. Browse to select the certificate. The certificate must be in X.509 format and base64-encoded.
3. Browse to select the private key. It must correspond to the certificate you selected in Step 2.
4. Enter, and then confirm, the passphrase.
5. Click **Import Root CA**. The imported CA is stored in `/opt/WCG/sxsuite/conf/CA_default/PCA`.

## Creating your new Root CA

Related topic:

[Creating a subordinate CA, page 128](#)

If you do not already have a Root CA, fill in the fields on this tab to create one. Be sure to back up any new internal Root CAs that you create. See [Backing up your internal Root CA, page 133](#) for details.

An asterisk (\*) on this page indicates a required field.

1. Select **Configure > SSL > Internal Root CA**, and then select **Create Root CA**.
2. Provide requested information in the fields, particularly noting the following:
  - The fields **Organization**, **Organizational Unit**, (this field is optional) and **Common Name** comprise a *distinguished name*.
    - For **Organization**, enter the name of your company.
    - For **Common Name**, enter the name of your company certificate authority.
  - The comment becomes part of the certificate. The first line you enter can be seen by end users.

- Enter, and then confirm, the passphrase. (A passphrase is similar to a password. Usually, however, it is longer to provide greater security. It is recommended that you use a strong passphrase, with a combination of numbers, characters, and upper- and lower-case letters.
3. Click **Generate and Deploy Certificate** to deploy the certificate to the Content Gateway server.

## Creating a subordinate CA

Creating a subordinate certificate authority (sub CA) enables you to take advantage of all the information already existing for your Root CA. However, the Root CA can revoke the sub CA at any time.

Follow these steps to generate a sub CA using OpenSSL and the certificate services in Microsoft Windows.

### Preparation

- ◆ **If you are not the Enterprise domain administrator, you will need to work with that person to get the correct domain permissions to generate a sub CA.**
- ◆ Install the **OpenSSL 0.9.8(x)** toolkit ([www.openssl.org](http://www.openssl.org)) on a Windows or Linux computer.

### Creating a Certificate Signing Request (CSR)

1. Create a CSR with OpenSSL.  
In a Windows Command Prompt or on the Linux command line, create a CSR with the following **openssl** command:

```
openssl req -new -newkey rsa:2048 -keyout wcg.key -out
wcg.csr
```

```
[root@JS-WCG ~]# openssl req -new -newkey rsa:2048 -keyout wcg.key -out wcg.csr
Generating a 2048 bit RSA private key
.....+++
.....+++
writing new private key to 'wcg.key'
Enter PEM pass phrase:
Verifying - Enter PEM pass phrase:
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) [GB]:US
State or Province Name (full name) [Berkshire]:California
Locality Name (eg, city) [Newbury]:San Diego
Organization Name (eg, company) [My Company Ltd]:Websense, INC.
Organizational Unit Name (eg, section) []:Technical Support
Common Name (eg, your name or your server's hostname) []:10.212.4.164
Email Address []:

Please enter the following 'extra' attributes
to be sent with your certificate request
A challenge password []:
An optional company name []:
[root@JS-WCG ~]#
```

2. There will be a series of questions. Answer each question and make note of the challenge password; it will be needed later in the process.

The openssl command generates 2 files:

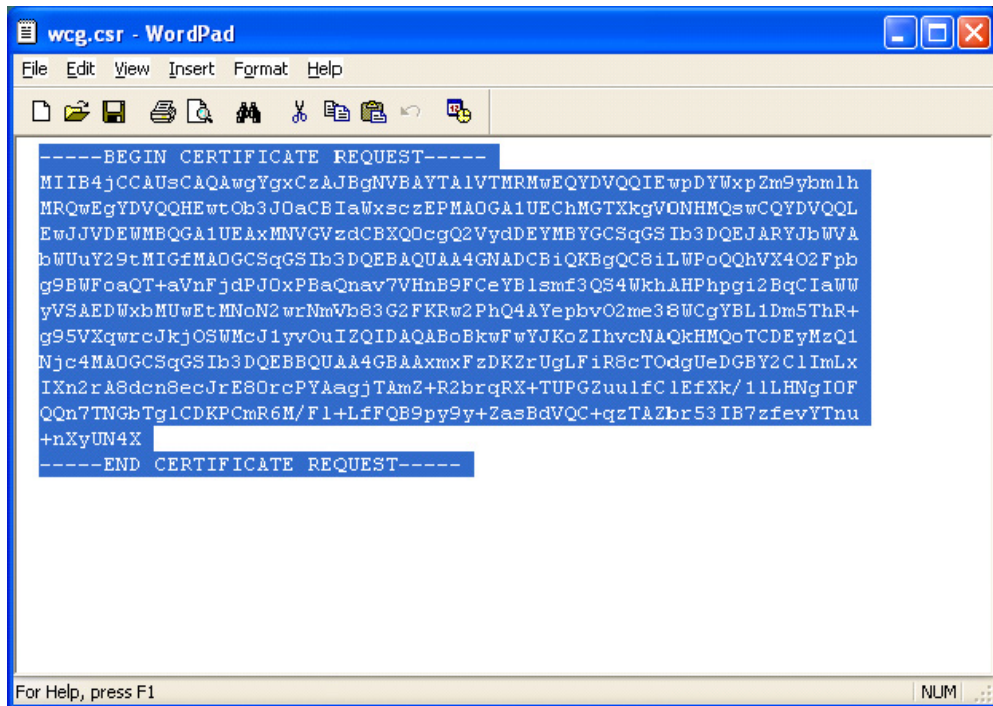
- **wcg.csr** -- the CSR that will be signed by the Certificate Authority to create the final certificate
- **wcg.key** -- the private key

3. If you created the CSR on a Linux system, copy it to your Windows host with WinSCP or some other file transfer utility.

## Signing the request

You must sign the request with Microsoft Certificate Services.

1. Open **wcg.csr** with **Wordpad** (to preserve the formatting) and copy the contents onto the clipboard (Edit > Select all; Edit > Copy).

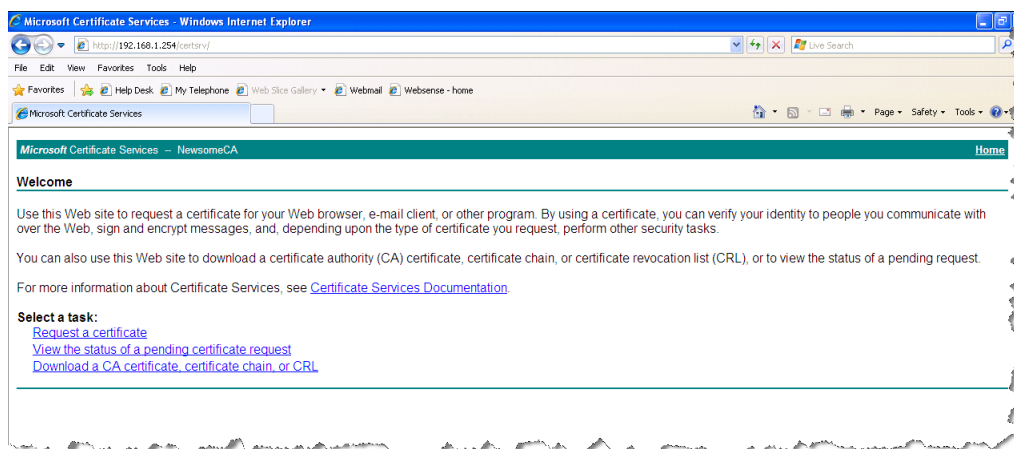


2. In **Internet Explorer**, navigate to the **Microsoft CA server**.

Enter the following URL:

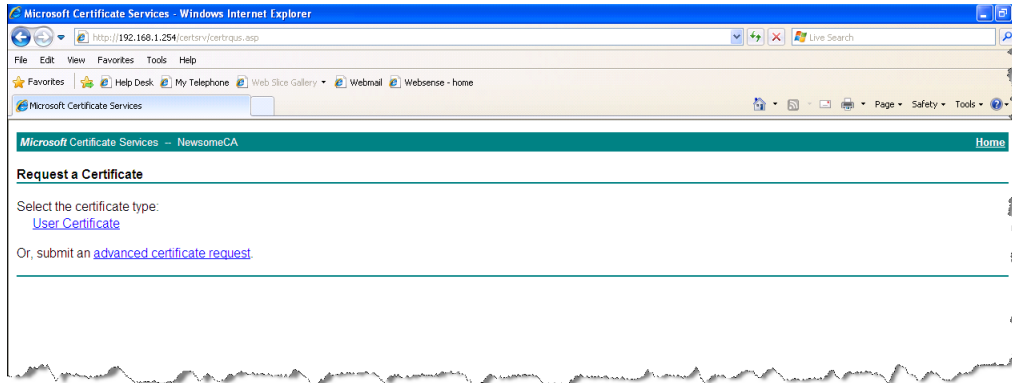
`http://<CA_server_IP_address>/certsrv`

The **Certificate Services** applet starts.

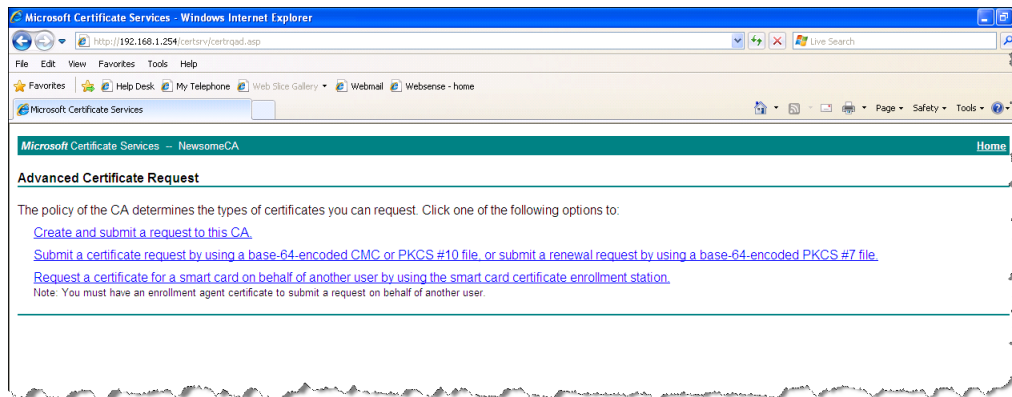




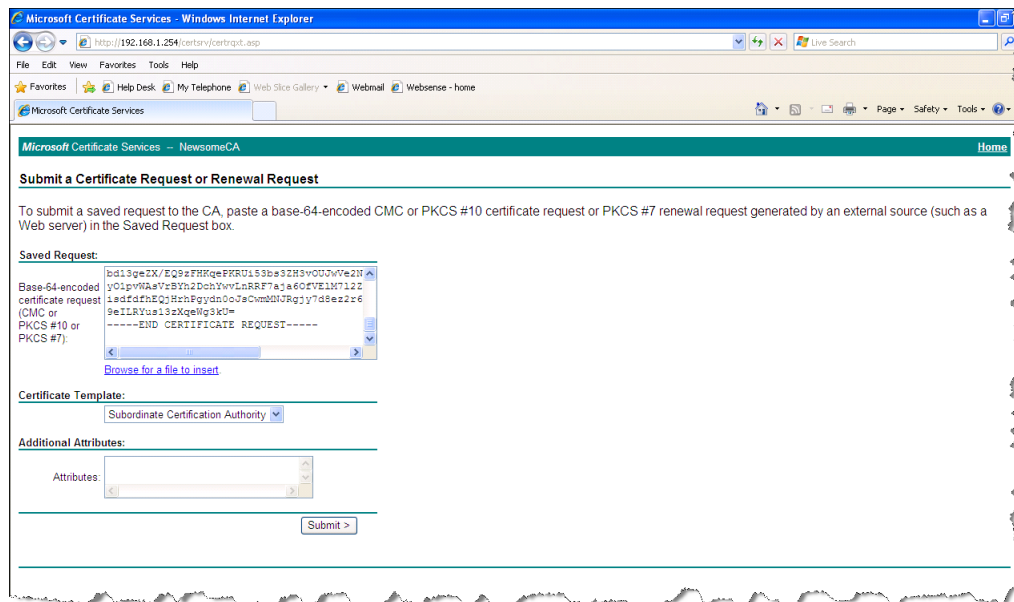
3. On the **Welcome** screen, below the **Select a task** heading, select **Request a certificate**. The **Request a certificate** page displays.



4. Select to submit an **advanced certificate request**.

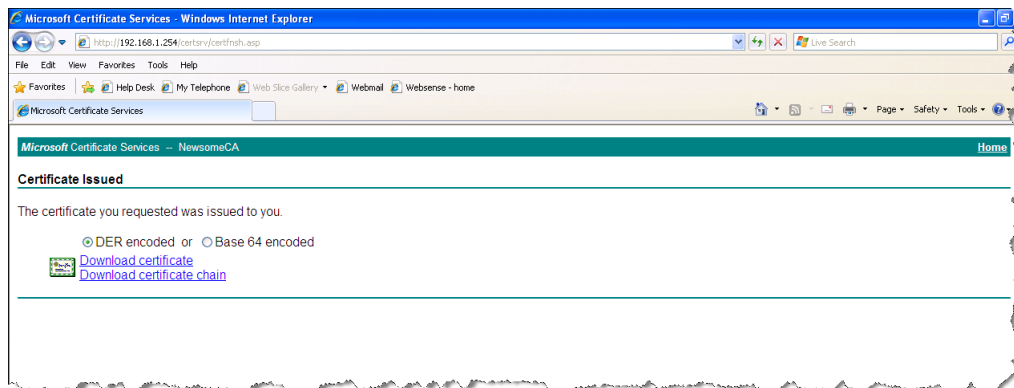


- On the **Advanced Certificate Request** screen, select **Submit a certificate request by using a base-64-encoded CMC**. The **Submit a Certificate Request or Renewal Request** screen displays.



- On the **Submit a Certificate Request or Renewal Request** screen, paste the content of the **wcg.csr** file (previously placed on the clipboard) in the **Certificate Template** drop down window and click **Submit**.

The certificate is issued and the **Certificate Issued** screen displays. If, instead, the **Certificate Pending** screen displays, you do not have sufficient privileges to create a sub CA. Contact your Enterprise domain administrator to complete the certificate creation process and then proceed to step 7.

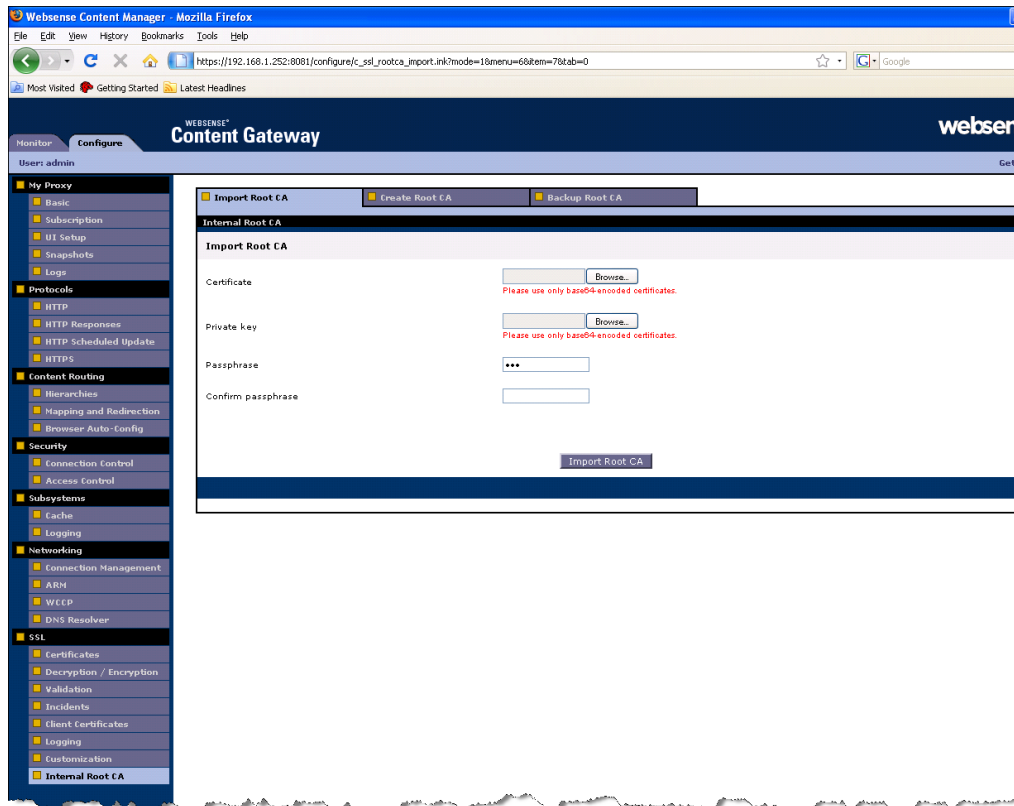


- Select the **Base 64 encoded** radio button and then select **Download certificate**. Save the certificate to your desktop. Later you will import it into Content Gateway.

With the base 64 encoded certificate on your desktop, along with the private key created during the CSR generating process, you are ready to import both into the Content Gateway SSL Manager.

## Importing the sub-CA into SSL Manager

1. Open Content Gateway Manager and navigate to **Configure > SSL > Internal Root CA > Import Root CA**.



2. **Browse** to select the certificate. The certificate must be in X.509 format and base-64-encoded.
3. **Browse** to select the private key. It must correspond to the certificate you selected in step 2.
4. Enter and then confirm the passphrase.
5. Click **Import Root CA**.
6. Restart Content Gateway.

## Backing up your internal Root CA

Always back up the public and private keys of your internal Root CAs before importing or creating new ones. This enables you to return to an earlier version of the certificate, if necessary. In addition, back up any new Root CAs that you import or create.

1. Navigate to **Configure > SSL > Internal Root CA > Backup Root CA**.

2. Click **Save Public CA Key** to view or save the public CA key. This public key must be trusted by the users' Web browsers. Consult your network administrator if you do not have the key.
3. Click **Save Private CA Key** to view or save the private CA key. Consult your network administrator if you do not have the key.

## Managing certificates

---

Related topics:

[Adding new certificate authorities, page 135](#)

[Backing up certificates, page 136](#)

[Restoring certificates, page 136](#)

All certificate authorities trusted by Internet Explorer 7 are listed on the tab **Configure > SSL > Certificates > Certificate Authorities**; destination servers (traffic outbound from SSL Manager) can trust the Web servers with these certificates. Note that a small “i” appears before the name of some certificates validated via CRL (certificate revocation lists) or OCSP (online certification status protocol). These certificates provide URLs where you can verify their revocation status. See [Keeping revocation information up to date, page 141](#) for information on checking the revocation status of a certificate. SSL Manager checks the revocation status of a certificate for both inbound and outbound traffic.

Click on the name of a certificate authority to:

- ◆ [View a certificate, page 134](#)
- ◆ [Delete a certificate, page 134](#)
- ◆ [Change the allow/deny status of a certificate, page 135](#)

### View a certificate

1. Navigate to **Configure > SSL > Certificates > Certificate Authorities**.
2. Select the name of the authority whose status you want view.
3. In the pop-up window, select **Click to view certificate**.
4. Follow the directions in the Opening window to open or save the file.

### Delete a certificate

1. Navigate to **Configure > SSL > Certificates > Certificate Authorities**.
2. Select the name of the certificate authority you want to delete.
3. In the pop-up window, select **Click to delete certificate**.
4. Confirm or deny that you want to delete the certificate.

5. If you confirm that you want to delete the certificate, check that the certificate is no longer listed on **Configure > SSL > Certificates > Certificate Authorities**.

## Change the allow/deny status of a certificate

1. Navigate to **Configure > SSL > Certificates > Certificate Authorities**.
2. Select the name of the authority whose status you want to change.
3. In the pop-up window, select **Click to change status to**. Depending on the status of the certificate, your choice is **allow** or **deny**. If you change the status to deny, a red X appears next to the name of the certificate authority in the certificate authority tree. If you change the status to allow, a green circle appears next to the name of the certificate authority.

## Adding new certificate authorities

Related topics:

[Backing up certificates, page 136](#)

[Restoring certificates, page 136](#)

Use the page **Configure > SSL > Certificates > Add Root CA** to manually import additional certificate authorities. Certificates that you import manually have a default status of allow.



### Important

It is recommended that you back up your current certificates before making any changes, such as adding or deleting certificates. See [Backing up certificates, page 136](#). If you want to back up your entire Content Gateway configuration, see [Saving and restoring configurations, page 101](#).

1. Click **Browse** to navigate through the directory structure to find certificates. Look for files that have a “.cer” extension. The certificate must be in X.509 format and base64-encoded.
2. Click **Add Certificate Authority**.
3. If the import was successful, check that the new certificate is listed on **Configure > SSL > Certificates > Certificate Authorities**.

New CAs are also added when users visit a site signed by that authority. These certificates may be allowed or denied. See [Change the allow/deny status of a certificate, page 135](#) for additional information.

## Backing up certificates

As a precaution, it is recommended that you back up the database containing the CA certificates whenever you make changes, such as adding or deleting a certificate. They can then be restored at a later date.

Backing up certificates also backs up your SSL Manager settings.

Use the page **Configure > SSL > Certificates > Backup Certificates** to back up certificates and your SSL Manager settings.

► Click **Back Up Configuration to Database**.

To back up not only certificates, but your entire Content Gateway configuration, see [Saving and restoring configurations](#), page 101.

## Restoring certificates

Restoring certificates also restores the configuration database. However, because revocation lists are updated on a regular basis, they are not restored as part of this process. See [Keeping revocation information up to date](#), page 141 for information on updating certificate revocation lists.

Use the page **Configure > SSL > Certificates > Restore Certificates** to restore the configuration database, which includes certificates and your SSL Manager settings.

1. Click **Browse** to navigate to the location of the backup certificate database.
2. Click **Restore**. You receive a message telling you that the restore was successful and indicating where the previous certificate database was backed up.

If you are running multiple proxies, use this restore feature to ensure that all the proxies have the same configuration.

## Decryption and Encryption

---

[Configuring SSL Manager for inbound traffic](#), page 136

[Configuring SSL Manager for outbound traffic](#), page 137

## Configuring SSL Manager for inbound traffic

Related topics:

[Configuring SSL Manager for outbound traffic](#), page 137

Use the page **Configure > SSL > Decryption / Encryption > Inbound** to configure how SSL Manager handles inbound traffic. Inbound traffic travels from the browser to SSL Manager, where the content is decrypted and inspected.

1. Select **IP Address** to forward authentication credentials to the next proxy.
2. Select **Send VIA-Header** to add a special header to the HTTP header to describe the proxy chain traffic passed through. This can be helpful in troubleshooting. If you do not want to include a VIA-Header, do not select this box.
3. Under **Protocol Settings**, indicate which protocols you want SSL Manager to support. Supported protocols are SSLv2 and v3, and TLS v1. Select the protocol that your enterprise browser supports; you must select at least one protocol. The default is SSLv2. These settings override the settings for these protocols in the users' browsers.

You can select different protocols for outbound traffic.

4. The cipher list describes available algorithms and level of encryption between the client and SSL Manager. The default settings indicate to use all available ciphers except the eNULL and the ADH Suite. The strongest cipher (providing the highest level of encryption) is applied first. This can be set to a different level of encryption than for outbound traffic. Setting encryption to a high level for inbound traffic can help ensure the integrity and security of your system.

Additional cipher settings are:

- **High** encryption cipher suites: those with key lengths larger than 128 bits, and some cipher suites with 128-bit keys.
- **Medium** encryption cipher suites: those using 128 bit encryption.
- **Low** encryption cipher suites: those using 64- or 56-bit encryption algorithms but excluding export cipher suites.

For inbound requests (requests from a client browser in your organization to SSL Manager), consider using Low encryption to improve performance.

For more information on ciphers, refer to [www.openssl.org/docs](http://www.openssl.org/docs).

5. Click **Apply**.
6. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Configuring SSL Manager for outbound traffic

Use the page **Configure > SSL > Decryption / Encryption > Outbound** to configure how SSL Manager handles outbound traffic. Outbound traffic travels from SSL Manager to the destination Web server. SSL Manager checks the revocation status of this site's certificate before forwarding re-encrypted data to it.

1. Select **IP Address** to forward authentication credentials from one proxy to the next if there are multiple proxies between SSL Manager and the destination host.
2. Select **Send VIA-Header** to add a special header to the HTTP header to describe the proxy chain traffic passed through. This can be helpful in troubleshooting. If you do not want to include a VIA-Header, do not select this box.

3. Under **Protocol Settings**, indicate which protocols you want SSL Manager to support. Supported protocols are SSLv2 and v3, and TLS v1. Select the protocol that your enterprise browser supports; you must select at least one protocol. The default is SSLv2. These settings override the settings for these protocols in the users' browsers.

You can select different protocols for inbound traffic.

4. Select **Session Cache** if you want to cache keys until the time specified in Session Cache Timeout elapses. This can improve performance. If keys are not cached, each request is negotiated again.
5. Indicate, in seconds, how long keys should be kept in the cache. The default is 300 seconds (5 minutes).
6. The cipher list describes available algorithms and level of encryption between the client and SSL Manager. The default settings indicate to use all available ciphers except the eNULL and the ADH Suite. The strongest cipher (providing the highest level of encryption) is applied first. This can be set to a different level of encryption than for inbound traffic. Setting encryption to a high level for outbound traffic can help ensure the integrity and security of your system.

Additional cipher settings are:

- **High** encryption cipher suites: those with key lengths larger than 128 bits, and some cipher suites with 128-bit keys.
- **Medium** encryption cipher suites: those using 128 bit encryption.
- **Low** encryption cipher suites: those using 64- or 56-bit encryption algorithms but excluding export cipher suites.

For outbound requests (requests from SSL Manager to the destination server that is receiving the encrypted data), consider using one of the higher encryption levels to improve security.

For more information on ciphers, refer to [www.openssl.org/docs](http://www.openssl.org/docs).

7. Click **Apply**.
8. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Validating certificates

---

SSL certificate verification is an essential element of SSL security. It is through certificate exchange and verification that the client, in this case Content Gateway SSL Manager, and the origin server verify that each is who they say they are. In SSL Manager, this task is performed by the certificate verification engine. Use the tabs on **Configure > My Proxy > SSL > Validation** to enable and configure certificate verification.

For information about options when verification fails and you prefer to trust the site, see [Bypassing verification](#), page 141.



Related topics:

[Bypassing verification, page 141](#)

[Keeping revocation information up to date, page 141](#)

## Configuring validation

1. Navigate to the page **Configure > SSL > Validation > General**.
2. Select or clear **Enable the certificate verification engine** to enable or disable certificate verification and checking for certificate revocation. **If this option is not selected, checking does not occur.**

If you are not familiar with certificate verification and are concerned that your users may be impeded from accessing legitimate sites, you could leave certificate verification disabled and monitor traffic. After a period, you could enable the feature and specify how SSL Manager should handle frequently accessed sites by creating incidents. See [Managing Web HTTPS site access, page 143](#).



### Important

If you disable the certificate verification engine, you need to provide information only on the following pages:

- Configure > SSL > Decryption / Encryption > Inbound
- Configure > SSL > Decryption / Encryption > Outbound
- Configure > SSL > Logging pages
- Configure > SSL > Customization > Connection Error

3. Select **Deny Certificates where the common name does not match the URL** to define how the proxy handles those cases where the common name of the certificate does not match the URL of the Web server. For example, a certificate from [www.company.com](#) does not match the URL [www.company.de](#).
4. Select **Allow wildcard certificates** if you want to accept a single certificate for an entire domain. This means that individual servers within that domain are not verified; they are all included because of the wildcard.
5. Select **No expired or not yet valid certificates** to deny access to sites whose certificates fit that criteria. If this box is not selected, access to those sites is permitted.



### Note

Self-signed certificates (certificates without an official certificate authority) are considered invalid and belong in this category.

6. Select **Verify entire certificate chain** to verify all certificates between a certificate and its root certificate authority.

7. Select **Check certification revocation by CRL** to use certificate revocation lists (CRLs) to check a certificate's revocation state.
8. Select **Check certification revocation by OCSP** to use the Online Certificate Status Protocol to check a certificate's revocation state. Currently, OCSP is not used as widely as CRLs, so it is recommended that you indicate CRL in this field and use OCSP as a backup to CRLs.

**Note**

Certification revocation lists are used far more widely. It is recommended that you use OCSP in addition to, rather than instead of, CRLs. See [Keeping revocation information up to date](#), page 141 for more information on CRLs and OCSP.

---

9. If you enable checking by both CRLs and OCSP, indicate which method SSL Manager should use first for revocation checking.
10. Indicate whether access should be permitted or denied to sites whose certificate revocation status cannot be determined. If this option is selected, access is also denied to sites whose certificates do not contain CRL or OCSP information. You can see this information when you select a certificate authority and choose view certificate. See [View a certificate](#), page 134 for details. **This can result in a highly restrictive security policy, with many access denials.** You can allow for exceptions by using the incident list to manage access to Web sites. See [Managing Web HTTPS site access](#), page 143.
11. For troubleshooting purposes, you can run an external program on incidents. An incident is logged whenever a client receives an access denied message. See [Managing Web HTTPS site access](#), page 143 for more information on incidents. Enter the path to the script in this field.

The minimum permissions for running this script should be as follows:

```
chmod 700 /opt/WCG/sxsuite/bin/script.sh
chown Websense /opt/WCG/sxsuite/bin/script.sh
chgrp Websense /opt/WCG/sxsuite/bin/script.sh
```

It is recommended that you copy and paste for following script for help in troubleshooting. It captures the following pieces of information and writes them to a file.

- The account that created the incident
- The client IP or the IP address of the previous proxy if the client IP address is not forwarded
- The ID of the incident as shown in the incident list
- A detailed message on what caused the incident
- The profile within the account that caused the incident
- The host section of the URL that precipitated the incident

```
#!/bin/sh
OUTFILE=/home/Websense/incidents.log
```

```
date >> $OUTFILE
echo "Account: $SCIP_INCIDENT_ACCOUNT" >> $OUTFILE
echo "Client-IP: $SCIP_INCIDENT_CLIENTIP" >> $OUTFILE
echo "Incident-ID: $SCIP_INCIDENT_ID" >> $OUTFILE
echo "Detailed Message: $SCIP_INCIDENT_MESSAGE" >> $OUTFILE
echo "Profile: $SCIP_INCIDENT_PROFILE" >> $OUTFILE
echo "Destination Host URL: $SCIP_INCIDENT_REMOTEHOST" >>
$OUTFILE
echo "User: $SCIP_INCIDENT_USER" >> $OUTFILE
echo >> $OUTFILE
```

**Important**

It is recommended that you do not enter any of the other commands in the `/opt/WCG/sxsuite/bin/` directory in this field, and that you exercise caution if you enter a script other than the one provided above.

---

## Bypassing verification

---

Use the **Configure > SSL > Validation > Verification Bypass** page to enable users to visit a site even if the certificate is invalid.

1. Select **Permit users to visit sites with certificate failure after confirmation** to enable users to proceed to a site after they have been informed that the site has an invalid certificate. If this check box is not selected, users do not have the option to browse to the site.
2. Select **Enable the SSL session cache for bypassed certificates** to store information about bypassed certificates in cache and reuse the connections.
  - If this option is selected, performance is better, but not all users are notified that they are trying to access a site where verification has failed.
  - If this option is not selected, all users are notified about sites that do not have valid certificates, but performance is not as fast.
3. For **Timeout**, specify the period of inactivity that elapses between notifications to users who bypassed this site that the site has an invalid certificate. The default is 6 minutes (360 seconds).

It is recommended that you deploy initially with bypass verification enabled. Then, as the incident rate changes, you can use the incident list to enforce policy. See [Managing Web HTTPS site access](#), page 143.

## Keeping revocation information up to date

---

It is recommended that before your site accepts certificates, it checks the status of the certificate to ensure that it has not been revoked. There are two methods of doing this:

through CRLs (see [Certificate revocation lists](#), page 142) and through OCSP (see [Online certification status protocol \(OCSP\)](#), page 142).

## Certificate revocation lists

Use the **Configure > SSL > Validation > Revocation Settings** page to configure how SSL Manager keeps revocation information current. By default, SSL Manager downloads CRLs on a daily basis.

1. For daily downloads of the CRLs, select **Download the CRL at**, and select the time when the CRL download occurs.
2. Click **Apply**.

Use this page as well if you need an immediate CRL update.

1. Click **Update CRL Now** to download the CRLs at a time other than that specified. For example, if your subscription includes SSL Manager, download the CRLs after you install the program.



### Note

The CRL files can contain thousands of certifications, so downloading CRLs can take some time and consume CPU resources. It is recommended that you download CRLs at a time when Internet traffic on your system is light.

---

2. Click **View CRL Update Progress** to see the status of the update.

For more information on certificate revocation lists, see RFC 3280.

## Online certification status protocol (OCSP)

OCSP is a protocol that operates on a request/response basis. That is, when a site wants to verify the revocation status of a certificate, it sends a request to the CA about the status of the certificate. The CA then responds, confirming the validity (or revocation) of the certificate.

OCSP, because it is dealing with requests, rather than downloading CRLs, can provide improved performance. However, not all CAs provide responses, so CRLs can provide information about the status of more certificates.

SSL Manager enables you to cache OCSP responses about the revocation state of a certificate. Caching responses may be useful in environments with high amounts of SSL traffic and where saving bandwidth is important.

Use the **Configure > SSL > Validation > Revocation Settings** page to configure how SSL Manager keeps revocation information current.

1. Specify, in days, how long OCSP data should be cached. If you do not want to cache OCSP data, enter **0**. The maximum is 1000 days
2. Click **Apply**.

For more information on OCSP, see RFC 2560.

## Managing Web HTTPS site access

---

Related topics:

[Viewing incidents, page 143](#)  
[Changing the status of an incident, page 145](#)  
[Deleting an incident, page 145](#)  
[Changing the text of a message, page 145](#)  
[Viewing incident details, page 145](#)  
[Adding Web sites to the incident list, page 146](#)

These tabs can help you manage access to Web sites and can aid the Help Desk in troubleshooting access issues. Entries and changes made to this page are saved in the SSL Manager database.

When a client receives an access denial message because the Web site does not comply with security policies, SSL Manager generates an *incident*. See [Viewing incidents, page 143](#).

If you want to specify how SSL Manager treats a particular site, you can add that to the incident list as well. See [Adding Web sites to the incident list, page 146](#).

## Viewing incidents

Use the **Configure > SSL > Incidents > Incident List** page to see a report of those times when clients received an access denial message. You can use the fields in this report to determine how SSL Manager treats requested access to a site in the future.

- ▶ To view incidents:
  - To view a specific incident, enter the ID number and click **Search**.
  - To view the complete list, click **Show All**.

### The incident report

You can sort on any column by clicking on the small triangle next to the column heading.

The incident report contains these fields:

Field	Description
ID	Assigned by the system, this is the incident ID number, also called the Ticket ID. The Help Desk can ask the user for the Ticket ID in the error message and quickly retrieve it from the URL Incident List. The end user sees the Ticket ID and a denial message.
Status	Determines how SSL Manager will treat this Web site in the future. Four conditions are possible: <ul style="list-style-type: none"> <li>• Allow Users can access the site even if the certificate is not valid. Traffic is decrypted, and certificate checking is disabled.</li> <li>• Blacklisted The site is completely blocked. Users cannot access this site even if the Verification Bypass is configured.</li> <li>• Block If certificate verification fails, access to the Web site is blocked, unless Verification Bypass is configured, in which case the block page includes a “Visit site anyway” button. See <a href="#">Bypassing verification</a>, page 141.</li> <li>• Tunnel The site is tunneled. Traffic is not decrypted and SSL Manager does not check the certificate. Tunneling can be used to bypass inspection of trusted sites and improve performance. You can change the status of a Web site via the drop-down box in the Action column.</li> </ul>
Type	Indicates whether the site was added based on its URL or its certificate. It is recommended that you add sites to the incident list by certificate. See <a href="#">Adding Web sites to the incident list</a> , page 146.
URL	The URL of a site whose certificate could not be validated.
Message	Enables you to edit the error message. See <a href="#">Changing the text of a message</a> , page 145 for information on customizing error messages. The pencil and the magnifying glass each represent links. See <a href="#">Viewing incident details</a> , page 145 for details on these links.
Action	Enables you to change the status of an incident. Also allows you to delete the incident. See <a href="#">Deleting an incident</a> , page 145.

## Changing the status of an incident

When you change the status of an incident, you are changing how SSL Manager will treat the listed URL in the future.

1. Navigate to **Configure > SSL > Incidents > Incident List**.
2. Select one of the following from the drop-down list in the Actions column. See [The incident report, page 143](#) for an explanation of these options.
  - Tunnel
  - Block
  - Blacklist
  - Allow
3. Click **Go**. The icon in the Status column changes to reflect the new status.

## Deleting an incident

1. Navigate to **Configure > SSL > Incidents > Incident List**.
2. Select the incident to delete. If the incident is not visible, you can search by ID. See [Viewing incidents, page 143](#).
3. In the Action column, select **Delete** from the Action drop-down list, and then click **Go**.

## Changing the text of a message

1. Navigate to **Configure > SSL > Incidents > Incident List**.
2. Locate the incident you want to examine more closely. See [Viewing incidents, page 143](#).
3. Click the pencil to open a window where you can change the text of this error message. For example, the Help Desk can add more detail to an error message.
4. Click **Submit** when the new text is complete, or click **Close Window** if you are not making any changes.

## Viewing incident details

1. Navigate to **Configure > SSL > Incidents > Incident List**.
2. Locate the incident you want to examine more closely. See [Viewing incidents, page 143](#).
3. Click the magnifying glass to see additional details about the incident, such as the:
  - Description (this is the message that appears in the incident listing)
  - Time the incident was created
  - Time the incident was modified
  - Incident count (how many times users have tried to access this site)

## Adding Web sites to the incident list

Use **Configure > SSL > Incidents > Add Website** page to specify sites that you want to allow, blacklist, or tunnel. Sites that are added manually are assigned chronological Ticket IDs. These appear on the incident list. See [Viewing incidents, page 143](#).

1. Enter the URL of the site you are adding to the Incident List.
2. Select either **By Certificate** or **By URL**.
  - **By Certificate** provides greater security. If you add a Web site by certificate, clients cannot bypass the policy by using the IP address rather than the URL. When you select By Certificate, SSL Manager retrieves the server certificate and adds the site to the incident list. See [Viewing incidents, page 143](#).  
  
If sites are blocked by certificates, wildcard certificates are not accepted, even if the common name is recognized.
  - Select **By URL** to tunnel, allow, or blacklist the site.
3. In the Action drop-down list, specify if the site should be added with **Tunnel**, **Allow**, or **Blacklist** status. See [The incident report, page 143](#) for details.
  - **Tunnel:** (Valid for **By URL** only) The site is tunneled. Traffic is not decrypted and SSL Manager does not check the certificate.
  - **Allow:** Users can access the site even if the certificate is not valid. Traffic is decrypted, and certificate checking is disabled.
  - **Blacklist:** The site is completely blocked. Users cannot access this site even if the Verification Bypass is configured.
4. Click **Apply**.

It is recommended that you manually add sites to the incident list after you have monitored your network traffic for a period of time, with the certificate verification engine disabled. (See [Configuring validation, page 139](#).) This enables you to improve performance by tunneling trusted sites and blocking those you know should not be accessed. See [The incident report, page 143](#) for information about assigning a status, such as tunneling, to a site and incident.

---

## Client certificates

For security, the destination server may request a client certificate.

Related topics:

[Importing client certificates, page 147](#)

[When a client certificate is always required: the hostlist, page 147](#)

[Deleting client certificates, page 147](#)

## When a client certificate is requested

1. Navigate to **Configure > SSL > Client Certificates > General**.



2. Select **Tunnel** or **Create incident** to specify how SSL Manager should handle that certificate and site. You must choose **Create incident** if you want any disposition other than tunnel (white listing). White listing will always provide the certificate to the server. See [The incident report](#), page 143 for a listing of possible dispositions.
3. Click **Apply**.

## Importing client certificates

Use the **Configure > SSL > Client Certificates > Import** page to import certificates from the organization represented by the client.



---

### Important

Remember to use only X.509-formatted, base64-encoded certificates.

---

1. Enter the name of the client certificate.
2. Enter the public key for the certificate. You may need to check with your network administrator for the key.
3. Enter the private key for the certificate. You may need to check with your network administrator for the key.
4. Enter, and then confirm, the passphrase. It is recommended that you use a strong passphrase, with a combination of numbers, characters, and upper- and lower-case letters. You may need to check with your network administrator for the passphrase.
5. Click **Import**.

## When a client certificate is always required: the hostlist

Use the **Configure > SSL > Client Certificates > Hostlist** page to list those destination servers that always require a client certificate. Be sure to import the certificate before adding it to the hostlist. See [Importing client certificates](#), page 147.

1. Enter the URL of the destination server that requires the client certificate.
2. In the **Client Certificate** drop-down list, select the name of the client certificate. Only certificates you have already imported appear in this list.
3. Click **Add**.

## Deleting client certificates

Use the **Configure > SSL > Client Certificates > Manage Certificates** page to delete imported client certificates.

1. Select the certificate you want to delete.
2. Click **Delete**.

## Configuring SSL Manager logging

Related topics:

[How long should SSL log files be kept?, page 149](#)

[How big can SSL log files grow?, page 149](#)

[What fields should appear in the SSL access log files?, page 149](#)

SSL Manager creates 2 types of log files.

- ◆ Activity logs. These logs monitor SSL Manager activity and include messages at a level specified in the user interface
- ◆ Access logs

You can log activity for both inbound (client to SSL Manager) and outbound (SSL Manager to server) traffic. You have the option of logging data to the system log (syslog) or to a file.

Use the **Configure > SSL > Logging > General** page to specify the name and location of log files.

1. For *inbound* traffic, select the type of log files you want to keep. For activity logs, you are specifying the level of detail in the log.
2. Enter a number from 1 to 7 to indicate the level of detail you want logged. Note that each level provides more information; level 7 is the most verbose. The levels of logging and granularity are:

1 (alert)	Log conditions that should be corrected immediately, such as a corrupted system file
2 (critical)	Log conditions such as device failures
3 (normal)	Log errors
4 (warning)	Log warnings
5 (notice)	Log conditions that are not error conditions, but may still require attention
6 (information)	Log informational messages
7 (debugging)	Log debugging information. Level 7 includes the most log output.

3. Indicate if log data should go to the syslog or to a file.
4. Repeat [Step 2](#) and [Step 3](#) for the access log file.
5. For *outbound* traffic, repeat [Step 2](#) through [Step 4](#).
6. Click **Apply**.

Logs are written to `/opt/WCG/sxsuite/log`.

## How long should SSL log files be kept?

A new set of log files is created every 24 hours. By default, this occurs at midnight. This rotation happens regardless of the size of the log file. In addition, the log file is rotated if it reaches its maximum size before the scheduled rotation. In that case, the scheduled rotation still takes place at midnight. See [How big can SSL log files grow?](#), page 149 for information on specifying the maximum log size.

Use the **Configure > SSL > Logging > Options** page to specify how long to keep log files.

1. Specify, in days, how long log files should be kept. The default is 3.
2. Set any additional options on this page and then click **Apply**.

## How big can SSL log files grow?

Log files are rotated every night at midnight. However, a new log file is started when the file reaches its specified maximum size, even if this is before the scheduled daily rotation. Because the size of log files is checked every minute, it is possible that a log file may be larger than its maximum size for a brief period.

When a log file reaches its maximum size, it is saved with an extension of “.x” (where x is 1, 2, or 3, etc.), and a new file is started. If this should happen multiple times in a 24-hour period, you must indicate how many files (generations) should be kept. See [How long should SSL log files be kept?](#), page 149 for information on log rotation.

Use the **Configure > SSL > Logging > Options** page to specify how large log files can grow.

1. Indicate, in KB, the maximum size for log files. The default is 50,000 KB.
2. For generations, indicate how many log files should be kept if the file reaches its maximum size multiple times before daily rotation. Once this number is reached and new log files are created, the oldest log file is deleted. The default is 3 generations.
3. Set any additional options on this page and then click **Apply**.

## What fields should appear in the SSL access log files?

Use the **Configure > SSL > Logging > Options** page to add or delete fields to the log file.

1. Delete or add fields in the Access log file customization box. The fields are:

time_stamp	The timestamp in the following format:[YYYY.MM.DD HH:MM:SS]
time_of_day	The timestamp in raw format: Sec.mSec starting from 1st Jan 1970 UTC
src_ip	The client's IP Address

auth_user	The user who has been authenticated
account	The account the user belongs to
profile	The user's profile
req_line	The Request in the following format: "method path protocol/version.subversion". For example: GET / HTTP/1.1
status_code	The HTTP status response code sent by the Web server
user_agent	The name of the client browser
referer	The host section of the URL
content_type	Content, such as HTML, text, image, etc.
content_length	In bytes
server_host	IP address of the Web server
bytes_from_client	Bytes transferred from the client to SSL Manager
bytes_to_client	Bytes transferred from SSL Manager to the client
bytes_from_server	Bytes transferred from the Web server to SSL Manager
bytes_to_server	Bytes transferred from SSL Manager to the Webserver

2. Click **Apply**.

## Customizing SSL connection failure messages

---

You can customize the message users receive when:

- ◆ They are trying to connect to a site that has an invalid certificate. See [Certificate validation failed, page 151](#).
- ◆ There is a connection failure. See [SSL connection failure, page 151](#).

The following variables are available within the message templates.

%P	Protocol (HTTP or HTTPS)
%h	The IP address and port of the host of the proxy that generated the message
%o	The IP address of the host of the proxy that generated the message
%H	Remote hostname of the request
%t	Time
%s	Name of the SSL Manager server
%u	Complete URL

\$\$DETAILS	Detailed error message
\$\$TICKET_ID	The ID number of the incident.

## Certificate validation failed

Use the **Configure > SSL > Customization > Certificate Failure** page to customize the message users receive when certificate validation fails.



### Note

You may find it helpful to click **Preview** to see how the default message appears.

1. Edit the HTML code in the window to reflect your message. See [Customizing SSL connection failure messages, page 150](#) for a listing of variables you can use in the message.
2. Click **Preview** to see your changes.
3. Repeat steps 1 and 2 until the message appears appropriately.
4. Click **Apply** to confirm your edits or **Cancel** to return to the original message.

## SSL connection failure

Use the **Configure > SSL > Customization > Connect Error** page to customize the message users receive when SSL Manager is unable to connect to the destination Web server.



### Note

You may find it helpful to click **Preview** to see how the default message appears.

1. Edit the text in the window to reflect your message. See [Customizing SSL connection failure messages, page 150](#) for a listing of variables you can use in the message.
2. Click **Preview** to see your changes.
3. Repeat steps 1 and 2 until the message appears appropriately.
4. Click **Apply** to confirm your edits or **Cancel** to return to the original message.



# 14

## Security

Websense Content Gateway enables you to establish secure communication between the Content Gateway system and other computers on the network. You can:

- ◆ Control which clients are allowed to access the proxy cache. See [Controlling client access to the proxy](#), page 153.
- ◆ Control and secure access to Content Gateway Manager using:
  - Administrator accounts (see [Setting the administrator ID and password](#), page 154 and [Creating a list of user accounts](#), page 155).
  - SSL (Secure Sockets Layer) protection for encrypted, authenticated access (see [Using SSL for secure administration](#), page 156).
- ◆ Create filtering rules to control access to the Internet, specify special authentication requirements, and control other traffic transiting the proxy. See [Filtering Rules](#), page 156.
- ◆ Configure Content Gateway integration into your firewall and control traffic through the SOCKS server. See [Configuring SOCKS firewall integration](#), page 159.
- ◆ Configure the proxy to use multiple DNS servers to match your site's security configuration. See [Using the Split DNS option](#), page 161.
- ◆ Configure Content Gateway to perform user authentication. The proxy supports Integrated Windows Authentication (with Kerberos), legacy NTLM (NTLMSSP), LDAP, and RADIUS user authentication. There is also support for multiple authentication methods with multiple authentication realms. See [Proxy user authentication](#), page 162.

### Controlling client access to the proxy

---

You can configure Content Gateway to allow only certain clients to use the proxy. To do so, you specify IP addresses and IP address ranges in **ip\_allow.config**. To deny access to specific IP addresses, do not include them in the file.

1. Navigate to the **Configure > Security > Connection Control > Proxy Access** page.
2. Click **Edit File** to open the configuration file editor for the **ip\_allow.config** file.

3. Enter information in the fields provided, and then click **Add**. The fields are described in [Configuration Options](#).
4. Click **Apply** to save the information, and then click **Close**.

**Note**

If an unauthorized client tries to access Content Gateway, a message is displayed in their browser, indicating that the requested content cannot be obtained.

---

## Controlling access to Content Gateway Manager

---

You can restrict access to Content Gateway Manager to ensure that only authenticated users can change configuration options and view performance and network traffic statistics.

You can:

- ◆ Set the master administrator ID and password. A user who logs on to Content Gateway Manager with the administrator ID has access to all Content Gateway Manager activities. See [Setting the administrator ID and password](#), page 154.
- ◆ Create and maintain a list of user accounts that determines who can log on to Content Gateway Manager and which activities they can perform. See [Creating a list of user accounts](#), page 155.
- ◆ Create an access control list of IP addresses that defines which machines can access Content Gateway Manager. See [Controlling host access to Content Gateway Manager](#), page 155.
- ◆ Use SSL for secure administration. See [Using SSL for secure administration](#), page 156.

## Setting the administrator ID and password

During installation, you assign a password that controls administrative access to Content Gateway Manager. A user who logs on to Content Gateway Manager using the correct ID and password can view all the statistics on the Monitor tab and change any configuration options on the Configure tab.

You can change the administrator ID and password at any time.

1. Navigate to the **Configure > My Proxy > UI Setup > Login tab**.
2. Make sure that **Basic Authentication** is enabled.

When Basic Authentication is disabled, any user can access Content Gateway Manager unless you have set up a list of IP addresses that are denied access (see [Controlling host access to Content Gateway Manager](#), page 155).

3. To change the current administrator ID, type a new ID in the **Login** field of the **Administrator** section.



4. To change the current password, type the current password in the Old Password field. Type the new password in the New Password field, and then retype the new password in the New Password (Retype) field.  
If you have forgotten the current administrator password, see [How do you access Content Gateway Manager if you forget the master administrator password?](#), page 424.
5. Click **Apply**.

## Creating a list of user accounts

If a single administrator ID and password for Content Gateway Manager is not sufficient security for your needs, you can create a list of user accounts that define who has access to the Content Gateway Manager and which activities they can perform.

1. Navigate to **Configure > My Proxy > UI Setup > Login**.
2. Enter the name of the user allowed to access Content Gateway Manager.
3. Enter the password for the user, and then enter the password again in the New Password (Retype) field.
4. Click **Apply**.
5. In the **Access** drop-down list of the user table, select which Content Gateway Manager activities the user can perform:
  - Select **No Access** to disable Content Gateway Manager access for the user.
  - Select **Monitor Only** to allow the user to view statistics from the Monitor tab only.
  - Select **Monitor and View Configuration** to allow the user to view statistics from the Monitor tab and to view configuration options from the Configure tab.
  - Select **Monitor and Modify Configuration** to allow the user to view statistics from the **Monitor** tab and to change configuration options from the Configure tab.
6. Click **Apply**.
7. Repeat [Step 2](#) through [Step 6](#) for each user allowed to access Content Gateway Manager.
8. Make sure that **Basic Authentication** is enabled.

Content Gateway checks user names and passwords only if this option is enabled.

## Controlling host access to Content Gateway Manager

In addition to using an administrator ID and user accounts, you can control which hosts have access to Content Gateway Manager.

1. Navigate to **Configure > My Proxy > UI Setup Access**.
2. In the Access Control area, click **Edit File** to open the configuration file editor for the **mgmt\_allow.config** file.

3. Enter information in the fields provided, and then click **Add**. All the fields are described in [UI Setup, page 252](#).
4. Click **Apply**, and then click **Close**.

## Using SSL for secure administration

Websense supports the Secure Sockets Layer protocol (SSL) to provide protection for remote administrative monitoring and configuration using Content Gateway Manager. SSL security provides authentication of both ends of a network connection using certificates and provides privacy using encryption.

To use SSL, you must:

- ◆ Obtain an SSL certificate
- ◆ Enable the Content Gateway Manager SSL option

### Obtaining an SSL certificate

You can obtain an SSL certificate from a recognized certificate authority (for example, VeriSign). Install the certificate in the Content Gateway **config** directory (**/opt/WCG/bin**). You must either rename the certificate to the default filename **private\_key.pem**, or specify the name of the certificate using Content Gateway Manager (follow the procedure in [Enabling SSL, page 156](#)).

### Enabling SSL

After you have obtained an SSL certificate, you can enable SSL.

1. Navigate to the **Configure > My Proxy > UI Setup > General** tab.
2. Enable the **HTTPS** option.
3. In the Certificate File field, specify the filename of the SSL certificate.  
You have to change the filename only if the certificate file does not use the default name **private\_key.pem**.
4. Click **Apply**.

## Filtering Rules

---

Content Gateway supports the ability to create rules that inspect requests for certain parameters and, when matched, apply a specified action. Rules can be created to:

- ◆ Deny or allow URL requests
- ◆ Allow specified applications, or requests to specified Web sites to bypass authentication
- ◆ Keep or strip header information from client requests

- ◆ Prevent specified applications from transiting the proxy



#### Note

To create rules for NTLM and LDAP authentication, see [Multiple realm authentication, page 179](#). To get started with Content Gateway authentication options, see [Proxy user authentication, page 162](#).

Filtering rules are created and modified on the **Configure > Security > Access Control > Filtering** tab. Rules are stored in the **filter.config** file.

Rules are applied in the order listed, top to bottom. Only the first match is applied. If no rule matches, the request proceeds.

Secondary specifiers are optional. More than one secondary specifier can be used in a rule. However, you cannot repeat a secondary specifier.

See [filter.config](#) for information about the structure of stored rules.

## Creating filtering rules

1. Go to the **Configure > Security > Access Control > Filtering** tab and click **Edit File** to open [filter.config](#) in the file editor.
2. Select a Rule Type from the drop down list. The Rule Type specifies the action the rule will apply. The supported options are:
  - allow** — allows particular URL requests to bypass authentication; the proxy caches and serves the requested content.
  - deny** — denies requests for objects from specific destinations. When a request is denied, the client receives an access denied message.
  - keep\_hdr** — specifies which client request header information to keep.
  - strip\_hdr** — specifies which client request header information to strip.



#### Note

The “radius” rule type is **not** supported.

3. Select a Primary Destination Type and then enter a corresponding value in the Primary Destination Value field. Primary Destination Types include:
  - dest\_domain** — a requested domain name. The value is a domain name.
  - dest\_host** — a requested hostname. The value is a hostname.
  - dest\_ip** — a requested IP address. The value is an IP address.
  - url\_regex** — a regular expression to be found in a URL. The value is a regular expression.
4. If the Primary Destination Type is **keep\_hdr** or **strip\_hdr**, select the type of information to keep or strip from the Header Type drop down list. Options include:

- **date**
- **host**
- **cookie**
- **client\_ip**

5. If the rule applies only to inbound traffic on a specific port, enter a value for **Proxy Port**.
6. Provide values for any desired **Secondary Specifiers**. They include:

**Time** — Specifies a time range, such as 08:00-14:00.

**Prefix** — Specifies a prefix in the path part of a URL.

**Suffix** — Specifies a file suffix in the URL.

**Source IP** address — Specifies a single client IP address, or an IP address range of clients.

**Port** — Specifies the port in a requested URL.

**Method** — Specifies a request URL method:

- get
- post
- put
- trace

**Scheme** — Specifies the protocol of a requested URL. Options are:

- HTTP
- HTTPS
- FTP (for FTP over HTTP only)

**User-Agent** — Specifies a request header User-Agent value. This is a regular expression (regex).

You can use the User-Agent field to create application filtering rules that:

- Allow particular applications that don't properly handle authentication challenges to bypass authentication
  - Block particular client-based applications from accessing the Internet
- See the Websense knowledge base article titled "When authentication prevents devices, browsers, and custom applications from working with the proxy" for more information and several examples.

7. When you have finished defining the rule, click **Add** to add the rule and then **Apply** to save the rule.
8. When you are done adding rules, click **Apply** to save all the changes and then click **Close** to close the edit window.

### Editing a rule:

1. Go to **Configure > Security > Access Control > Filtering** and click **Edit File** to open [filter.config](#) in the file editor.
2. In the list, select the rule to be modified and change the values as desired.
3. Click **Set** to update the rule and click **Apply** to save the rule.
4. Click **Close** to close the edit window.

---

## Configuring SOCKS firewall integration

---

SOCKS is commonly used as a network firewall that allows hosts behind a SOCKS server to gain full access to the Internet and prevents unauthorized access from the Internet to hosts inside the firewall.

When the proxy receives a request for content that is not in the cache or is stale, it must request the content from the origin server. In a SOCKS configuration, instead of accessing the origin server directly, the proxy goes through a SOCKS server. The SOCKS server authorizes communication between the proxy and the origin server and relays the data to the origin server. The origin server then sends the content back to the proxy through the SOCKS server.

The proxy caches the content and sends it to the client.

Content Gateway can act as a SOCKS client, where it receives and serves HTTP or FTP requests as usual. It can also act as a SOCKS proxy, relaying requests to and from the SOCKS server (usually on port 1080). Content Gateway cannot and does not act as a SOCKS server.



---

### Note

Content Gateway does not perform authentication with the client. However, Content Gateway can perform user name and password authentication with a SOCKS server running SOCKS version 5.

---

## Configuring the proxy to use a SOCKS firewall

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the Features table, click **SOCKS On** in the Security section.
3. Click **Apply**.
4. Navigate to **Configure > Security > SOCKS > General**.
5. Specify the SOCKS version running on your SOCKS servers.
6. Click **Apply**.
7. Click the **Server** tab.
8. In the Default Servers field of the SOCKS Server section, enter the host names of your default SOCKS servers and the ports through which the proxy communicates with the SOCKS servers. Separate the hostname and the port with a colon (:) and separate each entry with a semicolon (;). For example:  

```
socks1:1080;socks2:4080
```
9. Click **Apply**.
10. In the SOCKS Server Rules area, click **Edit File** to perform additional SOCKS server configuration, such as SOCKS server bypass and authentication.

The configuration file editor for the **socks.config** file opens.

11. Enter information in the fields provided, and then click **Add**. All the fields are described in [Configuration Options](#).
12. Click **Apply**, and then click **Close**.
13. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Setting SOCKS proxy options

To configure Content Gateway as a SOCKS proxy, you must enable the SOCKS proxy option and specify the port on which Content Gateway accepts SOCKS traffic from SOCKS clients.

As a SOCKS proxy, Content Gateway can receive SOCKS packets (usually on port 1080) from the client and forwards all requests directly to the SOCKS server.



### Note

You must set SOCKS proxy options in addition to enabling the SOCKS option and specifying SOCKS server information described in [Configuring the proxy to use a SOCKS firewall](#), page 159.

1. Navigate to **Configure > Security > SOCKS > Proxy**.
2. Enable **SOCKS Proxy**.
3. Specify the port on which Content Gateway accepts SOCKS traffic. The default is port 1080.
4. Click **Apply**.
5. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Setting authentication

---

For SOCKS version 5, you can configure the proxy to use username and password authentication with the SOCKS server. You specify the username and password the proxy must use in the **socks.config** file.

1. Navigate to **Configure > Security > SOCKS > Server** to display the **socks.config** file.
2. At the end of the file, add a line using the following format:  

```
auth u username password
```

*username* is the username and *password* is the password Content Gateway must use for authentication with the SOCKS version 5 server.
3. Click **Apply**.
4. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Setting SOCKS server bypass

You can configure Content Gateway to bypass the SOCKS server and access certain origin servers directly (SOCKS Server bypass).

1. Navigate to **Configure > Security > SOCKS > Server** to display the **socks.config** file.
2. Enter a line in the file specifying the IP addresses or IP address range of the origin servers that you want Content Gateway to access directly. Use the following format:

```
no_socks IPaddresses or IPaddress range
```

*IPaddresses* or *IPaddress range* is a comma-separated list of the IP addresses or IP address ranges associated with the origin servers you want Content Gateway to access directly.

Never specify the all networks broadcast address: 255.255.255.255.

3. Click **Apply**
4. Click **Restart** on **Configure > My Proxy > Basic > General**.

### Example

To configure Content Gateway to access the origin servers associated with the range of IP addresses 123.14.15.1 - 123.14.17.4 and the IP address 113.14.18.2 directly without going through the SOCKS server.

```
no_socks 123.14.15.1 - 123.14.17.4, 113.14.18.2
```

## Using the Split DNS option

You can configure Content Gateway to use multiple DNS servers, depending on your security requirements. For example, you can configure Content Gateway to look to one set of DNS servers to resolve host names on your internal network, while allowing DNS servers outside the firewall to resolve hosts on the Internet. This maintains the security of your intranet, while continuing to provide direct access to sites outside your organization.

To configure Split DNS, you must perform the following tasks:

- ◆ Specify the rules for performing DNS server selection based on the destination domain, the destination host, or a URL regular expression.
- ◆ Enable the Split DNS option.

In Content Gateway Manager:

1. Go to the **Configure > Networking > DNS Resolver > Split DNS** tab.
2. Enable the **Split DNS** option.

3. In the **Default Domain** field, enter the default domain for split DNS requests. Content Gateway appends this value automatically to a host name that does not include a domain before determining which DNS server to use.
4. In the **DNS Servers Specification** area, click **Edit File** to open the configuration file editor for the [splitdns.config](#) file.
5. Enter information in the fields provided, and then click **Add**. All the fields are described in [splitdns.config](#).
6. Click **Apply**, and then click **Close**.
7. On the **Split DNS** tab, click **Apply** to save your configuration.
8. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Proxy user authentication

---

Related topics:

[Browser limitations](#), page 164  
[Transparent proxy authentication settings](#), page 165  
[Integrated Windows Authentication](#), page 166  
[Legacy NTLM authentication](#), page 171  
[LDAP authentication](#), page 173  
[RADIUS authentication](#), page 176  
[Multiple realm authentication](#), page 179

Content Gateway supports several methods of authenticating users before they are allowed access to content. These methods can be used together with Websense Web Security user identification agents to provide failover should proxy user authentication become unavailable. For an overview of user authentication options and best practices, go to the [Websense Technical Library](#) and search for *Web Security Gateway authentication and identification*.

In both explicit and transparent proxy modes, Content Gateway supports user authentication with:

- ◆ [Integrated Windows Authentication](#), page 166 (with Kerberos)
- ◆ [Legacy NTLM authentication](#), page 171 (NTLMSSP)
- ◆ [LDAP authentication](#), page 173
- ◆ [RADIUS authentication](#), page 176

In addition, Content Gateway supports [Multiple realm authentication](#), page 179, to authenticate:

- ◆ Distinct sets of IP addresses against specific domains
- ◆ Traffic on specific ports against specific domains (explicit proxy only)



- ◆ Combinations of the above (explicit proxy only)

For each realm (definition below), an authentication method (Integrated Windows Authentication, NTLM, or LDAP) is specified. Using this feature, multiple methods can be used to authenticate users in multiple realms.

### Terms in the context of multiple realm authentication

- ◆ A **domain** is a Windows Active Directory domain.
- ◆ A **realm** is a Windows Active Directory domain that does not have an outbound trust relationship with other domains. It therefore requires that its members be authenticated by a domain controller within the domain.

### Selecting the authentication mode

The authentication mode is selected in Content Gateway Manager in the **Authentication** section of the **Configure > My Proxy > Basic** page. Configuring authentication for multiple realm environments begins with selecting the **Multiple Realm Authentication** option.

### Supported domain controllers and directories

- ◆ Windows NT domain controllers
- ◆ Windows 2003 and 2008 Active Directory
- ◆ Novell eDirectory 8.7 and 8.8 (LDAP only)
- ◆ Oracle DSEE 11g, Sun Java 7 and 6.2 (LDAP only)

### Best practices when using Windows Active Directory

If you have one Active Directory domain, or if all of your Active Directory domains share inbound and outbound trust relationships, the best option is to use Integrated Windows Authentication.

If you have multiple realms and authentication is a requirement, you must use the multiple realm option. For details, including a discussion of policy application limits, see [Multiple realm authentication](#), page 179.

If user identification is sufficient, you can use one of the Web Security user identification options. See the section titled *User Identification* in TRITON -- Web Security Help.

### Transparent user authentication

Content Gateway supports both transparent (Single Sign-On) and interactive (prompted) authentication. Transparent authentication is supported with Integrated Windows Authentication and Legacy NTLM. Some browsers provide only limited support. See [Browser limitations](#), page 164.

On Windows networks, Single Sign-On allows users to sign on only once so that they can transparently access all authorized network resources. Therefore, if a user has already logged on to the Windows network successfully, the credentials specified

during Windows logon are used for proxy authentication and the user is not prompted again for a username and password.

Interactive authentication is supported in networks that are not configured for Single Sign-On and for use with browsers that don't support Single Sign-On. With interactive authentication, users are prompted for credentials before they can access content through Content Gateway.

### **Backup domain controllers**

For Integrated Windows Authentication and Legacy NTLM, Content Gateway supports the specification of backup domain controllers for failover. If the primary domain controller does not respond to proxy requests, Content Gateway contacts the next domain controller in the list (the backup domain controller). For the next request, the proxy tries to contact the primary domain controller again and then contacts the backup domain controller if the connection fails.

## **Browser limitations**

**Not all Web browsers fully support transparent authentication (no-prompt).**

### **Internet Explorer 7, 8 and 9**

- ◆ Full support of transparent authentication

### **Mozilla Firefox 3 and 4**

- ◆ Full support of transparent authentication

### **Google Chrome 6, 7, 8, 9, 10**

- ◆ Transparent authentication supported with IWA
- ◆ Transparent authentication **not** supported with Legacy NTLM; always challenges user for credentials

### **Opera 10**

- ◆ Transparent authentication **not** supported; always challenges user for credentials
- ◆ HTTPS with IWA not supported.

### **Windows Safari 4, 5, and Safari on iPad iOS4**

- ◆ Transparent authentication **not** supported; always challenges user for credentials
- ◆ HTTPS with IWA partially supported. The entire page does not always display.



#### **Note**

When prompted for credentials, if the user does not enter a domain name, a “session timeout” error can result, or the user may be re-prompted.

---

## Transparent proxy authentication settings

When Content Gateway is a transparent proxy that also performs user authentication, several special authentication-related configuration options should be set. In Content Gateway Manager, go to the **Configuration > Security > Access Control > Transparent Proxy Authentication** tab.

- ◆ **Redirect Hostname** (optional) — specifies an alternate hostname for the proxy. Redirect Hostname is not needed and is not used by Integrated Windows Authentication (IWA).

By default, authenticating clients are redirected to the hostname of the Content Gateway machine. If clients are unable to resolve that hostname through DNS, or if an alternate DNS name for the proxy is defined, that hostname can be specified in the **Redirect Hostname** field.



### Note

In order to ensure that the authentication for transparent proxy users occurs transparently (i.e., without prompting the user for credentials), the browser must be configured so that the Redirect Hostname is in its **Intranet Zone**. Typically, this is achieved by ensuring that the Redirect Hostname is in the same domain as the computer on which the browser is running. For example, if the client is **workstation.example.com** and the Redirect Hostname is **proxyhostname.example.com**, the browser will allow authentication to occur transparently, without prompting the user. Consult your browser documentation.

- ◆ **Authentication Mode** — specifies the transparent authentication mode. Content Gateway must be set to one of the following modes:
  - **IP mode:** In IP mode (the default), the client IP address is associated with a username when the session is authenticated. Requests made from that IP address are not authenticated again until the **Session TTL** expires (Session Time-To-Live; default = 15 minutes). Requests made from that IP address within the time-to-live are considered to be made by the user associated with that IP address.
  - **Cookie Mode:** Cookie mode is used to uniquely identify users who share a single IP address, such as in a terminal server environments, in proxy chaining environments, or where network address translation (NAT) occurs.
- ◆ **Session TTL** — Once the user's session is authenticated, the session is valid for the duration of time specified in **Session TTL** (Time-To-Live; default = 15 minutes). The supported range of values is 5-65535 minutes.

Whenever changes are made to any of these fields, click **Apply** to save your changes and then restart the proxy to put the changes into effect.

**Note**

Content Gateway supports transparent authentication in proxy clusters using WCCP load balancing. However, the assignment method distribution attribute must be the source IP. For more information see [WCCP load distribution](#), page 48.

## Integrated Windows Authentication

Integrated Windows Authentication (IWA) provides a very secure and robust method of authenticating users who all belong to shared-trust, Windows domains (one or many).

Integrated Windows Authentication:

- ◆ Uses Kerberos
- ◆ Supports Windows Active Directory 2003 and 2008
- ◆ Supports NTLM in both explicit and transparent proxy modes
- ◆ Supports NTLMv2 with Session Security and NTLMv1 with Session Security
- ◆ Supports Internet Explorer 7, 8, and 9, Firefox 3 and 4, Google Chrome 6, 7, 8, 9, and 10, Windows Safari 4 and 5, Safari 4 on iPad iOS4, and Opera 10
- ◆ Supports UTF-8 user names
- ◆ Supports fall back to interactive authentication (prompted)
- ◆ Can be used with the Multiple Realm Authentication option
- ◆ Requires that clients be joined to the trusted domain
- ◆ Requires that client browsers specify the Fully Qualified Domain Name (FQDN) of Content Gateway as an intranet site or trusted site
- ◆ In explicit proxy deployments, browsers must specify the FQDN of Content Gateway

### Integrated Windows Authentication: Configuration summary

Follow these steps to configure Integrated Windows Authentication (IWA):

- ◆ In Content Gateway Manager, enable IWA on the **Configure > My Proxy > Basic** page. Click **Apply**.
- ◆ Join Content Gateway to the Windows domain. See [Configuring Integrated Windows Authentication](#) for a list of required conditions.
- ◆ If Content Gateway is a transparent proxy, configure [Transparent proxy authentication settings](#).
- ◆ Configure the **Global Authentication Options**. These options apply to NTLM authentication when IWA negotiates NTLM or falls back to NTLM.

## Configuring Integrated Windows Authentication

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the **Authentication** section, click Integrated Windows Authentication **On**, and click **Apply**.
3. In the **Authentication** section, click the **Configure** link to navigate to **Configure > Security > Access Control**.
4. Join the Windows domain.

To join the domain:

- Content Gateway must be able to resolve the domain name.
- Content Gateway system time must be synchronized with the domain controller's time, plus or minus 1 minute.
- The correct domain Administrator name and password must be specified.
- There must be TCP/UDP connectivity to the domain controller(s) (ports 88, 389, 445).
- If backup domain controllers are configured, they and their Kerberos Distribution Center (KDC) services must be reachable by Content Gateway on the network.



### Important

All clients must be joined to the domain.

Browsers and other proxy clients must be configured to specify the FQDN of Content Gateway as an intranet site or trusted site.

- a. In the **Domain Name** field, enter the fully qualified domain name.
- b. In the **Administrator Name** field enter the Windows Administrator user name.
- c. In the **Administrator Password** field enter the Windows Administrator password.

The name and password are used only during the join and are not stored.

- d. Select how to locate the domain controller:
    - **Auto-detect using DNS**
    - **DC name or IP address**
- If the domain controller is specified by name or IP address, you can also specify backup domain controllers in a comma separated list, no spaces.

- e. In the **Content Gateway Hostname** field, confirm that the hostname is the correct hostname and that it is no more than 15 characters (no more than 11 characters on V-Series appliances). If it is longer, it must be shortened if IWA is to be used. The length restriction results from the 15 character limit on NetBIOS hostnames.

**Warning**

The hostname should not be changed after the domain is joined. If it is changed, IWA will immediately stop working and will not work again until the domain is unjoined and then re-joined with the new hostname.

---

- f. Click **Join Domain**. If there is an error, ensure that the conditions outlined above are met and then see [Failure to join the domain](#).
5. If Content Gateway is deployed as a transparent proxy, configure the [Transparent proxy authentication settings](#) and then continue with the next step.
6. Configure the NTLM global settings. Navigate to the **Configure > Security > Access Control > Global Authentication Options** tab.

**Note**

These settings apply when IWA negotiates NTLM or falls back to NTLM.

---

- a. **Fail Open** is enabled by default. Fail Open allows requests to proceed when authentication fails due to:
  - No response from the domain controller
  - Malformed messages from the client
  - Invalid SMB responses

With Fail Open, when Web filtering is used with the proxy and an XID agent is configured, if IWA authentication fails the requester can still be identified by the XID agent and appropriate policy applied.

Disable Fail Open if you want to stop requests from proceeding to the Internet when the above listed authentication failure conditions occur.
- b. **Credential Caching** is enabled by default. Credential caching applies only when Content Gateway is deployed as an explicit proxy. Credentials are cached only when authentication is successful. To disable credential caching, select **Disable**.
- c. **Caching TTL** sets the time-to-live for entries in the credential cache. The default TTL is 900 seconds (15 minutes). To change the TTL, enter a new value in the entry field. The range of supported values is 300 to 86400 seconds.
- d. If some users use terminal servers to access the Internet through the proxy (e.g., Citrix servers), you must create a list of those servers in the **Multi-user IP Exclusions** field. Credentials for such users are not cached. Enter a comma separated list of IP addresses and IP address ranges.

Configuration is now complete. Restart Content Gateway and run some test traffic through the proxy to verify that authentication is working as expected. If there is a problem, see [Troubleshooting Integrated Windows Authentication](#).

### To unjoin the current domain and join a new domain

1. Navigate to the **Configure > Security > Access Control > Integrated Windows Authentication** tab and click **Unjoin**.
2. To join a new domain, in the **Domain Name** field, enter the fully qualified domain name.
3. In the **Administrator Name** field enter the Windows Administrator user name.
4. In the **Administrator Password** field enter the Windows Administrator password. The name and password are used only during the join and are not stored.
5. Select how to locate the domain controller:
  - **Auto-detect using DNS**
  - **DC name or IP address**

If the domain controller is specified by name or IP address, you can also specify backup domain controllers in a comma separated list, no spaces.
6. Click **Join Domain**.

### To change the way the domain controller is found

1. Navigate to the **Configure > Security > Access Control > Integrated Windows Authentication** tab.
2. In the **Domain Controller** section, select how to locate the domain controller:
  - **Auto-detect using DNS**
  - **DC name or IP address**

If the domain controller is specified by name or IP address, you can also specify backup domain controllers in a comma separated list, no spaces.
3. Click **Apply**.

## Troubleshooting Integrated Windows Authentication

This section covers 2 common problems:

- ◆ [Failure to join the domain](#)
- ◆ [Failure to authenticate clients](#)

### Failure to join the domain

These conditions are required for Content Gateway to join a domain:

- ◆ Content Gateway must be able to resolve the domain name.
- ◆ Content Gateway system time must be synchronized with the domain controller's time, plus or minus 1 minute.
- ◆ The correct domain Administrator name and password must be specified.

- ◆ There must be TCP/UDP connectivity to the domain controller(s) (ports 88, 389, 445).
- ◆ If backup domain controllers are configured, they and their Kerberos Distribution Center (KDC) services, must be reachable by Content Gateway on the network.

**Troubleshooting:**

- ◆ Errors encountered in the join action are reported at the top of the screen (the Integrated Windows Authentication tab).
- ◆ The error message usually includes a link to the failure log where you can get more details.
- ◆ Join failures are logged to **/opt/WCG/logs/smbadmin.join.log**
- ◆ In most cases, the failure message in the log is a standard Samba and Kerberos error message that is easily found with an Internet search.

**Failure to authenticate clients**

These conditions are required to authenticate clients:

- ◆ Content Gateway clients must be a member of the same domain as that joined by Content Gateway.
- ◆ Client system time must be in sync with the domain controller and Content Gateway to plus or minus 1 minute.
- ◆ Explicit proxy clients must **not** be configured to send requests to the IP address of Content Gateway. Clients must use the Fully Qualified Domain Name (FQDN) of Content Gateway. If the IP address is used, NTLM authentication is always performed.
- ◆ The Content Gateway FQDN must be in DNS and resolvable by all proxy clients.
- ◆ Browsers and proxy clients must specify the FQDN of Content Gateway as an intranet site or trusted site.

**Troubleshooting:**

In Content Gateway Manager, use the **Diagnostic Test** function on the **Monitor > Security > Integrated Windows Authentication** tab. This Monitor page displays authentication request statistics and provides the diagnostic test function.

The **Diagnostic Test** function performs connectivity and authentication testing and reports errors. It also shows domain controller TCP port connectivity and latency.

Errors and messages are logged to:

- ◆ /var/log/messages
- ◆ content\_gateway.out
- ◆ /opt/WCG/logs/smbadmin.log
- ◆ /opt/WCG/logs/smbadmin.join.log

**Performance issues:**



- ◆ **IWA (Kerberos):** Authentication performance is bound by CPU. There is no communication to the domain controllers for Kerberos authentication.
- ◆ **NTLM and Basic:** Domain controller responsiveness effects performance. The **Monitor > Security > Integrated Windows Authentication** page shows average response time.

## Legacy NTLM authentication

Content Gateway supports the NTLM (NT LAN Manager) authentication protocol as a method of ensuring that users in a Windows network are authenticated before they access the Internet.



### Important

This implementation of NTLM support (Legacy NTLM) relies solely on the NTLMSSP protocol. Although it performs reliably as documented in this section, it is highly recommended that the [Integrated Windows Authentication](#) mode be used instead. It provides more robust and secure support for NTLM.

When the Legacy NTLM option is enabled, the proxy challenges users who request content for proof of their credentials. The proxy then sends the proof of the user's credentials directly to the Windows domain controller to be validated. If the credentials are valid, the proxy serves the requested content and stores the credentials in the NTLM cache for future use. If the credentials are not valid, the proxy sends an *authentication failed* message.

### Restrictions:

1. **WINS resolution** is not supported. Domain controllers must have host names that can be resolved by a DNS server.
2. **Extended security** is not supported and cannot be enabled on the domain controller.
3. **NTLM2 session security** is not supported and cannot be enabled on clients. In the Security Settings area of the Windows operating system, inspect the **Network Security: Minimum session security** settings.
4. **NTLMv2** is not supported with Active Directory 2008. The required **Network Security: LAN Manager Authentication** setting is described in step 5 of *Configuring NTLM proxy authentication*, below.
5. Not all browsers support transparent NTLM authentication. See [Browser limitations](#), page 164.
6. NTLM credential caching is performed when authentication is successful in explicit mode. Transparent proxy authentication caching is handled separately and is configured on the **Configuration > Security > Access Control > Transparent Proxy Authentication** tab.

## Configuring Legacy NTLM authentication

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the Authentication section, click **Legacy NTLM On**, and click **Apply**.
3. Navigate to **Configure > Security > Access Control > Legacy NTLM**.
4. In the **Domain Controller Hostnames** field, enter the hostname of the primary domain controller, followed, optionally, by a comma separated list of backup domain controllers. The format of the hostname must be:

```
host_name[:port] [%netbios_name]
```

or

```
IP_address[:port] [%netbios_name]
```



### Note

If you are using Active Directory 2008, you must include the netbios\_name or use SMB port 445. If you **do not** use port 445, you must ensure that the Windows Network File Sharing service is running on the Active Directory server. See your Windows Server 2008 documentation for details.

---



### Note

If you are using Active Directory 2008, in the Windows **Network Security** configuration, **LAN Manager Authentication level** must be set to **Send NTLM response only**. See your Windows Server 2008 documentation for details.

---

5. Enable **Load Balancing** if you want the proxy to balance the load when sending authentication requests to multiple domain controllers.



### Note

When multiple domain controllers are specified, even if load balancing is disabled, when the load on the primary domain controller reaches the maximum number of connections allowed, new requests are sent to a secondary domain controller as a short-term failover provision, until such time that the primary domain controller can accept new connections.

---

6. **Fail Open** is enabled by default. Fail Open allows requests to proceed when authentication fails due to:
  - No response from the domain controller
  - Malformed messages from the client
  - Invalid SMB responses

With Fail Open, when Web filtering is used with the proxy and an XID agent is configured, if NTLM authentication fails the requester can still be identified by the XID agent and appropriate policy applied.

Disable Fail Open if you want to stop requests from proceeding to the Internet when the above listed authentication failure conditions occur.

7. **Credential Caching** is enabled by default. Credential caching applies only when Content Gateway is deployed as an explicit proxy. Credentials are cached only when authentication is successful. To disable credential caching, select **Disable**.
8. **Caching TTL** sets the time-to-live from entries in the credential cache. The default TTL is 900 seconds (15 minutes). To change the TTL, enter a new value in the entry field. The range of supported values is 300 to 86400 seconds.
9. If some users use terminal servers to access the Internet through the proxy (e.g., Citrix servers), you must create a list of those servers in the **Multi-user IP Exclusions** field. Credentials for such users are not cached. Enter a comma separated list of IP addresses and IP address ranges.
10. Click **Apply**.
11. Click **Restart** on **Configure > My Proxy > Basic > General**.

Optionally, you can also:

- ◆ Configure Content Gateway to allow certain clients to access specific sites on the Internet without being authenticated by the NTLM server; See [Access Control, page 276](#).
- ◆ Configure an alternate Content Gateway hostname for authentication, set the Authentication Mode (IP Mode or Cookie Mode), and set the session time-to-live period; See [Transparent proxy authentication settings, page 165](#).

## LDAP authentication

Content Gateway supports the LDAP option to ensure that users are authenticated with an LDAP server before accessing content through the proxy.



### Important

In environments with multiple realms (domains that do not share trust relationships), configure LDAP authentication through the [Multiple realm authentication](#) option.

When the LDAP option is enabled, the proxy acts as an LDAP client and directly challenges users who request content for a username and password. After receiving the username and password, the proxy contacts the LDAP server to check that the credentials are correct. If the LDAP server accepts the username and password, the proxy serves the client with the requested content and stores the username and password in the Content Gateway LDAP cache; all future authentication requests for that user are served from the LDAP cache until the cache entry expires. If the LDAP server rejects the username and password, the user's browser displays a message indicating that authorization failed and prompts again for a username and password.

LDAP authentication supports both simple and anonymous bind.

## Configuring Content Gateway to be an LDAP client

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the Authentication section, click **LDAP On**, and then click **Apply**.
3. Navigate to **Configure > Security > Access Control > LDAP**.
4. Enable **Purge Cache on Authentication Failure** to configure the proxy to delete the authorization entry for the client from LDAP cache if authorization fails.
5. Enter the hostname of the LDAP server.
6. Enter the port on which Content Gateway communicates with the LDAP server. The default is port 389.



### Note

When the LDAP directory service is Active Directory, requests from users located outside the global catalog's base domain will fail to authenticate. This is because the default port for LDAP is 389 and requests sent to 389 search for objects only within the global catalog's base domain. To authenticate users from outside the base domain, change the LDAP port to 3268. Requests sent to 3268 search for objects in the entire forest.

7. Enable Secure LDAP if you want the proxy to use secure communication with the LDAP server. Secure communication is performed on port 636 or 3269. Change the port value in the previous field, if necessary.
8. Select the type of your directory service to set the filter for searching. The default is **sAMAccountName** for Active Directory. Select **uid** for eDirectory or other directory services.
9. Enter the Full Distinguished Name (fully qualified name) of a user in the LDAP-based directory service. For example:  
`CN=John Smith, CN=USERS, DC=MYCOMPANY, DC=COM`  
Enter a maximum of 128 characters in this field.  
If no value is specified for this field, the proxy attempts to bind anonymously.
10. Enter a password for the user specified in the previous step.
11. Enter the Base Distinguished Name (DN). Obtain this value from your LDAP administrator.
12. Click **Apply**.
13. Click **Restart** on **Configure > My Proxy > Basic > General**.

As optional steps, you can:

- ◆ Change LDAP cache options. See [Setting LDAP cache options](#), page 175.
- ◆ Configure Content Gateway to allow certain clients to access specific sites on the Internet without being authenticated by the LDAP server. See [Access Control](#), page 276).

- ◆ Configure an alternate Content Gateway hostname for authentication, set the Authentication Mode (IP Mode or Cookie Mode), and set the session time-to-live period. See [Transparent proxy authentication settings](#), page 165.

## Setting LDAP cache options

By default, the LDAP cache is configured to store 5000 entries and each entry is considered fresh for 3000 minutes. Change these options by editing the **records.config** file.

1. Open the **records.config** file located in the Content Gateway **config** directory (**/opt/WCG/config**).
2. Edit the following variables:

Variable	Description
<code>proxy.config.ldap.cache.size</code>	Specify the number of entries allowed in the LDAP cache. The default value is 5000. The minimum value is 256.
<code>proxy.config.ldap.auth.ttl_value</code>	Specify the number of minutes that Content Gateway can store username and password entries in the LDAP cache.
<code>proxy.config.ldap.cache.storage_size</code>	Specify the maximum amount of space (in bytes) that the LDAP cache can occupy on disk.  When modifying this value, you must update the value of <b>proxy.config.ldap.cache.size</b> proportionally. For example, if you double the storage size, also double the cache size.  Modifying this variable without modifying <b>proxy.config.ldap.cache.size</b> causes the LDAP subsystem to stop functioning.

3. Save and close the file.
4. From the Content Gateway **bin** directory (**/opt/WCG/bin**), run **content\_line -L** to restart the proxy on the local node or **content\_line -M** to restart the proxy on all the nodes in a cluster.

## Configuring secure LDAP

By default, LDAP traffic is transmitted unsecured. You can make LDAP traffic confidential and secure by using Secure Sockets Layer (SSL) / Transport Layer Security (TLS) technology. You can enable LDAP over SSL (LDAPS) by installing a

properly formatted certificate from either a Microsoft certification authority (CA) or a non-Microsoft CA.

To use LDAPS with Content Gateway:

1. Open the **records.config** file located in the Content Gateway **config** directory (**/opt/WCG/config**).
2. Add following entry to **records.config**:  
`CONFIG proxy.config.ldap.secure.bind.enabled INT 1`
3. Navigate to **Configure > Security > Access Control > LDAP** and change the port to 3269.

**Note**

The Directory Service must be configured to support LDAPS authentication. Please refer to the documentation provided by your directory provider for instructions.

---

## RADIUS authentication

Content Gateway supports the RADIUS option to ensure that users are authenticated with a RADIUS server before accessing content through the proxy.

When the RADIUS option is enabled, Content Gateway acts as a RADIUS client and directly challenges users who request content for a username and password. After receiving the username and password, Content Gateway contacts the RADIUS server to check that the credentials are correct. If the RADIUS server accepts the username and password, the proxy serves the client with the requested content and stores the username and password entry in the RADIUS cache; all future authentication requests for that user are served from the RADIUS cache until the entry expires. If the RADIUS server rejects the username and password, the user's browser displays a message indicating that authorization failed and prompts again for a username and password.

Content Gateway supports a primary RADIUS server and a secondary RADIUS server for failover. If the primary server does not respond to the proxy request within the specified timeout (60 seconds by default), Content Gateway tries to check the username and password again. If a response from the primary RADIUS server is not received after the maximum number of retries (10 by default), the proxy contacts the secondary RADIUS server. If Content Gateway cannot contact the secondary RADIUS server, the user is prompted again for a username and password.

The RADIUS cache is held in memory and stored on disk. Content Gateway updates the data on disk every 60 seconds. In addition, Content Gateway stores username and password entries in the RADIUS cache for 60 minutes. If a password and username entry is expired in the RADIUS cache, Content Gateway contacts the RADIUS server to accept or reject the username and password.

To configure Content Gateway to be a RADIUS client:

- ◆ Enable the RADIUS option.
- ◆ Specify the hostname or IP address of the primary and secondary (optional) RADIUS servers, and the port and shared key that Content Gateway uses to communicate with the RADIUS servers.

See [Configuring Content Gateway to be a RADIUS client](#), page 177.

## Configuring Content Gateway to be a RADIUS client

1. Navigate to **Configure > My Proxy > Basic > General**.
2. In the Authentication section, click Radius **On**, and then click **Apply**.
3. Navigate to **Configure > Security > Access Control > Radius**.
4. Enter the hostname of your primary RADIUS server.
5. Enter the port number through which Content Gateway communicates with the primary RADIUS server.
6. Enter the key used for encoding.
7. If you are using a secondary RADIUS server, enter the hostname, port, and shared key in the appropriate fields of the **Secondary Radius Server (Optional)** area.
8. Click **Apply**.
9. Click **Restart** on **Configure > My Proxy > Basic > General**.



### Note

In addition to performing these procedures, you must add the Content Gateway machine as a trusted client on the primary and secondary RADIUS servers and provide the shared key you want to use for the Content Gateway machine (the shared key must be the same one you specify in the procedure below). See your RADIUS server documentation.

## Setting RADIUS cache and server timeout options

By default, the RADIUS cache and RADIUS server timeout options are configured as follows:

- ◆ The RADIUS cache is configured to store 1,000 entries and each entry is considered fresh for 60 minutes.
- ◆ Content Gateway can try to re-establish a connection to the RADIUS server if the connection remains idle for 10 seconds and can retry the connection a maximum of 10 times.

Change these default values by editing the **records.config** file.

1. Open the **records.config** file located in the Content Gateway **config** directory (**/opt/WCG/config**).

## 2. Edit the following variables:

Variable	Description
<code>proxy.config.radius.auth.min_timeout</code>	Specify the amount of time in seconds that the Content Gateway connection to the RADIUS server remains idle before Content Gateway closes the connection.
<code>proxy.config.radius.auth.max_retries</code>	Specify the maximum number of times Content Gateway tries to connect to the RADIUS server.
<code>proxy.config.radius.cache.size</code>	Specify the number of entries allowed in the RADIUS cache.  The minimum value is 256 entries. If you enter a value lower than 256, Content Gateway signals a SEGV.
<code>proxy.config.radius.auth.ttl_value</code>	Specify the number of minutes that Content Gateway can store username and password entries in the RADIUS cache.
<code>proxy.config.radius.cache.storage_size</code>	Specify the maximum amount of space that the RADIUS cache can occupy on disk.  This value must be at least 100 times the number of entries. It is recommended that you provide the maximum amount of disk space possible.

3. Save and close the file.
4. From the Content Gateway **bin** directory (`/opt/WCG/bin`), run **content\_line -L** to restart Content Gateway on the local node or **content\_line -M** to restart WCG on all the nodes in a cluster.



## Multiple realm authentication

### Related topics:

[Transparent proxy authentication settings](#), page 165

[Global authentication options](#), page 183

[Multiple realm authentication: Domains](#), page 182

[Creating an Integrated Windows Authentication realm rule](#), page 184

[Creating an LDAP authentication realm rule](#), page 186

[Working with authentication realm rules](#), page 188

[Multiple Realm Authentication use cases](#), page 189

[Troubleshooting Multiple Realm Authentication](#), page 191

Multiple realm authentication is for environments that have multiple domains that are essentially isolated for the purposes of user authentication by a lack of mutual inbound and outbound trust relationships. Therefore, users in these domains must be authenticated by a domain controller within their domain. With respect to this feature, these domains are called **realms**.



### Note

If all of the users in your network can be authenticated by domain controllers that share trust relationships, you don't need to create rules for multiple authentication realms. In this case the best practice is to use the authentication method that is best suited to your directory service.

Multiple realm authentication allows distinct authentication rules to be written for each domain, thereby supporting the use of multiple authentication methods (IWA, legacy NTLM, LDAP) at the same time. For example, RealmA might be an Active Directory domain for which you want to authenticate users with Integrated Windows Authentication. RealmB might be an LDAP domain for which you must authenticate users with LDAP. This is easy to accomplish with multiple realm authentication. For 3 hypothetical scenarios, see [Multiple Realm Authentication use cases](#), page 189.

In explicit proxy environments, authentication rules can be written for traffic inbound on specific ports. This allows for authentication rules that specify the proxy port, source IP addresses, authentication method, and realm.



---

**Important**

In a multiple realm environment, Content Gateway may authenticate users that Web Security does not know about (are outside User Services primary domain). In these cases, Content Gateway can be configured to send an “alias” user name that Web Security knows about. Or, to apply the default policy, send no name. This selection is made in the Advanced Options of each rule you define.

For a more detailed description, see [Unknown users and the ‘alias’ option](#), below.

---

## How does support for multiple realm authentication work?

In networks with multiple realms, rules are defined to direct sets of IP addresses, or traffic on specific ports, to distinct domain controllers. These rules are defined on the **Configure > Security > Access Control > Authentication Realms** tab. Rules are stored in the [auth.config](#) file.

- ◆ Multiple realm authentication rules can be defined for IWA, Legacy NTLM, and LDAP sources.
- ◆ One or more authentication rule can be defined for each realm.
- ◆ The specifiers used in each realm rule type (IWA, legacy NTLM, LDAP) differ.
- ◆ **Rules are applied from the list top down; the first match is applied. If the IP address is not matched by any rule, no authentication is attempted.**
- ◆ Transactions are logged with the name used by Filtering Service.
- ◆ Proxy authentication statistics are collected and reported discreetly for each authentication method. See [Security, page 225](#) (in the Statistics section).



---

**Important**

Content Gateway must be configured with a DNS server that can resolve the fully qualified domain name (FQDN) of Content Gateway for every realm used by Integrated Windows Authentication. If this isn’t done, IWA rules fail to work. How to configure the DNS server is up to the network administrator. One option is to configure a DNS transfer zone (Sub Zone) between the primary DNS server of Content Gateway and the DNS server of each authentication realm.

---

## Unknown users and the ‘alias’ option

In multiple realm environments, it’s possible for Content Gateway to authenticate a user who, when passed to Web Security, is not recognized because the name is not in the User Services directory. When an authenticated user name is passed to Web Security but not matched, the default policy is applied. There are several ways to address this:

- ◆ Change the Web Security User Services configuration to see and add the names to its directory.
- ◆ Add the unrecognized names to Web Security’s primary domain. The names must match exactly. Define policies for the new names.
- ◆ For users who match a particular realm rule, pass an alias name and add the alias name to Web Security’s primary domain. The names must match exactly. Define a policy for the alias name.
- ◆ If the existing Web Security default policy is sufficient, do nothing, or for every user who matches a particular realm rule, in the realm rule select to use a blank (empty) alias.

For some illustrative use cases, see [Multiple Realm Authentication use cases](#).

## Multiple realm authentication configuration summary

- ◆ Join all of the Windows domains to be used with Integrated Windows Authentication rules (domains can be added or removed later, but rules cannot be created for a domain that is not joined). See [Multiple realm authentication: Domains, page 182](#).
- ◆ If Content Gateway is an explicit proxy and you want to bring in traffic on multiple ports, specify the ports on the **Configure > Protocol > HTTP** tab.



### Note

- ◆ You must also configure your clients to use the correct port.

- ◆ If Content Gateway is a transparent proxy, make [Transparent proxy authentication settings, page 165](#)
- ◆ Configure the [Global authentication options, page 183](#)
- ◆ Create authentication rules
  - [Creating an Integrated Windows Authentication realm rule, page 184](#)
  - [Creating a legacy NTLM authentication realm rule, page 185](#)
  - [Creating an LDAP authentication realm rule, page 186](#)

## Multiple realm authentication: Domains

Before you can create an Integrated Windows Authentication realm rule, you must join each realm's domain.



---

### Important

All clients to be authenticated in a given domain must be joined to that domain.

---

To be able to join a domain:

- Content Gateway must be able to resolve the domain name.
- Content Gateway system time must be synchronized with the domain controller's time, plus or minus 1 minute.
- The correct domain Administrator name and password must be specified.
- There must be TCP/UDP connectivity to the domain controller(s) (ports 88, 389, 445).
- If backup domain controllers are configured, they and their Kerberos Distribution Center (KDC) services, must be reachable by Content Gateway on the network.

To join a domain:

1. Navigate to the **Configure > Security > Access Control > Integrated Windows Authentication** tab.
2. In the **Domain Name** field, enter the fully qualified domain name.
3. In the **Administrator Name** field enter the Windows Administrator user name.
4. In the **Administrator Password** field enter the Windows Administrator password.  
The name and password are used during the join only and are not stored.
5. Select how to locate the domain controller:

- **Auto-detect using DNS**
- **DC name or IP address**

If the domain controller is specified by name or IP address, you can also specify backup domain controllers in a comma separated list, no spaces.

6. Click **Join Domain**.

The **Joined Domains** section maintains a list of joined domains and controls for unjoining and changing the method of finding a domain.

For troubleshooting tips, see [Failure to join the domain](#).

### To unjoin a domain

In the **Joined Domains** section, select the domain you want to unjoin and click **Unjoin Domain**.

## To change the way the domain controller is found

1. In the **Joined Domains** section, select how to locate the domain controller:
  - **Auto-detect using DNS**
  - **DC name or IP address**

If the domain controller is specified by name or IP address, you can also specify backup domain controllers in a comma separated list, no spaces.
2. Click **Apply**.

## Global authentication options

These settings apply when IWA negotiates NTLM or falls back to NTLM, or when legacy NTLM is used.

1. Navigate to the **Configure > Security > Access Control > Global Authentication Options** tab.
2. **Fail Open** is enabled by default. Fail Open allows requests to proceed when authentication fails due to:
  - No response from the domain controller
  - Malformed messages from the client
  - Invalid SMB responses

With Fail Open, when Web filtering is used with the proxy and an XID agent is configured, if NTLM authentication fails the requester can still be identified by the XID agent and appropriate policy applied.

Disable Fail Open if you want to stop requests from proceeding to the Internet when the above listed authentication failure conditions occur.
3. **Credential Caching** is enabled by default. Credential caching applies only when Content Gateway is deployed as an explicit proxy. Credentials are cached only when authentication is successful. To disable credential caching, select **Disable**.
4. **Caching TTL** sets the time-to-live for entries in the credential cache. The default TTL is 900 seconds (15 minutes). To change the TTL, enter a new value in the entry field. The range of supported values is 300 to 86400 seconds.
5. If some users use terminal servers to access the Internet through the proxy (e.g., Citrix servers), you must create a list of those servers in the **Multi-user IP Exclusions** field. Credentials for such users are not cached. Enter a comma separated list of IP addresses and IP address ranges.



### Note

Content Gateway supports transparent authentication in proxy clusters using WCCP load balancing. However, the assignment method distribution attribute must be the source IP. For more information see [Configuring service groups in Content Gateway Manager](#), page 55.

## Creating an Integrated Windows Authentication realm rule

Before creating a rule for a realm that is accessed through Integrated Windows Authentication, you need to join the domain. You also need to know:

- ◆ The name of the domain that the rule applies to
- ◆ The set of source IP addresses from the clients that will be authenticated. These can be a mix of individual IP addresses and/or IP address ranges.
- ◆ Or, the unique port number on which traffic is inbound (explicit proxy only)
- ◆ Or, a combination of both of the above (explicit proxy only)



---

### Note

After entering all specifiers, you must click **Add** before you click **Apply**. If Apply is clicked first, or the edit window is closed, all of the entry fields are cleared.

---

1. In Content Gateway Manager, go to **Configure > Security > Access Control** and review or specify the **Domain**, **Global Authentication Options**, and, if applicable, **Transparent Proxy Authentication** settings.
2. If needed, on the **Domains** tab add the new domain (realm).
3. Go to the **Configure > Security > Access Control > Authentication Realms** tab. A list of all existing authentication realm rules is displayed at the top of the page.
4. Click **Edit file** to open the rule editor.
5. Select **Integrated Windows Authentication** from the **Rule Type** drop down list.
6. Select **Enable** if you want the rule to be active when the rule definition process is complete (after the rule is added and the proxy is restarted, steps 12 and 14 below).
7. Give the rule a unique **Rule Name**. A concise, descriptive name makes identification and administration of rules easier.
8. If the rule is to be applied to specific IP addresses, in the **Source IP** field, enter a comma-separated list of individual IP addresses and IP address ranges. Do not use spaces. For example:  
10.4.1.1,10.12.1.1-10.12.254.254  
Source IP address ranges can overlap. Overlapping ranges may be useful as a quick way of identifying sub-groups in a large pool.  
In overlapping ranges, the first match is used.
9. If the rule is to be applied to traffic coming in on a specific port, select the **Proxy Port** from the drop down list (valid for explicit proxy only).
10. To specify an alias name to send to Filtering Service, open **Advanced Settings** and select **Aliasing**. In the field, specify the name to use. If no name is specified (the entry field is left blank), Web Security will behave as configured when servicing requests that do not include a user name. For more information about aliasing, see [Unknown users and the 'alias' option](#).

11. In the **Integrated Windows Authentication Specifiers** section, in the **Domain/Realm** drop down list, select the realm that the rule applies.
12. Click **Add** to add the rule.
13. At the top of the page, check and adjust the position of the rule in the rule list. The first rule matched is applied.
14. Click **Apply** and then restart Content Gateway to put the rule into effect.



### Warning

If a rule has invalid values, a warning message displays that identifies the invalid rule.

## Creating a legacy NTLM authentication realm rule

Before you create a rule for an NTLM authentication realm, you need to know:

- ◆ The set of source IP addresses from the clients that will be authenticated. These can be a mix of individual IP addresses and IP address ranges.
- ◆ Or, the unique port number on which traffic is inbound (explicit proxy only)
- ◆ Or, a combination of both of the above (explicit proxy only)
- ◆ The name or IP address, and port number of the primary domain controller and any secondary domain controllers to be used for load balancing or failover.



### Note

After entering all specifiers, you must click **Add** before you click **Apply**. If **Apply** is clicked first, or the edit window is closed, all of the entry fields are cleared.

1. In Content Gateway Manager, go to **Configure > Security > Access Control** and review or specify the **Domain**, **Global Authentication Options**, and, if applicable, **Transparent Proxy Authentication** settings.
2. Go to **Configure > Security > Access Control > Authentication Realms**. A list of all existing authentication realm rules is displayed at the top of the page.
3. Click **Edit file** to open the rule editor.
4. Select **NTLM** from the **Rule Type** drop down list.
5. Select **Enable** if you want the rule to be active when the rule definition process is complete (after the rule is added and the proxy is restarted, steps 12 and 14 below).
6. Give the rule a unique **Rule Name**. A concise, descriptive name makes identification and administration of rules easier.
7. If the rule is to be applied to specific IP addresses, in the **Source IP** field, enter a comma-separated list of individual IP addresses and IP address ranges. Do not use spaces. For example:  
10.4.1.1,10.12.1.1-10.12.254.254

Source IP address ranges can overlap. Overlapping ranges may be useful as a quick way of identifying sub-groups in a large pool.

In overlapping ranges, the first match is used.

8. If the rule is to be applied to traffic coming in on a specific port, select the **Proxy Port** from the drop down list.
9. To specify an alias name to send to Filtering Service, open **Advanced Settings** and select **Aliasing**. In the field, specify the name to use. If no name is specified (the entry field is left blank), Web Security will behave as configured when servicing requests that do not include a user name. For more information about aliasing, see [Unknown users and the 'alias' option](#).
10. In **DC List**, enter the IP address and port number of the primary domain controller. If no port is specified, Content Gateway uses port 139.

You can also specify secondary domain controllers in a comma-separated list. The supported formats are:

host\_name[:port][%netbios\_name]

IP\_address[:port][%netbios\_name]

The **netbios\_name** is required with Active Directory 2008.

11. Select **DC Load Balance** to enable load balancing between domain controllers.

**Note**

When multiple domain controllers are specified, even if load balancing is disabled, when the load on the primary domain controller reaches the maximum number of connections allowed, new requests are sent to a secondary domain controller as a short-term failover provision, until such time that the primary domain controller can accept new connections.

---

12. Click **Add** to add the rule.
13. At the top of the page, check and adjust the position of the rule in the rule list. The first rule matched is applied.
14. Click **Apply** and then restart Content Gateway to put the rule into effect.

**Warning**

If a rule has invalid values, a warning message displays that identifies the invalid rule.

---

## Creating an LDAP authentication realm rule

Before you create an LDAP authentication realm rule, you need to know:

- ◆ The set of source IP addresses to send to the LDAP server. These can be a mix of individual IP addresses and IP address ranges.
- ◆ Or, the unique port number on which traffic is inbound (explicit proxy only)



- ◆ Or, a combination of both of the above (explicit proxy only)
- ◆ The name and port number of the LDAP server.
- ◆ The LDAP base distinguished name.
- ◆ The LDAP bind distinguished name and password.
- ◆ Optionally, an LDAP attribute name and value.



#### Note

After entering all specifiers, you must click **Add** before you click **Apply**. If Apply is clicked first, or the edit window is closed, all entry fields are cleared.

1. In Content Gateway Manager, go to **Configure > Security > Access Control** and review or specify the **Domain**, **Global Authentication Options**, and, if applicable, **Transparent Proxy Authentication** settings.
2. Go to **Configure > Security > Access Control > Authentication Realms**. A list of all existing authentication realm rules is displayed at the top of the page.
3. Click **Edit file** to open the rule editor.
4. Select **LDAP** from the **Rule Type** drop down list.
5. Select **Enable** if you want the rule to be active when the rule definition process is complete (after the rule is added and the proxy is restarted, steps 19 and 21 below).
6. Give the rule a unique **Rule Name**. A concise, descriptive name makes identification and administration of rules easier
7. If the rule is to be applied to specific IP addresses, in the **Source IP** field, enter a comma-separated list of individual IP addresses and IP address ranges. Do not use spaces. For example:  
10.4.1.1,10.12.1.1-10.12.254.254  
Source IP address ranges can overlap. Overlapping ranges may be useful as a quick way of identifying sub-groups in a large pool.  
In overlapping ranges, the first match is used.
8. If the rule is to be applied to traffic inbound on a specific port, select the **Proxy Port** from the drop down list.
9. To specify an alias name to send to Filtering Service, open **Advanced Settings** and select **Aliasing**. In the field, specify the name to use. If no name is specified (the entry field is left blank), Web Security will behave as configured when servicing requests that do not include a user name. For more information about aliasing, see [Unknown users and the 'alias' option](#).
10. In the **LDAP Server Name** field, enter the fully qualified domain name and port number, or IP address of the LDAP server.
11. If the LDAP server port is other than the default (389), in the **LDAP Server Port** field, enter the LDAP server port.
12. Enter the **LDAP Base Distinguished Name**. Obtain this value from your LDAP administrator.

13. Optionally, enter the LDAP UID filter. Use this field to specify the server type when it differs from the **Server Type** value specified on the **LDAP** tab (the default value). Enter **sAMAccountName** for Active Directory, or **uid** for any other service.
14. In the **Bind DN** field, enter the bind distinguished name. This must be a Full Distinguished Name of a user in the LDAP directory service. For example:  
CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM
15. In the **Bind Password** field, enter the password for the name given in the **Bind DN** field.
16. Check **Secure LDAP** if you want Content Gateway to use secure communication with the LDAP server.
17. Optionally, enter an LDAP attribute name.
18. Optionally, enter an LDAP attribute value.
19. Click **Add** to add the rule.
20. At the top of the page, check and adjust the position of the rule in the rule list. The first rule matched is applied.
21. Click **Apply** and then restart Content Gateway to put the rule into effect.

**Warning**

If a rule has invalid values, a warning message displays that identifies the invalid rule.

---

## Working with authentication realm rules

### Editing a rule

1. On the **Configure > Security > Access Control > Authentication Realms** tab, click **Edit File**.
2. In the table of rules, click on the rule to be changed. Its values populate the fields in the definition area.
3. Make the desired changes, click **Set** and then click **Apply**.
4. Click **Close** to return to the **Authentication Realms** tab.
5. **Restart** Content Gateway to put the changes into effect.

### Reordering the list of rules

Authentication realm rules are applied top-down in the list.

1. On the **Configure > Security > Access Control > Authentication Realms** tab, click **Edit File**.
2. In the table of rules, click on the rule that you want to reposition in the list, and then click the down or up arrow on the left to reposition the rule.
3. When the rules are in the desired order, click **Apply**.
4. Click **Close** to return to the **Authentication Realms** tab.

5. **Restart** Content Gateway to put the changes into effect.

### Deleting a rule

1. On the **Configure > Security > Access Control > Authentication Realms** tab, click **Edit File**.
2. In the table of rules, click on the rule to be deleted and click the “X” button on the left.
3. When you are done deleting rules, click **Apply**.
4. Click **Close** to return to the **Authentication Realms** tab.
5. **Restart** Content Gateway to put the changes into effect.

## Multiple Realm Authentication use cases

### Use case 1:

This describes a common case in which a second domain is added to an existing, single-domain environment. Content Gateway is an explicit proxy; clients use a PAC file.

An organization—let’s call them Quality Corp—uses a software installation of Content Gateway. They have one domain (QCORP), and one domain controller. They use NTLM to authenticate users.

Quality Corp acquires New Corp who has their own domain (NCORP) and domain controller. They use LDAP to authenticate users.

Quality Corp would like to manage the combined employees in a single domain, but isn’t ready to make the infrastructure changes. Until they are, they would like to have a separate use policy for New Corp users (i.e., not use the “default” user on the QCORP domain).

The Multiple Realm Authentication feature makes this possible.

To configure the solution, Quality Corp would:

1. Enable Multiple Realm Authentication.
2. Add a second, non-default HTTP port (**Configure > Protocols > HTTP**). This port will be used by all members of NCORP.
3. Create a PAC file for members of NCORP that causes them to connect to Content Gateway on the new, second port.
4. Create Multiple Realm Authentication rules, one each for the QCORP and NCORP domains:
  - a. Define an NCORP rule for connections on the second port. Specify in the Advanced Settings area that the user to use for policy determination is the static string “NCorpUser”.
  - b. Define the QCORP rule to handle all other connections.
5. Add “NCorpUser” to the QCORP domain as a valid user and create policy for that user in TRITON—Web Security.

At this point, everyone connecting to Content Gateway from NCORP is authenticated against the NCORP domain controller and gets the group policy associated with NCorpUser. Note that no individual user-based policy or features, such as quota time, are possible in this scenario. Transactions are logged as NCorpUser. This is all performed with no effect on the authentication, policy, or logging of users on the QCORP domain.

### **Use case 2:**

This describes a common case in which a second domain is added to an existing, single-domain environment. Content Gateway is an explicit proxy; clients use a PAC file.

An organization—let's call it BigStars—uses a software installation of Content Gateway. They have one domain (BIG), and one domain controller. They use NTLM to authenticate users.

A group in the company converts to Apple computers, which can't be authenticated with NTLM. The IT group installs an LDAP server and creates a new domain—BIGAPL—for the Apple users.

Because this group of users previously existed and was managed on the primary domain (BIG), the IT department expects that both user-based policy and logging still apply.

The Multiple Realm Authentication feature makes this possible.

To configure the solution, BigStars would:

1. Verify that every user in BIGAPL is also in BIG with the exact same user name.
2. Enable Multiple Realm Authentication.
3. Add a second, non-default HTTP port (**Configure > Protocols > HTTP**). This port will be used by all members of BIGAPL.
4. Create a PAC file for members of BIGAPL that causes them to connect to Content Gateway on the new, second port.
5. Create Multiple Realm Authentication rules, one each for the BIGAPL and BIG domains.
  - a. Define the BIGAPL rule for connections on the second port.
  - b. Define the BIG rule to handle all other connections.

At this point, all members of BIGAPL are authenticated with LDAP, but maintain their individual policy as specified by their existing NTLM identities. Logs and reports also refer to that same user.

### **Use case 3:**

This describes a common case in which a second, special-purpose domain is added to an existing, single-domain environment. Content Gateway is a transparent proxy using WCCP v2.

An organization—let's call it Creative Corp—uses a software installation of Content Gateway. They have one domain (CCORP), and one domain controller. They use NTLM to authenticate users.

Creative Corp is about to launch a new product and wants to make a big splash. They decide to have an open house complete with kiosks, demonstrations, and presenters. The kiosks only need the default Internet policy to properly demonstrate the new product. The IT manager wants to keep the kiosk network as walled off from the corporate intranet as possible. In this scenario, logging individual users isn't a requirement.

The Multiple Realm Authentication feature makes this possible.

To configure the solution, Creative Corp would:

1. Build a new, temporary network complete with its own domain controller. Let's call this domain CTEMP.
2. Add one or more users to CTEMP. They can either match one-to-one with existing users on the primary domain, or be one or more generic users for use by the presenters.
3. Redirect Internet traffic on CTEMP to Content Gateway with WCCP v2.
4. Enable Multiple Realm Authentication.
5. Create Multiple Realm Authentication rules, one each for the CTEMP and CCORP domains:
  - a. Define the CTEMP rule to apply to all connections coming from the IP address range assigned to the CTEMP domain. In the Advanced Settings area, specify that Aliasing and leave the field blank. This has the result of applying the default policy to all users of CTEMP.
  - b. Define the CCORP rule to handle all other connections.

At this point, anyone using the Internet on one of the kiosks is authenticated against the CTEMP network and has the "default" policy applied to their requests.

## Troubleshooting Multiple Realm Authentication

In multiple realm authentication, problems often present as:

- ◆ Users are *not* challenged when a challenge is expected
- ◆ Users *are* challenged when no challenge is expected
- ◆ User authentication is performed against the wrong domain

These problems occur in one of the following phases of user authentication processing:

- ◆ General user authentication logic (outlined below)
- ◆ Realm rule definition and matching
- ◆ User authentication protocol processing (IWA, NTLM, LDAP; for IWA troubleshooting, see [Troubleshooting Integrated Windows Authentication.](#))

## Multiple realm authentication logic

Multiple realm authentication always applies the following logic:

1. The rules in **filter.config** are checked and applied. This action occurs as a first step in every type of Content Gateway user authentication. If a filtering rule is matched, the rule is applied and user authentication processing stops. See [Filtering Rules](#), page 156.
2. If no filtering rule matches, realm rule matching is performed. The requestor's IP address is checked, top-down, against the rule set. If the IP address matches a rule, the source port is checked, if the rule defines one. The first rule match is applied. **If no rule matches, authentication is not attempted.**
3. If a rule is matched, the specified authentication protocol is applied against the specified domain. All rule configuration details are applied.
4. If the user is authenticated, the request proceeds or is denied per Web Security policy.
5. The transaction is logged.

To see how the logic is applied in a running environment, you can temporarily enable user authentication debug output. Among other details, the debug output shows the parsing of rules and matching. See [Enabling and disabling user authentication debug output](#).

## Troubleshooting

When multiple realm authentication doesn't produce the expected results, it is recommended that you troubleshoot the problem in the following order:

1. **Check Network Address Translation (NAT)**  
Confirm that there is no unexpected IP address NAT. Network address translation has the result that the original source IP address is changed to another address before user authentication is performed. In Content Gateway Manager, go to **Configure > Networking > ARM > General** and examine the rules in **ipnat.config**.
2. **Check the rules in filter.config**  
Confirm that there is no unexpected matching of a **filter.config** rule. Among other purposes, filter.config rules can be used to bypass user authentication. See [Filtering Rules](#).
3. **Check realm rule matching**  
Using the IP address of a user who is or is not being challenged as expected, walk through each realm rule, top to bottom, examining the settings to find the first match. Be meticulous in your analysis. A common problem is that the IP address falls within a too-broad IP address range.  
  
If the rule uses an alias, confirm that the alias is present in the User Service of the primary domain controller.  
  
For explicit clients configured to send traffic to a specific port, check both the rule and the configuration of the client's browser.
4. **Check the domain**

If you are getting the match you expect, verify that the domain is reachable and that the user is a member of the domain. If yes, troubleshoot the problem at the authentication protocol level. For IWA, see [Troubleshooting Integrated Windows Authentication](#).

## 5. When Content Gateway is in a proxy chain

If Content Gateway is a member of a proxy chain, verify that X-Forwarded-For headers are sent by the downstream proxy and read by Content Gateway.

- Use a packet sniffer to inspect inbound packets from the downstream proxy. Look for properly formed X-Forwarded-For headers.
- In Content Gateway Manager, go to **Configure > My Proxy > Basic**, scroll to the bottom of the page and verify that **Read authentication from child proxy** is enabled. If it's not, select **On**, click **Apply**, and then restart Content Gateway.

## Enabling and disabling user authentication debug output



### Warning

Debug output should not be left enabled. Debug output slows proxy performance and can fill the file system with log output.

Debug log information is written to: `/opt/WCG/logs/content_gateway.out`

To enable user authentication debug information, edit: `/opt/WCG/config/records.config`

```
(root)# vi /opt/WCG/config/records.config
```

Find and modify the following parameters and assign values as shown:

```
CONFIG proxy.config.diags.debug.enabled INT 1
CONFIG proxy.config.diags.debug.tags STRING
auth_* | winauth.* | ldap.* | ntlm.*
```

Save and close the file. Force Content Gateway to reread the file with the command:

```
(root)# /opt/WCG/bin/content_line -x
```

Follow the flow of debug information with the **tail -f** command:

```
(root)# tail -f /opt/WCG/logs/content_gateway.out
```

Use **Ctrl+C** to terminate the command.

When you have collected the debug output you want (after one or several user authentication processes is complete), disable debug output by editing `records.config` and modifying the parameter value as shown.

```
(root)# CONFIG proxy.config.diags.debug.enabled INT 0
```

Save and close the file. Force Content Gateway to reread the file with the command:

```
(root)# /opt/WCG/bin/content_line -x
```



# 15

## Working With Log Files

### Related topics:

[Event log files](#), page 196  
[Managing event log files](#), page 197  
[Event log file formats](#), page 198  
[Rolling event log files](#), page 204  
[Splitting event log files](#), page 207  
[Collating event log files](#), page 209  
[Viewing logging statistics](#), page 212  
[Viewing log files](#), page 213  
[Example event log file entries](#), page 214

Websense Content Gateway keeps 3 types of log files:

- ◆ *System log files* record system information, which includes messages about the state of Content Gateway and any errors or warnings that it produces. This information might include a note that event log files were rolled, a warning that cluster communication timed out, or an error indicating that Content Gateway was restarted. (Content Gateway posts alarms signifying error conditions on Content Gateway Manager; see [Working with alarms](#), page 107, for details.)

All system information messages are logged with the system-wide logging facility **syslog** under the daemon facility. The **syslog.conf** configuration file (stored in the **/etc** directory) specifies where these messages are logged. A typical location is **/var/log/messages**.

The **syslog** process works on a system-wide basis, so it is the single repository for messages from all Content Gateway processes, including **content\_gateway**, **content\_manager**, and **content\_cop**.

Each log entry in the log contains information about the date and time the error was logged, the hostname of the proxy server that reported the error, and a description of the error or warning.

See [Websense Content Gateway error messages](#), page 411, for a list of the system information messages that Content Gateway logs.

- ◆ *Error log files* record information about why a transaction was in error.

- ◆ *Event log files* (also called *access log files*) record information about the state of each transaction that Content Gateway processes.

Content Gateway creates both error and event log files and records system information in system log files. You can disable event logging and/or error logging. It is recommended that you log errors only or disable logging during peak usage hours.

- ▶ On the **Configure > Subsystems > Logging** tab, select one of the following options: **Log Transactions and Errors**, **Log Transactions Only**, **Log Errors Only**, or **Disabled**.

## Event log files

---

Event log files record information about every request that Websense Content Gateway processes. By analyzing the log files, you can determine how many people use the proxy cache, how much information each person requested, what pages are most popular, and so on.

Content Gateway supports several standard log file formats, such as Squid and Netscape, and user-defined custom formats. You can analyze the standard format log files with off-the-shelf analysis packages. To help with log file analysis, you can separate log files so that they contain information specific to protocol or hosts. You can also configure Content Gateway to roll log files automatically at specific intervals during the day.

The following sections describe how to:

- ◆ **Manage your event log files**  
You can choose a central location for storing log files, set how much disk space to use for log files, and set how and when to roll log files. See [Managing event log files](#), page 197.
- ◆ **Choose different event log file formats**  
You can choose which standard log file formats you want to use for traffic analysis (for example, Squid or Netscape). Alternatively, you can use the Content Gateway custom format, which is XML-based and enables you to institute more control over the type of information recorded in log files. See [Event log file formats](#), page 198.
- ◆ **Roll event log files automatically**  
You can configure Content Gateway to roll event log files at specific intervals during the day so that you can identify and manipulate log files that are no longer active. See [Rolling event log files](#), page 204.
- ◆ **Separate log files according to hosts**  
You can configure the proxy to create separate log files for different protocols based on the host. See [Splitting event log files](#), page 207.
- ◆ **Collate log files from different nodes**  
You can designate one or more nodes on the network to serve as log collation servers. These servers, which might either be stand-alone or part of Content

Gateway, enable you to keep all logged information in well-defined locations. See [Collating event log files, page 209](#).

- ◆ View statistics about the logging system  
Content Gateway provides statistics about the logging system. You can access the statistics through Content Gateway Manager or through the command line interface. See [Viewing logging statistics, page 212](#).
- ◆ View log files  
You can view the system, event, and error log files that Content Gateway creates. You can view an entire log file, a specified last number of lines in the log file, or all lines that contain a specified string.
- ◆ Interpret log file entries for the standard log file formats. See [Example event log file entries, page 214](#).

## Managing event log files

---

You can manage your event log files and control where they are located, how much space they can consume, and how low disk space in the logging directory is handled.

### Choosing the logging directory

By default, Content Gateway writes all event log files in the **logs** directory, which is located in the directory where you installed Content Gateway. To use a different directory, see [Setting log file management options, page 198](#).

### Controlling logging space

You can control the amount of disk space that the logging directory can consume. This allows the system to operate smoothly within a specified space window for a long period of time.

After you establish a space limit, Content Gateway continues to monitor the space in the logging directory. When the free space dwindles to the headroom limit (see [Setting log file management options, page 198](#)), Content Gateway enters a low space state and takes the following actions:

- ◆ If the autodelete option (discussed in [Rolling event log files, page 204](#)) is *enabled*, Content Gateway identifies previously rolled log files (log files with a **.old** extension) and starts deleting files one by one—beginning with the oldest file—until it emerges from the low state. Content Gateway logs a record of all files it deletes in the system error log.
- ◆ If the autodelete option is *disabled* or there are not enough old log files to delete for the system to emerge from its low space state, Content Gateway issues a warning and continues logging until space is exhausted. Content Gateway resumes event logging when enough space becomes available for it to exit its low

space state. You can make space available by removing files from the logging directory or by increasing the logging space limit.

You can run a **cron** script in conjunction with Content Gateway to automatically remove old log files from the logging directory (before Content Gateway enters the low space state) and relocate them to a temporary partition. Once the files are relocated, you can run log analysis scripts on them, and then you can compress the logs and move them to an archive location or delete them.

## Setting log file management options

1. Navigate to **Configure > Subsystems > Logging**.
2. In the **Log Directory** field, enter the path to the directory in which you want to store event log files. This can be an absolute path or a path relative to the directory in which Content Gateway is installed. The default directory is **logs**, located in the Content Gateway installation directory.



### Note

The directory you specify must already exist.

The Websense user must have read/write permissions for the directory storing the log files.

---

3. In the **Limit** field of the **Log Space** area, enter the maximum amount of space you want to allocate to the logging directory. The default value is 20480 MB.



### Note

All files in the logging directory contribute to the space used, even if they are not log files.

---

4. In the **Headroom** field, enter the tolerance for the log space limit. The default value is 100 MB.

If the **Auto-Delete Rolled Files** option is enabled in the **Log Rolling** section, autodeletion is triggered when the amount of free space available in the logging directory is less than the headroom. For information about log file rolling, see [Rolling event log files, page 204](#).

5. Click **Apply**.

## Event log file formats

---

Websense Content Gateway supports the following log file formats:

- ◆ *Standard formats*, such as Squid or Netscape (see [Using standard formats, page 199](#))
- ◆ the Content Gateway *custom format* (see [Custom format, page 199](#))

In addition to the standard and custom log file format, you must choose whether to save log files in *binary* or *ASCII*. See [Choosing binary or ASCII](#), page 202.



### Important

Event log files consume a large amount of disk space. Creating log entries in multiple formats at the same time can consume disk resources very quickly and affect proxy performance.

## Using standard formats

The standard log formats include Squid, Netscape Common, Netscape Extended, and Netscape Extended-2.

The standard log file formats can be analyzed with a wide variety of off-the-shelf log-analysis packages. You should use one of the standard event log formats unless you need information that these formats do not provide. See [Custom format](#), page 199.

By default, Content Gateway is configured to use the Netscape Extended log file format only.

### Setting standard log file format options

1. Navigate to **Configure > Subsystems > Logging > Formats**.
2. Enable the format you want to use.
3. Select the log file type (**ASCII** or **binary**).
4. In the **Filename** field, enter the name you want to use for your event log files.
5. In the **Header** field, enter a text header that appears at the top of the event log files. Leave this field blank if you do not want to use a text header.
6. Click **Apply**.
7. Click **Restart** on **Configure > My Proxy > Basic > General**.

## Custom format

The XML-based custom log format is more flexible than the standard log file formats, giving you more control over the type of information in your log files. Create a custom log format if you need data for analysis that is not available in the standard formats. You can decide what information to record for each Content Gateway transaction and create filters to define which transactions to log.

The heart of the custom logging feature is an XML-based logging configuration file (**logs\_xml.config**) that enables you to create modular descriptions of logging objects. The **logs\_xml.config** file uses three types of objects to create custom log files:

- ◆ The **LogFormat** defines the content of the log file using printf-style format strings.

- ◆ The **LogFilter** defines a filter so that you include or exclude certain information from the log file.
- ◆ The **LogObject** specifies all the information needed to produce a log file. For example:
  - The name of the log file (required).
  - The format to be used (required). This can be a standard format (Squid or Netscape) or a previously defined custom format (a previously defined **LogFormat** object).
  - The file mode (ASCII, Binary, or ASCII\_PIPE). The default is ASCII.

The ASCII\_PIPE mode writes log entries to a UNIX named pipe (a buffer in memory). Other processes can then read the data using standard I/O functions. The advantage of using this option is that Content Gateway does not have to write to disk, freeing disk space and bandwidth for other tasks.

**Note**

When the buffer is full, Content Gateway drops log entries and issues an error message indicating how many entries were dropped. Content Gateway writes only complete log entries to the pipe; therefore, only full records are dropped.

---

- Any filters you want to use (previously defined **LogFilter** objects).
- The collation servers that are to receive the log files.
- The protocols you want to log (if the protocols tag is used, Content Gateway logs only transactions from the protocols listed; otherwise, all transactions for all protocols are logged).
- The origin servers you want to log (if the servers tag is used, Content Gateway logs only transactions for the origin servers listed; otherwise, transactions for all origin servers are logged).
- The header text you want the log files to contain. The header text appears at the beginning of the log file, just before the first record.
- The log file rolling options.

**Note**

To generate a custom log format, you must specify at least one **LogObject** definition. One log file is produced for each **LogObject** definition. You can create a custom log format by through Content Gateway Manager or by editing a configuration file.

---

1. On **Configure > Subsystems > Logging > Custom**, enable the **Custom Logging** option.
2. The **Custom Log File Definitions** area displays the `logs_xml.config` file. Add **LogFormat**, **LogFilter**, and **LogObject** specifications to the configuration file.

For detailed information about the **logs\_xml.config** file and associated object specifications, see [logs\\_xml.config](#), page 335.

3. Click **Apply**.

## Creating summary log files

Content Gateway performs several hundred operations per second; therefore, event log files can grow quite large. Using SQL-like aggregate operators, you can configure Content Gateway to create summary log files that summarize a set of log entries over a specified period of time. This can reduce the size of the log files generated.

You generate a summary log file by creating a **LogFormat** object in the XML-based logging configuration file (**logs\_xml.config**) using the following SQL-like aggregate operators:

- ◆ **COUNT**
- ◆ **SUM**
- ◆ **AVERAGE**
- ◆ **FIRST**
- ◆ **LAST**

You can apply each of these operators to specific fields, requesting it to operate over a specified interval.

Summary log files represent a trade-off between convenience and information granularity. Since you must specify a time interval during which only a single record is generated, you can lose information. If you want the convenience of summary logs and need the detail of a conventional log file, consider creating and enabling two custom log formats—one using aggregate operators and the other not using aggregate operators.

To create a summary log file format:

1. Navigate to **Configure > Subsystems > Logging > Custom** to display the **logs\_xml.config** file.
2. Define the format of the log file as follows:

```
<LogFormat>
  <Name = "summary"/>
  <Format = "%<operator(field)> : %<operator(field)>"/>
  <Interval = "n"/>
</Format>
```

where:

*operator* is one of the five aggregate operators (**COUNT**, **SUM**, **AVERAGE**, **FIRST**, **LAST**). You can specify more than one operator in the format line.

*field* is the logging field that you want to aggregate.

*n* is the interval in seconds between summary log entries.

For more information, see [logs\\_xml.config](#), page 335.

For example, the following format generates one entry every 10 seconds, with each entry summarizing the time stamp of the last entry of the interval, a count of the number of entries seen within that 10-second interval, and the sum of all bytes sent to the client:

```
<LogFormat>
  <Name = "summary"/>
  <Format = "%<LAST(cqts)> : %<COUNT(*)> :
    %<SUM(psql)>"/>
  <Interval = "10"/>
</Format>
```



### Important

You cannot create a format specification that contains both aggregate operators and regular fields. For example, the following specification would be invalid:

```
<Format = "%<LAST(cqts)> : %<COUNT(*)> :
  %<SUM(psql)> : %<cqu>"/>
```

---

3. Define a **LogObject** that uses this format.
4. Click **Apply**.

## Choosing binary or ASCII

You can configure Content Gateway to create event log files in either of the following:

- ◆ **ASCII:** these files can be processed using standard, off-the-shelf log-analysis tools. However, Content Gateway must perform additional processing to create the files in ASCII, resulting in an increase in overhead. Also, ASCII files tend to be larger than the equivalent binary files. ASCII log files have a **.log** filename extension by default.
- ◆ **Binary:** these files generate lower system overhead, as well as generally occupying less space on the disk, depending on the type of information being logged. You must, however, use a converter application before you can read or analyze these files using standard tools. Binary log files use a **.blog** filename extension by default.

While binary log files typically require less disk space, this is not always the case. For example, the value 0 (zero) requires only one byte to store in ASCII but requires four bytes when stored as a binary integer. If you define a custom format that logs IP addresses, a binary log file would require only four bytes of storage per 32-bit address. However, the same IP address stored in dot notation would require around 15 characters (bytes) in an ASCII log file.

For standard log formats, you select **Binary** or **ASCII** on the **Configure > Subsystems > Logging > Formats** tab in Content Gateway Manager. See [Setting](#)



[standard log file format options](#), page 199. For the custom log format, you specify ASCII or Binary mode in the **LogObject**. Refer to [Custom format](#), page 199.

**Note**

For custom log files, in addition to the ASCII and Binary options, you can also write log entries to a UNIX named pipe (a buffer in memory). Other processes can then read the data using standard I/O functions. The advantage of using this option is that Content Gateway does not have to write to disk, freeing disk space and bandwidth for other tasks. In addition, writing to a pipe does not stop when logging space is exhausted because the pipe does not use disk space. See [logs\\_xml.config](#), page 335, for more information about the ASCII\_PIPE option.

Before selecting ASCII versus binary for your log files, consider the type of data that will be logged. Try logging for one day using ASCII and then one day using binary. Assuming that the number of requests is roughly the same for both days, you can calculate a rough metric comparing the two formats.

## Using logcat to convert binary logs to ASCII

You must convert a binary log file to ASCII before you can analyze it using standard tools.

1. Change to the directory containing the binary log file.
2. Make sure that the **logcat** utility is in your path.
3. Enter the following command:

```
logcat options input_filename...
```

The following table describes the command-line options.

Option	Description
<code>-o output_file</code>	Specifies where the command output is directed.
<code>-a</code>	Automatically generates the output filename based on the input filename. If the input is from <b>stdin</b> , this option is ignored. For example: <pre>logcat -a squid-1.blog squid-2.blog squid-3.blog</pre> generates: <pre>squid-1.log, squid-2.log, squid-3.log</pre>
<code>-S</code>	Attempts to transform the input to Squid format, if possible.
<code>-C</code>	Attempts to transform the input to Netscape Common format, if possible.
<code>-E</code>	Attempts to transform the input to Netscape Extended format, if possible.
<code>-2</code>	Attempt to transform the input to Netscape Extended-2 format, if possible.

**Note**

Use only one of the following options at any given time:  
**-S**, **-C**, **-E**, or **-2**.

If no input files are specified, **logcat** reads from the standard input (**stdin**). If you do not specify an output file, **logcat** writes to the standard output (**stdout**).

For example, to convert a binary log file to an ASCII file, you can use the **logcat** command with either of the following options:

```
logcat binary_file > ascii_file  
logcat -o ascii_file binary_file
```

The binary log file is not modified by this command.

---

## Rolling event log files

Websense Content Gateway provides automatic log file rolling. This means that at specific intervals during the day, Content Gateway closes its current set of log files and opens new log files.

Log file rolling offers the following benefits:

- ◆ It defines an interval over which log analysis can be performed.
- ◆ It keeps any single log file from becoming too large and assists in keeping the logging system within the specified space limits.

- ◆ It provides an easy way to identify files that are no longer being used so that an automated script can clean the logging directory and run log analysis programs.

You should roll log files several times a day. Rolling every six hours is a good guideline to follow.

## Rolled log filename format

Websense Content Gateway provides a consistent name format for rolled log files that allows you to identify log files.

When Content Gateway rolls a log file, it saves and closes the old file and starts a new file. Content Gateway renames the old file to include the following information:

- ◆ The format of the file (for example, **squid.log**).
- ◆ The hostname of the Content Gateway server that generated the log file.
- ◆ Two timestamps separated by a hyphen (-). The first time stamp is a lower bound for the time stamp of the first record in the log file. The lower bound is the time when the new buffer for log records is created. Under low load, the first time stamp in the filename can be different from the timestamp of the first entry. Under normal load, the first time stamp in the filename and the time stamp of the first entry are similar.

The second time stamp is an upper bound for the time stamp of the last record in the log file (this is normally the rolling time).

- ◆ The suffix **.old**, which makes it easy for automated scripts to find rolled log files.

The timestamps have the following format:

```
%Y%M%D.%Hh%Mm%Ss-%Y%M%D.%Hh%Mm%Ss
```

The following table describes the format:

Code	Definition	Example
%Y	The year in four-digit format	2000
%M	The month in two-digit format, from 01-12	07
%D	The day in two-digit format, from 01-31	19
%H	The hour in two-digit format, from 00-23	21
%M	The minute in two-digit format, from 00-59	52
%S	The second in two-digit format, from 00-59	36

The following is an example of a rolled log filename:

```
squid.log.mymachine.20000912.12h00m00s-  
20000913.12h00m00s.old
```

In this example, the file is squid log format and the host machine is mymachine. The first time stamp indicates a date and time of year 2000, month September, and day 12

at 12:00 noon. The second time stamp indicates a date and time of year 2000, month September, and day 13 at 12:00 noon. At the end, the file has a .old suffix.

The logging system buffers log records before writing them to disk. When a log file is rolled, the log buffer might be partially full. If so, the first entry in the new log file will have a time stamp earlier than the time of rolling. When the new log file is rolled, its first time stamp will be a lower bound for the time stamp of the first entry. For example, suppose logs are rolled every three hours, and the first rolled log file is:

```
squid.log.mymachine.19980912.12h00m00s-  
19980912.03h00m00s.old
```

If the lower bound for the first entry in the log buffer at 3:00:00 is 2:59:47, the next log file, when rolled, will have the following time stamp:

```
squid.log.mymachine.19980912.02h59m47s-  
19980912.06h00m00s.old
```

The contents of a log file are always between the two timestamps. Log files do not contain overlapping entries, even if successive timestamps appear to overlap.

## Rolling intervals

Log files are rolled at specific intervals relative to a given hour of the day. Two options control when log files are rolled:

- ◆ The offset hour, which is an hour between 0 (midnight) and 23
- ◆ The rolling interval

Both the offset hour and the rolling interval determine when log file rolling starts. Rolling occurs every rolling interval *and* at the offset hour.

For example, if the rolling interval is six hours and the offset hour is 0 (midnight), the logs roll at midnight (00:00), 06:00, 12:00, and 18:00 each day. If the rolling interval is 12 hours and the offset hour is 3, logs roll at 03:00 and 15:00 each day.

## Setting log file rolling options

1. Navigate to **Configure > Subsystems > Logging > General**.
2. In the **Log Rolling** section, ensure the **Log Rolling** option is enabled (the default).
3. In the **Offset Hour** field, enter a specific time each day you want log file rolling to take place. Content Gateway forces the log file to be rolled at the offset hour each day.  
You can enter any hour in the range 0 (midnight) to 23.
4. In the **Interval** field, enter the amount of time Content Gateway enters data in the log files before rotation takes place.

The minimum value is 300 seconds (five minutes). The maximum value is 86400 seconds (one day).

**Note**

If you start Content Gateway within a few minutes of the next rolling time, rolling may not occur until the following rolling time.

5. Ensure the **Auto-Delete Rolled Files** option is enabled (the default). This enables auto deletion of rolled log files when available space in the log directory is low.  
Auto deletion is triggered when the amount of free space available in the log directory is less than the headroom.
6. Click **Apply**.

**Note**

You can fine tune log file rolling settings for a custom log file in the **LogObject** specification in the **logs.xml.config** file. The custom log file uses the rolling settings in its **LogObject**, which override the default settings you specify in Content Gateway Manager or the **records.config** file described above.

---

## Splitting event log files

---

By default, Websense Content Gateway uses standard log formats and generates log files that contain HTTP and FTP transactions in the same file. However, you can enable host log splitting if you prefer to log transactions for different origin servers in separate log files.

### HTTP host log splitting

HTTP host log splitting enables you to record HTTP and FTP transactions for different origin servers in separate log files. When HTTP host log splitting is enabled, Content Gateway creates a separate log file for each origin server listed in the **log\_hosts.config** file (see [Editing the log\\_hosts.config file](#), page 208).

When HTTP host log splitting is enabled, Content Gateway generates separate log files for HTTP/FTP transactions, based on the origin server.

For example, if the **log\_hosts.config** file contains the two origin servers **uni.edu** and **company.com**, and the Squid format is enabled, Content Gateway generates the following log files:

Log Filename	Description
squid-uni.edu.log	All HTTP and FTP transactions for <b>uni.edu</b>
squid-company.com.log	All HTTP and FTP transactions for <b>company.com</b>
squid.log	All HTTP and FTP transactions for other hosts

Content Gateway also enables you to create XML-based custom log formats that offer even greater control over log file generation based on protocol and host name. See [Custom format, page 199](#).

## Setting log splitting options

1. Navigate to **Configure > Subsystems > Logging > Splitting**.
2. Enable the **Split Host Logs** option to record all HTTP and FTP transactions for each origin server listed in the **log\_hosts.config** file in a separate log file. Disable the **Split Host Logs** option to record all HTTP and FTP transactions for each origin server listed in the **log\_hosts.config** file in the same log file.
3. Click **Apply**.

## Editing the log\_hosts.config file

The default **log\_hosts.config** file is located in **/opt/WCG/config**. To record HTTP and FTP transactions for different origin servers in separate log files, you must specify each origin server's hostname on a separate line in the file.



### Note

You can specify keywords in the **log\_hosts.config** file to record in a separate log file all transactions from origin servers that contain the specified keyword in their names. For example, if you specify the keyword **sports**, Content Gateway records all HTTP and FTP transactions from **sports.yahoo.com** and **www.foxsports.com** in a log file called **squid-sport.log** (if the Squid format is enabled).



### Note

If Content Gateway is clustered and if you enable log file collation, it is recommended that you use the same **log\_hosts.config** file on every node in the cluster.

1. Open the **log\_hosts.config** file located in **/opt/WCG/config**.
2. Enter the hostname of each origin server on a separate line in the file. For example:

```
webserver1
webserver2
webserver3
```
3. Save and close the file.
4. To apply the changes, run the following command from the Content Gateway **bin** directory (**/opt/WCG/bin**):

```
./content_line -x
```

## Collating event log files

---

You can use the log file collation feature to keep all logged information in one place. This allows you to analyze Content Gateway as a whole rather than as individual nodes and to use a large disk that might only be located on one of the nodes in a cluster.

Content Gateway collates log files by using one or more nodes as log collation servers and all remaining nodes as log collation clients. When a node generates a buffer of event log entries, it determines whether it is the collation server or a collation client. The collation server node simply writes all log buffers to its local disk, just as it would if log collation were not enabled.

The collation client nodes prepare their log buffers for transfer across the network and send the buffers to the log collation server. When the log collation server receives a log buffer from a client, it writes it to its own log file as if it were generated locally. If log clients cannot contact their log collation server, they write their log buffers to their local disks, into *orphan* log files. Orphan log files require manual collation. Log

collation servers can be stand-alone or they can be part of a node running Content Gateway.



**Note**

Log collation can have an impact on network performance. Because all nodes are forwarding their log data buffers to the single collation server, a bottleneck might occur in the network, where the amount of data being sent to a single node in the network exceeds the node's ability to process it quickly.

---



**Note**

Collated log files contain time-stamp information for each entry, but entries do not appear in the files in strict chronological order. You can sort collated log files before doing analysis.

---

## Configuring Content Gateway to be a collation server

1. Navigate to **Configure > Subsystems > Logging > Collation**.
2. In the **Collation Mode** section, enable the **Be A Collation Server** option.
3. In the **Log Collation Port** field, enter the port number used for communication with collation clients. The default port number is 8085.
4. In the **Log Collation Secret** field, enter the password used to validate logging data and prevent the exchange of arbitrary information.



**Note**

All collation clients must use this same secret.

---

5. Click **Apply**.



**Important**

If you modify the collation port or secret after connections between the collation server and collation clients have been established, you must restart Content Gateway.

---

## Configuring Content Gateway to be a collation client

1. Navigate to **Configure > Subsystems > Logging > Collation**.



2. In the **Collation Mode** section, enable the **Be a Collation Client** option to set the Content Gateway node as a collation client and send the active standard formatted log entries (such as Squid and Netscape) to the log collation server.

**Note**

To send custom XML-based formatted log entries to the collation server, you must add a log object specification to the **logs\_xml.config** file. See [Custom format](#), page 199.

3. In the **To Collation Server** field, enter the hostname of the collation server. This could be the Content Gateway collation server or a stand-alone collation server.
4. In the **Log Collation Port** field, enter the port number used for communication with the collation server. The default port number is 8085.
5. In the **Log Collation Secret** field, enter the password used to validate logging data and prevent the exchange of arbitrary information. This must be the same secret you set on the collation server.
6. Enable the **Log Collation Host Tagged** option if you want to preserve the origin of log entries in the collated log files.
7. In the **Log Collation Orphan Space** field, enter the maximum amount of space (in megabytes) you want to allocate to the logging directory on the collation client for storing orphan log files. (Orphan log files are created when the log collation server cannot be contacted). The default value is 25 MB.
8. Click **Apply**.

**Important**

If you modify the collation port or secret after connections between the collation clients and collation server have been established, you must restart Content Gateway.

## Using a stand-alone collator

If you do not want the log collation server to be a Content Gateway node, you can install and configure a stand-alone collator (SAC) which can dedicate more of its power to collecting, processing, and writing log files.

**Note**

The stand-alone collator is currently available for the Linux platform only.

1. Configure your Content Gateway nodes as log collation clients. See [Configuring Content Gateway to be a collation client](#), page 210.
2. Copy the **sac** binary from the Content Gateway **bin** directory (**/opt/WCG/bin**) to the machine serving as the stand-alone collator.

3. Create a directory called **config** in the directory that contains the **sac** binary.
4. Create a directory called **internal** in the **config** directory you created in [Step 3](#). This directory will be used internally by the stand-alone collator to store lock files.
5. Copy the **records.config** file (**/opt/WCG/config**) from a Content Gateway node configured to be a log collation client to the **config** directory you created in [Step 3](#) on the stand-alone collator.

The **records.config** file contains the log collation secret and port you specified when configuring nodes to be collation clients. The collation port and secret must be the same for all collation clients and servers.

6. Open the **records.config** file on the stand-alone collator and edit the following variable:

Variable	Description
<i>proxy.config.log2.logfile_dir</i>	<p>Specify the directory where you want to store the log files. You can specify an absolute path to the directory or a path relative to the directory from which the <b>sac</b> binary is executed.</p> <p>Note: The directory must already exist on the machine serving as the stand-alone collator.</p>

7. Save and close the file.
8. Enter the following command:

```
sac -c config
```

---

## Viewing logging statistics

---

Content Gateway generates statistics about the logging system that help you see the following information:

- ◆ How many log files (formats) are currently being written.
- ◆ The current amount of space being used by the logging directory, which contains all of the event and error logs.
- ◆ The number of access events that have been written to log files since Content Gateway installation. This counter represents one entry in one file. If multiple formats are being written, a single event will create multiple event log entries.
- ◆ The number of access events skipped (because they were filtered out) since Content Gateway installation.
- ◆ The number of access events that have been written to the event error log since Content Gateway installation.

You can view the statistics from the Monitor tab in Content Gateway Manager or retrieve them through the command-line interface. See [Monitoring Traffic](#), page 103.

## Viewing log files

Related topics:

[Squid format](#), page 215

[Netscape examples](#), page 216

You can view the system, event, and error log files that Content Gateway creates from Content Gateway Manager. You can view an entire log file, a specified last number of lines in the log file, or all lines that contain a specified string.

You can also delete a log file or copy it to your local system.



### Note

You must have the correct user permissions to copy and delete log files.



### Note

Content Gateway displays only the first 1 MB of data in the log file. If the log file you select is larger than 1 MB, Content Gateway truncates the file and displays a warning message indicating that the file is too big.

You can now access log files through Content Gateway Manager.

1. Navigate to **Configure > My Proxy > Logs > System**.
2. To view, copy, or delete a system log file, go to [Step 3](#).  
To view, copy, or delete an event or error log file, select the **Access** tab.
3. In the **Log File** drop-down list, select the log file you want to view, copy, or delete.

Content Gateway lists the system log files logged with the system-wide logging facility **syslog** under the daemon facility.

Content Gateway lists the event log files located in the directory specified in the **Logging Directory** field in the **Configure > Subsystems > Logging > General** tab or by the configuration variable **proxy.config.log2.logfile\_dir** in the **records.config** file. The default directory is **logs** in the Content Gateway installation directory.

4. In the **Action** area, select one of the following options:

- **Display the selected log file** to view the entire log file. If the file is larger than 1 MB, only the first MB of data is displayed.
- **Display last lines of the selected file** to view the last lines of the log file. Enter the number of lines you want to view in the field provided.
- **Display lines that match in the selected log file** to view all the lines in the log file that match a particular string. Enter the string in the field provided.
- **Remove the selected log file** to delete the selected log file from the Content Gateway system.
- **Save the selected log file in local filesystem** to save a copy of the selected log file on your local system.

5. Click **Apply**.

If you selected to view the log file, Content Gateway displays the file at the end of the page.

If you selected to delete the log file, Content Gateway deletes the file. You are not prompted to confirm the deletion.

If you selected to save the log file, you are prompted for the location where you want to save the file on your local system.

## Example event log file entries

---

This section shows examples of a log file entry in each of the standard log formats supported by Content Gateway:

- ◆ [Squid format, page 215](#)
- ◆ [Netscape examples, page 216](#)
- ◆ [Netscape Extended format, page 216](#)
- ◆ [Netscape Extended-2 format, page 216](#)

## Squid format

The following figure shows a sample log entry in a **squid.log** file. The table below describes each field.

The diagram shows a sample log entry from a squid.log file with fields numbered 1 through 10. The log entry is: 987548934.123 19 209.131.54.138 TCP\_HIT/200 4771 GET http://europe.cnn.com/EUROPE/potd/2001/04/17/tz.pullitzer.ap.jpg - NONE/- image/jpeg. The fields are: 1: 987548934.123, 2: 19, 3: 209.131.54.138, 4: TCP\_HIT/200, 5: 4771, 6: GET, 7: http://europe.cnn.com/EUROPE/potd/2001/04/17/tz.pullitzer.ap.jpg, 8: -, 9: NONE/-, 10: image/jpeg. A bracket labeled '7 cont'd' spans from the end of field 7 to the start of field 8.

Field	Description
1	The client request time stamp in Squid format; the time of the client request in seconds since January 1, 1970 UTC (with millisecond resolution).
2	The time the proxy spent processing the client request; the number of milliseconds between the time that the client established the connection with the proxy and the time that the proxy sent the last byte of the response back to the client.
3	The IP address of the client's host machine.
4	The cache result code; how the cache responded to the request: HIT, MISS, and so on. Cache result codes are described in <a href="#">In Squid- and Netscape-format log files, what do the cache result codes mean?</a> , page 425. The proxy response status code (the HTTP response status code from Content Gateway to client).
5	The length of the Content Gateway response to the client in bytes, including headers and content.
6	The client request method: GET, POST, and so on.
7	The client request canonical URL; blanks and other characters that might not be parsed by log analysis tools are replaced by escape sequences. The escape sequence is a percentage sign followed by the ASCII code number of the replaced character in hex.
8	The authenticated client's user name. A hyphen (-) means that no authentication was required.
9	The proxy hierarchy route; the route Content Gateway used to retrieve the object. The proxy request server name; the name of the server that fulfilled the request. If the request was a cache hit, this field contains a hyphen (-).
10	The proxy response content type; the object content type taken from the Content Gateway response header.

## Netscape examples

### Netscape Common format

The following figure shows a sample log entry in a **common.log** file. The table below describes each field.

```

1      2      3      4      5
209.131.54.138 - - [17/Apr/2001:16:20:28 -0700] "GET http://europe.cnn.com/
EUROPE/potd/2001/04/17/tz.pullitzer.ap.jpg HTTP/1.0" 200 4473
                    5 cont'd                      6      7
  
```

### Netscape Extended format

The following figure shows a sample log entry in an **extended.log** file. The table below describes each field.

```

1      2 3      4      5
209.131.54.138 - - [17/Apr/2001:16:20:28 -0700] "GET http://europe.cnn.com/EUROPE/potd/2001/
04/17/tz.pullitzer.ap.jpg HTTP/1.0" 200 4473 000 0 0 0 458 297 0 0 0
                    5 cont'd                      6  7  8  9 10 11 12 13 14 15 16
  
```

### Netscape Extended-2 format

The following figure shows a sample log entry in an **extended2.log** file. The table below describes each field.

```

1      2 3      4      5
209.131.54.138 - - [17/Apr/2001:16:20:28 -0700] "GET http://europe.cnn.com/EUROPE/potd/2001/04/
17/tz.pullitzer.ap.jpg HTTP/1.0" 200 4473 000 0 0 0 458 297 0 0 0 NONE FIN FIN TCP_MEM_HIT
                    5 cont'd                      6  7  8  9 10 11 12 13 14 15 16 17 18 19 20
  
```

Field	Description
<b>Netscape Common</b>	
1	The IP address of the client's host machine.
2	This hyphen (-) is always present in Netscape log entries.
3	The authenticated client user name. A hyphen (-) means no authentication was required.
4	The date and time of the client's request, enclosed in brackets.
5	The request line, enclosed in quotes.

Field	Description
6	The proxy response status code (HTTP reply code).
7	The length of the Content Gateway response to the client in bytes.
	<b>Netscape Extended</b>
8	The origin server's response status code.
9	The server response transfer length; the body length in the origin server's response to the proxy, in bytes.
10	The client request transfer length; the body length in the client's request to the proxy, in bytes.
11	The proxy request transfer length; the body length in the proxy request to the origin server.
12	The client request header length; the header length in the client's request to the proxy.
13	The proxy response header length; the header length in the proxy response to the client.
14	The proxy request header length; the header length in the proxy request to the origin server.
15	The server response header length; the header length in the origin server's response to the proxy.
16	The time Content Gateway spent processing the client request; the number of seconds between the time that the client established the connection with the proxy and the time that the proxy sent the last byte of the response back to the client.
	<b>Netscape Extended-2</b>
17	The proxy hierarchy route; the route Content Gateway used to retrieve the object.
18	The client finish status code: FIN if the client request completed successfully or INTR if the client request was interrupted.
19	The proxy finish status code: FIN if the Content Gateway request to the origin server completed successfully or INTR if the request was interrupted.
20	The cache result code; how the Content Gateway cache responded to the request: HIT, MISS, and so on. Cache result codes are described in <a href="#">In Squid- and Netscape-format log files, what do the cache result codes mean?</a> , page 425.





# A

## Statistics

This appendix describes the following statistics on the Content Gateway Manager Monitor tab:

- ◆ [My Proxy](#), page 219
- ◆ [Protocols](#), page 222
- ◆ [Security](#), page 225
- ◆ [Subsystems](#), page 229
- ◆ [Networking](#), page 231
- ◆ [Performance](#), page 235
- ◆ [SSL Key Data](#), page 238

### My Proxy

---

My Proxy statistics are divided into the following categories:

- ◆ [Summary](#), page 219
- ◆ [Node](#), page 221
- ◆ [Graphs](#), page 222
- ◆ [Alarms](#), page 222

### Summary

Statistic/Field	Description
	<b>Subscription Details</b>
Feature	Lists features purchased, such as SSL Manager, and scanning options. See <a href="#">Working With Encrypted Data</a> , page 121, for information on SSL Manager, and also <i>Analyze Content with the Scanning Options</i> in the TRITON - Web Security online Help.
Purchased Status	Indicates if a feature has been purchased or not.

Statistic/Field	Description
Expiration Date	If a feature has been purchased, displays the expiration date of the subscription.
	<b>More Detail</b>
Subscription key	Displays the subscription key. See <a href="#">Entering your subscription key</a> , page 12.
Last successful subscription download time	Displays the time of the last successful validation of the subscription key. The check is made once a day.
Connection status	Displays the Content Gateway connection status to Policy Server, Policy Broker, and Filtering Service.
	<b>Scanning Data Files</b>
Engine Name	Displays the name of each scanning engine.
Engine Version	Displays the version number of the scanning engine.
Data File Version	Displays the version number of the data file currently in use by the scanning engine.
Content Classification Analytics library version	Displays the version number of the Content Classification Analytics library.
Last time Content Gateway loaded databases and settings	Displays the time and date when Content Gateway last successfully loaded that analytics data files, settings, and policies.
Last time Content Gateway checked for updates	Displays the time and date when Content Gateway last successfully communicated with the Websense download server to check for data file updates.
	<b>Node Details</b>
Node	Name of the Content Gateway node or cluster.
On/Off	Indicates if the proxy is running (the proxy and manager services are running).
Objects Served	Total number of objects served by the Content Gateway node.
Ops/Sec	Number of operations per second processed by the Content Gateway node.
Hit Rate	Percentage of HTTP requests served from the cache, averaged over the past 10 seconds.
Throughput (Mbit/sec)	Number of megabits per second passing through the Content Gateway node (and cluster).
HTTP Hit (ms)	Amount of time it takes for an HTTP object that is fresh in the cache to be served to the client.
HTTP Miss (ms)	Amount of time it takes for an HTTP object that is not in the cache or is stale to be served to the client.

Statistic/Field	Description
SSL Manager Configuration Server	When multiple Content Gateway nodes are deployed in a cluster and SSL Management clustering is enabled, this field displays the IP address of the SSL Manager Configuration Server. If the address is a link, the current system is <b>not</b> the server. Click the link to log on to the SSL Manager Configuration Server.
	<b>More Detail</b>
cache hit rate	Percentage of HTTP requests served from the cache, averaged over the past 10 seconds. This value is refreshed every 10 seconds.
errors	Percentage of requests that end in early hangups.
aborts	Percentage of aborted requests.
active clients	Current number of open client connections.
active servers	Current number of open origin server connections.
node IP address	IP address assigned to the node. If virtual IP addressing is enabled, several virtual IP addresses could be assigned to this node.
cache free space	Amount of free space in the cache.
HostDB hit rate	Ratio of host database hits to total host database lookups, averaged over a 10-second period.

## Node

Statistic	Description
	<b>Node Summary</b>
Status	Indicates if Content Gateway is running on this node (active or inactive).
Up Since	Date and time Content Gateway was started.
Clustering	Indicates if clustering is on or off on this node.
	<b>Cache</b>
Document Hit Rate	Ratio of cache hits to total cache requests, averaged over 10 seconds. This value is refreshed every 10 seconds.
Bandwidth Savings	Ratio of bytes served from the cache to total requested bytes, averaged over 10 seconds. This value is refreshed every 10 seconds.
Cache Percent Free	Ratio of cache free space to total cache space.
	<b>In Progress</b>
Open Server Connections	Number of currently open origin server connections.

Statistic	Description
Open Client Connections	Number of currently open client connections.
Cache Transfers in Progress	Number of cache transfers (cache reads and writes) in progress.
	<b>Network</b>
Client Throughput (Mbit/Sec)	Number of megabits per second passing through the node (and cluster).
Transactions per Second	Number of HTTP transactions per second.
	<b>Name Resolution</b>
Host Database Hit Rate	Ratio of host database hits to total host database lookups, averaged over 10 seconds. This value is refreshed every 10 seconds.
DNS Lookups per Second	Number of DNS lookups per second.

## Graphs

The Graphs page displays the same statistics listed on the [Node](#) page (cache performance, current connections and transfers, network, and name resolution) but in graphical format. You can choose the statistics you want to present in a graph. See [Viewing statistics](#), page 103.

## Alarms

Websense Content Gateway signals an alarm when it detects a problem (for example, if the space allocated to event logs is full or if Content Gateway cannot write to a configuration file) and displays a description of the alarm in the alarm message window. In addition, the **Alarm! [pending]** bar at the top of the Content Gateway Manager display indicates when alarms are detected and how many alarms exist.

After you have read an alarm message, click **Clear** in the alarm message window to dismiss the alarm. Clicking **Clear** only dismisses alarm messages; it does not actually resolve the cause of the alarms.

For information about working with alarms, see [Working with alarms](#), page 107.

## Protocols ---

Protocol statistics are divided into the following categories:

- ◆ [HTTP](#), page 223
- ◆ [FTP](#), page 225

# HTTP

Statistic	Description
	<b>General</b>
<b>Client</b>	
Total Document Bytes	Total amount of HTTP data served to clients since installation.
Total Header Bytes	Total amount of HTTP header data served to clients since installation.
Total Connections	Total number of HTTP client connections since installation.
Current Connections	Current number of HTTP client connections
Transactions in Progress	Total number of HTTP client transactions in progress.
<b>Server</b>	
Total Document Bytes	Total amount of HTTP data received from origin servers since installation.
Total Header Bytes	Total amount of HTTP header data received from origin servers since installation.
Total Connections	Total number of HTTP server connections since installation.
Current Connections	Current number of HTTP server connections
Transactions in Progress	Total number of HTTP server connections currently in progress.
	<b>Transaction</b>
<b>Hits</b>	
Fresh	Percentage of hits that are fresh and their average transaction times.
Stale Revalidated	Percentage of hits that are stale and revalidated and turn out to be still fresh and served, and their average transaction times.
<b>Misses</b>	
Now Cached	Percentage of requests for documents that were not in the cache (but are now) and their average transaction times.
Server No Cache	Percentage of requests for HTTP objects that were not in the cache, but have server no-cache headers (cannot be cached); and their average transaction times.
Stale Reloaded	Percentage of misses that are revalidated and turn out to be changed, reloaded, and served, and their average transaction times.

Statistic	Description
Client No Cache	Percentage of misses with client no-cache headers and their average transaction times.
<b>Errors</b>	
Connection Failures	Percentage of connect errors and their average transaction times.
Other Errors	Percentage of other errors and their average transaction times.
<b>Aborted Transactions</b>	
Client Aborts	Percentage of client-aborted transactions and their average transaction times.
Questionable Client Aborts	Percentage of transactions that could possibly be client aborted and their average transaction times.
Partial Request Hangups	Percentage of early hangups (after partial requests) and their average transaction times.
Pre-Request Hangups	Percentage of pre-request hangups and their average transaction times.
Pre-Connect Hangups	Percentage of pre-connect hangups and their average transaction times.
<b>Other Transactions</b>	
Unclassified	Percentage of unclassified transactions and their average transaction times.
	<b>FTP over HTTP</b>
<b>Connections</b>	
Open Server Connections	Number of open connections to the FTP server.
Successful PASV Connections	Number of successful PASV connections since installation.
Failed PASV Connections	Number of failed PASV connections since installation.
Successful PORT Connections	Number of successful PORT connections since installation.
Failed PORT Connections	Number of failed PORT connections since installation.
<b>Cache Statistics</b>	
Hits	Number of HTTP requests for FTP objects served from the cache.
Misses	Number of HTTP requests for FTP objects forwarded directly to the origin server because the object is not in the cache or is stale.
Lookups	Number of times Content Gateway looked up an HTTP request for an FTP object in the cache.

## FTP

Statistic	Description
<b>Client</b>	
Open Connections	Number of client connections currently open.
Bytes Read	Number of client request bytes read since installation.
Bytes Written	Number of client request bytes written since installation.
<b>Server</b>	
Open Connections	Number of FTP server connections currently open.
Bytes Read	The number of bytes read from FTP servers since installation.
Bytes Written	Number of bytes written to the cache since installation.

## Security

Security statistics are divided into the following categories:

- ◆ [Integrated Windows Authentication](#), page 226
- ◆ [LDAP](#), page 227
- ◆ [Legacy NTLM](#), page 228
- ◆ [SOCKS](#), page 228
- ◆ [Data Security](#), page 228



### Note

Even when multiple authentication realm rules are used, Content Gateway reports authentication statistics discreetly for each authentication method (IWA, LDAP, Legacy NTLM).

## Integrated Windows Authentication

Statistic	Description
	<b>Diagnostic Test</b> This function runs diagnostic tests on the Kerberos connection to the selected domain. Results are displayed on screen and written to /opt/WCG/logs/content_gateway.out and /opt/WCG/logs/smbadmin.log.
Domain drop down box	Select a joined domain. Unless Multiple Realm Authentication is configured, there will only be 1 joined domain.
Run Test button	Click to initiate a test.
	<b>Kerberos request counters</b>
Total Kerberos requests	The total number of Kerberos authentication requests.
Authentication succeeded	The number of Kerberos authentication requests that resulted in successful authentication.
Authentication failed	The number of Kerberos authentication requests that resulted in authentication failure.
Kerberos errors	The number of Kerberos process errors.
	<b>NTLM request counters</b>
Total NTLM requests	The total number of NTLM authentication requests.
Authentication succeeded	The number of NTLM authentication requests that resulted in successful authentication.
Authentication failed	The number of NTLM authentication requests that resulted in authentication failure.
NTLM request errors	The number of NTLM process errors.
NTLM within negotiate requests	The number of NTLM requests encapsulated in Negotiate requests.
	<b>Basic authentication request counters</b>
Total basic authentication requests	The total number of basic authentication requests.
Authentication succeeded	The number of basic authentication requests that resulted in successful authentication.
Authentication failed.	The number of basic authentication requests that resulted in authentication failure.
Basic authentication request errors	The number of basic authentication process errors.
	<b>Performance counters</b>
Kerberos - Average time per transaction	The average time, in milliseconds, to complete a Kerberos transaction.



Statistic	Description
NTLM - Average time per transaction	The average time, in milliseconds, to complete a NTLM transaction.
Basic - Average time per transaction	The average time, in milliseconds, to complete a basic transaction.
Average helper latency per transaction	The average time for Samba to process an authentication request.
Time authentication spent offline	<p>The time, in seconds, that Content Gateway was unable to perform NTLM authentication due to service or connectivity failures. (This measure does not apply to Kerberos because no communication with the DC is needed.)</p> <p>If the Global Fail Open option is enabled, proxy requests proceed without authentication.</p> <p>The counter is incremented when connectivity is reestablished after a failure.</p>
Number of times authentication servers or services went offline	The number of times that connectivity with authentication servers or services has been lost.

## LDAP

Statistic	Description
	<b>Cache</b>
Hits	Number of hits in the LDAP cache.
Misses	Number of misses in the LDAP cache.
	<b>Errors</b>
Server	Number of LDAP server errors.
	<b>Unsuccessful Authentications</b>
Authorization Denied	Number of times the LDAP Server denied authorization.
Authorization Timeouts	Number of times authorization timed out.
Authentication Cancelled	<p>Number of times authentication was terminated after LDAP authentication was started and before it was completed.</p> <p><b>Note:</b> This does <b>not</b> count the number of times that an authentication request was cancelled by the client by clicking “Cancel” in the dialog box that prompts for credentials.</p>

## Legacy NTLM

Statistic	Description
	<b>Cache</b>
Hits	Number of hits in the NTLM cache.
Misses	Number of misses in the NTLM cache.
	<b>Errors</b>
Server	Number of NTLM server errors.
	<b>Unsuccessful Authentications</b>
Authorization Denied	Number of times the NTLM server denied authorization.
Authentication Cancelled	Number of times authentication was cancelled.
Authentication Rejected	Number of times authentication failed because the queue was full.
	<b>Queue Size</b>
Authentication Queued	Number of requests that are currently queued because all of the domain controllers are busy.

## SOCKS

Statistic	Description
Unsuccessful Connections	Number of unsuccessful connections to the SOCKS server since Content Gateway was started.
Successful Connections	Number of successful connections to the SOCKS server since Content Gateway was started.
Connections in Progress	Number of connections to the SOCKS server currently in progress.

## Data Security

Statistic	Description
Total Posts	Total number of posts sent to Data Security.
Total Analyzed	Total number of posts analyzed by Data Security.
FTP Analyzed	Total number of FTP requests analyzed by Data Security.

Statistic	Description
Blocked Requests	Total number of requests blocked after analysis and policy enforcement.
Allowed Requests	Total number of requests allowed after analysis and policy enforcement.
Failed Requests	Total number of posts sent to Data Security that timed out or otherwise failed to complete.
Huge Requests	Total number of requests that exceeded the maximum transaction size.
Tiny Requests	Total number of requests that were smaller than the minimum transaction size.
Decrypted Requests	Total number of SSL requests decrypted and sent to Data Security.

## Subsystems

Subsystems statistics are divided into the following categories:

- ◆ [Cache](#) , page 229
- ◆ [Clustering](#), page 230
- ◆ [Logging](#), page 231

## Cache



### Note

Cache statistics may be non-zero even if all content sent to Content Gateway is not cacheable. Content Gateway performs a cache-read even if the client sends a no-cache control header.

Statistic	Description
	<b>General</b>
Bytes Used	Number of bytes currently used by the cache.
Cache Size	Number of bytes allocated to the cache.
	<b>Ram Cache</b>
Bytes	Total size of the RAM cache, in bytes.
Hits	Number of document hits from the RAM cache.
Misses	Number of document misses from the RAM cache. The documents may be hits from the cache disk.

Statistic	Description
	<b>Reads</b>
In Progress	Number of cache reads in progress (HTTP and FTP).
Hits	Number of cache reads completed since Content Gateway was started (HTTP and FTP).
Misses	Number of cache read misses since Content Gateway was started (HTTP and FTP).
	<b>Writes</b>
In Progress	Number of cache writes in progress (HTTP and FTP).
Successes	Number of successful cache writes since Content Gateway was started (HTTP and FTP).
Failures	Number of failed cache writes since Content Gateway was started (HTTP and FTP).
	<b>Updates</b>
In Progress	Number of HTTP document updates in progress. An update occurs when the Content Gateway revalidates an object, finds it to be fresh, and updates the object header.
Successes	Number of successful cache HTTP updates completed since Content Gateway was started.
Failures	Number of cache HTTP update failures since Content Gateway was started.
	<b>Removes</b>
In Progress	Number of document removes in progress. A remove occurs when the Content Gateway revalidates a document, finds it to be deleted on the origin server, and deletes it from the cache (includes HTTP and FTP removes).
Successes	Number of successful cache removes completed since Content Gateway was started (includes HTTP and FTP removes).
Failures	Number of cache remove failures since Content Gateway was started (includes HTTP and FTP removes).

## Clustering

Statistic	Description
Clustering Nodes	Number of clustering nodes.

## Logging

Statistic	Description
Currently Open Log Files	Number of event log files (formats) that are currently being written.
Space Used for Log Files	Current amount of space being used by the logging directory, which contains all of the event and error logs.
Number of Access Events Logged	Number of access events that have been written to log files since Content Gateway installation. This counter represents one entry in one file. If multiple formats are being written, a single access creates multiple event log entries.
Number of Access Events Skipped	Number of access events skipped (because they were filtered out) since Content Gateway installation.
Number of Error Events Logged	Number of access events that have been written to the event error log since Content Gateway installation.

## Networking

Networking statistics are divided into the following categories:

- ◆ [System](#), page 231
- ◆ [ARM](#), page 232
- ◆ [ICAP](#), page 233
- ◆ [WCCP](#), page 233
- ◆ [DNS Resolver](#), page 235
- ◆ [Virtual IP](#), page 235

## System

Statistic/Field	Description
	<b>General</b>
Hostname	The hostname assigned to this Content Gateway machine.
Default Gateway	IP address of the default gateway used to forward packets from this Content Gateway machine to other networks or subnets.
Search Domain	Search domain that this Content Gateway machine uses.
Primary DNS	IP address of the primary DNS server that this Content Gateway machine uses to resolve host names.

Statistic/Field	Description
Secondary DNS	Secondary DNS server that this Content Gateway machine uses to resolve host names.
Tertiary DNS	Third DNS server that this Content Gateway machine uses to resolve host names.
	<b>NIC &lt;interface_name&gt;</b>
Status	Indicates whether the NIC is up or down.
Start on Boot	Indicates whether the NIC is configured to start on boot.
IP address	The assigned IP address of the NIC.
Netmask	The netmask that goes with the IP address.
Gateway	The configured default gateway IP address for the NIC.

## ARM

Statistic	Description
	<b>Network Address Translation (NAT) Statistics</b>
Client Connections Natted	Number of client connections redirected transparently by the ARM.
Client Connections in Progress	Number of client connections currently in progress with the ARM.
Total Packets Natted	Number of packets translated by the ARM.
DNS Packets Natted	Number of DNS packets translated by the ARM.
	<b>Bypass Statistics</b>
Total Connections Bypassed	Total number of connections bypassed by the ARM.
Connections Dynamically Bypassed	Total number of connections dynamically bypassed. See <a href="#">Dynamic bypass rules</a> , page 62.
DNS Packets Bypassed	Number of DNS packets bypassed by the ARM.
Connections Shed	Total number of connections shed. See <a href="#">Connection load shedding</a> , page 64.
	<b>HTTP Bypass Statistics</b>
Bypass on Bad Client Request	Number of requests forwarded directly to the origin server because Content Gateway encountered non-HTTP traffic on port 80.
Bypass on 400	Number of requests forwarded directly to the origin server because an origin server returned a 400 error.
Bypass on 401	Number of requests forwarded directly to the origin server because an origin server returned a 401 error.

Statistic	Description
Bypass on 403	Number of requests forwarded directly to the origin server because an origin server returned a 403 error.
Bypass on 405	Number of requests forwarded directly to the origin server because an origin server returned a 405 error.
Bypass on 406	Number of requests forwarded directly to the origin server because an origin server returned a 406 error.
Bypass on 408	Number of requests forwarded directly to the origin server because an origin server returned a 408 error.
Bypass on 500	Number of requests forwarded directly to the origin server because an origin server returned a 500 error.

## ICAP

Statistic	Description
Total Posts	Total number of posts sent to Data Security.
Total Analyzed	Total number of posts analyzed by Data Security.
FTP Analyzed	Total number of FTP requests analyzed by Data Security.
Blocked Requests	Total number of requests blocked after analysis and policy enforcement.
Allowed Requests	Total number of requests allowed after analysis and policy enforcement.
Failed Requests	Total number of posts sent to Data Security that timed out or otherwise failed to complete.
Huge Requests	Total number of requests that exceeded the maximum transaction size.
Decrypted Requests	Total number of SSL requests decrypted and sent to Data Security.

## WCCP

WCCP v2 statistics are displayed only if WCCP version v2 is enabled.

Statistic/Field	Description
	<b>WCCP v2.0 Statistics</b>
<b>WCCP Fragmentation</b>	
Total Fragments	Total number of WCCP fragments.
Fragmentation Table Entries	Number of entries in the fragmentation table.

Statistic/Field	Description
Out of Order Fragments	Number of fragments out of order.
Matches	Number of fragments that match a fragment in the fragmentation table.
<b>Service group name</b>	
Service Group ID	Service Group ID for the protocol being serviced.
Configured mode	The forward, return and assignment settings.
IP Address	IP address to which the router is sending traffic.
Leader's IP Address	IP address of the leader in the WCCP cache farm.
Number of Buckets Assigned	Number of buckets assigned to this Content Gateway node. Determined by the value of Weight and the current active nodes.
Number of Caches	The number of caches in the WCCP cache farm.
Number of Routers	The number of routers sending traffic to this Content Gateway node.
Router IP Address	<p>IP address of the WCCP router sending traffic to Content Gateway.</p> <p><b>Note:</b> If the WCCP router is configured with multiple IP addresses, as for example when the router is configured to support multiple VLANs, the IP address reported in <b>Monitor &gt; Networking &gt; WCCP</b> statistics, and in packet captures, may differ from the IP address configured here. This is because the router always reports traffic on the highest active IP address.</p> <p>One way to get the router to always report the same IP address is to set the router's loopback address to a value higher than the router's highest IP address, then the loopback address is always reported as the router's IP address. This is the recommended configuration.</p>
Router ID Received	The number of times that Content Gateway has received WCCP protocol messages from the router(s).
Router Negotiated mode	The return, forward, and assignment modes negotiated with the router.



## DNS Proxy

Statistic	Description
Total Requests	Total number of DNS requests received from clients.
Hits	Number of DNS cache hits.
Misses	Number of DNS cache misses.

## DNS Resolver

Statistic	Description
	<b>DNS Resolver</b>
Total Lookups	Total number of DNS lookups (queries to name servers) since installation.
Successes	Total number of successful DNS lookups since installation.
Average Lookup Time (ms)	Average DNS lookup time.
	<b>Host Database</b>
Total Lookups	Total number of lookups in the Content Gateway host database since installation.
Total Hits	Total number of host database lookup hits since installation.
Average TTL (min)	Average time to live in minutes.

## Virtual IP

The Virtual IP table displays the virtual IP addresses that are managed by the proxies in the cluster.

## Performance

Performance graphs allow you to monitor Websense Content Gateway performance and analyze network traffic. Performance graphs also provide information about virtual memory usage, client connections, document hit rates, hit and miss rates, and so on. Performance graphs are created by the Multi Router Traffic Grapher tool (MRTG). MRTG uses 5-minute intervals to accumulate statistics.

Performance graphs provide the following information.

Statistic	Description
Overview	Displays a subset of the graphs available.
Daily	Displays graphs that provide historical information for the current day.
Weekly	Displays graphs that provide historical information for the current week.
Monthly	Displays graphs that provide historical information for the current month.
Yearly	Displays graphs that provide historical information for the current year.

**Important**

To run the Multi Router Traffic Grapher tool in Linux, you must have Perl version 5.005 or later installed on your Content Gateway system.

---

A description is given adjacent to each graph. Click on a graph to get the daily, weekly, monthly, and yearly on a single screen.

These graphs are produced, sorted alphabetically:

- Active Client Connections
- Active Native FTP Client Connections
- Active Origin Server Connections
- Active Parent Proxy Connections
- Bandwidth Savings
- Cache Read
- Cache Reads Per Second
- Cache Writes
- Cache Writes Per Second
- Client Transactions Per Second
- Content Gateway Manager Memory Usage
- Content Gateway Uptime
- CPU Available
- CPU Busy
- Data Security Module Memory Usage
- Disk Cache Usage
- DNS Cache Usage

- HTTP Abort Latency
- HTTP and HTTPS Transactions Per Second
- HTTP Cache Hit Latency
- HTTP Cache Miss Latency
- HTTP Connection Errors & Aborts (Count)
- HTTP Connection Errors & Aborts (Percentage)
- HTTP Document Hit Rate
- HTTP Error Latency
- HTTP Hits & Misses (Count)
- HTTP Hits & Misses (Percentage)
- HTTP POST and FTP PUT Transactions Per Second
- Microsoft Internet Explorer Browser Requests (Percentage)
- MRTG Runtime
- Network Reads
- Network Writes
- RAM Cache Read I/O Hit Rate
- RAM Cache Usage
- SSL Manager Memory Usage
- TCP CLOSE\_WAIT Connections
- TCP Connect Rate
- TCP ESTABLISHED Connections
- TCP FIN\_WAIT\_1 Connections
- TCP FIN\_WAIT\_2 Connections
- TCP LAST\_ACK Connections
- TCP Segments Transmitted
- TCP Throughput
- TCP TIME\_WAIT Connections
- Transaction Buffer Memory Usage
- WCCP Exceptional Input Fragments
- WCCP Fragment Table Size
- WCCP Input Fragments
- Web Security Scanned Transactions (Percentage)
- Web Security Slow Scanned Transactions
- Web Security Slow Transactions
- Websense Content Gateway Memory Usage

## SSL

The following tabs are supported by SSL Manager:

[SSL Key Data](#), page 238

[CRL Statistics](#), page 239

[Reports](#), page 239

### SSL Key Data

These fields provide information about the status of the SSL connection and activity between the client and SSL Manager and SSL Manager and the destination server.

Statistic/Field	Description
<b>SSL Inbound Key Data</b>	
Is alive	Online indicates that SSL Manager is enabled
Current SSL connections	Number of active inbound (browser to SSL Manager) SSL requests
Total SSL server connections	Number of browser requests
Total finished SSL server connections	Number of browser requests where data went to SSL Manager for decryption
Total SSL server renegotiation requests	Number of browser requests renegotiated due to handshake failures or invalid certificates between the browser and SSL Manager
<b>SSL Outbound Key Data</b>	
Is alive	Online indicates that SSL Manager is enabled
Current SSL connections	Number of active outbound (SSL Manager to designating server) SSL requests
Total SSL client connections	Number of browser requests
Total finished SSL client connections	Number of requests where data went from SSL Manager to the destination server
Total SSL client renegotiation requests	Number of requests were renegotiated due to handshake failures or invalid certificates between SSL Manager and the destination server
Total SSL session cache hits	Number of times that a request was validated by a key in the session cache
Total SSL session cache misses	Number of times that a request could not be validated by a key in the session cache
Total SSL session cache timeouts	Number of time keys were removed from the session cache because the timeout period expired

## CRL Statistics

These fields provide information about certificate status.

Statistic/Field	Description
	<b>CRL Statistics</b>
CRL list count	The number of certificates on the Certificate Revocation List. This list is downloaded every night. See <a href="#">Keeping revocation information up to date</a> , page 141.
	<b>OCSP Statistics</b>
OCSP good count	The number of responses that certificates are valid.
OCSP unknown count	The number of OCSP responses where the certificate cannot be verified.
OCSP revoked count	The number of certificates found to have been revoked (CRL & OCSP)

## Reports

See [Creating reports with SSL Manager](#), page 110 for information on creating reports on certificate authorities or incidents.



# B

## Commands and Variables

### Websense Content Gateway commands

---

Use the command line to execute individual commands and when scripting multiple commands in a shell.

To run commands, become root:

```
su
```

Execute Content Gateway commands from the Content Gateway **bin** directory.



#### Note

If the Content Gateway **bin** directory is not in your path, prepend the command with:

```
./
```

For example:

```
./content_line -p
```

Command	Description
WCGAdmin start	Starts the Content Gateway service
WCGAdmin stop	Stops the Content Gateway service
WCGAdmin restart	Stops the Content Gateway service and then starts it again
WCGAdmin status	Displays the status (running or not running) of the Content Gateway services: Content Gateway, Content Gateway Manager, and <b>content_cop</b> .
WCGAdmin help	Displays a list of the WCGAdmin commands
content_line -p socket_path	Specifies the location (directory and path) of the file used for Content Gateway command line and Content Gateway Manager communication. The default path is <b>install_dir/config/cli</b>

Command	Description
<code>content_line -r variable</code>	Displays specific performance statistics or a current configuration setting. For a list of the variables you can specify, see <a href="#">Websense Content Gateway variables</a> , page 242.
<code>content_line -s variable -v value</code>	Sets configuration variables. <i>variable</i> is the configuration variable you want to change and <i>value</i> is the value you want to set. See <a href="#">records.config</a> , page 347, for a list of the configuration variables you can specify.
<code>content_line -h</code>	Displays the list of Content Gateway commands.
<code>content_line -x</code>	Initiates a Content Gateway configuration file reread. Executing this command is similar to clicking <b>Apply</b> in Content Gateway Manager.
<code>content_line -M</code>	Restarts the <b>content_manager</b> process and the <b>content_gateway</b> process on all the nodes in a cluster.
<code>content_line -L</code>	Restarts the <b>content_manager</b> process and the <b>content_gateway</b> process on the local node.
<code>content_line -S</code>	Shuts down Content Gateway on the local node.
<code>content_line -U</code>	Starts Content Gateway on the local node.
<code>content_line -B</code>	Bounces Content Gateway cluster-wide. Bouncing Content Gateway shuts down and immediately restarts the proxy cache node-by-node.
<code>content_line -b</code>	Bounces Content Gateway on the local node. Bouncing Content Gateway shuts down and immediately restarts the proxy cache on the local node.

## Websense Content Gateway variables

You can change the value of a specific configuration variable on the command line with the **content\_line -s** command. The variables that can be set are described in [records.config](#), page 347.

You can view statistics related to specific variables on the command line with the **content\_line -r** command. See below for a list of variables.

See, also, [Viewing statistics from the command line](#), page 106, and [Command-line interface](#), page 99.

## Statistics

The following table lists the variables you can specify on the command line to view individual statistics. See [Statistics](#), page 219 for additional information.

To view a statistic, at the prompt enter:



```
content_line -r variable
```

Statistic	Variable
	<b>Summary</b>
Node name	<i>proxy.node.hostname</i>
Objects served	<i>proxy.node.user_agents_total_documents_served</i>
Transactions per second	<i>proxy.node.user_agent_xacts_per_second</i>
	<b>Node</b>
Document hit rate	<i>proxy.node.cache_hit_ratio_avg_10s</i> <i>proxy.cluster.cache_hit_ratio_avg_10s</i>
Bandwidth savings	<i>proxy.node.bandwidth_hit_ratio_avg_10s</i> <i>proxy.cluster.bandwidth_hit_ratio_avg_10s</i>
Cache percent free	<i>proxy.node.cache.percent_free</i> <i>proxy.cluster.cache.percent_free</i>
Open origin server connections	<i>proxy.node.current_server_connections</i> <i>proxy.cluster.current_server_connections</i>
Open client connections	<i>proxy.node.current_client_connections</i> <i>proxy.cluster.current_client_connections</i>
Cache transfers in progress	<i>proxy.node.current_cache_connections</i> <i>proxy.cluster.current_cache_connections</i>
Client throughput (Mbits/sec)	<i>proxy.node.client_throughput_out</i> <i>proxy.cluster.client_throughput_out</i>
Transactions per second	<i>proxy.node.http.user_agent_xacts_per_second</i> <i>proxy.cluster.http.user_agent_xacts_per_second</i>
DNS lookups per second	<i>proxy.node.dns.lookups_per_second</i> <i>proxy.cluster.dns.lookups_per_second</i>
Host database hit rate	<i>proxy.node.hostdb.hit_ratio_avg_10s</i> <i>proxy.cluster.hostdb.hit_ratio_avg_10s</i>
	<b>HTTP</b>
Total document bytes from client	<i>proxy.process.http.user_agent_response_document_total_size</i>
Total header bytes from client	<i>proxy.process.http.user_agent_response_header_total_size</i>
Total connections to client	<i>proxy.process.http.current_client_connections</i>
Client transactions in progress	<i>proxy.process.http.current_client_transactions</i>
Total document bytes from origin server	<i>proxy.process.http.origin_server_response_document_total_size</i>

Statistic	Variable
Total header bytes from origin server	<i>proxy.process.http.origin_server_response_header_total_size</i>
Total connections to origin server	<i>proxy.process.http.current_server_connections</i>
Origin server transactions in progress	<i>proxy.process.http.current_server_transactions</i>
	<b>FTP</b>
Currently open FTP connections	<i>proxy.process.ftp.connections_currently_open</i>
Successful PASV connections	<i>proxy.process.ftp.connections_successful_pasv</i>
Unsuccessful PASV connections	<i>proxy.process.ftp.connections_failed_pasv</i>
Successful PORT connections	<i>proxy.process.ftp.connections_successful_port</i>
Unsuccessful PORT connections	<i>proxy.process.ftp.connections_failed_port</i>
	<b>WCCP</b>
WCCP router's IP address	<i>proxy.node.wccp.router_ip</i>
WCCP router status	<i>proxy.node.wccp.router_status</i>
WCCP node IP address	<i>proxy.node.wccp.my_ip</i>
Percentage of WCCP traffic received	<i>proxy.node.wccp.my_share</i>
Number of WCCP heartbeats	<i>proxy.node.wccp.hbeats_received</i>
Enabled	<i>proxy.node.wccp.enabled</i>
WCCP leader's IP address	<i>proxy.node.wccp.leader_ip</i>
Number of active WCCP nodes	<i>proxy.node.wccp.number_of_caches_up</i>
	<b>Cache</b>
Bytes used	<i>proxy.process.cache.bytes_used</i>
Cache size	<i>proxy.process.cache.bytes_total</i>
Lookups in progress	<i>proxy.process.cache.lookup.active</i>
Lookups completed	<i>proxy.process.cache.lookup.success</i>
Lookup misses	<i>proxy.process.cache.lookup.failure</i>

<b>Statistic</b>	<b>Variable</b>
Reads in progress	<i>proxy.process.cache.read.active</i>
Reads completed	<i>proxy.process.cache.read.success</i>
Read misses	<i>proxy.process.cache.read.failure</i>
Writes in progress	<i>proxy.process.cache.write.active</i>
Writes completed	<i>proxy.process.cache.write.success</i>
Write failures	<i>proxy.process.cache.write.failure</i>
Updates in progress	<i>proxy.process.cache.update.active</i>
Updates completed	<i>proxy.process.cache.update.success</i>
Update failures	<i>proxy.process.cache.update.failure</i>
Removes in progress	<i>proxy.process.cache.remove.active</i>
Remove successes	<i>proxy.process.cache.remove.success</i>
Remove failures	<i>proxy.process.cache.remove.failure</i>
	<b>Host DB</b>
Total lookups	<i>proxy.process.hostdb.total_lookups</i>
Total hits	<i>proxy.process.hostdb.total_hits</i>
Time TTL (min)	<i>proxy.process.hostdb.ttl</i>
	<b>DNS</b>
DNS total lookups	<i>proxy.process.dns.total_dns_lookups</i>
Average lookup time (ms)	<i>proxy.process.dns.lookup_avg_time</i>
DNS successes	<i>proxy.process.dns.lookup_successes</i>
	<b>Cluster</b>
Bytes read	<i>proxy.process.cluster.read_bytes</i>
Bytes written	<i>proxy.process.cluster.write_bytes</i>
Connections open	<i>proxy.process.cluster.connections_open</i>
Total operations	<i>proxy.process.cluster.connections_opened</i>
Network backups	<i>proxy.process.cluster.net_backup</i>
Clustering nodes	<i>proxy.process.cluster.nodes</i>
	<b>SOCKS</b>
Unsuccessful connections	<i>proxy.process.socks.connections_unsuccessful</i>
Successful connections	<i>proxy.process.socks.connections_successful</i>
Connections in progress	<i>proxy.process.socks.connections_currently_open</i>

Statistic	Variable
	<b>Logging</b>
Currently open log files	<i>proxy.process.log2.log_files_open</i>
Space used for log files	<i>proxy.process.log2.log_files_space_used</i>
Number of access events logged	<i>proxy.process.log2.event_log_access</i>
Number of access events skipped	<i>proxy.process.log2.event_log_access_skip</i>
Number of error events logged	<i>proxy.process.log2.event_log_error</i>

# C

## Configuration Options

The following configuration options are available on the Content Gateway Manager Configure pane:

[My Proxy](#), page 247

[Protocols](#), page 257

[Content Routing](#), page 270

[Security](#), page 275

[Subsystems](#), page 289

[Networking](#), page 294

### My Proxy

---

The My Proxy configuration options are divided into the following categories:

[Basic](#), page 248

[Subscription](#), page 252

[UI Setup](#), page 252

[Snapshots](#), page 255

[Logs](#), page 256

## Basic

When you set these options, ensure that each option is running on a unique port.

Option	Description
	<b>General</b>
Restart	Restarts the proxy and manager services (the <b>content_gateway</b> and <b>content_manager</b> processes). You must restart the proxy and manager services after modifying certain configuration options. In a cluster configuration, the <b>Restart</b> button restarts the proxy and manager services on all the nodes in the cluster.
Proxy Name	Specifies the name of your Content Gateway node (by default, this is the hostname of the machine running Content Gateway). If this node is part of a cluster, this option specifies the name of the Content Gateway cluster (in a Content Gateway cluster, all nodes must share the same name).
Alarm email	Specifies the email address to which Content Gateway sends alarm notifications.
	<b>Features</b>
Protocols: FTP	Enables or disables processing of FTP requests from FTP clients. When this option is enabled, Content Gateway accepts FTP requests from FTP clients. When this option is disabled, Content Gateway does not accept FTP requests from FTP clients. If you change this option, you must restart Content Gateway.
Protocols: HTTPS	Enable or disable processing of HTTPS requests (encrypted data) using SSL Manager. After selecting <b>HTTPS On</b> , you must provide additional information on the <b>Configure &gt; Protocols &gt; HTTPS</b> page and on the <b>Configure &gt; SSL</b> pages. See <a href="#">Working With Encrypted Data</a> , page 121.
Networking: ARM	Enables or disables the ARM. If you change this option, you must restart Content Gateway. See <a href="#">Enabling the ARM</a> , page 44.
Networking: WCCP	Enable this option if you are using a WCCP v2-enabled router for transparent redirection to Content Gateway. WCCP v1 is <b>not</b> supported. See <a href="#">Transparent interception with WCCP v2 devices</a> , page 46. If you change this option, you must restart Content Gateway.
Networking: DNS Proxy	Enables or disables the DNS proxy caching option. When enabled, Content Gateway resolves DNS requests on behalf of clients. This option offloads remote DNS servers and reduces response time for DNS lookups. See <a href="#">DNS Proxy Caching</a> , page 91.

Option	Description
Networking: Virtual IP	Enables or disables the virtual IP failover option. When this option is enabled, Content Gateway maintains a pool of virtual IP addresses that it assigns to the nodes in a cluster as necessary. See <a href="#">Virtual IP failover</a> , page 74.
Networking: Data Security	Enables a connection to Websense Data Security. There are 2 options: <ul style="list-style-type: none"> <li>Registration with a Data Security Management Server for use with a co-located Data Security policy engine (must be version 7.5 or later)</li> <li>ICAP communication to a remote Data Security Suite deployment (may be version 7.1, or earlier)</li> </ul> See <a href="#">Working With Websense Data Security</a> , page 113. If you change this option, you must restart Content Gateway.
Networking: Data Security: Integrated on-box	Enables registration with a Data Security Management Server for use with a co-located Data Security policy engine. See <a href="#">Registering and configuring on-box Data Security</a> , page 115.
Networking: Data Security: ICAP	Enables ICAP for use with Data Security Suite. See <a href="#">Configuring the ICAP client</a> , page 117.
Security: SOCKS	Enables or disables the SOCKS option. When SOCKS is enabled, Content Gateway can talk to your SOCKS servers. See <a href="#">Configuring the proxy to use a SOCKS firewall</a> , page 159. If you change this option, you must restart Content Gateway.
Authentication: None	The proxy will not perform user authentication. This is the default setting.
Authentication: Integrated Windows Authentication	Enables or disables Integrated Windows Authentication (IWA). When IWA is enabled, users are authenticated by IWA before they are allowed access to content. See <a href="#">Integrated Windows Authentication</a> , page 166. If you change this option, you must restart Content Gateway.
Authentication: LDAP	Enables or disables LDAP proxy authentication. When LDAP is enabled, you can ensure that users are authenticated by an LDAP server before accessing content from the cache. See <a href="#">LDAP authentication</a> , page 173. If you change this option, you must restart Content Gateway.

Option	Description
Authentication: Radius	<p>Enables or disables RADIUS proxy authentication. When RADIUS is enabled, you can ensure that users are authenticated by a RADIUS server before accessing content from the cache. See <a href="#">RADIUS authentication</a>, page 176.</p> <p>If you change this option, you must restart Content Gateway.</p>
Authentication: Legacy NTLM	<p>Enables or disables legacy NTLM (NTLMSSP) user authentication. When legacy NTLM is enabled, users in a Windows network are authenticated by a Domain Controller before accessing content.</p> <p>See <a href="#">Legacy NTLM authentication</a>, page 171.</p> <p>If you change this option, you must restart Content Gateway.</p>
Authentication: Multiple Realm Authentication	<p>Enables or disables multiple realm authentication. Multiple realm authentication supports environments that have multiple domains that do not share trust relationships, thus requiring that specific users be authenticated by specific domain controllers.</p> <p>See <a href="#">Multiple realm authentication</a>, page 179.</p> <p>If you change this option, you must restart Content Gateway.</p>
Authentication: Read authentication from child proxy	<p>Enables or disables the reading of X-Authenticated-User and X-Forwarded-For header values in incoming requests. This option is disabled by default.</p> <p>Enable this option when Content Gateway is the parent (upstream) proxy in a chain and the child (downstream) proxy is sending X-Authenticated-User and X-Forwarded-For header values to facilitate authentication.</p>
Authentication: Send authentication to parent proxy	<p>Enables or disables the insertion of X-Authenticated-User header values in outgoing requests. This option is disabled by default.</p> <p>Enable this option when Content Gateway is the child (downstream) proxy in a chain and the parent (upstream) proxy wants X-Authenticated-User values to facilitate authentication.</p>



Option	Description
	<b>Clustering</b>
Cluster: Type	<p>Specifies the clustering mode:</p> <p>Select <b>Single Node</b> to run this Content Gateway server as a single node. This node will not be part of a cluster.</p> <p>Select <b>Management Clustering</b> to activate management clustering mode. The nodes in the cluster share configuration information and you can administer all the nodes at the same time.</p> <p>For complete information about clustering, see <a href="#">Clusters, page 69</a>.</p> <p>If you change this option, you must restart Content Gateway.</p>
Cluster: Interface	<p>Specifies the interface on which Content Gateway communicates with other nodes in the cluster. For example, <b>eth0</b>.</p> <p>It is recommended that you use a dedicated secondary interface.</p> <p>Node configuration information is multicast, in plain text, to other Content Gateway nodes on the same subnet. Therefore, Websense recommends that clients be located on a separate subnet from Content Gateway nodes (multicast communications for clustering are not routed).</p> <p>On V-Series appliances, P1 (eth0) is the recommended interface. However, you may also use P2 (eth1) if you want to isolate cluster management traffic.</p> <p>See <a href="#">Changing clustering configuration, page 72</a>.</p> <p>If you change this option, you must restart Content Gateway.</p>
Cluster: Multicast Group Address	<p>Specifies the multicast group address on which Content Gateway communicates with its cluster peers.</p> <p>See <a href="#">Changing clustering configuration, page 72</a>.</p>
Cluster: SSL Manager Configuration Server	<p>Specifies the IP address of the SSL Manager Configuration Server. When Content Gateway is restarted, the SSL Manager Configuration Server (primary) is identified to all members of the cluster. All SSL configuration changes must be made on the primary. See <a href="#">SSL Manager clustering, page 70</a>.</p>

## Subscription

Option	Description
	<b>Subscription Management</b>
Subscription Key	Displays the subscription key you received from Websense. This key reflects the products you have purchased. If Content Gateway is used with Web Security Gateway or Web Security Gateway Anywhere, this is the subscription key you entered in TRITON – Web Security. If Content Gateway is deployed with only Websense Data Security Suite, you must enter your Content Gateway subscription key in this field.
	<b>Scanning</b>
<b>Policy Server</b>	
IP address	Specify the IP address of the Websense Web Security Policy Server.
Port	Specify the port used by the Websense Web Security Policy Server.
<b>Filtering Service</b>	
IP address	Specify the IP address of the Websense Web Security Filtering Service.
Port	Specify the port used by the Websense Web Security Filtering Service.
<b>Action for Communication Errors</b>	
Permit traffic	Permits all pages if communication with Policy Server or Filtering Service fails.
Block traffic	Blocks all pages if communication with Policy Server or Filtering Service fails.

## UI Setup

Option	Description
	<b>General</b>
UI Port	Specifies the port on which browsers can connect to Content Gateway Manager. The port must be on the Content Gateway system and it must be dedicated to Content Gateway use. The default port is 8081.  If you change this setting, you must restart Content Gateway.

Option	Description
SSL UI Port	<p>Specifies for port for the SSL Manager user interface. Through this interface you can specify data decryption and certificate management. The default port is 8071. See <a href="#">Working With Encrypted Data</a>, page 121.</p> <p>The Content Gateway Manager interface and the SSL Manager interface must be on different ports.</p> <p>If you change this setting, you must restart Content Gateway.</p>
HTTPS: Enable/Disable	<p>Enables or disables support for SSL connections to Content Gateway Manager. SSL provides protection for remote administrative monitoring and configuration. To use SSL for Content Gateway Manager connections, you must install an SSL certificate on the Content Gateway server machine. For more information, see <a href="#">Using SSL for secure administration</a>, page 156.</p>
HTTPS: Certificate File	<p>Specifies the name of the SSL certificate file used to authenticate users who want to access Content Gateway Manager.</p>
Monitor Refresh Rate	<p>Specifies how often Content Gateway Manager refreshes the statistics on the <b>Monitor</b> pane. The default value is 30 seconds.</p>
	<b>Login</b>
Basic Authentication	<p>Enables or disables basic authentication. When this option is enabled, Content Gateway checks the administrator login and password or the user name and password (if user accounts have been configured) whenever a user tries to access Content Gateway Manager.</p>
Administrator: Login	<p>Specifies the administrator login. The administrator login is the master login that has access to both Configure and Monitor mode in Content Gateway Manager.</p> <p>Note: Content Gateway checks the administrator login only if the Basic Authentication option is enabled.</p>

Option	Description
Administrator: Password	<p>Lets you change the administrator password that controls access to Content Gateway Manager.</p> <p>To change the password, enter the current password in the <b>Old Password</b> field, and then enter the new password in the <b>New Password</b> field. Retype the new password in the <b>New Password (Retype)</b> field, and then click <b>Apply</b>.</p> <p>Note: Content Gateway checks the administrator login and password only if the Basic Authentication option is enabled.</p> <p>During installation, you select the administrator password. The installer automatically encrypts the password and stores the encryptions in the <b>records.config</b> file so that no one can read them. Each time you change the password in Content Gateway Manager, Content Gateway updates the <b>records.config</b> file. If you forget the administrator password and cannot access the Content Gateway Manager, see <a href="#">How do you access Content Gateway Manager if you forget the master administrator password?</a>, page 424.</p>
Additional Users	<p>Lists the current user accounts and lets you add new user accounts. User accounts determine who has access Content Gateway Manager and which activities they can perform. You can create a list of user accounts if a single administrator login and password is not sufficient security for your needs.</p> <p>To create a new account, enter the user login in the <b>New User</b> field, and then enter the user password in the <b>New Password</b> field. Retype the user password in the <b>New Password (Retype)</b> field, and then click <b>Apply</b>. Information for the new user is displayed in the table. From the <b>Access</b> drop-down list in the table, select the activities that the new user can perform (Monitor, Monitor and View Configuration, or Monitor and Modify Configuration). For more information about user accounts, see <a href="#">Creating a list of user accounts</a>, page 155.</p> <p>Note: Content Gateway checks the user login and password only if the Basic Authentication option is enabled.</p>
	<b>Access</b>
Access Control	<p>Displays a table listing the rules in the <a href="#">mgmt_allow.config</a> file that specify the remote hosts allowed to access Content Gateway Manager. The entries in this file ensure that only authenticated users can change configuration options and view performance and network traffic statistics.</p> <p>Note: By default, all remote hosts are allowed to access the Content Gateway Manager.</p>
Refresh	<p>Updates the table to display the most up-to-date rules in the <b>mgmt_allow.config</b> file.</p>

Option	Description
Edit File	Opens the configuration file editor so that you can edit and add rules to the <b>mgmt_allow.config</b> file.
	<b>mgmt_allow.config Configuration File Editor</b>
rule display box	Lists the <b>mgmt_allow.config</b> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list. Content Gateway applies the rules in the order listed, starting from the top.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.
IP Action	Lists the type of rules you can add. An <b>ip_allow</b> rule allows the remote hosts specified in the <b>Source IP</b> field to access Content Gateway Manager. An <b>ip_deny</b> rule denies the remote hosts specified in the <b>Source IP</b> field access to Content Gateway Manager.
Source IP	Specifies the IP addresses that are allowed or denied access to Content Gateway Manager. You can enter a single IP address (111.111.11.1) or a range of IP addresses (0.0.0.0-255.255.255.255).
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.

## Snapshots

Option	Description
	<b>File System</b>
Change Snapshot Directory	Specifies the directory in which snapshots are stored on this Content Gateway node.
Snapshots: Save Snapshot	Specifies the name of the configuration snapshot you want to take. Click <b>Apply</b> to save the configuration on the local node. Content Gateway saves the configuration snapshot in the directory specified in the <b>Change Snapshot Directory</b> field.  It is recommended that you take a snapshot before performing system maintenance or attempting to tune system performance. Taking a snapshot takes only a few seconds and can save you hours of correcting configuration mistakes.

Option	Description
Snapshots: Restore/Delete Snapshot	Lists the snapshots that are stored on this node. Select the snapshot that you want to restore or delete from the drop-down list.
Snapshots: Restore Snapshot from “directory_name” Directory	Restores the snapshot selected in the <b>Restore/Delete Snapshot</b> drop-down box. In a cluster configuration, snapshots are restored on all nodes in the cluster.
Snapshots: Delete Snapshot from “directory_name” Directory	Deletes the snapshot selected in the <b>Restore/Delete Snapshot</b> drop-down box.
<b>FTP Server</b>	
FTP Server	Specifies the name of the FTP server from which you want to restore a configuration snapshot or to which you want to save a configuration snapshot.
Login	Specifies the login needed to access the FTP server.
Password	Specifies the password needed to access the FTP server.
Remote Directory	Specifies the directory on the FTP server from which you want restore, or in which you want to save a configuration snapshot.
Restore Snapshot	Lists the configuration snapshots on the FTP server that you can restore. This field appears after you have logged on to the FTP server successfully.
Save Snapshot to FTP Server	Specifies the name of the configuration snapshot you want to take and save on the FTP server. This field appears after you have logged on to the FTP server successfully.

## Logs

Option	Description
	<b>System</b>
Log File	Lists the system log files you can view, delete or copy to your local system. Content Gateway lists the system log files logged with the system-wide logging facility <b>syslog</b> under the daemon facility.
Action: Display the selected log file	When this option is enabled, Content Gateway displays the first MB of the system log file selected in the <b>Log File</b> drop-down list. To view the entire file, select “Save the selected log file in local filesystem” and view the file with a local viewer.

Option	Description
Action: Display last lines of the selected file	When this option is enabled, Content Gateway displays the last specified number of lines in the selected system log file.
Action: Display lines that match in the selected log file	When this option is enabled, Content Gateway displays all the lines in the selected system log file that match the specified string.
Action: Remove the selected log file	When this option is enabled, Content Gateway deletes the selected log file.
Action: Save the selected log file in local filesystem	When this option is enabled, Content Gateway saves the selected log file on the local system in a location you specify.
	<b>Access</b>
Log File	Lists the event or error log files you can view, delete or copy to your local system. Content Gateway lists the event log files located in the directory specified in the <b>Logging Directory</b> field under <b>Subsystems/Logging</b> and by the configuration variable <b>proxy.config.log2.logfile_dir</b> in the <b>records.config</b> file. The default directory is <b>logs</b> in the Content Gateway installation directory.
Action: Display the selected log file	When this option is enabled, Content Gateway displays the first MB of the event or error log file selected in the <b>Log File</b> drop-down list.  To view the entire file, select “Save the selected log file in local filesystem” and view the file with a local viewer.
Action: Display last lines of the selected file	When this option is enabled, Content Gateway displays the last specified number of lines in the event or error log file selected from the <b>Log File</b> drop-down list.
Action: Display lines that match in the selected log file	When this option is enabled, Content Gateway displays all the lines in the selected event or error log file that match the specified string.
Remove the selected log file	When this option is enabled, Content Gateway deletes the selected log file.
Action: Save the selected log file in local filesystem	When this option is enabled, Content Gateway saves the selected log file on the local system in a location you specify.

## Protocols

The Protocol configuration options are divided into the following categories:

[HTTP](#), page 258

[HTTP Responses](#), page 266

[HTTP Scheduled Update](#), page 267

[HTTPS](#), page 268

[FTP](#), page 269

## HTTP

Option	Description
	<b>General</b>
HTTP Proxy Server Port	Specifies the port that Content Gateway uses when acting as a Web proxy server for HTTP traffic or when serving HTTP requests transparently. The default port is 8080.  If you change this option, you must restart Content Gateway.
Secondary HTTP Proxy Server Ports	<b>For explicit proxy configurations</b> only, specifies additional ports on which Content Gateway listens for HTTP traffic.  Transparent proxy configurations always send all HTTP traffic to port 8080.
Unqualified Domain Name Expansion	Enables or disables <b>.com</b> name expansion. When this option is enabled, Content Gateway attempts to resolve unqualified hostnames by redirecting them to the expanded address, prepended with <b>www.</b> and appended with <b>.com</b> . For example, if a client makes a request to <i>company</i> , Content Gateway redirects the request to <b>www.company.com</b> .  If local domain expansion is enabled (see <a href="#">DNS Resolver</a> , page 303), Content Gateway attempts local domain expansion before <b>.com</b> domain expansion; Content Gateway tries <b>.com</b> domain expansion only if local domain expansion fails.
Send HTTP 1.1 by Default	Enables the sending of HTTP 1.1 as the first request to the origin server (the default). If the origin server replies with HTTP 1.0, Content Gateway switches to HTTP 1.0 (most origin servers use HTTP 1.1). When disabled, HTTP 1.0 is used in the first request to the origin server. If the origin server replies with HTTP 1.1, Content Gateway switches to HTTP 1.1.
Reverse DNS	Enables reverse DNS lookup when the URL has an IP address (instead of a hostname) and there are rules in <b>filter.config</b> , <b>cache.config</b> , or <b>parent.config</b> . This is necessary when rules are based on destination hostname and domain name.



Option	Description
Tunnel Ports	<p>Specifies the ports to which Content Gateway allows tunneling. This is a space separated list that also accepts port ranges (e.g. 1-65535).</p> <p>When SSL is not enabled, all traffic destined for the specified ports is allowed to tunnel to an origin server. When SSL is enabled, traffic to any port that is also listed in the HTTPS Ports field is not tunneled, but is decrypted and filtering policy is applied.</p>
HTTPS Ports	<p>Specifies the ports on which traffic is decrypted and policy is applied when SSL is enabled. When SSL is disabled, traffic to these ports is not decrypted, and filtering policy is applied based on:</p> <ul style="list-style-type: none"> <li>• In explicit proxy, the server hostname in the CONNECT request.</li> <li>• In transparent mode, the server hostname in the server's certificate.</li> </ul>
FTP over HTTP: Anonymous Password	<p>Specifies the anonymous password Content Gateway must use for FTP server connections that require a password. This option affects FTP requests from HTTP clients.</p>
FTP over HTTP: Data Connection Mode	<p>An FTP transfer requires two connections: a control connection to inform the FTP server of a request for data and a data connection to send the data. Content Gateway always initiates the control connection. FTP mode determines whether Content Gateway or the FTP server initiates the data connection.</p> <p>Select <b>PASV then PORT</b> for Content Gateway to attempt PASV connection mode first. If PASV mode fails, Content Gateway tries PORT mode and initiates the data connection. If successful, the FTP server accepts the data connection.</p> <p>Select <b>PASV only</b> for Content Gateway to initiate the data connection to the FTP server. This mode is firewall friendly, but some FTP servers do not support it.</p> <p>Select <b>PORT only</b> for the FTP server to initiate the data connection and for Content Gateway to accept the connection.</p> <p>The default value is <b>PASV then PORT</b>.</p>
	<b>Cacheability</b>
Caching: HTTP Caching	<p>Enables or disables HTTP caching. When this option is enabled, Content Gateway serves HTTP requests from the cache. When this option is disabled, Content Gateway acts as a proxy server and forwards all HTTP requests directly to the origin server.</p>

Option	Description
Caching: FTP over HTTP Caching	Enables or disables FTP over HTTP caching. When this option is enabled, Content Gateway serves FTP requests from HTTP clients from the cache. When this option is disabled, Content Gateway acts as a proxy server and forwards all FTP requests from HTTP clients directly to the FTP server.
Behavior: Required Headers	<p>Specifies the minimum header information required for an HTTP object to be cacheable.</p> <p>Select <b>An Explicit Lifetime Header</b> to cache only HTTP objects with <b>Expires</b> or <b>max-age</b> headers.</p> <p>Select <b>A Last-Modified Header</b> to cache only HTTP objects with <b>lastmodified</b> headers.</p> <p>Select <b>No Required Headers</b> to cache HTTP objects that do not have <b>Expires</b>, <b>max-age</b>, or <b>last-modified</b> headers. This is the default option.</p> <p>Caution: By default, Content Gateway caches all objects (including objects with no headers). It is recommended that you change the default setting only for specialized proxy situations. If you configure Content Gateway to cache only HTTP objects with <b>Expires</b> or <b>max-age</b> headers, the cache hit rate is reduced (very few objects have explicit expiration information).</p>
Behavior: When to Revalidate	<p>Specifies how Content Gateway evaluates HTTP object freshness in the cache:</p> <p>Select <b>Never Revalidate</b> to never revalidate HTTP objects in the cache with the origin server (Content Gateway considers all HTTP objects in the cache to be fresh).</p> <p>Select <b>Always Revalidate</b> to always revalidate HTTP objects in the cache with the origin server (Content Gateway considers all HTTP objects in the cache to be stale).</p> <p>Select <b>Revalidate if Heuristic Expiration</b> to verify the freshness of an HTTP object with the origin server if the object contains no <b>Expires</b> or <b>Cache-Control</b> headers; Content Gateway considers all HTTP objects without <b>Expires</b> or <b>Cache-Control</b> headers to be stale.</p> <p>Select <b>Use Cache Directive or Heuristic</b> to verify the freshness of an HTTP object with the origin server when Content Gateway considers the object in the cache to be stale according to object headers, absolute freshness limit, and/or rules in the <b>cache.config</b> file. This is the default option.</p> <p>For more information about revalidation, see <a href="#">Revalidating HTTP objects</a>, page 21.</p>

Option	Description
Behavior: Add “no-cache” to MSIE Requests	<p>Specifies when Content Gateway adds <code>no-cache</code> headers to requests from Microsoft Internet Explorer. Certain versions of Microsoft Internet Explorer do not request cache reloads from transparent caches when the user presses the browser <b>Refresh</b> button. This can prevent content from being loaded directly from the origin servers. You can configure Content Gateway to treat Microsoft Internet Explorer requests more conservatively, providing fresher content at the cost of serving fewer documents from cache.</p> <p>Select <b>To All MSIE Requests</b> to always add <code>no-cache</code> headers to all requests from Microsoft Internet Explorer.</p> <p>Select <b>To IMS MSIE Requests</b> to add <code>no-cache</code> headers to IMS (If Modified Since) Microsoft Internet Explorer requests.</p> <p>Select <b>Not to Any MSIE Requests</b> to never add <code>no-cache</code> headers to requests from Microsoft Internet Explorer.</p>
Behavior: Ignore “no-cache” in Client Requests	<p>When this option is enabled, Content Gateway ignores <code>no-cache</code> headers in client requests and serves the requests from the cache.</p> <p>When this option is disabled, Content Gateway does not serve requests with <code>no-cache</code> headers from the cache but forwards them to the origin server.</p>
Freshness: Minimum Heuristic Lifetime	Specifies the minimum amount of time that an HTTP object can be considered fresh in the cache.
Freshness: Maximum Heuristic Lifetime	Specifies the maximum amount of time that an HTTP object can be considered fresh in the cache.
Freshness: FTP Document Lifetime	Specifies the maximum amount of time that an FTP file can stay in the cache. This option affects FTP requests from HTTP clients only.
Maximum Alternates	<p>Specifies the maximum number of alternate versions of HTTP objects Content Gateway can cache.</p> <p>Caution: If you enter 0 (zero), there is no limit to the number of alternates cached. If a popular URL has thousands of alternates, you might observe increased cache hit latencies (transaction times) as Content Gateway searches over the thousands of alternates for each request. In particular, some URLs can have large numbers of alternates due to cookies. If Content Gateway is set to vary on cookies, you might encounter this problem.</p>
Vary Based on Content Type: Enable/ Disable	Enables or disables caching of alternate versions of HTTP documents that do not contain the <b>Vary</b> header. If no <b>Vary</b> header is present, Content Gateway varies on the headers specified below, depending on the document’s content type.
Vary by Default on Text	Specifies the header field on which Content Gateway varies for text documents.

Option	Description
Vary by Default on Images	Specifies the header field on which Content Gateway varies for images.
Vary by Default on Other Document Types	Specifies the header field on which Content Gateway varies for anything other than text and images.
Dynamic Caching: Caching Documents with Dynamic URLs	<p>When this option is enabled, Content Gateway attempts to cache dynamic content. Content is considered dynamic if it contains a question mark (?), a semicolon (;), <b>cgi</b>, or if it ends in <b>.asp</b>.</p> <p>Caution: It is recommended that you configure Content Gateway to cache dynamic content for specialized proxy situations only.</p>
Dynamic Caching: Caching Response to Cookies	<p>Specifies how responses to requests that contain cookies are cached:</p> <p>Select <b>Cache All but Text</b> to cache cookies that contain any type of content except text. This is the default.</p> <p>Select <b>Cache Only Image Types</b> to cache cookies that contain images only.</p> <p>Select <b>Cache Any Content-Type</b> to cache cookies that contain any type of content.</p> <p>Select <b>No Cache on Cookies</b> to not cache cookies at all.</p>
Caching Policy/Forcing Document Caching	Displays a table listing the rules in the <b>cache.config</b> file that specify how a particular group of URLs should be cached. This file also lets you force caching of certain URLs for a specific amount of time.
Refresh	Updates the table to display the most up-to-date rules in the <b>cache.config</b> file. Click <b>Refresh</b> after you have added or modified rules with the configuration file editor.
Edit File	Opens the configuration file editor so that you can edit and add rules to the <b>cache.config</b> file.
	<b>cache.config Configuration File Editor</b>
Rule display box	Lists the <b>cache.config</b> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.

Option	Description
Rule Type	<p>Lists the type of rules you can add to the <b>cache.config</b> file:</p> <p>A <b>never-cache</b> rule configures Content Gateway to never cache specified objects.</p> <p>An <b>ignore-no-cache</b> rule configures Content Gateway to ignore all <b>Cache-Control: no-cache</b> headers.</p> <p>An <b>ignore-client-no-cache</b> rule configures Content Gateway to ignore <b>Cache-Control: no-cache</b> headers from client requests.</p> <p>An <b>ignore-server-no-cache</b> rule configures Content Gateway to ignore <b>Cache-Control: no-cache</b> headers from origin server responses.</p> <p>A <b>pin-in-cache</b> rule configures Content Gateway to keep objects in the cache for a specified time.</p> <p>A <b>revalidate</b> rule configures Content Gateway to consider objects fresh in the cache for a specified time.</p> <p>A <b>ttl-in-cache</b> rule configures Content Gateway to serve certain HTTP objects from the cache for the amount of time specified in the <b>Time Period</b> field regardless of certain caching directives in the HTTP request and response headers.</p>
Primary Destination Type	<p>Lists the primary destination types:</p> <p><b>dest_domain</b> is a requested domain name.</p> <p><b>dest_host</b> is a requested hostname.</p> <p><b>dest_ip</b> is a requested IP address.</p> <p><b>url_regex</b> is a regular expression to be found in a URL.</p>
Primary Destination Value	<p>Specifies the value of the primary destination type. For example, if the Primary Destination Type is <b>dest_ip</b>, the value for this field can be 123.456.78.9.</p>
Additional Specifier: Time Period	<p>Specifies the amount of time that applies to the <b>revalidate</b>, <b>pin-in-cache</b>, and <b>ttl-in-cache</b> rule types. The following time formats are allowed:</p> <p><b>d</b> for days (for example 2d)</p> <p><b>h</b> for hours (for example, 10h)</p> <p><b>m</b> for minutes (for example, 5m)</p> <p><b>s</b> for seconds (for example, 20s)</p> <p>mixed units (for example, 1h15m20s)</p>
Secondary Specifiers: Time	<p>Specifies a time range, such as 08:00-14:00.</p>
Secondary Specifiers: Prefix	<p>Specifies a prefix in the path part of a URL.</p>
Secondary Specifiers: Suffix	<p>Specifies a file suffix in the URL.</p>
Secondary Specifiers: Source IP	<p>Specifies the IP address of the client.</p>

Option	Description
Secondary Specifiers: Port	Specifies the port in a requested URL.
Secondary Specifiers: Method	Specifies a request URL method.
Secondary Specifiers: Scheme	Specifies the protocol of a requested URL.
Secondary Specifiers: User-Agent	Specifies a request header User-Agent value.
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.
<b>Privacy</b>	
Insert Headers: Client-IP	When enabled, Content Gateway inserts the <b>Client-IP</b> header into outgoing requests to retain the client's IP address.
Insert Headers: Via	When enabled, Content Gateway inserts a <b>Via</b> header into the outgoing request.
Insert Headers: X-Forwarded-For	When enabled, Content Gateway inserts an <b>X-Forwarded-For</b> header into the outgoing request.
Remove Headers: Client-IP	When this option is enabled, Content Gateway removes the <b>Client-IP</b> header from outgoing requests to protect the privacy of your users.
Remove Headers: Cookie	When this option is enabled, Content Gateway removes the <b>Cookie</b> header from outgoing requests to protect the privacy of your users. The <b>Cookie</b> header often identifies the user that makes a request.
Remove Headers: From	When this option is enabled, Content Gateway removes the <b>From</b> header from outgoing requests to protect the privacy of your users. The <b>From</b> header identifies the client's email address.
Remove Headers: Referer	When this option is enabled, Content Gateway removes the <b>Referer</b> header from outgoing requests to protect the privacy of your users. The <b>Referer</b> header identifies the Web link that the client selects.
Remove Headers: User-Agent	When this option is enabled, Content Gateway removes the <b>User-Agent</b> header from outgoing requests to protect the privacy of your users. The <b>User-Agent</b> header identifies the agent that is making the request, usually a browser.
Remove Headers: Remove Others	Specifies headers other than <b>From</b> , <b>Referer</b> , <b>User-Agent</b> , and <b>Cookie</b> , that you want to remove from outgoing requests to protect the privacy of your users.

Option	Description
	<b>Timeouts</b>
Keep-Alive Timeouts: Client	<p>Specifies (in seconds) how long Content Gateway keeps connections to clients open for a subsequent request after a transaction ends. Each time Content Gateway opens a connection to accept a client request, it handles the request and then keeps the connection alive for the specified timeout period. If the client does not make another request before the timeout expires, Content Gateway closes the connection. If the client does make another request, the timeout period starts again.</p> <p>The client can close the connection at any time.</p>
Keep-Alive Timeouts: Origin Server	<p>Specifies (in seconds) how long Content Gateway keeps connections to origin servers open for a subsequent transfer of data after a transaction ends. Each time Content Gateway opens a connection to download data from an origin server, it downloads the data and then keeps the connection alive for the specified timeout period. If Content Gateway does not need to make a subsequent request for data before the timeout expires, it closes the connection. If it does, the timeout period starts again.</p> <p>The origin server can close the connection at any time.</p>
Inactivity Timeouts: Client	<p>Specifies how long Content Gateway keeps connections to clients open if a transaction stalls. If Content Gateway stops receiving data from a client or the client stops reading the data, Content Gateway closes the connection when this timeout expires.</p> <p>The client can close the connection at any time.</p>
Inactivity Timeouts: Origin Server	<p>Specifies how long Content Gateway keeps connections to origin servers open if the transaction stalls. If Content Gateway stops receiving data from an origin server, it does not close the connection until this timeout has expired.</p> <p>The origin server can close the connection at any time.</p>
Active Timeouts: Client	<p>Specifies how long Content Gateway remains connected to a client. If the client does not finish making a request (reading and writing data) before this timeout expires, Content Gateway closes the connection.</p> <p>The default value of 0 (zero) specifies that there is no timeout.</p> <p>The client can close the connection at any time.</p>

Option	Description
Active Timeouts: Origin Server Request	<p>Specifies how long Content Gateway waits for fulfillment of a connection request to an origin server.</p> <p>If Content Gateway does not establish connection to an origin server before the timeout expires, Content Gateway terminates the connection request.</p> <p>The default value of 0 (zero) specifies that there is no timeout.</p> <p>The origin server can close the connection at any time.</p>
Active Timeouts: Origin Server Response	<p>Specifies how long Content Gateway waits for a response from the origin server.</p>
FTP Control Connection Timeout	<p>Specifies how long Content Gateway waits for a response from an FTP server. If the FTP server does not respond within the specified time, Content Gateway abandons the client's request for data. This option affects FTP requests from HTTP clients only.</p> <p>The default value is 300.</p>

## HTTP Responses

Option	Description
	<b>General</b>
Response Suppression Mode	<p>If Content Gateway detects an HTTP problem with a particular client transaction (such as unavailable origin servers, authentication requirements, and protocol errors), it sends an HTML response to the client browser. Content Gateway has a set of hard-coded default response pages that explain each HTTP error in detail to the client.</p> <p>Select <b>Always Suppressed</b> if you do not want to send HTTP responses to clients.</p> <p>Select <b>Intercepted Traffic Only</b> if you want to send HTTP responses to nontransparent traffic only. (This option is useful when Content Gateway is running transparently and you do not want to indicate the presence of a cache.)</p> <p>Select <b>Never Suppressed</b> if you want to send HTTP responses to all clients.</p> <p>If you change this option, you must restart Content Gateway.</p>



Option	Description
	<b>Custom</b>
Custom Responses	<p>You can customize the responses Content Gateway sends to clients. By default, the responses you can customize are located in the Content Gateway <b>config/body_factory/default</b> directory.</p> <p>Select <b>Enabled Language-Targeted Response</b> to send your custom responses to clients in the language specified in the Accept-Language header.</p> <p>Select <b>Enabled in “default” Directory Only</b> to send the custom responses located in the default directory to clients.</p> <p>Select <b>Disabled</b> to disable the custom responses. If <b>Never Suppressed</b> or <b>Intercepted Traffic Only</b> is selected for the <b>Response Suppression Mode</b> option, Content Gateway sends the hard-coded default responses.</p> <p>If you change this option, you must restart Content Gateway.</p>
Custom Response Logging	<p>When enabled, Content Gateway sends a message to the error log each time custom responses are used or modified.</p> <p>If you change this option, you must restart Content Gateway.</p>
Custom Response Template Directory	<p>Specifies the directory where the custom responses are located. The default location is the Content Gateway <b>config/body_factory</b> directory.</p> <p>If you change this option, you must restart Content Gateway.</p>

## HTTP Scheduled Update

Option	Description
	<b>General</b>
Scheduled Update	Enables or disables the scheduled update option. When this option is enabled, Content Gateway can automatically update certain objects in the local cache at a specified time.
Maximum Concurrent Updates	Specifies the maximum number of simultaneous update requests allowed at any point. This option enables you to prevent the scheduled update process from overburdening the host. The default value is 100.
Retry on Update Error: Count	Specifies the number of times Content Gateway retries the scheduled update of a URL in the event of failure. The default value is 10 times.
Retry on Update Error: Interval	Specifies the delay in seconds between each scheduled update retry for a URL in the event of failure. The default value is 2 seconds.

Option	Description
	<b>Update URLs</b>
Force Immediate Update	When enabled, Content Gateway overrides the scheduling expiration time for all scheduled update entries and initiates updates every 25 seconds.
Scheduled Object Update	Displays a table listing the rules in the <a href="#">update.config</a> file that control how Content Gateway performs a scheduled update of specific local cache content.
Refresh	Updates the table to display the most up-to-date rules in the <b>update.config</b> file.
Edit File	Opens the configuration file editor so that you can edit and add rules to the <b>update.config</b> file.
	<b>update.config Configuration File Editor</b>
rule display box	Lists the <b>update.config</b> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.
URL	Specifies the URL to be updated.
Request Headers (Optional)	Specifies the list of headers (separated by semi-colons) passed in each GET request. You can define any request header that conforms to the HTTP specification. The default is no request header.
Offset Hour	Specifies the base hour used to derive the update periods. The range is 00-23 hours.
Interval	The interval, in seconds, at which updates should occur, starting at Offset Hour.
Recursion Depth	The depth to which referenced URLs are recursively updated, starting at the given URL. For example, a recursion depth of 1 will update the given URL, as well as all URLs immediately referenced by links from the original URL.

## HTTPS

Option	Description
	<b>General</b>
HTTPS Proxy Server Port	Specifies the port that Content Gateway uses when acting as a Web proxy server for HTTPS traffic. This is also known as the SSL Inbound Port.

Option	Description
SSL Outbound Port	Specifies the port HTTPS traffic goes to for re-encryption before being sent to its destination. The default is 8090.
Tunnel Skype	<p>Enables/disables the tunneling of Skype traffic when HTTPS (SSL Manager) is enabled and Content Gateway is an explicit proxy.</p> <p><b>To complete the configuration</b>, you must ensure that all users who are allowed to use Skype have a Filtering policy that allows <b>uncategorized</b> and <b>internet telephony</b>. This is required regardless of whether Skype is used with SSL enabled or not.</p> <p>Also, if Skype is not prevented, after the handshake it will route traffic over a non-HTTP port. To force Skype traffic to go through Content Gateway, a GPO should be used, as described in the <a href="#">Skype IT Administrators Guide</a>.</p> <p><b>Note:</b> This option is not necessary if SSL is not enabled.</p> <p><b>Note:</b> This option is not a valid option when Content Gateway is a transparent proxy.</p>

## FTP



### Note

The FTP configuration options appear on the Configure pane only if you have enabled FTP processing in the Features table on the **Configure > My Proxy > Basic > General** tab.

Option	Description
	<b>General</b>
FTP Proxy Server Port	Specifies the port that Content Gateway uses to accept FTP requests. The default port is 2121.
Listening Port Configuration	<p>Specifies how FTP opens a listening port for a data transfer.</p> <p>Select <b>Default Settings</b> to let the operating system choose an available port. Content Gateway sends 0 and retrieves the new port number if the listen succeeds.</p> <p>Select <b>Specify Range</b> if you want the listening port to be determined by the range of ports specified in the <b>Listening Port (Max)</b> and <b>Listening Port (Min)</b> fields.</p>

Option	Description
Default Data Connection Method	Specifies the default method used to set up data connections with the FTP server. Select <b>Proxy Sends PASV</b> to send a PASV to the FTP server and let the FTP server open a listening port. Select <b>Proxy Sends PORT</b> to set up a listening port on the Content Gateway side of the connection first.
Shared Server Connections	When enabled, server control connections can be shared between multiple anonymous FTP clients.
	<b>Timeouts</b>
Keep-Alive Timeout: Server Control	Specifies the timeout value when the FTP server control connection is not used by any FTP clients. The default value is 90 seconds.
Inactivity Timeouts: Client Control	Specifies how long FTP client control connections can remain idle. The default value is 900 seconds.
Inactivity Timeouts: Server Control	Specifies how long the FTP server control connection can remain idle. The default value is 120 seconds.
Active Timeouts: Client Control	Specifies the how long FTP client control connections can remain open. The default value is 14400 seconds.
Active Timeouts: Server Control	Specifies how long the FTP server control connection can remain open. The default value is 14400 seconds.

## Content Routing

---

The Content Routing configuration options are divided into the following categories:

*[Hierarchies](#), page 270*

*[Mapping and Redirection](#), page 273*

*[Browser Auto-Config](#), page 274*

## Hierarchies

Option	Description
	<b>Parenting</b>
Parent Proxy	Enables or disables the HTTP parent caching option. When this option is enabled, Content Gateway can participate in an HTTP cache hierarchy. You can point your Content Gateway server at a parent network cache (either another Content Gateway server or a different caching product) to form a cache hierarchy where a child cache relies upon a parent cache in fulfilling client requests.) See <i><a href="#">HTTP cache hierarchies</a></i> , page 77.

Option	Description
No DNS and Just Forward to Parent	<p>When enabled, and if HTTP parent caching is enabled, Content Gateway does no DNS lookups on requested hostnames.</p> <p>If rules in the <b>parent.config</b> file are set so that only selected requests are sent to a parent proxy, Content Gateway skips name resolution only for requests that are going to the parent proxy. Name resolution is performed as usual for requests that are not sent to a parent proxy. If the parent proxy is down and the child proxy can go directly to origin servers, the child does a NDNS resolution as required only when the parent is unavailable.</p>
Uncacheable Requests Bypass Parent	When enabled, and if parent caching is enabled, Content Gateway bypasses the parent proxy for uncacheable requests.
HTTPS Requests Bypass Parent	When enabled, Content Gateway bypasses the parent proxy for HTTPS requests.
Tunnel Requests Bypass Parent	When enabled, Content Gateway bypasses parent proxy for non-HTTPS tunnel requests.
Parent Proxy Cache Rules	<p>Displays a table listing the rules in the <a href="#">parent.config</a> file that identify the HTTP parent proxies used in an HTTP cache hierarchy and configure selected URL requests to bypass parent proxies.</p> <p>Rules are applied from the list top-down; the first match is applied.</p>
Refresh	Updates the table to display the most up-to-date rules in the <b>parent.config</b> file.
Edit File	Opens the configuration file editor so that you can edit and add rules to the <b>parent.config</b> file.
	<b>parent.config Configuration File Editor</b>
rule display box	Lists the <a href="#">parent.config</a> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.
Primary Destination Type	<p>Lists the primary destination types:</p> <p><b>dest_domain</b> is a requested domain name.</p> <p><b>dest_host</b> is a requested hostname.</p> <p><b>dest_ip</b> is a requested IP address.</p> <p><b>url_regex</b> is a regular expression to be found in a URL.</p>

Option	Description
Primary Destination Value	<p>Specifies the value of the primary destination type.</p> <p>For example:</p> <p>If the primary destination is <b>dest_domain</b>, a value for this field can be yahoo.com</p> <p>If the primary destination type is <b>dest_ip</b>, the value for this field can be 123.456.78.9.</p> <p>If the primary destination is <b>url_regex</b>, a value for this field can be politics.</p>
Parent Proxies	<p>Specifies the IP addresses or hostnames of the parent proxies and the port numbers used for communication. Parent proxies are queried in the order specified in the list. If the request cannot be handled by the last parent server in the list, it is routed to the origin server. Separate each entry with a semicolon; for example: <b>parent1:8080; parent2:8080</b></p>
Round Robin	<p>Select <b>true</b> for the proxy to go through the parent cache list in a round-robin based on client IP address.</p> <p>Select <b>strict</b> for the proxy to serve requests strictly in turn. For example, machine proxy1 serves the first request, proxy2 serves the second request, and so on.</p> <p>Select <b>false</b> if you do not want round-robin selection to occur.</p>
Go direct	<p>Select <b>true</b> for requests to bypass parent hierarchies and go directly to the origin server.</p> <p>Select <b>false</b> if you do not want requests to bypass parent hierarchies.</p>
Secondary Specifiers: Time	<p>Specifies a time range, using a 24-hour clock, such as 08:00-14:00. If the range crosses midnight, enter this as two comma-separated ranges. For example, if a range extends from 6:00 in the evening until 8:00 in the morning, enter the following:</p> <p><b>18:00 - 23:59, 0:00 - 8:00</b></p>
Secondary Specifiers: Prefix	<p>Specifies a prefix in the path part of a URL.</p>
Secondary Specifiers: Suffix	<p>Specifies a file suffix in the URL, such as .htm or .gif.</p>
Secondary Specifiers: Source IP	<p>Specifies the IP address or range of IP addresses of the clients.</p>
Secondary Specifiers: Port	<p>Specifies the port in a requested URL.</p>
Secondary Specifiers: Method	<p>Specifies a request URL method. For example:</p> <ul style="list-style-type: none"> <li>• get</li> <li>• post</li> <li>• put</li> <li>• trace</li> </ul>

Option	Description
Secondary Specifiers: Scheme	Specifies the protocol of a requested URL. This must be either HTTP or FTP.
Secondary Specifiers: User-Agent	Specifies a request header User-Agent value.

## Mapping and Redirection

Option	Description
Serve Mapped Hosts Only	Select <b>Required</b> if you want the proxy to serve requests only to origin servers listed in the mapping rules of the <a href="#">remap.config</a> file. If a request does not match a rule in the <b>remap.config</b> file, the browser receives an error. This option provides added security for your Content Gateway system.
Retain Client Host Header	When this option is enabled, Content Gateway retains the client host header in a request (it does not include the client host header in the mapping translation).
Redirect No-Host Header to URL	Specifies the alternate URL to which to direct incoming requests from older clients that do not provide a <code>Host :</code> header.  It is recommended that you set this option to a page that explains the situation to the user and advises a browser upgrade or provides a link directly to the origin server, bypassing the proxy. Alternatively, you can specify a map rule that maps requests without <code>Host :</code> headers to a particular server.
URL Remapping Rules	Displays a table listing the mapping rules in the <b>remap.config</b> file so that you can redirect HTTP requests permanently or temporarily without the proxy having to contact any origin servers.
Refresh	Updates the table to display the most up-to-date rules in the <b>remap.config</b> file.
Edit File	Opens the configuration file editor so that you can edit and add rules to the <b>remap.config</b> file.
	<b>remap.config Configuration File Editor</b>
rule display box	Lists the <b>remap.config</b> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.

Option	Description
Rule Type	<p>Lists the type of rules you can add to the <code>remap.config</code> file:</p> <p><b>redirect</b> redirects HTTP requests permanently without having to contact the origin server. Permanent redirects notify the browser of the URL change (by returning an HTTP status code 301) so that the browser can update bookmarks.</p> <p><b>redirect_temporary</b> redirects HTTP requests temporarily without having to contact the origin server. Temporary redirects notify the browser of the URL change for the current request only (by returning an HTTP status code 307).</p>
From Scheme	<p>Specifies the protocol of the mapping rule. “rtsp” and “mms” are <b>not</b> supported.</p> <p><b>Note:</b> Mapping a URL of one protocol (scheme) to a different protocol (scheme) is not supported.</p>
From Host	Specifies the hostname of the URL to map from.
From Port (Optional)	Specifies the port number in the URL to map from.
From Path Prefix (Optional)	Specifies the path prefix of the URL to map from.
To Host	Specifies the hostname of the URL to map to.
To Port (Optional)	Specifies the port number of the URL to map to.
To Path Prefix (Optional)	Specifies the path prefix of the URL to map to.
{undefined}	Specifies the media protocol type of the mapping rule. Not supported.

## Browser Auto-Config

Option	Description
	<b>PAC</b>
Auto-Configuration Port	<p>Specifies the port Content Gateway uses to download the auto-configuration file to browsers. The port cannot be assigned to any other process. The default port is 8083.</p> <p>If you change this option, you must restart Content Gateway.</p>
PAC Settings	Lets you edit the PAC file ( <b>proxy.pac</b> ). See <a href="#">Using a PAC file</a> , page 36.
	<b>WPAD</b>
WPAD Settings	Lets you edit the <b>wpad.dat</b> file. See <a href="#">Using WPAD</a> , page 38.



## Security

The Security configuration options are divided into the following categories:

[Connection Control](#), page 275

[Access Control](#), page 276

[SOCKS](#), page 287

### Connection Control

Option	Description
	<b>Proxy Access</b>
Access Control	Displays the rules in the <a href="#">ip_allow.config</a> file that control which clients can access the proxy. By default, all remote hosts are allowed to access the proxy.
Refresh	Updates the table to display the most up-to-date rules in the <b>ip_allow.config</b> file.
Edit File	Opens the configuration file editor for to the <b>ip_allow.config</b> file.
	<b>ip_allow.config Configuration File Editor</b>
rule display box	Lists the <a href="#">ip_allow.config</a> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.
IP Action	Lists the type of rules you can add. An <b>ip_allow</b> rule allows the clients listed in the Source IP field to access the proxy. An <b>ip_deny</b> rule denies the clients listed in the Source IP field access to the proxy.
Source IP	Specifies the IP address or range of IP addresses of the clients.
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.

## Data Security



### Note

The Data Security configuration options appear on the Configure pane only if you have enabled Data Security and selected **Integrated on-box** in the **Features** table on the **Configure > My Proxy > Basic > General** tab.

Option	Description
Data Security IP address	Specifies the IP address of the Data Security Management Server. This is where the Websense Data Security policy configuration and management is performed.
Analyze HTTPS Content	Select whether decrypted traffic should be sent to Websense Data Security for analysis or sent directly to the destination.
Analyze FTP Uploads	Select whether to send FTP upload requests to Websense Data Security for analysis. The FTP proxy feature must be enabled. See <a href="#">FTP</a> , page 269.

### Registration screen fields:

Option	Description
Data Security IP address	Specifies the IP address of the Data Security Management Server. This is where data security policy configuration and management is performed.
Data Security Manager user name	Specifies the account name of a Websense Data Security administrator. The administrator must have Deploy Settings privileges.
Data Security Manager user name	Specifies the password of the Websense Data Security administrator.
Register button	Initiate the registration action. This button is enabled only after data is entered in all fields.

## Access Control

Use the Access Control tabs to:

- ◆ Create custom filtering rules
- ◆ Configure proxy user authentication

The [Filtering](#) tab is always available on the **Access Control** page.

The [Transparent Proxy Authentication](#) tab is also always present, but it applies only if Content Gateway is deployed as a transparent proxy.

The other tabs are dynamic based on the authentication method selected in the **Authentication** section of **Configure > My Proxy**.

If *Integrated Windows Authentication* is selected, these tabs are displayed:

- **Integrated Windows Authentication**
- **Global Authentication Options** (apply to NTLM)

If *LDAP* is selected, this tab is displayed:

- **LDAP**

If *Radius* is selected, this tab is displayed:

- **Radius**

If *Legacy NTLM* is selected, this tab is displayed:

- **NTLM**

If *Multiple Realm Authentication* is selected, these tabs are displayed:

- **Domains**
- **Authentication Realms**
- **Global Authentication Options**

The table below describes the purpose of each field on each tab. It is suggested that you use your browser's Search feature to find the field that you're looking for.

For a complete description of Content Gateway user authentication features, see *Proxy user authentication*, page 162.

Option	Description
	<b>Filtering</b>
Filtering	Displays a table listing the rules in the <i>filter.config</i> file that deny or allow particular URL requests, and that keep or strip header information from client requests. Rules are applied based on first match in a top-down traversal of the list. If no rule matches, the request is allowed to proceed. NTLM and LDAP authentication rules are defined on the <b>Authentication Realms</b> tab and stored in the <i>auth.config</i> file (see its entry later in this table). For a detailed discussion of filtering rules, see <i>Filtering Rules</i> , page 156.
Refresh	Updates the table to display the most up-to-date rules in the <b>filter.config</b> file.
Edit File	Opens the configuration file editor for the <b>filter.config</b> file.

Option	Description
	<b>filter.config Configuration File Editor</b>
rule display box	Lists the rules currently stored in <i>filter.config</i> . Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page. Click Add after selecting or entering values for the rule.
Set	Updates the rule display box at the top of the configuration file editor page.
Rule Type	Specifies the rule type: Select <b>allow</b> to allow particular URL requests to bypass authentication; the proxy caches and serves the requested content. Select <b>deny</b> to deny requests for objects from specific destinations. When a request is denied, the client receives an access denied message. Select <b>keep_hdr</b> to specify which client request header information you want to keep. Select <b>strip_hdr</b> to specify which client request header information you want to strip. <b>Note:</b> The “radius” rule type is not supported.
Primary Destination Type	Lists the primary destination types: <b>dest_domain</b> is a requested domain name. <b>dest_host</b> is a requested hostname. <b>dest_ip</b> is a requested IP address. <b>url_regex</b> is a regular expression to be found in a URL.
Primary Destination Value	Specifies the value of the primary destination type. For example, if the primary destination type is <b>dest_ip</b> , the value for this field might be 123.456.78.9.
Additional Specifiers: Header Type	Specifies the client request header information that you want to keep or strip. This option applies to only <b>keep_hdr</b> or <b>strip_hdr</b> rule types.
Additional Specifiers: Realm (optional)	Not supported.
Additional Specifiers: Proxy Port (optional)	Specifies the proxy port to match for this rule.
Secondary Specifiers: Time	Specifies a time range, such as 08:00-14:00.
Secondary Specifiers: Prefix	Specifies a prefix in the path part of a URL.
Secondary Specifiers: Suffix	Specifies a file suffix in the URL.

Option	Description
Secondary Specifiers: Source IP	Specifies the IP address of the client.
Secondary Specifiers: Port	Specifies the port in a requested URL.
Secondary Specifiers: Method	Specifies a request URL method: <ul style="list-style-type: none"> <li>– <b>get</b></li> <li>– <b>post</b></li> <li>– <b>put</b></li> <li>– <b>trace</b></li> </ul>
Secondary Specifiers: Scheme	Specifies the protocol of a requested URL. Options are: <ul style="list-style-type: none"> <li>– <b>HTTP</b></li> <li>– <b>HTTPS</b></li> <li>– <b>FTP</b> (for FTP over HTTP only)</li> </ul> <b>Note:</b> rtsp and mms not supported.
Secondary Specifiers: User-Agent	Specifies the request header User-Agent value. Use this field to create application filtering rules that: <ul style="list-style-type: none"> <li>• Allow applications that don't properly handle authentication challenges to bypass authentication</li> <li>• Block specified client-based applications from accessing the Internet</li> </ul>
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.
<b>Integrated Windows Authentication</b>	
<p>The Integrated Windows Authentication page appears only if you have enabled IWA in the Features table on the <b>Configure &gt; My Proxy &gt; Basic &gt; General</b> tab.</p> <p>Use this page to join or unjoin the Windows domain. When a domain has been joined, the page provides a summary of the domain attributes and an Unjoin button.</p> <p>See <a href="#">Integrated Windows Authentication</a>, page 166.</p>	
Domain Name	Specifies the fully qualified Windows domain name.
Administrator Name	Specifies the Windows Administrator user name.
Administrator Password	Specifies the Windows Administrator password. <b>Note:</b> The name and password are used only during the join and are not stored.
Domain Controller	Specifies how to locate the domain controller: <ul style="list-style-type: none"> <li>• Auto-detect using DNS</li> <li>• DC name or IP address</li> </ul> <p>If the domain controller is specified by name or IP address, you can also specify backup domain controllers in a comma separated list.</p>

Option	Description
Content Gateway Hostname	<p>Specifies the Content Gateway hostname.</p> <p>Because IWA uses the hostname as a NetBIOS name when registering with Kerberos, the hostname cannot exceed 15 characters in length (a NetBIOS restriction), or 11 characters on V-Series appliances (V-Series adds 4 characters to the hostname to ensure that the hostname is unique across modules (Doms)).</p> <p><b>IMPORTANT:</b> Once the domain is joined the hostname cannot be changed. If it is, IWA will immediately stop working until the domain is unjoined and then rejoined with the new hostname.</p>
Join Domain	Click Join Domain to join the domain.
	<p><b>Global Authentication Options</b></p> <p>Use this page to set options that are applied when Integrated Windows Authentication performs NTLM authentication.</p>
Fail Open	<p>When enabled (default), allows client requests to proceed when authentication fails due to:</p> <ul style="list-style-type: none"> <li>• no response from the domain controller</li> <li>• malformed messages from the client</li> <li>• invalid SMB responses</li> </ul> <p><b>Note:</b> Password authentication failures are always failures.</p>
NTLM Credential Caching	Enables or disables the caching of user credentials after they have been authenticated by NTLM. Applies only when Content Gateway is an explicit proxy.
Caching TTL	Specifies the time-to-live (TTL) of entries in the cache. The default is 900 seconds (15 minutes).
Multi-user IP Exclusions	Specifies a comma-separated list of IP addresses and IP address ranges of network systems that host multiple users, such as terminal servers.

Option	Description
	<b>Transparent Proxy Authentication</b> Use this page when Content Gateway is a transparent proxy. For more information, see <a href="#">Transparent proxy authentication settings, page 165</a> .
Redirect Hostname (optional)	Specifies an alternate hostname for the proxy that can be resolved by DNS for all clients on the network. <b>Note:</b> Redirect Hostname is not needed and does not apply to Integrated Windows Authentication (IWA).
Authentication Mode	When transparent proxy authentication is configured, Content Gateway must be set to an authentication mode: <ul style="list-style-type: none"> <li>• <b>IP mode</b> (the default) causes the client IP address to be associated with a username when a session is authenticated. Requests made from that IP address are not authenticated again until the <b>Session TTL</b> expires. The default is 15 minutes.</li> <li>• <b>Cookie mode</b> is used to uniquely identify users who share a single IP address, such as, for example, in environments where proxy-chaining is used or where network address translation (NAT) occurs.</li> </ul>
Session TTL	Specifies the length of time, in minutes, before the client must re-authenticate. This is required for both IP and Cookie modes. The default is 15 minutes. The supported range of values is 5-65535 minutes.
	<b>LDAP</b> The LDAP configuration options appear on the Configure pane only if you have enabled LDAP in the Features table on the <b>Configure &gt; My Proxy &gt; Basic &gt; General</b> tab. For more information on configuring LDAP see <a href="#">LDAP authentication, page 173</a> .
Purge Cache on Authentication Failure	When this option is enabled, Content Gateway deletes the authorization entry for the client in the LDAP cache if authorization fails.
LDAP Server: Hostname	Specifies the hostname of the LDAP server. If you change this option, you must restart Content Gateway.
LDAP Server: Port	Specifies the port used for LDAP communication. The default port number is 389. If you change this option, you must restart Content Gateway.
LDAP Server: Secure LDAP	Specifies whether Content Gateway will use secure communication with the LDAP server. If enabled, set the LDAP Port field (above) to 636 or 3269 (the secure LDAP ports).
LDAP Server: Server Type	Specifies the search filter. Select either Active Directory or other directory services.

Option	Description
LDAP Server: Bind Distinguished Name	<p>Specifies the Full Distinguished Name (fully qualified name) of a user in the LDAP-based directory service. For example:</p> <p>CN=John Smith, CN=USERS, DC=MYCOMPANY, DC=COM</p> <p>Enter a maximum of 128 characters in this field.</p> <p>If you do not specify a value for this field, the proxy attempts to bind anonymously.</p>
LDAP Server: Password	Specifies a password for the user identified in the <b>Bind_DN</b> field.
LDAP Server: Base Distinguished Name	<p>Specifies the base Distinguished Name (DN). You can obtain this value from your LDAP administrator.</p> <p>You must specify a correct base DN; otherwise LDAP authentication will fail to operate.</p> <p>If you change this option, you must restart Content Gateway.</p>
<b>Radius</b>	
<p>The Radius configuration options appear on the Configure pane only if you have enabled Radius in the Features table on the <b>Configure &gt; My Proxy &gt; Basic &gt; General</b> tab.</p> <p>For more information on configuring Radius, see <a href="#">RADIUS authentication, page 176</a>.</p>	
Primary Radius Server: Hostname	<p>Specifies the hostname or IP address of the primary RADIUS authentication server.</p> <p>If you change this option, you must restart Content Gateway.</p>
Primary Radius Server: Port	<p>Specifies the port that Content Gateway uses to communicate with the primary RADIUS authentication server. The default port is 1812.</p> <p>If you change this option, you must restart Content Gateway.</p>
Primary Radius Server: Shared Key	<p>Specifies the key to use for encoding.</p> <p>If you change this option, you must restart Content Gateway.</p>
Secondary Radius Server (optional): Hostname	<p>Specifies the hostname or IP address of the secondary RADIUS authentication server.</p> <p>If you change this option, you must restart Content Gateway.</p>
Secondary Radius Server (optional): Port	<p>Specifies the port that Content Gateway uses to communicate with the secondary RADIUS authentication server. The default port is 1812.</p> <p>If you change this option, you must restart Content Gateway.</p>
Secondary Radius Server (optional): Shared Key	<p>Specifies the key to use for encoding.</p> <p>If you change this option, you must restart Content Gateway.</p>



Option	Description
	<b>Legacy NTLM</b>
	<p>The NTLM configuration options appear on the Configure pane only if you have enabled NTLM in the Features table on the <b>Configure &gt; My Proxy &gt; Basic &gt; General</b> tab.</p> <p>For more information on configuring NTLM, see <a href="#">Legacy NTLM authentication</a>, page 171.</p>
Domain Controller Hostnames	<p>Specifies the hostnames of the domain controllers in a comma separated list. The format is:</p> <p>host_name[:port] [%netbios_name]</p> <p>or</p> <p>IP_address[:port] [%netbios_name]</p> <p>If you are using Active Directory 2008, you must include the netbios_name or use SMB port 445.</p> <p>If you change this option, you must restart Content Gateway.</p>
Load Balancing	<p>Enables or disables load balancing. When enabled, Content Gateway balances the load when sending authentication requests to the domain controllers.</p> <p><b>Note:</b> When multiple domain controllers are specified, even if load balancing is disabled, when the load on the primary domain controller reaches the maximum number of connections allowed, new requests are sent to a secondary domain controller as a short-term failover provision, until such time that the primary domain controller can accept new connections.</p> <p>If you change this option, you must restart Content Gateway.</p>
Fail Open	<p>When enabled (default), allows client requests to proceed when authentication fails due to:</p> <ul style="list-style-type: none"> <li>• no response from the domain controller</li> <li>• malformed messages from the client</li> <li>• invalid SMB responses</li> </ul> <p><b>Note:</b> Password authentication failures are always failures.</p>
IPCredentials: Credential caching	Enables or disables NTLM credential caching. Applies only when Content Gateway is an explicit proxy.
IP Credentials: Caching TTL	Specifies the time-to-live, in seconds, for NTLM cached Credentials. The default is 900 seconds (15 minutes). The range of supported values is 300 to 86400 seconds.
IP Credentials: Multi-user IP Exclusions	<p>Specifies a comma separated list of multi-user IP addresses and IP address ranges for terminal servers, NAT firewalls, etc.</p> <p>Credentials for these users are not cached.</p>
	<b>Domains</b>

Option	Description
<p>The Domains page appears on the Access Control list only if you have enabled <b>Multiple Realm Authentication</b> in the Features table on the <b>Configure &gt; My Proxy &gt; Basic &gt; General</b> tab.</p> <p>Use this tab to join domains for which you will create authentication rules.</p> <p>For a complete description of multiple realm authentication, see <a href="#">Multiple realm authentication</a>, page 179.</p>	
Domain Name	Specifies the fully qualified Windows domain name.
Administrator Name	Specifies the Windows Administrator user name.
Administrator Password	Specifies the Windows Administrator password. <b>Note:</b> The name and password are used only during the join and are not stored.
Domain Controller	<p>Specifies how to locate the domain controller:</p> <ul style="list-style-type: none"> <li>• Auto-detect using DNS</li> <li>• DC name or IP address</li> </ul> <p>If the domain controller is specified by name or IP address, you can also specify backup domain controllers in a comma separated list.</p>
Content Gateway Hostname	<p>Specifies the Content Gateway hostname.</p> <p>Because IWA uses the hostname as a NetBIOS name when registering with Kerberos, the hostname cannot exceed 15 characters in length (a NetBIOS restriction), or 11 characters on V-Series appliances (V-Series adds 4 characters to the hostname to ensure that the hostname is unique across modules (Doms).</p> <p><b>IMPORTANT:</b> Once the domain is joined the hostname cannot be changed. If it is, IWA will immediately stop working until the domain is unjoined and then rejoined with the new hostname.</p>
Join Domain	Click Join Domain to join the domain.
Joined Domains list	Displays a list of joined domains.
Unjoin Domain button	To unjoin a domain, select a domain and click the button.
Realm Name	Displays the name of the domain selected in the Joined Domains list.
Fully Qualified Domain Name	Displays the FQDN of the domain selected in the Joined Domains list.
Content Gateway Hostname	Displays the hostname that client browsers must use in the browser proxy setting section when Integrated Windows Authentication (Kerberos) is configured.
Domain Controller	<p>Specifies how to locate the selected domain controller:</p> <ul style="list-style-type: none"> <li>• Auto-detect using DNS</li> <li>• DC name or IP address</li> </ul> <p>If the domain controller is specified by name or IP address, you can also specify backup domain controllers in a comma separated list.</p>

Option	Description
	<b>Multiple Realm Authentication</b>
	<p>In networks with multiple realms (domains that do not share reciprocal trust relationships), rules can be defined to direct sets of IP addresses to specific domain controllers.</p> <p>For more information, see <a href="#">Multiple realm authentication, page 179</a>.</p>
Authentication	<p>Displays a table listing the rules in the <a href="#">auth.config</a> file that direct specified IP addresses to particular domain controllers for authentication. In explicit proxy configuration, rules can be written for traffic inbound on specific ports.</p> <p>IWA, LDAP and NTLM rules can be configured.</p>
Refresh	Updates the table to display the current rules in the <b>auth.config</b> file.
Edit File	Opens the configuration file editor for the <b>auth.config</b> file.
	<b>auth.config Configuration File Editor</b>
rule display box	Lists the <a href="#">auth.config</a> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.
Rule Type	<p>Specifies the rule type:</p> <p>Select <b>Integrated Windows Authentication</b> for rules that will apply Kerberos.</p> <p>Select <b>Legacy NTLM</b> to specify rules that will apply the NTLMSSP method.</p> <p>Select <b>LDAP</b> to specify rules that will use LDAP.</p>
Status	Specifies that the rule is enabled or disabled after the rule is saved and Content Gateway is restarted.
Rule Name	Specifies a descriptive name for the rule (must be unique).
Source IP	<p>Specifies IP addresses or IP address ranges for this rule (must be entered without any spaces).</p> <p>Example: 10.1.1.1 or 0.0.0.0-255.255.255.255 or 10.1.1.1,20.2.2.2,3.0.0.0-3.255.255.255</p>
Proxy Port	Specifies the inbound port for traffic when Content Gateway is deployed as an explicit proxy.
Advanced Settings: Aliasing	Specifies an alias to send to the filtering service for all users who match this rule. The alias must be static. It can be empty (blank). The alias must exist in the primary domain controller (the DC visible to the filtering service).

Option	Description
IWA Specifiers: Domain/Realm	Specifies the domain (realm) the rule applies to.
NTLM Specifiers: DC List	Specifies the IP address and port number of the primary domain controller (if no port is specified, Content Gateway uses port 139), followed by a comma separated list of secondary domain controllers to be used for load balancing and failover.
NTLM Specifiers: DC Load Balance	Specifies whether load balancing is used: <ul style="list-style-type: none"> <li>0 = disabled</li> <li>1 = enabled</li> </ul> <p><b>Note:</b> When multiple domain controllers are specified, even if load balancing is disabled, when the load on the primary domain controller reaches the maximum number of connections allowed, new requests are sent to a secondary domain controller as a short-term failover provision, until such time that the primary domain controller can accept new connections.</p>
LDAP Specifiers: LDAP Server Name	Specifies the LDAP server name. This option applies to <code>ldap</code> rule types only.
LDAP Specifiers: LDAP Server Port	Specifies the LDAP Server Port (Optional - Default 389)
LDAP Specifiers: LDAP Base Distinguished Name	Specifies the LDAP Base Distinguished Name. This option applies to <code>ldap</code> rule types only.
LDAP Specifiers: Server Type	Sets the search filter to "sAMAccountName" for Active Directory, or to "uid" for other directory services.
LDAP Specifiers: Bind DN	Specifies the LDAP bind account distinguished name.
LDAP Specifiers: Bind Password	Specifies the LDAP bind account password.
LDAP Specifiers: Secure LDAP	Specifies whether Content Gateway will use secure communication with the LDAP server. If enabled, you must set LDAP port to one of the secure ports: 636 or 3269.
LDAP Specifiers: LDAP Attribute Name (Optional)	Specifies the LDAP attribute name.
LDAP Specifiers: LDAP Attribute Value (Optional)	Specifies the LDAP attribute pair.
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.

## SOCKS



### Note

The SOCKS configuration options appear on the Configure pane only if you have enabled SOCKS in the Features table on the **Configure > My Proxy > Basic > General** tab.

Option	Description
	<b>General</b>
SOCKS Version	<p>Specifies the version of SOCKS used on your SOCKS server. Content Gateway supports SOCKS version 4 and version 5.</p> <p>If you change this option, you must restart Content Gateway.</p>
	<b>Proxy</b>
SOCKS Proxy	<p>Enables or disables the SOCKS Proxy option. As a SOCKS proxy, WCG can receive SOCKS packets (usually on port 1080) from the client and forwards all requests directly to the SOCKS server.</p> <p>For more information about the SOCKS Proxy option, see <a href="#">Configuring SOCKS firewall integration</a>, page 159.</p> <p>If you change this option, you must restart Content Gateway.</p>
SOCKS Proxy Port	<p>Specifies the port on which Content Gateway accepts SOCKS traffic. This is usually port 1080.</p> <p>If you change this option, you must restart Content Gateway.</p>
	<b>Server</b>
SOCKS Server: Default Servers	<p>Specifies the names and the ports of the default SOCKS servers with which Content Gateway communicates. Each entry must be separated by a semicolon (;); for example: socks1:1080;socks2:4080</p> <p>If you change this option, you must restart Content Gateway.</p> <p>You can perform additional SOCKS server configuration in the <a href="#">socks.config</a> file.</p>
Socks Server Rules	<p>Displays a table listing the rules in the <code>socks.config</code> file that control the SOCKS servers Content Gateway must go through to access specific origin servers and the order in which Content Gateway goes through the SOCKS server list. You can also specify the origin servers that you want the proxy to access directly without going through the SOCKS server, and the user name and password used by Content Gateway to connect to a SOCKS version 5 server.</p>

Option	Description
Refresh	Updates the table to display the most up-to-date rules in the <b>socks.config</b> file.
Edit File	Opens the configuration file editor for the <b>socks.config</b> file.
	<b>socks.config Configuration File Editor</b>
rule display box	Lists the <i>socks.config</i> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.
Rule Type	<p>Specifies the rule type:</p> <p>Select <b>no_socks</b> to specify the origin servers you want the proxy to access directly without going through the SOCKS server. Enter the IP addresses of the origin servers in the <b>Destination IP</b> field.</p> <p>Select <b>auth</b> to specify the user name and password Content Gateway uses for authentication with a SOCKS version 5 server. Enter the username in the <b>Username</b> field and the password in the <b>Password</b> field.</p> <p>Select <b>multiple_socks</b> to specify the SOCKS servers Content Gateway must go through to reach specific origin servers. Enter the hostnames or the IP addresses of the SOCKS servers in the <b>SOCKS Servers</b> field and the IP addresses of the origin servers in the <b>Destination IP</b> field. Select how strictly Content Gateway should follow round robin from the <b>Round Robin</b> drop-down list.</p>
Username	<p>Specifies the username Content Gateway must use to authenticate with a SOCKS version 5 server.</p> <p>This field applies to an <b>auth</b> rule type only.</p>
Password	<p>Specifies the password Content Gateway must use to authenticate with a SOCKS version 5 server.</p> <p>This field applies to an <b>auth</b> rule type only.</p>
Destination IP	<p>For a <b>multiple_socks</b> rule, specify either a single IP address <i>or</i> a range of IP addresses of the origin servers with which Content Gateway must use the SOCKS servers specified in the <b>SOCKS Servers</b> field below.</p> <p>For a <b>no_socks</b> rule, specify the IP addresses of the origin servers that you want the proxy to access directly (without going through the SOCKS server). You can enter a single IP address, a range of IP addresses, or a list of IP addresses. Separate each entry in the list with a comma. Do not specify the all networks broadcast address: 255.255.255.255.</p>
SOCKS Servers	<p>Specify the hostnames or the IP addresses of the SOCKS servers you want to go through to service requests for the origin servers listed in the <b>Destination IP</b> field above. Separate each entry with a semicolon.</p> <p>This field applies to a <b>multiple_socks</b> rule type only.</p>

Option	Description
Round Robin	Specifies how strictly Content Gateway should follow round robin. You can select <b>strict</b> , or <b>false</b> . This field applies to a <code>multiple_socks</code> rule type only.
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.

## Subsystems

The Subsystems configuration options are divided into the following categories:

[Cache, page 289](#)

[Logging, page 291](#)

## Cache

Option	Description
	<b>General</b>
Allow Pinning	Enables or disables the cache pinning option, which lets you keep objects in the cache for a specified time. Set cache pinning rules in the <a href="#">cache.config</a> file.
Ram Cache Size	Specifies the size of the RAM cache, in bytes. The default size is 104857600 (100 MB). A value of “-1” directs Content Gateway to automatically size the RAM cache to approximately 1 MB per 1 GB of disk cache. If you change this option, you must restart Content Gateway.
Maximum Object Size	Specifies the maximum size allowed for objects in the cache. A value of 0 (zero) means that there is no size restriction.
	<b>Partition</b>
Cache Partition	Displays a table showing the rules in the <a href="#">partition.config</a> file that control how the cache is partitioned.
Refresh	Updates the table to display the most up-to-date rules in the <b>partition.config</b> file. Click this button after you have added or modified rules with the configuration file editor.
Edit File	Opens the configuration file editor so that you can edit and add rules to the <b>partition.config</b> file.

Option	Description
<b>partition.config Configuration File Editor</b>	
rule display box	Lists the <i>partition.config</i> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page. Enter information in the fields provided before you click this button.
Set	Updates the rule display box at the top of the page. Select a rule and change its properties before you click this button.
Partition Number	Specifies a partition number between 1 and 255.
Scheme	Specifies the content type stored in the partition. Only HTTP is supported.
Partition Size	Specifies the amount of cache space allocated to the partition. The size can be either a percentage of the total cache space or an absolute value in MB.
Partition Size Format	Specifies the format of the partition size: percentage or absolute.
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.
<b>Hosting</b>	
Cache Hosting	Displays a table listing the rules in the <b>hosting.config</b> file that controls which cache partitions are assigned to specific origin servers and domains.
Refresh	Updates the table to display the most up-to-date rules in the <b>hosting.config</b> file.
Edit File	Opens the configuration file editor for the <b>hosting.config</b> file. The configuration file editor page is described below.
<b>hosting.config Configuration File Editor</b>	
rule display box	Lists the <b>hosting.config</b> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.
Primary Destination Type	Specifies the primary destination rule type: Select <b>domain</b> if you want to partition the cache according to domain. Select <b>hostname</b> if you want to partition the cache according to hostname



Option	Description
Primary Destination Value	Specifies the domain or origin server's hostname whose content you want to store on a particular partition.
Partitions	Specifies the partitions on which you want to store the content that belongs to the origin server or domain specified. Separate each partition with a comma. Note: The partitions must already be created in the <b>partition.config</b> file. For information about creating partitions, see <a href="#">Partitioning the cache</a> , page 85.
Partitions	Specifies a comma-separated list of the partitions on which you want to store the content that belongs to the origin server or domain specified.
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.

## Logging

Option	Description
	<b>General</b>
Logging	Enables or disables event logging so that transactions are recorded into event log files and/or error log files. Select <b>Log Transactions and Errors</b> to log transactions into your selected event log files and errors in the error log files. Select <b>Log Transactions Only</b> to log transactions into your selected event log files only. Content Gateway does not log errors in the error log files. Select <b>Log Errors Only</b> to log errors in the error log files only. Content Gateway does not log transactions into your selected event log files. Select <b>Disabled</b> to turn off logging.
Log Directory	Specifies the path of the directory in which Content Gateway stores event logs. The path of this directory must be the same on every node in the Content Gateway cluster failover group. The default is: /opt/WCG/logs
Log Space: Limit	Specifies the maximum amount of space (in megabytes) allocated to the logging directory for the log files. Note: Transaction logs can consume a lot of space. You should set this limit high enough to accommodate at least a single day's worth of uncompressed transaction logs. Also, make sure that this limit is smaller than the actual space available on the partition that contains the logging directory.

Option	Description
Log Space: Headroom	Specifies the tolerance for the log space limit. If the <b>Auto-Delete Rolled Files</b> option is enabled, autodeletion is triggered when the amount of free space available in the logging directory is less than the headroom.
Log Rolling: Enable/Disable	Enables or disables log file rolling. To keep log files down to manageable sizes, you can roll them at regular intervals. See <a href="#">Rolling event log files</a> , page 204.
Log Rolling: Offset Hour	Specifies the hour when log rolling takes place. You can set a time of the day in the range 0 to 23. For example, if the offset hour is 0 (midnight) and the roll interval is 6, the log files are rolled at 00:00, 06:00, noon, and 18:00.
Log Rolling: Interval	Specifies the amount of time Content Gateway enters data in log files before rolling them to <b>.old</b> files. The minimum value is 300 seconds (five minutes). The default value is 21600 seconds (6 hours). The maximum value is 86400 (1 day).
Log Rolling: Auto-Delete Rolled Files	Enables autodeletion of rolled log files when available space in the log directory is low. Autodeletion is triggered when the amount of free space available in the log directory is less than the <b>Log Space Headroom</b> .
<b>Formats</b>	
Squid Format: Enable/Disable	Enables or disables the Squid log format.
Squid Format: ASCII/Binary	Select <b>ASCII</b> or <b>Binary</b> as the type of log files to be created.
Squid Format: Filename	Specifies the name used for Squid log files. The default filename is <b>squid.log</b> .
Squid Format: Header	Specifies the text header you want Squid log files to contain.
Netscape Common Format: Enable/Disable	Enables or disables the Netscape Common log format.
Netscape Common Format: ASCII/Binary	Select <b>ASCII</b> or <b>Binary</b> as the type of log file to be created.
Netscape Common Format: Filename	Specifies the name used for Netscape Common log files. The default filename is <b>common.log</b> .
Netscape Common Format: Header	Specifies the text header you want Netscape Common log files to contain.
Netscape Extended Format: Enable/Disable	Enables or disables the Netscape Extended log format.
Netscape Extended Format: ASCII/Binary	Select <b>ASCII</b> or <b>Binary</b> as the type of log file to be created.
Netscape Extended Format: Filename	Specifies the name used for Netscape Extended log files. The default filename is <b>extended.log</b> .

Option	Description
Netscape Extended Format: Header	Specifies the text header you want Netscape Extended log files to contain.
Netscape Extended 2 Format: Enable/Disable	Enables or disables the Netscape Extended-2 log format.
Netscape Extended 2 Format: ASCII/Binary	Select <b>ASCII</b> or <b>Binary</b> as the type of log file to be created.
Netscape Extended 2 Format: Filename	Specifies the name used for Netscape Extended-2 log files. The default filename is <b>extended2.log</b> .
Netscape Extended 2 Format: Header	Specifies the text header you want Netscape Extended-2 log files to contain.
<b>Collation</b>	
Collation Mode	<p>Specifies the log collation mode for this Content Gateway node. You can use the log file collation feature to keep all logged information in one place. For more information about log file collation, see <a href="#">Collating event log files</a>, page 209.</p> <p>Select <b>Collation Disabled</b> to disable log collation on this Content Gateway node.</p> <p>Select <b>Be a Collation Server</b> to configure this Content Gateway node to be the collation server.</p> <p>Select <b>Be a Collation Client</b> to configure this Content Gateway server to be a collation client. A Content Gateway server configured as a collation client sends only the active standard log files, such as Squid, Netscape Common, and so on, to the collation server. If you select this option, enter the hostname of the collation server for your cluster in the <b>Log Collation Server</b> field.</p> <p>Note: When logs are collated, the source of the log entry—its node of origin—is lost unless you turn on the <b>Log collation host tagged</b> option (described below).</p> <p>Log collation consumes cluster bandwidth in sending all log entries to a single node. It can therefore affect the performance of the cluster.</p> <p>If you want Content Gateway as a collation client to send custom (XML-based) log files, you must specify a LogObject in the <b>logs_xml.config</b> file.</p>
Log Collation Server	Specifies the hostname of the log collation server to which you want to send log files.
Log Collation Port	<p>Specifies the port used for communication between the collation server and client. You must specify a port number in all cases, except when log collation is inactive. The default port number is 8085.</p> <p>Note: Do not change the port number unless there is a conflict with another service already using the port.</p>
Log Collation Secret	Specifies the password for the log collation server and the other nodes in the cluster. This password is used to validate logging data and prevent the exchange of arbitrary information.

Option	Description
Log Collation Host Tagged	When this option is enabled, Content Gateway adds the hostname of the node that generated the log entry to end of the entry in the collated log file.
Log Collation Orphan Space	Specifies the maximum amount of space (in megabytes) allocated to the logging directory for storing orphan log files on the Content Gateway node. Content Gateway creates orphan log entries when it cannot contact the log collation server.
	<b>Custom</b>
Custom Logging	Enables or disables custom logging.
Custom Log File Definitions	Displays the <a href="#">logs_xml.config</a> file so that you can configure custom (XML-based) logging options.

## Networking

---

The Networking configuration options are divided into the following categories:

[Connection Management](#), page 294

[ARM](#), page 295

[WCCP](#), page 299

[DNS Proxy](#), page 302

[DNS Resolver](#), page 303

[ICAP](#), page 304

[Virtual IP](#), page 306

## Connection Management

Option	Description
	<b>Throttling</b>
Throttling Net Connections	<p>Specifies the maximum number of network connections that Content Gateway accepts.</p> <p>Setting a Content Gateway throttle limit helps to prevent system overload when traffic bottlenecks develop. When network connections reach this limit, Content Gateway queues new connections until existing connections close.</p> <p>Do not set this variable below the minimum value of 100.</p>

Option	Description
	<b>Load Shedding</b>
Maximum Connections	Specifies the maximum number of client connections allowed before the ARM (transparent mode) starts forwarding incoming requests directly to the origin server. The default value is 1 million connections.  If you change this option, you must restart Content Gateway.

## ARM



### Note

The ARM configuration options appear on the Configure pane only if you have enabled ARM in the Features table on the **Configure > My Proxy > Basic > General** tab.

Option	Description
	<b>General</b>
IP spoofing	Enables or disables the IP spoofing option, which configures Content Gateway to establish connections to origin servers with the client IP address instead of the Content Gateway IP address. For more information, see <a href="#">IP spoofing</a> , page 66.  <b>WARNING:</b> IP spoofing requires precise control of the routing paths on your network, overriding the normal routing process for traffic running on TCP port 80 and 443.
Network Address Translation (NAT)	Displays the redirection rules in the <a href="#">ipnat.conf</a> file that specify how incoming packets are readdressed when the proxy is serving traffic transparently. Content Gateway creates redirection rules during installation. You can modify these rules.
Refresh	Updates the table to display the most up-to-date rules in the <b>ipnat.conf</b> file.
Edit File	Opens the configuration file editor for the <b>ipnat.conf</b> file.
	<b>ipnat.conf Configuration File Editor</b>
rule display box	Lists the <a href="#">ipnat.conf</a> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.

Option	Description
Ethernet Interface	Specifies the Ethernet interface that traffic will use to access the Content Gateway machine: for example, <code>eth0</code> on Linux.
Connection Type	Specifies the connection type that applies for the rule: TCP or UDP.
Original Destination IP	Specifies the IP address from which traffic is sent. 0.0.0.0 matches all IP addresses.
Original Destination CIDR	Specifies the IP address in CIDR (Classless Inter-Domain Routing) format, such as 1.1.1.0/24. Entering a value in this field is optional.
Original Destination Port	Specifies the traffic destination port: for example, 80 for HTTP traffic.
Local Client IP	Specifies the IP address of your Content Gateway server.
Local Port	Specifies the proxy port: for example, 8080 for HTTP traffic.
User Protocol (Optional)	When <b>dns</b> is selected, the ARM redirects DNS traffic to Content Gateway; otherwise, DNS traffic is bypassed.
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes are discarded.
	<b>Static Bypass</b>
Static Bypass	Displays a table listing the rules in the <i>bypass.config</i> file that specify static transparency bypass rules. When transparency is enabled, the proxy uses these rules to determine whether to bypass incoming client requests or attempt to serve them transparently.
Refresh	Updates the table to display the most up-to-date rules in the <b>bypass.config</b> file.
Edit File	Opens the configuration file editor for the <b>bypass.config</b> file.
	<b>bypass.config Configuration File Editor</b>
rule display box	Lists the <i>bypass.config</i> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.

Option	Description
Rule Type	<p>Specifies the rule type:</p> <p>A <b>bypass</b> rule bypasses specified incoming requests.</p> <p>A <b>deny_dyn_bypass</b> rule prevents the proxy from bypassing specified incoming client requests dynamically (a deny bypass rule can prevent Content Gateway from bypassing itself).</p>
Source IP	<p>Specifies the source IP address in incoming requests that the proxy must bypass or deny bypass. The IP address can be one of the following:</p> <p>A simple IP address, such as 123.45.67.8</p> <p>In CIDR (Classless Inter-Domain Routing) format, such as 1.1.1.0/24.</p> <p>A range separated by a dash, such as 1.1.1.1-2.2.2.2</p> <p>Any combination of the above, separated by commas, such as 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123</p>
Destination IP	<p>Specifies the destination IP address of incoming requests that the proxy must bypass or deny bypass. The IP address can be one of the following:</p> <p>A simple IP address, such as 123.45.67.8</p> <p>In CIDR (Classless Inter-Domain Routing) format, such as 1.1.1.0/24</p> <p>A range separated by a dash, such as 1.1.1.1-2.2.2.2</p> <p>Any combination of the above, separated by commas, such as 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123</p>
Apply	Applies the configuration changes.
Close	<p>Exits the configuration file editor.</p> <p>Click <b>Apply</b> before you click <b>Close</b>; otherwise, all configuration changes will be lost.</p>
	<b>Dynamic Bypass</b>
Dynamic Bypass	<p>Enables or disables the dynamic bypass option to bypass the proxy and go directly to the origin server when clients or servers cause problems. Dynamic bypass rules are deleted when you stop Content Gateway.</p>
Behavior: Non-HTTP, Port 80	<p>Select <b>Enabled</b> to enable dynamic bypass when Content Gateway encounters non-HTTP traffic on port 80.</p> <p>Select <b>Disabled</b> to disable dynamic bypass when Content Gateway encounters non-HTTP traffic on port 80.</p> <p>Select <b>Source-Destination</b> to enable dynamic source/destination bypass when Content Gateway encounters non-HTTP traffic on port 80.</p> <p>Select <b>Destination Only</b> to enable dynamic destination bypass when Content Gateway encounters non-HTTP traffic on port 80.</p>

Option	Description
Behavior: HTTP 400	<p>Select <b>Enabled</b> to enable dynamic bypass when an origin server returns a 400 error.</p> <p>Select <b>Disabled</b> to disable dynamic bypass when an origin server returns a 400 error.</p> <p>Select <b>Source-Destination</b> to enable dynamic source/destination bypass when an origin server returns a 400 error.</p> <p>Select <b>Destination Only</b> to enable dynamic destination bypass when an origin server returns a 400 error.</p>
Behavior: HTTP 401	<p>Select <b>Enabled</b> to enable dynamic bypass when an origin server returns a 401 error.</p> <p>Select <b>Disabled</b> to disable dynamic bypass when an origin server returns a 401 error.</p> <p>Select <b>Source-Destination</b> to enable dynamic source/destination bypass when an origin server returns a 401 error.</p> <p>Select <b>Destination Only</b> to enable dynamic destination bypass when an origin server returns a 401 error.</p>
Behavior: HTTP 403	<p>Select <b>Enabled</b> to enable dynamic bypass when an origin server returns a 403 error.</p> <p>Select <b>Disabled</b> to disable dynamic bypass when an origin server returns a 403 error.</p> <p>Select <b>Source-Destination</b> to enable dynamic source/destination bypass when an origin server returns a 403 error.</p> <p>Select <b>Destination Only</b> to enable dynamic destination bypass when an origin server returns a 403 error.</p>
Behavior: HTTP 405	<p>Select <b>Enabled</b> to enable dynamic bypass when an origin server returns a 405 error.</p> <p>Select <b>Disabled</b> to disable dynamic bypass when an origin server returns a 405 error.</p> <p>Select <b>Source-Destination</b> to enable dynamic source/destination bypass when an origin server returns a 405 error.</p> <p>Select <b>Destination Only</b> to enable dynamic destination bypass when an origin server returns a 405 error.</p>
Behavior: HTTP 406	<p>Select <b>Enabled</b> to enable dynamic bypass when an origin server returns a 406 error.</p> <p>Select <b>Disabled</b> to disable dynamic bypass when an origin server returns a 406 error.</p> <p>Select <b>Source-Destination</b> to enable dynamic source/destination bypass when an origin server returns a 406 error.</p> <p>Select <b>Destination Only</b> to enable dynamic destination bypass when an origin server returns a 406 error.</p>



Option	Description
Behavior: HTTP 408	<p>Select <b>Enabled</b> to enable dynamic bypass when an origin server returns a 408 error.</p> <p>Select <b>Disabled</b> to disable dynamic bypass when an origin server returns a 408 error.</p> <p>Select <b>Source-Destination</b> to enable dynamic source/destination bypass when an origin server returns a 408 error.</p> <p>Select <b>Destination Only</b> to enable dynamic destination bypass when an origin server returns a 408 error.</p>
Behavior: HTTP 500	<p>Select <b>Enabled</b> to enable dynamic bypass when an origin server returns a 500 error.</p> <p>Select <b>Disabled</b> to disable dynamic bypass when an origin server returns a 500 error.</p> <p>Select <b>Source-Destination</b> to enable dynamic source/destination bypass when an origin server returns a 500 error.</p> <p>Select <b>Destination Only</b> to enable dynamic destination bypass when an origin server returns a 500 error.</p>

## WCCP



### Note

The WCCP configuration options appear on the Configure pane only if you have enabled WCCP in the Features table on the **Configure > My Proxy > Basic > General** tab.

The options on this page, and service group settings defined in the **wccp.config** configuration file, control the use of WCCP with Content Gateway.

Administrators are expected to have a good working knowledge of WCCP.

Only WCCP v2 is supported.

It is strongly recommended that you consult the documentation and the manufacturer's support site for information regarding optimal configuration and performance of your WCCP v2 device. Most devices should be configured to take best advantage of hardware-based redirection. With Cisco devices, the most recent version of IOS is usually best.

For every active WCCP service group, there must be a corresponding ARM NAT rule. See [ARM](#), page 295.

When multiple proxy servers are configured in a cluster, all settings **except** the Service Group Enabled/Disabled setting and Weight are propagated around the cluster.

For complete descriptions of Content Gateway support for WCCP v2, see [Transparent interception with WCCP v2 devices](#), page 46.

Option	Description
	<b>General</b>
WCCP Network Interface	Specifies the Ethernet interface Content Gateway uses to talk to the WCCP v2-enabled router(s). If you change this option, you must restart Content Gateway.
WCCP Service Groups	Displays a table of the service groups defined in the <b>wccp.config</b> file. WCCP service group configuration defines WCCP behavior. Column fields are explained in the Configuration Editor entries below.
Refresh	Refreshes the table to display the current definitions in the <b>wccp.config</b> file.
Edit File	Opens <b>wccp.config</b> in the configuration file editor.
	<b>wccp.config Configuration File Editor</b>
Service group display box	Lists the WCCP service group definitions. Select an entry in the list to edit it. Use the “X” button to delete the selection. List order has no meaning; therefore, the up and down arrows can be ignored.
Add	Adds a new service group definition. After Add is clicked, the new definition is displayed in the box at the top of the page.
Set	Accepts modifications to the selected service group definition, displaying the new values in the box at the top of the page.
	<b>Service Group Information</b>
Service Group Status	Enables or disables the service group. This setting is not propagated around a cluster, allowing a service group to be active only on selected members. If you change this option, you must restart Content Gateway.
Service Group Name	Specifies a unique service group name. This is as an aid to administration.
Service Group ID	Specifies a service group ID between 0-255. This ID must also be configured on the router(s). If the specified number is already in use, an error is displayed when Add or Set is clicked.
Protocol	Specifies the protocol, TCP or UDP, that applies to this service group.
Ports	Specifies up to 8 ports in a comma separated list.

Option	Description
	<b>Router Information</b>
Security (optional)	<p>Enables or disables security so that the router and Content Gateway can authenticate each other.</p> <p>If you enable security in Content Gateway, you must also enable security on the router. See your router documentation.</p> <p>If you change this option, you must restart Content Gateway.</p>
Security:Password	<p>Specifies the password used for authentication. The password must be the same password as that configured on the router and can be a maximum of eight characters long.</p> <p>If you change this option, you must restart Content Gateway.</p>
Multicast (optional)	<p>Enables or disables WCCP multicast mode.</p> <p>If you change this option, you must restart Content Gateway.</p>
Multicast: IP Address	<p>Specifies the multicast IP address.</p> <p>If you change this option, you must restart Content Gateway.</p>
WCCP Routers	<p>Specifies the IP addresses of up to 10 WCCP v2-enabled routers in a comma separated list.</p> <p>If multicast is not enabled, the routers in your network are not automatically discovered.</p> <p>If you change this option, you must restart Content Gateway.</p>
	<b>Mode Negotiation</b>
Packet Forward Method	<p>Specifies the preferred encapsulation method used by the WCCP router to transmit intercepted traffic to the proxy. If the router supports GRE and L2, the method specified here is used.</p>
Packet Return Method	<p>Specifies the preferred packet encapsulation method used to return intercepted traffic to the WCCP router.</p> <p><b>Note:</b> The proxy always adjusts to use a method that the router supports. If the router supports GRE and L2, the method specified here is used.</p> <p><b>Note:</b> Selecting L2 requires that the router or switch be Layer 2-adjacent (in the same subnet) as Content Gateway.</p>
	<b>Advanced Settings</b>

Option	Description
Assignment Method	<p>Specifies the method that the router will use to distribute intercepted traffic across multiple proxy servers. Choices are HASH and MASK.</p> <p>The MASK value is applied up to 6 significant bits (in a cluster, a total of 64 buckets are created).</p> <p>See your WCCP documentation for more information about assignment method. Use the value recommended in the manufacturer's documentation for your device.</p>
Distribution attribute(s)	<p>Specifies the attribute that the assignment method uses to determine which requests are distributed to which proxy servers.</p> <p>If the assignment method is HASH, select one or more distribution attributes.</p> <p>If the assignment method is MASK, select one distribution attribute.</p>
Weight	<p>Specifies the distribution of requests to servers in a cluster by proportional weighting. Set weight to a value that is the desired proportion of the total flow of traffic.</p> <p>When all cluster members have a value of 0 (the default), distribution is equal. If any member has a non-zero value, distribution is proportional, relative to the weight values of other members. Members that continue to have a value of zero, receive no traffic.</p>
Reverse Service Group ID	<p>For use only when IP spoofing is enabled.</p> <p>When IP spoofing is enabled, the proxy advertises a reverse service group for each enabled WCCP forward service group. <b>The reverse service group must be applied along the return path of origin server responses to the proxy.</b></p>

## DNS Proxy



### Note

The DNS Proxy configuration options appear on the Configure pane only if you have enabled DNS Proxy in the Features table on the **Configure > My Proxy > Basic > General** tab.

Option	Description
DNS Proxy Port	Specifies the port that Content Gateway uses for DNS traffic. The default port is 5353.

## DNS Resolver

Option	Description
	<b>Resolver</b>
Local Domain Expansion	Enables or disables local domain expansion so that Content Gateway can attempt to resolve unqualified hostnames by expanding to the local domain. For example, if a client makes a request to an unqualified host named <code>hostx</code> , and if the WCG local domain is <code>y.com</code> , Content Gateway expands the hostname to <code>hostx.y.com</code> .
	<b>Host Database</b>
DNS Lookup Timeout	Specifies the maximum number of seconds the proxy can wait for a lookup response from the Domain Name Server.
Foreground Timeout	Specifies how long DNS entries can remain in the database before they are flagged as stale. For example, if this timeout is 24 hours and a client requests an entry that has been in the database for 24 hours or longer, the proxy refreshes the entry before serving it. Caution: Setting the foreground timeout too low might slow response time. Setting it too high risks accumulation of incorrect information.
	<b>Split DNS</b>
Split DNS	Enables or disables the Split DNS option. When enabled, Content Gateway can use multiple DNS servers, depending on your security requirements. For example, you can configure the proxy to look to one set of DNS servers to resolve hostnames on your internal network, while allowing DNS servers outside the firewall to resolve hosts on the Internet. For information about using Split DNS, see <a href="#">Using the Split DNS option</a> , page 161.
Default Domain	Specifies the default domain used for split DNS requests. If a hostname does not include a domain, Content Gateway appends the default domain name to the hostname before choosing which DNS server to use.
DNS Servers Specification	Displays a table listing the rules in the <a href="#">splitdns.config</a> file that control which DNS server the proxy uses for resolving hosts under specific conditions.
Refresh	Updates the table to display the most up-to-date rules in the <a href="#">splitdns.config</a> file. Click this button after you have added or modified rules with the configuration file editor.

Option	Description
Edit File	Opens the configuration file editor so that you can edit and add rules to the <b>splitdns.config</b> file. The configuration file editor page is described below.
	<b>splitdns.config Configuration File Editor</b>
rule display box	Lists the <i>splitdns.config</i> file rules. Select a rule to edit it. The buttons on the left of the box allow you to delete or move the selected rule up or down in the list.
Add	Adds a new rule to the rule display box at the top of the configuration file editor page. Enter information in the fields provided before you click this button.
Set	Updates the rule display box at the top of the configuration file editor page. Select a rule and change its properties before you click this button.
Primary Destination Type	Specifies that DNS server selection is based on the destination domain ( <code>dest_domain</code> ), destination host ( <code>dest_host</code> ), or on a regular expression ( <code>url_regex</code> ).
Primary Destination Value	Specifies the value of the primary destination. Place the symbol “!” at the beginning of the value to specify the NOT logical operator.
DNS Server IP	Specifies the DNS server to use with the primary destination specifier. You can specify a port using a colon (:). If you do not specify a port, 53 is used. You can specify multiple DNS servers separated by spaces or by semicolons (;).
Default Domain Name (Optional)	Specifies the default domain name to use for resolving hosts. Only one entry is allowed. If you do not provide the default domain, the system determines its value from <b>/etc/resolv.conf</b> .
Domain Search List (Optional)	Specifies the domain search order. You can specify multiple domains separated by spaces or by semicolons (;). If you do not provide the search list, the system determines the value from <b>/etc/resolv.conf</b> .
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes are lost.

## ICAP



### Note

The ICAP configuration option appears on the Configure pane only if you have enabled **ICAP** in the **Features** table on the **Configure > My Proxy > Basic > General** tab.

ICAP provides an alternate interface to Websense Data Security and other data security services that are ICAP-conversant. A primary and backup URI can be specified, and failover and load balancing can be configured. See [Configuring the ICAP client](#), page 117 and the subsection for [ICAP failover and load balancing](#), page 118.

Option	Description
ICAP Service URI	<p>Specifies the Uniform Resource Identifier for the ICAP service. The format is:</p> <pre>icap://hostname:port/path</pre> <p>For example:</p> <pre>icap://ICAP_machine:1344/REQMOD</pre> <p>The default ICAP port is 1344. If you are using the default port, you need not specify it in the URI.</p> <p>An optional secondary URI service can be specified immediately after the first by adding a comma and the URI of the second service, no spaces.</p>
Analyze HTTPS Content	Select whether decrypted traffic should be sent to Data Security Suite for analysis or sent directly to the destination.
Analyze FTP Uploads	Select whether to send FTP upload requests to Websense Data Security Suite for analysis. The FTP proxy feature must be enabled. See <a href="#">FTP</a> , page 269.
Action for Communication Errors	Select whether to allow traffic or send a block page if Content Gateway receives an error while communication with Websense Data Security Suite.
Action for Large files	Select whether to allow traffic or send a block page if a file larger than the size limit specified in DSS is sent. The default size limit in DSS is 12 MB.

## Virtual IP

**Note**

The Virtual IP configuration options appear on the Configure pane only if you have enabled Virtual IP in the Features table on the **Configure > My Proxy > Basic > General** tab.

Option	Description
Virtual IP Addresses	Displays a table listing the virtual IP addresses managed by Content Gateway.
Refresh	Updates the table to display the most up-to-date list of virtual IP addresses. Click this button after you have added to or modified the list of virtual IP addresses with the configuration file editor.
Edit File	Opens the configuration file editor so that you can edit and add to the list of virtual IP addresses.
	<b>vaddrs.config Configuration File Editor</b>
rule display box	Lists the virtual IP addresses. Select a virtual IP address to edit it. The buttons on the left of the box allow you to delete or move the selected virtual IP address up or down in the list.
Add	Adds a new virtual IP address to the rule display box at the top of the configuration file editor page.
Set	Updates the rule display box at the top of the configuration file editor page.
Virtual IP Address	Specifies the virtual IP address managed by Content Gateway.
Ethernet Interface	Specifies the network interface assigned to the virtual IP address.
Sub-Interface	Specifies the subinterface ID. This is a number between 1 and 255 that the interface uses for the address.
Apply	Applies the configuration changes.
Close	Exits the configuration file editor. Click <b>Apply</b> before you click <b>Close</b> ; otherwise, all configuration changes will be lost.

## SSL

---

The SSL configuration options are divided into the following categories:

- ◆ Certificates (see [Managing certificates](#), page 134)



- ◆ Decryption/Encryption (see [Configuring SSL Manager for inbound traffic](#), page 136 and [Configuring SSL Manager for outbound traffic](#), page 137)
- ◆ Validation (see [Validating certificates](#), page 138)
- ◆ Incidents (see [Managing Web HTTPS site access](#), page 143)
- ◆ Client certificates (see [Client certificates](#), page 146)
- ◆ Logging (see [Configuring SSL Manager logging](#), page 148)
- ◆ Customization (see [Customizing SSL connection failure messages](#), page 150)
- ◆ Internal Root CA (see [Internal Root CA](#), page 126)



# D

## Event Logging Formats

### Custom logging fields

Related topic:

[Logging format cross-reference, page 312](#)

%<field symbol>	Description
{ <i>HTTP header field name</i> }cqh	Logs the information in the requested field of the client request HTTP header; for example, %<{Accept-Language}cqh> logs the <b>Accept-Language:</b> field in client request headers.
{ <i>HTTP header field name</i> }pqh	Logs the information in the requested field of the proxy request HTTP header; for example, %<{Authorization}pqh> logs the <b>Authorization:</b> field in proxy request headers.
{ <i>HTTP header field name</i> }psh	Logs the information in the requested field of the proxy response HTTP header; for example, %<{Retry-After}psh> logs the <b>Retry-After:</b> field in proxy response headers.
{ <i>HTTP header field name</i> }ssh	Logs the information in the requested field of the server response HTTP header; for example, %<{Age}ssh> logs the <b>Age:</b> field in server response headers.
caun	The client authenticated user name; result of the RFC931/ident lookup of the client user name.
cfsc	The client finish status code; specifies whether the client request to the proxy was successfully completed (FIN) or interrupted (INTR).
chi	The client host IP; the IP address of the client's host machine.
cqbl	The client request transfer length; the body length in the client's request to Content Gateway in bytes.
cqhl	The client request header length; the header length in the client's request to Content Gateway.

%<field symbol>	Description
cqhm	The HTTP method in the client request to Content Gateway: GET, POST, and so on (subset of cqt <sub>x</sub> ).
cqhv	The client request HTTP version.
cqtd	The client request time stamp; specifies the date of the client request in the format <i>yyyy-mm-dd</i> , where <i>yyyy</i> is the 4-digit year, <i>mm</i> is the 2-digit month, and <i>dd</i> is the 2-digit day.
cqtn	The client request time stamp; date and time of the client's request (in the Netscape time stamp format).
cqtq	The client request time stamp with millisecond resolution.
cqts	The client request time stamp in Squid format; the time of the client request in seconds since January 1, 1970.
cqtt	The client request time stamp; the time of the client request in the format <i>hh:mm:ss</i> , where <i>hh</i> is the 2-digit hour in 24-hour format, <i>mm</i> is the 2-digit minutes, and <i>ss</i> is the 2-digit seconds. For example, 16:01:19.
cqtx	The full HTTP client request text, minus headers. For example: GET http://www.company.com HTTP/1.0
cqu	The client request URI; universal resource identifier (URI) of the request from client to Content Gateway (subset of cqt <sub>x</sub> ).
cquc	The client request canonical URL; differs from <i>cqu</i> in that blanks (and other characters that might not be parsed by log analysis tools) are replaced by escape sequences. The escape sequence is a percentage sign followed by the ASCII code number in hex.
cqup	The client request URL path; specifies the argument portion of the URL (everything after the host). For example, if the URL is <b>http://www.company.com/images/x.gif</b> , this field displays <b>/images/x.gif</b> .
cqus	The client request URL scheme (HTTP, FTP, etc.).
crc	The cache result code; specifies how the cache responded to the request (HIT, MISS, and so on).
pfsc	The proxy finish status code; specifies whether the Content Gateway request to the origin server was successfully completed (FIN) or interrupted (INTR).
phn	The host name of the Content Gateway server that generated the log entry in collated log files.
phr	The proxy hierarchy route; the route that Content Gateway used to retrieve the object.
pqbl	The proxy request transfer length; the body length in the Content Gateway request to the origin server.

<b>%&lt;field symbol&gt;</b>	<b>Description</b>
pqhl	The proxy request header length; the header length in the Content Gateway request to the origin server.
pqsi	The proxy request server IP address (0 on cache hits and parent-ip for requests to parent proxies).
pqsn	The proxy request server name; the name of the server that fulfilled the request.
pscl	The proxy response transfer length; the length of the Content Gateway response to the client in bytes.
psct	The proxy response content type; content type of the document (for example, <code>img/gif</code> ) from server response header.
pshl	The proxy response header length; the header length in the Content Gateway response to the client.
psql	The proxy response transfer length in Squid format (includes header and content length).
pssc	The proxy response status code; the HTTP response status code from Content Gateway to the client.
shi	<p>The IP address resolved from the DNS name lookup of the host in the request. For hosts with multiple IP addresses, this field records the IP address resolved from that particular DNS lookup. This can be misleading for cached documents.</p> <p>For example, if the first request was a cache miss and came from IP1 for server S and the second request for server S resolved to IP2 but came from the cache, the log entry for the second request will show IP2.</p>
shn	The host name of the origin server.
sscl	The server response transfer length; response length, in bytes, from origin server to Content Gateway.
sshl	The server response transfer length; the body length in the origin server's response to Content Gateway in bytes.
sshv	The server response HTTP version (1.0, 1.1, and so on).
sssc	The server response status code; the HTTP response status code from origin server to Content Gateway.
ttms	The time Content Gateway spends processing the client request; the number of milliseconds between the time that the client establishes the connection with Content Gateway and the time that Content Gateway sends the last byte of the response back to the client.

%<field symbol>	Description
<code>ttmsf</code>	The time Content Gateway spends processing the client request as a fractional number of seconds; specifies the time in millisecond resolution, but instead of formatting the output as an integer (as with <code>ttms</code> ), the display is formatted as a floating-point number representing a fractional number of seconds. For example, if the time is 1500 milliseconds, this field displays 1.5 while the <code>ttms</code> field displays 1500 and the <code>tts</code> field displays 1.
<code>tts</code>	The time Content Gateway spends processing the client request; the number of seconds between the time that the client establishes the connection with the proxy and the time that the proxy sends the last byte of the response back to the client.
<code>wc</code>	The pre-defined or custom category of the URL for the data being scanned. For example, "News and Media".
<code>wct</code>	The content type of the web page. For example, "text/html; charset=UTF-8".
<code>wsds</code>	The scan disposition string such as CATEGORY_BLOCKED, PERMIT_ALL, FILTERED_AND_PASSED, etc.
<code>wsr</code>	The scan recommended bit ("true" or "false"). The URL database identifies and recommends data that should be analyzed further. Depending on the policy used, the data may or may not be analyzed further.
<code>wstms</code>	The scan time in milliseconds that it took to scan a downloaded file or page.
<code>wui</code>	The authenticated user's ID used to select the policy for scanning data of the client request.

## Logging format cross-reference

---

The following sections illustrate the correspondence between Content Gateway logging fields and standard logging fields for the Squid and Netscape formats.

### Squid logging formats

Squid	Content Gateway Field Symbols
time	cqts
elapsed	ttms
client	chi

Squid	Content Gateway Field Symbols
action/code	crc/pssc
size	psql
method	cqhm
url	cquc
ident	caun
hierarchy/from	phr/pqsn
content	psct

For example, if you want to create a custom format called `short_sq` based on the first three Squid fields, enter a line in the **logs.config** file as follows:

```
format:enabled:1:short_sq:%<cqts> %<ttms>
%<chi>:short_sq:ASCII:none
```

See [Custom format](#), page 199, for more information about defining custom log files.

## Netscape Common logging formats

Netscape Common	Content Gateway Field Symbols
host	chi
usr	caun
[time]	[cqtn]
“req”	“cctx”
s1	pssc
c1	pscl

## Netscape Extended logging formats

Netscape Extended	Content Gateway Field Symbols
host	chi
usr	caun
[time]	[cqtn]
“req”	“cctx”

<b>Netscape Extended</b>	<b>Content Gateway Field Symbols</b>
s1	pssc
c1	pscl
s2	sssc
c2	sscl
b1	cqbl
b2	pqbl
h1	cqhl
h2	pshl
h3	pqhl
h4	sshl
xt	tts

## Netscape Extended-2 logging formats

<b>Netscape Extended-2</b>	<b>Content Gateway Field Symbols</b>
host	chi
usr	caun
[time]	[cqtn]
“req”	“cctx”
s1	pssc
c1	pscl
s2	sssc
c2	sscl
b1	cqbl
b2	pqbl
h1	cqhl
h2	pshl
h3	pqhl
h4	sshl
xt	tts
route	phr
pfs	cfsc



<b>Netscape Extended-2</b>	<b>Content Gateway Field Symbols</b>
ss	pfsc
crc	crc



# E

## Configuration Files

Websense Content Gateway contains the following configuration files that you can edit to customize the proxy.

- ◆ [auth.config](#), page 319
- ◆ [bypass.config](#), page 322
- ◆ [cache.config](#), page 324
- ◆ [filter.config](#), page 327
- ◆ [hosting.config](#), page 330
- ◆ [ip\\_allow.config](#), page 332
- ◆ [ipnat.conf](#), page 333
- ◆ [log\\_hosts.config](#), page 334
- ◆ [logs\\_xml.config](#), page 335
- ◆ [mgmt\\_allow.config](#), page 342
- ◆ [parent.config](#), page 343
- ◆ [partition.config](#), page 346
- ◆ [records.config](#), page 347
- ◆ [remap.config](#), page 401
- ◆ [socks.config](#), page 402
- ◆ [splitdns.config](#), page 404
- ◆ [storage.config](#), page 406
- ◆ [update.config](#), page 406
- ◆ [wccp.config](#), page 408

### Specifying URL regular expressions (url\_regex)

Entries of type `url_regex` within the configuration files use regular expressions to perform a match.

The following table offers examples to illustrate how to create a valid `url_regex`.

Value	Description
<code>x</code>	Matches the character <code>x</code> .
<code>.</code>	Match any character.
<code>^</code>	Specifies beginning of line.
<code>\$</code>	Specifies end of line.
<code>[xyz]</code>	A <i>character class</i> . In this case, the pattern matches either <code>x</code> , <code>y</code> , or <code>z</code> .
<code>[abj-oZ]</code>	A <i>character class</i> with a range. This pattern matches <code>a</code> , <code>b</code> , any letter from <code>j</code> through <code>o</code> , or <code>Z</code> .
<code>[^A-Z]</code>	A <i>negated character class</i> . For example, this pattern matches any character except those in the class.
<code>r*</code>	Zero or more <code>r</code> 's, where <code>r</code> is any regular expression.
<code>r+</code>	One or more <code>r</code> 's, where <code>r</code> is any regular expression.
<code>r?</code>	Zero or one <code>r</code> , where <code>r</code> is any regular expression.
<code>r{2,5}</code>	From two to five <code>r</code> 's, where <code>r</code> is any regular expression.
<code>r{2,}</code>	Two or more <code>r</code> 's, where <code>r</code> is any regular expression.
<code>r{4}</code>	Exactly 4 <code>r</code> 's, where <code>r</code> is any regular expression.
<code>"[xyz]"images"</code>	The literal string <code>[xyz]"images"</code>
<code>\X</code>	If <code>X</code> is <code>a</code> , <code>b</code> , <code>f</code> , <code>n</code> , <code>r</code> , <code>t</code> , or <code>v</code> , then the ANSI-C interpretation of <code>\x</code> ; Otherwise, a literal <code>X</code> . This is used to escape operators such as <code>*</code> .
<code>\0</code>	A NULL character.
<code>\123</code>	The character with octal value 123.
<code>\x2a</code>	The character with hexadecimal value 2a.
<code>(r)</code>	Matches an <code>r</code> ; where <code>r</code> is any regular expression. You can use parentheses to override precedence.
<code>rs</code>	The regular expression <code>r</code> , followed by the regular expression <code>s</code> .
<code>r s</code>	Either an <code>r</code> or an <code>s</code> .
<code>#&lt;n&gt;#</code>	Inserts an <i>end</i> node causing regular expression matching to stop when reached. The value <code>n</code> is returned.

## Examples

You can specify `dest_domain=mydomain.com` to match any host in `mydomain.com`. Likewise, you can specify `dest_domain=.` to match any request.

## auth.config

The **auth.config** file stores rules that direct specified IP addresses and IP address ranges, and/or traffic on specified inbound ports (explicit proxy only) to distinct domain controllers. This feature is called [Multiple realm authentication](#), page 179. Authentication realm rules are defined on the **Configure > Security > Access Control > Authentication Realms** tab.

- ◆ Multiple realm authentication is supported for Integrated Windows Authentication (IWA), legacy NTLM, and LDAP authentication only.
- ◆ Each authentication rule specifies source IP addresses, and/or inbound port (explicit proxy only), the authentication method, the domain, and additional related options.
- ◆ Multiple rules can be active at the same time. In this way, multiple authentication methods can be used at the same time.
- ◆ The specifiers used in IWA, LDAP, and NTLM rules differ.
- ◆ Rules are applied from the list top-down; only the first match is applied. If the IP address is not matched by any rule, no authentication is attempted.



### Note

If all of the clients in your network are authenticated by authentication servers that share trust relationships, you don't need to create rules for multiple authentication realms.

## Format

Each line in **auth.config** contains an authentication rule that consists of a set of tags, each followed by its value. Authentication rules have the format:

```
type=<auth_type> name=<profile_name> src_ip=<IP addresses> <additional tags>
```

The following table lists the tags that are common to all rules.

Universal Tags	Allowed Value
type	Takes a string denoting the rule type: winauth, ntlm, ldap
enabled	Specifies whether the rule will be active: <ul style="list-style-type: none"> <li>• 0 = disabled</li> <li>• 1 = enabled</li> </ul>
name	Is a simple, unique name used in logging.
src_ip	Takes a comma separated list of IP addresses and IP address ranges.
proxy_port (optional)	Takes a port number.

Universal Tags	Allowed Value
use_alias	Specifies the user name sent to filtering service if authentication is successful. <ul style="list-style-type: none"> <li>• 0 = send actual authenticated user name (default).</li> <li>• 1 = send a blank username</li> <li>• 2 = send the string specified in auth_name_string</li> </ul>
auth_name_string	Only active if use_alias=2. Specifies the static string to be sent as the user name for all successful authentications using this rule.

The following table lists the additional tags used in Integrated Windows Authentication rules.

IWA Tags	Allowed Value
winauth_realm	Specifies the joined Windows domain to use with the rule. Content Gateway must be joined and active in that domain.

The following table lists the additional tags used in an NTLM rule.

Universal Tags	Allowed Value
dc_list	Takes the IP address and port number of the primary domain controller (if no port is specified, Content Gateway uses port 139), followed by a comma separated list of secondary domain controllers to be used for load balancing and failover.
dc_load_balance (optional)	Specifies whether load balancing is used: <ul style="list-style-type: none"> <li>• 0 = disabled</li> <li>• 1 = enabled</li> </ul> <p><b>Note:</b> When multiple domain controllers are specified, even if load balancing is disabled, when the load on the primary domain controller reaches the maximum number of connections allowed, new requests are sent to a secondary domain controller as a short-term failover provision, until such time that the primary domain controller can accept new connections.</p>

The following table lists the additional tags used in an LDAP rule.

LDAP Tag	Allowed Value
server_name	Specifies the fully qualified domain name of the LDAP server.
server_port (optional)	Specifies the LDAP server port. The default is 389. If Secure LDAP is enabled, set the port to 636 or 3269 (the secure LDAP ports).
base_dn (optional)	Specifies the LDAP base distinguished name.
uid_filter (optional)	Specifies the type of service, if different from that configured on the LDAP tab. Enter <b>sAMAccountName</b> for Active Directory, or <b>uid</b> for any other service.
bind_dn (optional)	Specifies the bind distinguished name. This must be a Full Distinguished Name of a user in the LDAP directory service. For example: CN=John Smith,CN=USERS,DC=MYCOMPANY,DC=COM
bind_pwd (optional)	Specifies the password for the bind distinguished name.
sec_bind	Specifies whether Content Gateway will use secure communication with the LDAP server. <ul style="list-style-type: none"> <li>• 0 = disabled</li> <li>• 1 = enabled</li> </ul> If enabled, set the LDAP port to 636 or 3269 (secure LDAP ports).
attr	Specifies an LDAP attribute name.
attr_value	Specifies an LDAP attribute value.

## Examples

Integrated Windows Authentication:

```
type=winauth name=CorpHQ src_ip=10.1.1.1,10.10.0.0-10.100.254.254 proxy_port=0 status=1 domain=BigCorp.com
```

NTLM:

```
type=ntlm name=CorpHQ src_ip=10.1.1.1,12.13.0.0-12.13.0.128
dc_list=HQdc1.BigCorp.com,HQdc2.BigCorp.com
```

LDAP:

```
type=ldap name=CorpHQ src_ip=10.1.1.1,12.13.0.0-12.13.0.128
server_name=HQldap1.BigCorp.com server_port=389
```

**Note**

Rules are applied by first match in the order listed.

---

## bypass.config

---

The **bypass.config** file contains *static* bypass rules that Content Gateway uses in transparent proxy caching mode. Static bypass rules instruct Content Gateway to bypass certain incoming client requests so that they are served by the origin server.

The **bypass.config** file also accepts *dynamic* deny bypass rules. See [Dynamic deny bypass rules](#), page 323.

You can configure three types of static bypass rules:

- ◆ *Source bypass* rules configure the proxy to bypass a particular source IP address or range of IP addresses. For example, you can bypass clients that do not want to use caching.
- ◆ *Destination bypass* rules configure the proxy to bypass a particular destination IP address or range of IP addresses. For example, you can bypass origin servers that use IP authentication based on the client's real IP address.

**Important**

Destination bypass rules prevent the proxy from caching an entire site. You will experience hit rate impacts if the site you bypass is popular.

- ◆ *Source/destination pair* bypass rules configure the proxy to bypass requests that originate from the specified source to the specified destination. For example, you can route around specific client-server pairs that experience broken IP authentication or out-of-band HTTP traffic problems when cached. Source/destination bypass rules can be preferable to destination rules because they block a destination server only for users that experience problems.



## Format

Bypass rules have the following format:

```
bypass src ipaddress | dst ipaddress | src ipaddress AND dst
ipaddress
```

Option	Description
<i>src ipaddress</i>	<p>Specifies the source (client) IP address in incoming requests that the proxy must bypass.</p> <p><i>ipaddress</i> can be one of the following:</p> <p>A simple IP address, such as 123.45.67.8</p> <ul style="list-style-type: none"> <li>• In CIDR (Classless Inter-Domain Routing) format, such as 1.1.1.0/24</li> <li>• A range separated by a dash, such as 1.1.1.1-2.2.2.2</li> <li>• Any combination of the above, separated by commas, such as 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123</li> </ul>
<i>dst ipaddress</i>	<p>Specifies the destination (origin server) IP address in incoming requests that the proxy must bypass.</p> <p><i>ipaddress</i> can be one of the following:</p> <p>A simple IP address, such as 123.45.67.8</p> <ul style="list-style-type: none"> <li>• In CIDR (Classless Inter-Domain Routing) format, such as 1.1.1.0/24</li> <li>• A range separated by a dash, such as 1.1.1.1-2.2.2.2</li> <li>• Any combination of the above, separated by commas, such as 1.1.1.0/24, 25.25.25.25, 123.1.23.1-123.1.23.123</li> </ul>
<i>src ipaddress</i> AND <i>dst ipaddress</i>	<p>Specifies the source and destination IP address pair that the proxy must bypass.</p> <p><i>ipaddress</i> must be a single IP address, such as 123.45.67.8</p>

## Dynamic deny bypass rules

In addition to static bypass rules, the **bypass.config** file also accepts *dynamic deny* bypass rules.

Deny bypass rules prevent the proxy from bypassing certain incoming client requests dynamically (a deny bypass rule can prevent the proxy from bypassing itself).

Dynamic deny bypass rules can be source, destination, or source/destination and have the following format:

```
deny_dyn_bypass src ipaddress | dst ipaddress | src
ipaddress AND dst ipaddress
```

For a description of the options, see the table in [Format, page 323](#).

**Note**

For the dynamic deny bypass rules to work, you must enable the **Dynamic Bypass** option in Content Gateway Manager or set the variable `proxy.config.arm.bypass_dynamic_enabled` to 1 in the **records.config** file.

**Important**

Static bypass rules overwrite dynamic deny bypass rules. Therefore, if a static bypass rule and a dynamic bypass rule contain the same IP address, the dynamic deny bypass rule is ignored.

## Examples

The following example shows source, destination, and source/destination *bypass* rules:

```
bypass src 1.1.1.0/24, 25.25.25.25, 128.252.11.11-128.252.11.255
bypass dst 24.24.24.0/24
bypass src 25.25.25.25 AND dst 24.24.24.0
```

The following example shows source, destination, and source/destination *dynamic deny bypass* rules:

```
deny_dyn_bypass src 128.252.11.11-128.252.11.255
deny_dyn_bypass dst 111.111.11.1
deny_dyn_bypass src 111.11.11.1 AND dst 111.11.1.1
```

## cache.config

---

The **cache.config** file defines how the proxy caches Web objects. You can add caching rules to specify the following configuration:

- ◆ Not to cache objects from specific IP addresses
- ◆ How long to pin particular objects in the cache
- ◆ How long to consider cached objects as fresh

- ◆ Whether to ignore no-cache directives from the server



### Important

After you modify this file, run `content_line -x` from the Content Gateway **bin** directory (`/opt/WCG/bin`) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

## Format

Each line in the **cache.config** file contains a caching rule. Content Gateway recognizes three space-delimited tags:

```
primary_destination=value secondary_specifier=value
action=value
```

The following table lists the possible primary destinations and their allowed values.

Primary Destination	Allowed Value
dest_domain	A requested domain name
dest_host	A requested hostname
dest_ip	A requested IP address
url_regex	A regular expression to be found in a URL

Secondary specifiers are optional in the **cache.config** file. The following table lists the possible secondary specifiers and their allowed values.



### Note

You can use more than one secondary specifier in a rule. However, you cannot repeat a secondary specifier.

Secondary Specifier	Allowed Value
port	A requested URL port
scheme	A request URL protocol; one of the following: <ul style="list-style-type: none"> <li>• HTTP</li> <li>• FTP</li> </ul>
prefix	A prefix in the path part of a URL
suffix	A file suffix in the URL

Secondary Specifier	Allowed Value
method	A request URL method; one of the following: <ul style="list-style-type: none"> <li>• get</li> <li>• put</li> <li>• trace</li> </ul>
time	A time range, such as 08:00-14:00
src_ip	A client IP address.
user_agent	A request header User-Agent value.

The following table lists the possible actions and their allowed values.

Action	Value
action	One of the following values: <ul style="list-style-type: none"> <li>• <code>never-cache</code> configures the proxy to never cache specified objects.</li> <li>• <code>ignore-no-cache</code> configures the proxy to ignore all <code>Cache-Control: no-cache</code> headers.</li> <li>• <code>ignore-client-no-cache</code> configures the proxy to ignore <code>Cache-Control: no-cache</code> headers from client requests.</li> <li>• <code>ignore-server-no-cache</code> configures the proxy to ignore <code>Cache-Control: no-cache</code> headers from origin server responses.</li> </ul>
pin-in-cache	The amount of time you want to keep the object(s) in the cache. The following time formats are allowed: <ul style="list-style-type: none"> <li>• <i>d</i> for days (for example 2d)</li> <li>• <i>h</i> for hours (for example, 10h)</li> <li>• <i>m</i> for minutes (for example, 5m)</li> <li>• <i>s</i> for seconds (for example, 20s)</li> <li>• mixed units (for example, 1h15m20s)</li> </ul>
revalidate	The amount of time you want to consider the object(s) fresh. Use the same time formats as <code>pin-in-cache</code> .
ttd-in-cache	The amount of time you want to keep objects in the cache regardless of <code>Cache-Control</code> response headers. Use the same time formats as <code>pin-in-cache</code> and <code>revalidate</code> .

## Examples

The following example configures the proxy to never cache FTP documents requested from the IP address 112.12.12.12:

```
dest_ip=112.12.12.12 scheme=ftp action=never-cache
```

The following example configures the proxy to keep documents with URLs that contain the regular expression `politics` and the path **prefix/viewpoint** in the cache for 12 hours:

```
url_regex=politics prefix=/viewpoint pin-in-cache=12h
```

The following example configures the proxy to revalidate `gif` and `jpeg` objects in the domain `mydomain.com` every 6 hours and all other objects in `mydomain.com` every hour:

```
dest_domain=mydomain.com suffix=gif revalidate=6h
dest_domain=mydomain.com suffix=jpeg revalidate=6h
dest_domain=mydomain.com revalidate=1h
```

**Note**

The rules are applied in the order listed.

---

## filter.config

---

Filtering rules stored in **filter.config** allow you to:

- ◆ Deny or allow URL requests
- ◆ Keep or strip header information from client requests
- ◆ Allow specified applications or requests to specified web sites to bypass authentication
- ◆ Prevent specified applications from transiting the proxy

Filtering rules are most conveniently defined in Content Gateway Manager on the **Configure > Security > Access Control > Filtering** tab. See [Creating filtering rules](#), page 157.

**Note**

Filtering rules for NTLM and LDAP are defined on the **Access Control > Authentication Realms** tab and stored in the [auth.config](#) file.

---

**Important**

After you modify the file, run `content_line -x` from the Content Gateway **bin** directory (`/opt/WCG/bin`) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

---

## Format

Each line in **filter.config** is a filtering rule. Content Gateway applies the rules in the order listed, starting at the top of the file. If no rule matches, the request is allowed to proceed.

Content Gateway recognizes three space-delimited tags:

```
primary_destination=value secondary_specifier=value action=value
```

The following table lists the possible primary destinations.

Primary Destination	Allowed Value
dest_domain	A requested domain name
dest_host	A requested hostname
dest_ip	A requested IP address
url_regex	A regular expression to be found in a URL

Secondary specifiers are optional. The following table lists the possible secondary specifiers and their purpose.



### Note

You can use more than one secondary specifier in a rule. However, you cannot repeat a secondary specifier.

Secondary Specifier	Allowed Value
time	A time range, such as 08:00-14:00
prefix	A prefix in the path part of a URL
suffix	A file suffix in the URL
src_ip	A single client IP address, or a client IP address range.
port	A requested URL port
method	A request URL method; one of the following: <ul style="list-style-type: none"> <li>• get</li> <li>• post</li> <li>• put</li> <li>• trace</li> </ul>

Secondary Specifier	Allowed Value
scheme	A request URL protocol. You can specify one of the following: <ul style="list-style-type: none"> <li>• HTTP</li> <li>• HTTPS</li> <li>• FTP (for FTP over HTTP only)</li> </ul>
user_agent	A request header User-Agent value.

The following table lists the possible actions and their allowed values.

Action	Allowed Value
action	Specify one of the following: <ul style="list-style-type: none"> <li>• <b>allow</b> - to allow particular URL requests to bypass authentication. The proxy caches and serves the requested content.</li> <li>• <b>deny</b> - to deny requests for HTTP or FTP objects from specific destinations. When a request is denied, the client receives an access denied message.</li> <li>• <b>radius</b> - not supported.</li> </ul>
keep_hdr	The client request header information that you want to keep. You can specify the following options: <ul style="list-style-type: none"> <li>• date</li> <li>• host</li> <li>• cookie</li> <li>• client_ip</li> </ul>
strip_hdr	The client request header information that you want to strip. You can specify the same options as with <b>keep_hdr</b> .

## Examples

The following example configures Content Gateway to deny all FTP document requests to the IP address 112.12.12.12:

```
dest_ip=112.12.12.12 scheme=ftp action=deny
```

The following example configures Content Gateway to keep the client IP address header for URL requests that contain the regular expression `politics` and whose path prefix is

**/viewpoint:**

```
url_regex=politics prefix=/viewpoint keep_hdr=client_ip
```

The following example configures Content Gateway to strip all cookies from client requests destined for the origin server **www.server1.com**:

```
dest_host=www.server1.com strip_hdr=cookie
```

The following example configures Content Gateway to disallow **puts** to the origin server **www.server2.com**:

```
dest_host=www.server2.com method=put action=deny
```

Content Gateway applies the rules in the order listed in the file. For example, the following sample **filter.config** file configures Content Gateway to do the following:

- ◆ Allow all users (except those trying to access internal.com) to access server1.com
- ◆ Deny all users access to notthatsite.com

```
dest_host=server1.com action=allow
dest_host=notthatsite.com action=deny
```

## hosting.config

---

The **hosting.config** file lets you assign cache partitions to specific origin servers and domains so that you can manage your cache space more efficiently and restrict disk usage.

For step-by-step instructions on partitioning the cache according to origin servers and domains, see [Partitioning the cache according to origin server or domain](#), page 86.



### Note

Before you can assign cache partitions to specific origin servers and domains, you must partition your cache according to size and protocol in the **partition.config** file. For more about cache partitioning, see [Partitioning the cache](#), page 85. For a description of the **partition.config** file, see [partition.config](#), page 346.

After you modify the **hosting.config** file, run **content\_line -x** from the Content Gateway **bin** directory to apply the changes. When you apply the changes to a node in a cluster, Content Gateway automatically applies the changes to all nodes in the cluster.



### Important

The partition configuration must be the same on all nodes in a cluster.

## Format

Each line in the **hosting.config** file must have one of the following formats:

```
hostname=hostname partition=partition_numbers
domain=domain_name partition=partition_numbers
```

where:



**hostname** is the fully qualified hostname of the origin server whose content you want to store on a particular partition (for example, `www.myhost.com`).

**domain\_name** is the domain whose content you want to store on a particular partition (for example, `mydomain.com`).

**partition\_numbers** is a comma-separated list of the partitions on which you want to store the content that belongs to the origin server or domain listed. The partition numbers must be valid numbers listed in the **partition.config** file (see [partition.config](#), page 346).



---

**Note**

If you want to allocate more than one partition to an origin server or domain, enter the partitions in a comma-separated list on one line. The **hosting.config** file cannot contain multiple entries for the same origin server or domain.

---

## Generic Partition

When configuring the **hosting.config** file, you must assign a generic partition to use for content that does not belong to any of the origin servers or domains listed. If all partitions for a particular origin server become corrupt, Content Gateway uses the generic partition to store content for that origin server.

The generic partition must have the following format:

```
hostname=* partition=partition_numbers
```

where **partition\_numbers** is a comma-separated list of generic partitions.

## Examples

The following example configures the proxy to store content from the domain **mydomain.com** in partition 1 and content from **www.myhost.com** in partition 2. The proxy stores content from all origin servers in partitions 3 and 4.

```
domain=mydomain.com partition=1
hostname=www.myhost.com partition=2
hostname=* partition=3,4
```

## ip\_allow.config

---

The **ip\_allow.config** file controls client access to the proxy. You can specify ranges of IP addresses that are allowed to use Content Gateway.



### Important

After you modify the file, run `content_line -x` from the Content Gateway **bin** directory (**/opt/WCG/bin**) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

## Format

Each line in the **ip\_allow.config** file must have the following format:

```
src_ip=ipaddress action=ip_allow | ip_deny
```

where *ipaddress* is the IP address or range of IP addresses of the clients allowed to access the proxy.

The action `ip_allow` allows the specified clients to access the proxy.

The action `ip_deny` denies the specified clients to access the proxy.

By default, the **ip\_allow.config** file contains the following line, which allows all clients to access the proxy. Comment out or delete this line before adding rules to restrict access.

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

## Examples

The following example allows all clients to access the proxy:

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

The following example allows all clients on a specific subnet to access the proxy:

```
src_ip=123.12.3.000-123.12.3.123 action=ip_allow
```

The following example denies all clients on a specific subnet to access the proxy:

```
src_ip=123.45.6.0-123.45.6.123 action=ip_deny
```

## ipnat.conf

---

The **ipnat.conf** file contains redirection rules that specify how incoming packets are readdressed when the proxy is serving traffic transparently. Content Gateway creates the redirection rules during installation. You can modify these rules.



---

**Important**

After you modify this file, you must restart the proxy.

---

## Format

Each line in the **ipnat.conf** file must have the following format:

```
rdr interface 0.0.0.0/0 port dest -> ipaddress port proxy  
tcp|udp
```

where:

*interface* is the Ethernet interface that traffic will use to access the Content Gateway machine (for example, `eth0` on Linux).

*dest* is the traffic destination port (for example, `80` for HTTP traffic).

*ipaddress* is the IP address of your Content Gateway server.

*proxy* is the Content Gateway proxy port (usually `8080` for HTTP traffic).

## Examples

The following example configures the ARM to readdress all incoming HTTP traffic to the Content Gateway IP address (`111.111.11.1`) on the Content Gateway proxy port `8080`:

```
rdr hme0 0.0.0.0/0 port 80 -> 111.111.11.1 port 8080 tcp
```

## log\_hosts.config

---

To record HTTP/FTP transactions for different origin servers in separate log files, you must list each origin server's hostname in the **log\_hosts.config** file. In addition, you must enable the HTTP host splitting option (see [HTTP host log splitting](#), page 207).



### Note

It is recommended that you use the same **log\_hosts.config** file on every Content Gateway node in your cluster.



### Important

After you modify this file, run `content_line -x` from the Content Gateway **bin** directory (`/opt/WCG/bin`) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

## Format

Each line in the **log\_hosts.config** file has the following format:

*hostname*

where *hostname* is the hostname of the origin server.



### Note

You can specify keywords in the **log\_hosts.config** file to record all transactions from origin servers with the specified keyword in their names in a separate log file. See the example below.

## Examples

The following example configures Content Gateway to create separate log files containing all HTTP/FTP transactions for the origin servers `webserver1`, `webserver2`, and `webserver3`.

```
webserver1
webserver2
webserver3
```

The following example records all HTTP and FTP transactions from origin servers that contain `sports` in their names (for example, `sports.yahoo.com` and

www.foxsports.com) in a log file called **squid-sport.log** (the Squid format is enabled):

```
sports
```

## logs\_xml.config

---

The **logs\_xml.config** file defines the custom log file formats, filters, and processing options. The format of this file is modeled after XML, the Extensible Markup Language.

### Format

The **logs\_xml.config** file contains the following specifications:

- ◆ **LogFormat** specifies the fields to be gathered from each protocol event access. See [LogFormat](#), page 336.
- ◆ **LogFilter** specifies the filters that are used to include or exclude certain entries being logged based on the value of a field within that entry. See [LogFilter](#), page 337.
- ◆ **LogObject** specifies an object that contains a particular format, a local filename, filters, and collation servers. See [LogObject](#), page 338.



#### Note

The **logs\_xml.config** file ignores extra white space, blank lines, and all comments.

---

## LogFormat

The following table lists the LogFormat specifications.

Field	Allowed Inputs
<code>&lt;Name = "valid_format_name"/&gt;</code>	Required. Valid format names include any name except squid, common, extended, or extended2, which are pre-defined formats. There is no default for this tag.
<code>&lt;Format = "valid_format_specification"/&gt;</code>	Required. A valid format specification is a printf-style string describing each log entry when formatted for ASCII output. Use '%<field>' as placeholders for valid field names. For more information, see <a href="#">Custom logging fields, page 309</a> . The specified field can be of two types: Simple: for example, %<cqu> A field within a container, such as an HTTP header or a Content Gateway statistic. Fields of this type have the syntax: '%<{field}container>'. 
<code>&lt;Interval = "aggregate_interval_secs"/&gt;</code>	Use this tag when the format contains aggregate operators. The value "aggregate_interval_secs" represents the number of seconds between individual aggregate values being produced. The valid set of aggregate operators are: <ul style="list-style-type: none"> <li>• COUNT</li> <li>• SUM</li> <li>• AVG</li> <li>• FIRST</li> <li>• LAST</li> </ul>

## LogFilter

The following table lists the LogFilter specifications.

Field	Allowed Inputs
<code>&lt;Name = "valid_filter_name"/&gt;</code>	Required. All filters must be uniquely named.
<code>&lt;Condition = "valid_log_field valid_operator valid_comparison_value"/&gt;</code>	<p>Required. This field contains the following elements:</p> <p><code>valid_log_field</code> - the field that will be compared against the given value. For more information, see <a href="#">Logging format cross-reference, page 312</a>.</p> <p><code>valid_operator_field</code> - any one of the following: MATCH, CASE_INSENSITIVE_MATCH, CONTAIN, CASE_INSENSITIVE_CONTAIN. MATCH is true if the field and value are identical (case sensitive). CASE_INSENSITIVE_MATCH is similar to MATCH, only case insensitive. CONTAIN is true if the field contains the value (the value is a substring of the field). CASE_INSENSITIVE_CONTAIN is a case-insensitive version of CONTAIN.</p> <p><code>valid_comparison_value</code> - any string or integer matching the field type. For integer values, all of the operators are equivalent and mean that the field must be equal to the specified value.</p> <p>Note: There are no negative comparison operators. If you want to specify a negative condition, use the <b>Action</b> field to REJECT the record.</p>
<code>&lt;Action = "valid_action_field"/&gt;</code>	Required. ACCEPT or REJECT. This instructs Content Gateway to either accept or reject records satisfying the condition of the filter.

## LogObject

The following table lists the `LogObject` specifications.

Field	Allowed Inputs
<code>&lt;Format = "valid_format_name" /&gt;</code>	Required. Valid format names include the predefined logging formats: <code>squid</code> , <code>common</code> , <code>extended</code> , and <code>extended2</code> , as well as any previously-defined custom log formats. There is no default for this tag.
<code>&lt;Filename = "file_name" /&gt;</code>	<p>Required. The filename to which the given log file is written on the local file system or on a remote collation server. No local log file will be created if you fail to specify this tag. All filenames are relative to the default logging directory.</p> <p>If the name does not contain an extension (for example, <code>squid</code>), the extension <code>.log</code> is automatically appended to it for ASCII logs and <code>.blog</code> for binary logs. (See <code>&lt;Mode = "valid_logging_mode" /&gt;</code> below.)</p> <p>If you do not want an extension to be added, end the filename with a single dot (<code>.</code>): for example, <code>squid.</code></p>



Field	Allowed Inputs
<code>&lt;Mode = "valid_logging_mode"/&gt;</code>	<p>Valid logging modes include <code>ascii</code>, <code>binary</code>, and <code>ascii_pipe</code>. The default is <code>ascii</code>.</p> <p>Use <code>ascii</code> to create event log files in human-readable form (plain ASCII).</p> <p>Use <code>binary</code> to create event log files in binary format. Binary log files generate lower system overhead and occupy less space on the disk (depending on the information being logged). You must use the <code>logcat</code> utility to translate binary log files to ASCII format before you can read them.</p> <p>Use <code>ascii_pipe</code> to write log entries to a UNIX named pipe (a buffer in memory). Other processes can then read the data using standard I/O functions. Content Gateway does not have to write to disk, freeing disk space and bandwidth for other tasks. In addition, writing to a pipe does not stop when logging space is exhausted because the pipe does not use disk space.</p> <p>Note: If you are using a collation server, the log is written to a pipe on the collation server. A local pipe is created even before a transaction is processed so that you can see the pipe right after Content Gateway starts. However, pipes on a collation server <i>are</i> created when Content Gateway starts.</p>
<code>&lt;Filters = "list_of_valid_filter_names"/&gt;</code>	A comma-separated list of names of any previously defined log filters. If more than one filter is specified, all filters must accept a record for the record to be logged.
<code>&lt;Protocols = "list_of_valid_protocols"/&gt;</code>	A comma-separated list of the protocols this object should log. Valid protocol names include <code>HTTP</code> .
<code>&lt;ServerHosts = "list_of_valid_servers"/&gt;</code>	A comma-separated list of valid hostnames. This tag indicates that only entries from the named servers will be included in the file.
<code>&lt;CollationHosts = "list_of_valid_hostnames"/&gt;</code>	A comma-separated list of collation servers to which all log entries (for this object) are forwarded. Collation servers can be specified by name or IP address. Specify the collation port with a colon after the name (for example, <code>host:port</code> ).

Field	Allowed Inputs
<code>&lt;Header = "header"/&gt;</code>	The header text you want the log files to contain. The header text appears at the beginning of the log file, just before the first record.
<code>&lt;RollingEnabled = "truth value"/&gt;</code>	<p>Enables or disables log file rolling for the <i>LogObject</i>. This setting overrides the value for the configuration setting <b>Log Rolling: Enabled/Disabled</b> in Content Gateway Manager or <i>proxy.config.log2.rolling_enabled</i> in the <b>records.config</b> file.</p> <p>Set “truth value” to 1 or true to enable rolling; set it to 0 or false to disable rolling for this particular <i>LogObject</i>.</p>
<code>&lt;RollingIntervalSec = "seconds"/&gt;</code>	<p>Specifies the seconds between log file rolling for the <i>LogObject</i>. This setting overrides the value for the configuration setting <b>Log Rolling: Interval</b> in Content Gateway Manager or <i>proxy.config.log2.rolling_interval_sec</i> in the <b>records.config</b> file. This option allows you to specify different rolling intervals for different <i>LogObjects</i>.</p>
<code>&lt;RollingOffsetHr = "hour"/&gt;</code>	<p>Specifies an hour (from 0 to 23) at which rolling is guaranteed to “align”. Rolling may start before then, but a rolled file will be produced only at that time. The impact of this setting is only noticeable if the rolling interval is larger than one hour. This setting overrides the configuration setting <b>Log Rolling: Offset Hour</b> in Content Gateway Manager or <i>proxy.config.log2.rolling_offset_hr</i> in the <b>records.config</b> file.</p>

## Examples

The following is an example of a *LogFormat* specification collecting information using three common fields:

```
<LogFormat>
<Name = "minimal"/>
<Format = "%<chi> : %<cqu> : %<pssc>"/>
</LogFormat>
```

The following is an example of a LogFormat specification using aggregate operators:

```
<LogFormat>
<Name = "summary"/>
<Format = "%<LAST(cqts)> : %<COUNT(*)> : %<SUM(psql)>"/>
<Interval = "10"/>
</LogFormat>
```

The following is an example of a LogFilter that will cause only REFRESH\_HIT entries to be logged:

```
<LogFilter>
<Name = "only_refresh_hits"/>
<Action = "ACCEPT"/>
<Condition = "%<pssc> MATCH REFRESH_HIT"/>
</LogFilter>
```

**Note**

When specifying the field in the filter condition, you can omit the %<. This means that the following filter is equivalent to the example directly above:

```
<LogFilter>
  <Name = "only_refresh_hits"/>
  <Action = "ACCEPT"/>
  <Condition = "pssc MATCH REFRESH_HIT"/>
</LogFilter>
```

---

The following is an example of a LogObject specification that creates a local log file for the minimal format defined earlier. The log filename will be **minimal.log** because this is an ASCII log file (the default).

```
<LogObject>
<Format = "minimal"/>
<Filename = "minimal"/>
</LogObject>
```

The following is an example of a LogObject specification that includes only HTTP requests served by hosts in the domain company.com or by the specific server server.somewhere.com. Log entries are sent to port 4000 of the collation host logs.company.com and to port 5000 of the collation host 209.131.52.129.

```
<LogObject>
<Format = "minimal"/>
<Filename = "minimal"/>
<ServerHosts = "company.com, server.somewhere.com"/>
<Protocols = "http"/>
<CollationHosts =
"logs.company.com:4000, 209.131.52.129:5000"/>
</LogObject>
```

## WELF (WebTrends Enhanced Log Format)

Content Gateway supports WELF, the WebTrends Enhanced Log Format, so that you can analyze Content Gateway log files with WebTrends reporting tools. A predefined `<LogFormat>` that is compatible with WELF is provided at the end of the `logs.config` file (shown below). To create a WELF format log file, create a `<LogObject>` that uses this predefined format.

```
<LogFormat>
<Name = "welf"/>
<Format = "id=firewall time=\"%<cqtd> %<cqtd>\\" fw=%<phn>
pri=6 proto=%<cqus> duration=%<ttmsf> sent=%<psql>
rcvd=%<cqhl> src=%<chi> dst=%<shi> dstname=%<shn>
user=%<caun> op=%<cqhm> arg=\"%<cqup>\\" result=%<pssc>
ref=\"%<{Referer}>cqh>\\" agent=\"%<{user-agent}>cqh>\\"
cache=%<crc>"/>
</LogFormat>
```

## mgmt\_allow.config

---

The **mgmt\_allow.config** file specifies the IP addresses of remote hosts allowed access or denied access to Content Gateway Manager.



### Important

After you modify this file, run `content_line -x` from the Content Gateway **bin** directory (`/opt/WCG/bin`) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

## Format

Each line in the **mgmt\_allow.config** file has the following format:

```
src_ip=ipaddress action=ip_allow|ip_deny
```

where *ipaddress* is the IP address or range of IP addresses allowed to access Content Gateway Manager.

*action* must specify either `ip_allow` to allow access to Content Gateway Manager or `ip_deny` to deny access.

By default, the **mgmt\_allow.config** file contains the following line, which allows all remote hosts to access Content Gateway Manager. Comment out or delete this line before adding rules to restrict access.

```
src_ip=0.0.0.0-255.255.255.255 action=ip_allow
```

## Examples

The following example configures Content Gateway to allow only one user to access Content Gateway Manager:

```
src_ip=123.12.3.123 action=ip_allow
```

The following example configures Content Gateway to allow a range of IP addresses to access Content Gateway Manager:

```
src_ip=123.12.3.000-123.12.3.123 action=ip_allow
```

The following example configures Content Gateway to deny the IP address 123.45.67.8 access to the Content Gateway Manager:

```
src_ip=123.45.67.8 action=ip_deny
```

## parent.config ---

The **parent.config** file identifies the HTTP parent proxies used in an HTTP cache hierarchy. Use this file to perform the following configuration:

- ◆ Set up parent cache hierarchies, with multiple parents and parent failover
- ◆ Configure selected URL requests to bypass parent proxies

Rules are applied from the list top-down; the first match is applied. Bypass rules are usually placed above parent proxy designation rule(s).

Content Gateway uses the **parent.config** file only when the HTTP parent caching option is enabled. See [Configuring Content Gateway to use an HTTP parent cache](#), page 78.



### Important

After you modify this file, run `content_line -x` from the Content Gateway **bin** directory (`/opt/WCG/bin`) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

---

## Format

Each line in the **parent.config** file must contain a parent caching rule. Content Gateway recognizes three space-delimited tags:

```
primary_destination=value secondary_specifier=value  
action=value
```

The following table lists the possible primary destinations and their allowed values.

Primary Destination	Allowed Value
dest_domain	A requested domain name
dest_host	A requested hostname
dest_ip	A requested IP address or range of IP addresses separated by a dash (-).
url_regex	A regular expression to be found in a URL

Secondary specifiers are optional in the `parent.config` file. The following table lists the possible secondary specifiers and their allowed values.

Secondary Specifier	Allowed Value
time	A time range, such as 08:00-14:00, during which the parent cache is used to serve requests
prefix	A prefix in the path part of a URL
suffix	A file suffix in the URL
src_ip	A client IP address.
port	A requested URL port
scheme	A request URL protocol; one of the following: <ul style="list-style-type: none"><li>• HTTP</li><li>• FTP</li></ul>
method	A request URL method; one of the following: <ul style="list-style-type: none"><li>• get</li><li>• post</li><li>• put</li><li>• trace</li></ul>
user_agent	A request header User-Agent value.

The following table lists the possible actions and their allowed values.

Action	Allowed Value
parent	An ordered list of parent servers. If the request cannot be handled by the last parent server in the list, it will be routed to the origin server. You can specify either a hostname or an IP address. You must specify the port number.
round_robin	One of the following values: <ul style="list-style-type: none"> <li>• <code>true</code> - Content Gateway goes through the parent cache list in a round-robin based on client IP address.</li> <li>• <code>strict</code> - Content Gateway machines serve requests strictly in turn. For example, machine <code>proxy1</code> serves the first request, <code>proxy2</code> serves the second request, and so on.</li> <li>• <code>false</code> - round-robin selection does not occur.</li> </ul>
go_direct	One of the following values: <ul style="list-style-type: none"> <li>• <code>true</code> - requests bypass parent hierarchies and go directly to the origin server.</li> <li>• <code>false</code> - requests do not bypass parent hierarchies.</li> </ul>

## Examples

The following rule configures a parent cache hierarchy consisting of Content Gateway (which is the child) and two parents, `p1.x.com` and `p2.x.com`. The proxy forwards the requests it cannot serve to the parent servers `p1.x.com` and `p2.x.com` in a round-robin fashion because `round_robin=true`.

```
dest_domain=. method=get parent="p1.x.com:8080;
p2.y.com:8080" round_robin=true
```

The following rule configures Content Gateway to route all requests containing the regular expression `politics` and the path `/viewpoint` directly to the origin server (bypassing any parent hierarchies):

```
url_regex=politics prefix=/viewpoint go_direct=true
```

The following rule is a typical destination bypass rule:

```
dest_domain=example.com go_direct=true
```



### Important

Every line in the **parent.config** file must contain *either* a `parent=` or `go_direct=` directive.

A bypass rule that includes `parent=` *and* `go_direct=true`, causes the specified `dest_domain` to be sent to the parent while all other domains are bypassed (the opposite of the usual intended action).

## partition.config

---

The **partition.config** file lets you manage your cache space more efficiently by creating cache partitions of different sizes. You can further configure these partitions to store data from certain origin servers and domains in the [hosting.config](#) file. This allows you to take better advantage of caching of frequently visited sites where the content changes infrequently.



### Important

The partition configuration must be the same on all nodes in a cluster.

---

You must stop Content Gateway before you change the cache partition size.

## Format

For each partition you want to create, enter a line with the following format:

```
partition=partition_number scheme=protocol_type  
size=partition_size
```

where:

**partition\_number** is a number between 1 and 255 (the maximum number of partitions is 255).

**protocol\_type** is **http**.



### Note

Only HTTP is supported at this time. Streaming media content—**mixt**—is not supported.

---

**partition\_size** is the amount of cache space allocated to the partition. This value can be either a percentage of the total cache space or an absolute value. The absolute value must be a multiple of 128 MB, where 128 MB is the smallest value. If you specify a percentage, the size is rounded down to the closest multiple of 128 MB. Each partition is striped across several disks to achieve parallel I/O. For example, if there are four disks, a 1 GB partition will have 256 MB on each disk (assuming each disk has enough free space available).



### Note

If you do not allocate all the disk space in the cache, the extra disk space is not used. You can use the extra space later to create new partitions without deleting and clearing the existing partitions.

---



## Examples

The following example partitions the cache evenly:

```
partition=1 scheme=http size=50%
partition=2 scheme=http size=50%
```

## records.config

---

The **records.config** file is a list of configurable variables used by Content Gateway.

Many of the values are set when you set configuration options in Content Gateway Manager, or through the command-line interface. Some configuration options can be set only by editing variables in the **records.config** file.



### Warning

Do not change the **records.config** variables unless you are certain of the effect. Many variables are coupled, meaning that they interact with other variables. Changing a single variable in isolation can cause Content Gateway to fail.

**Whenever possible, use Content Gateway Manager to configure Content Gateway.**



### Important

After you modify this file, to apply the changes run `content_line -x` from the Content Gateway **bin** directory (**/opt/WCG/bin**). When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

## Format

Each variable has the following format:

```
CONFIG variable_name DATATYPE variable_value
```

where *DATATYPE* is INT (an integer), STRING (a string), or FLOAT (a floating point).

## Examples

In the following example, the variable **proxy.config.proxy\_name** is of datatype **string** and its value is **contentserver1**. This means that the name of the Content Gateway proxy is **contentserver1**.

```
CONFIG proxy.config.proxy_name STRING contentserver1
```

In the following example, the variable **proxy.config.arm.enabled** is a yes/no flag. A value of 0 (zero) disables the option. A value of 1 enables the option.

```
CONFIG proxy.config.arm.enabled INT 0
```

In the following example, the variable sets the cluster startup timeout to 10 seconds.

```
CONFIG proxy.config.cluster.startup_timeout INT 10
```

## Configuration variables

The following tables describe the configuration variables listed in the **records.config** file.

*System variables*

*Local manager*

*Virtual IP manager*

*Alarm configuration*

*ARM (transparency configuration)*

*Load shedding configuration (ARM)*

*Authentication basic realm*

*LDAP*

*RADIUS authentication*

*NTLM*

*Integrated Windows Authentication*

*Transparent authentication*

*HTTP engine*

*Parent proxy configuration*

*Cache control*

*Heuristic expiration*

*Dynamic content and content negotiation*

*Anonymous FTP password*

*Cached FTP document lifetime*

*FTP transfer mode*

*FTP engine*

*Customizable user response pages*

*SOCKS processor*

*Net subsystem**Cluster subsystem**Cache**DNS**DNS proxy**Logging configuration**URL remap rules**Scheduled update configuration**WCCP configuration**SSL Decryption**ICAP**Connectivity, analysis, and boundary conditions*

## System variables

Configuration Variable Data Type	Data Type	Default Value	Description
proxy.config.proxy_name	STRING		Specifies the name of the Content Gateway node.
proxy.config.bin_path	STRING	bin	Specifies the location of the Content Gateway <b>bin</b> directory. This is the directory in which the Content Gateway binary files are placed by the installer.
proxy.config.proxy_binary	STRING	content_gateway	Specifies the name of the executable that runs the <b>content_gateway</b> process.
proxy.config.proxy_binary_opts	STRING	-M	Specifies the command-line options for starting <b>content_gateway</b> .
proxy.config.manager_binary	STRING	content_manager	Specifies the name of the executable that runs the <b>content_manager</b> process.
proxy.config.cli_binary	STRING	content_line	Specifies the name of the executable that runs the <b>content_line</b> interface.
proxy.config.watch_script	STRING	content_cop	Specifies the name of the executable that runs the <b>content_cop</b> process.

Configuration Variable Data Type	Data Type	Default Value	Description
proxy.config.env_prep	STRING	example_prep.sh	Specifies the script that is executed before the <b>content_manager</b> process spawns the <b>content_gateway</b> process.
proxy.config.config_dir	STRING	config	Specifies the directory, relative to bin_path (above), that contains the Content Gateway configuration files.
proxy.config.temp_dir	STRING	/tmp	Specifies the directory used for Content Gateway temporary files
proxy.config.alarm_email	STRING	websense	Specifies the email address to which Content Gateway sends alarm messages.  During installation, you can specify the email address; otherwise, Content Gateway uses the Content Gateway user account name as the default value.
proxy.config.syslog_facility	STRING	LOG_DAEMON	Specifies the facility used to record system log files.  See <a href="#">Working With Log Files</a> , page 195.
proxy.config.cop.core_signal	INT	3	Specifies the signal sent by <b>content_cop</b> to its managed processes— <b>content_manager</b> and <b>content_gateway</b> —to stop them. <b>Note: Do not change the value of this variable.</b>
proxy.config.cop.sleep_time	INT	45	Specifies the interval, in seconds, between heartbeat tests performed by <b>content_cop</b> to test the health of the <b>content_manager</b> and <b>content_gateway</b> processes. <b>Note: Do not change the value of this variable.</b>
proxy.config.cop.linux_min_swapfree_kb	INT	10240	This variable is not used.
proxy.config.cop.linux_min_memfree_kb	INT	10240	This variable is not used.

Configuration Variable Data Type	Data Type	Default Value	Description
proxy.config.output.logfile	STRING	content_gateway.out	Specifies the name and location of the file that contains warnings, status messages, and error messages produced by the Content Gateway processes.  If no path is specified, Content Gateway creates the file in its logging directory.
proxy.config.snapshot_dir	STRING	snapshots	Specifies the directory in which Content Gateway stores configuration snapshots on the local system. Unless you specify an absolute path, this directory is located in the Content Gateway <b>config</b> directory.
proxy.config.attach_debugger_script	STRING	attach_debugger	This variable should be used only on the direction of Websense Technical Support.  If set, when the <b>content_gateway</b> process resets, a debug script (in /opt/WCG/bin) is run.

## Local manager

Configuration Variable	Data Type	Default Value	Description
proxy.config.lm.sem_id	INT	11452	Specifies the semaphore ID for the local manager.  <b>Note: Do not change the value of this variable.</b>
proxy.local.cluster.type	INT	3	Sets the clustering mode: <ul style="list-style-type: none"> <li>• 2 = management-only mode</li> <li>• 3 = no clustering</li> </ul>
proxy.config.cluster.rsport	INT	8087	Specifies the reliable service port. The reliable service port is used to send configuration information between the nodes in a cluster. All nodes in a cluster must use the same reliable service port.
proxy.config.cluster.mcport	INT	8088	Specifies the multicast port. The multicast port is used for node identification. All nodes in a cluster must use the same multicast port.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.cluster.mc_group_addr</code>	STRING	224.0.1.37	Specifies the multicast address for cluster communications. All nodes in a cluster must use the same multicast address.
<code>proxy.config.cluster.mc_ttl</code>	INT	1	Specifies the multicast Time-To-Live for cluster communications.
<code>proxy.config.cluster.log_bogus_mc_msgs</code>	INT	1	Enables (1) or disables (0) logging of bogus multicast messages.
<code>proxy.config.admin.html_doc_root</code>	STRING	ui	Specifies the document root for Content Gateway Manager.
<code>proxy.config.admin.web_interface_port</code>	INT	8081	Specifies the Content Gateway Manager port.
<code>proxy.config.admin.autoconf_port</code>	INT	8083	Specifies the autoconfiguration port.
<code>proxy.config.admin.overseer_port</code>	INT	-1	Specifies the port used for retrieving and setting statistics and configuration variables. This port is disabled by default.
<code>proxy.config.admin.admin_user</code>	STRING	admin	Specifies the administrator ID that controls access to Content Gateway Manager.
<code>proxy.config.admin.admin_password</code>	STRING		Specifies the encrypted administrator password that controls access to Content Gateway Manager. You cannot edit the password; however, you can specify a value of NULL to clear the password. <a href="#">See <i>How do you access Content Gateway Manager if you forget the master administrator password?</i>, page 424.</a>
<code>proxy.config.admin.basic_auth</code>	INT	1	Enables (1) or disables (0) basic user authentication to control access to Content Gateway Manager.  Note: If basic authentication is <i>not</i> enabled, any user can access Content Gateway Manager to monitor and configure Content Gateway.
<code>proxy.config.admin.use_ssl</code>	INT	1	Enables the Content Gateway Manager SSL option for secure communication between a remote host and the Content Gateway Manager.

Configuration Variable	Data Type	Default Value	Description
proxy.config.admin.ssl_cert_file	STRING	server.pem	Specifies the filename of the SSL certificate installed on the Content Gateway system for secure communication between a remote host and Content Gateway Manager.
proxy.config.admin.number_config_bak	INT	3	Specifies the maximum number of copies of rolled configuration files to keep.
proxy.config.admin.user_id	STRING	root	Specifies the non-privileged user account designated to Content Gateway.
proxy.config.admin.ui_refresh_rate	INT	30	Specifies the refresh rate for the display of statistics in the Monitor pages of Content Gateway Manager.
proxy.config.admin.log_mgmt_access	INT	0	Enables (1) or disables (0) logging of all Content Gateway Manager transactions to the <b>lm.log</b> file.
proxy.config.admin.log_resolve_hostname	INT	1	When enabled (1), the hostname of the client connecting to Content Gateway Manager is recorded in the <b>lm.log</b> file. When disabled (0), the IP address of the client connecting to Content Gateway Manager is recorded in the <b>lm.log</b> file.
proxy.config.admin.subscription	STRING	NULL	Not used.
proxy.config.admin.supported_cipher_list	STRING	RC4-MD5, RC4-SHA, AES128-SHA, DHE-RSA-AES128-SHA, DHE-DSS-AES128-SHA, DES-CBC3-SHA, EDH-RSA-DES-CBC3-SHA, EDH-DSS-DES-CBC3-SHA	A comma-separated list, no spaces, of ciphers allowed when a browser establishes a secure connection with Content Gateway Manager. No validation is performed on the string. The first good value is used. If there is no good value, the browser is not allowed to connect to the manager and an error is returned.
proxy.config.lm.display_reset_alarm	INT	0	When enabled (1), email is sent to the administrator ( <b>proxy.config.alarm_email</b> ) whenever Content Gateway resets. Default is 0.

## Process manager

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.process_manager.mgmt_port</code>	INT	8084	Specifies the port used for internal communication between the <b>content_manager</b> process and the <b>content_gateway</b> process.

## Virtual IP manager

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.vmap.enabled</code>	INT	0	Enables (1) or disables (0) the virtual IP option.

## Alarm configuration

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.alarm.bin</code>	STRING	<code>example_alarm_bin.sh</code>	Specifies the name of the script file that can execute certain actions when an alarm is signaled. The default file is a sample script named <b>example_alarm_bin.sh</b> located in the <b>bin</b> directory. You must edit the script to suit your needs.
<code>proxy.config.alarm.abs_path</code>	STRING	NULL	Specifies the full path to the script file specified by <b>proxy.config.alarm.bin</b> (prior entry).



## ARM (transparency configuration)

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.arm.enabled</code>	INT	1	Enables (1) or disables (0) the ARM, which is used for transparent proxy caching, IP spoofing, and ARM security. See <a href="#">Enabling the ARM</a> , page 44.
<code>proxy.config.arm.ignore_ifp</code>	INT	1	When NAT rules are applied, configures Content Gateway to use any available interface when sending packets back to the client, rather than the one that triggered the NAT rule.
<code>proxy.config.arm.always_query_dest</code>	INT	0	<p>When enabled (1), Content Gateway always asks the ARM for the original destination IP address of incoming requests. This is done instead of doing a DNS lookup on the hostname of the request.</p> <p>When enabled, IP addresses are logged, instead of domain names.</p> <p>When disabled, domain names are logged. See <a href="#">Reducing DNS lookups</a>, page 65 for additional information.</p> <p>It is recommended that you do not enable this variable if Content Gateway is running in <i>both</i> explicit proxy and transparent proxy modes. In explicit proxy mode, the client does not perform a DNS lookup on the hostname of the origin server, so Content Gateway must do it.</p>
<code>proxy.config.http.outgoing_ip_spoofing_enabled</code>	INT	0	<p>Enables (1) or disables (0) the IP spoofing option, which allows Content Gateway to establish connections to origin servers with the client IP address instead of the Content Gateway IP address.</p> <p>Note: The variable <b>proxy.config.arm.enabled</b> must be enabled for the IP spoofing option to work.</p> <p>See <a href="#">IP spoofing</a>, page 66.</p>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.arm.bypass_dynamic_enabled</code>	INT	0	Enables (1) or disables (0) the adaptive bypass option to bypass the proxy and go directly to the origin server when clients or servers cause problems. See <a href="#">Dynamic bypass rules, page 62</a> .
<code>proxy.config.arm.bypass_use_and_rules_bad_client_request</code>	INT	0	Enables (1) or disables (0) dynamic source/destination bypass in the event of non-HTTP traffic on port 80. Note: The variable <b>proxy.config.arm.bypass_on_bad_client_request</b> must also be enabled for this option to work.
<code>proxy.config.arm.bypass_use_and_rules_400</code>	INT	0	Enables (1) or disables (0) dynamic generation of source/destination bypass rules when an origin server returns a 400 error. Note: The variable <b>proxy.config.arm.bypass_on_400</b> must also be enabled for this option to work.
<code>proxy.config.arm.bypass_use_and_rules_401</code>	INT	0	Enables (1) or disables (0) dynamic generation of source/destination bypass rules when an origin server returns a 401 error. Note: The variable <b>proxy.config.arm.bypass_on_401</b> must also be enabled for this option to work.
<code>proxy.config.arm.bypass_use_and_rules_403</code>	INT	0	Enables (1) or disables (0) dynamic generation of source/destination bypass rules when an origin server returns a 403 error. Note: The variable <b>proxy.config.arm.bypass_on_403</b> must also be enabled for this option to work.
<code>proxy.config.arm.bypass_use_and_rules_405</code>	INT	0	Enables (1) or disables (0) dynamic generation of source/destination bypass rules when an origin server returns a 405 error. Note: The variable <b>proxy.config.arm.bypass_on_405</b> must also be enabled for this option to work.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.arm.bypass_use_and_rules_406</code>	INT	0	Enables (1) or disables (0) dynamic generation of source/destination bypass rules when an origin server returns a 406 error. Note: The variable <b>proxy.config.arm.bypass_on_406</b> must also be enabled for this option to work.
<code>proxy.config.arm.bypass_use_and_rules_408</code>	INT	0	Enables (1) or disables (0) dynamic generation of source/destination bypass rules when an origin server returns a 408 error. Note: The variable <b>proxy.config.arm.bypass_on_408</b> must also be enabled for this option to work.
<code>proxy.config.arm.bypass_use_and_rules_500</code>	INT	0	Enables (1) or disables (0) dynamic generation of source/destination bypass rules when an origin server returns a 500 error. Note: The variable <b>proxy.config.arm.bypass_on_500</b> must also be enabled for this option to work.
<code>proxy.config.arm.bypass_on_bad_client_request</code>	INT	0	Enables (1) or disables (0) dynamic destination bypass in the event of non-HTTP traffic on port 80.
<code>proxy.config.arm.bypass_on_400</code>	INT	0	Enables (1) or disables (0) dynamic generation of destination bypass rules when an origin server returns a 400 error.
<code>proxy.config.arm.bypass_on_401</code>	INT	0	Enables (1) or disables (0) dynamic generation of destination bypass rules when an origin server returns a 401 error.
<code>proxy.config.arm.bypass_on_403</code>	INT	0	Enables (1) or disables (0) dynamic generation of destination bypass rules when an origin server returns a 403 error.
<code>proxy.config.arm.bypass_on_405</code>	INT	0	Enables (1) or disables (0) dynamic generation of destination bypass rules when an origin server returns a 405 error.
<code>proxy.config.arm.bypass_on_406</code>	INT	0	Enables (1) or disables (0) dynamic generation of destination bypass rules when an origin server returns a 406 error.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.arm.bypass_on_408</code>	INT	0	Enables (1) or disables (0) dynamic generation of destination bypass rules when an origin server returns a 408 error.
<code>proxy.config.arm.bypass_on_500</code>	INT	0	Enables (1) or disables (0) dynamic generation of destination bypass rules when an origin server returns a 500 error.

## Load shedding configuration (ARM)

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.arm.loadshedding.max_connections</code>	INT	1000000	Specifies the maximum number of client connections allowed before the proxy starts forwarding incoming requests directly to the origin server.

## Authentication basic realm

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.proxy.authenticate.basic.realm</code>	STRING	NULL	Specifies the authentication realm name. If the default of <b>NULL</b> is specified, <b>Content Gateway</b> is used.
<code>proxy.config.auth_type</code>	INT	3	Specifies the type of client authentication. <ul style="list-style-type: none"> <li>• 0 = None</li> <li>• 1 = LDAP</li> <li>• 2 = RADIUS</li> <li>• 3 = Legacy NTLM</li> <li>• 4 = Integrated Window Authentication</li> <li>• 5 = Multiple Realm Authentication</li> </ul>
<code>proxy.config.multiauth.enabled</code>	INT	0	Enables (1) or disables (0) multiple realm authentication. Tells Content Gateway to use <code>auth.config</code> for multiple authentication methods.

## LDAP

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.ldap.auth.enabled</code>	INT	0	Enables (1) or disables (0) LDAP proxy authentication. See <a href="#">LDAP authentication</a> , page 173.
<code>proxy.config.ldap.cache.size</code>	INT	5000	Specifies the maximum number of entries allowed in the LDAP cache.  If this value is modified, you must update the value of <b>proxy.config.ldap.cache.storage_size</b> proportionally. For example, if you double the cache size, also double the cache storage size.
<code>proxy.config.ldap.cache.storage_size</code>	INT	24582912	Specifies the size of the LDAP cache in bytes. This is directly related to the number of entries in the cache.  If this value is modified, you must update the value of <b>proxy.config.ldap.cache.size</b> proportionally. For example, if you double the storage size, also double the cache size.  Modifying this variable without modifying <b>proxy.config.ldap.cache.size</b> can cause the LDAP subsystem to stop functioning.
<code>proxy.config.ldap.auth.ttl_value</code>	INT	3000	Specifies the amount of time (in minutes) that entries in the cache remain valid.
<code>proxy.config.ldap.auth.purge_cache_on_auth_fail</code>	INT	1	When enabled (1), configures Content Gateway to delete the authorization entry for the client in the LDAP cache if authorization fails.
<code>proxy.config.ldap.proc.ldap.server.name</code>	STRING	NULL	Specifies the LDAP server name.
<code>proxy.config.ldap.proc.ldap.server.port</code>	INT	389	Specifies the LDAP server port.
<code>proxy.config.ldap.proc.ldap.base.dn</code>	STRING	NULL	Specifies the LDAP Base Distinguished Name (DN). Obtain this value from your LDAP administrator.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.ldap.proc.ldap.uid_filter</code>	STRING	<b>sAMAccountName</b>	Specifies the LDAP login name/ID. Use this as a filter to search the full DN database. For eDirectory or other directory services, enter <b>uid</b> in this field.
<code>proxy.config.ldap.secure.bind.enabled</code>	INT	0	When enabled (1), configures the proxy to use secure LDAP (LDAPS) to communicate with the LDAP server. Secure communication is usually performed on port 636 or 3269.
<code>proxy.config.ldap.proc.ldap.server.bind_dn</code>	STRING	NULL	Specifies the Full Distinguished Name (fully qualified name) of a user in the LDAP-based directory service. For example: CN=John Smith, CN=USERS, DC=MYCOMPANY, DC=COM Enter a maximum of 128 characters in this field. If no value is specified for this field, the proxy attempts to bind anonymously.
<code>proxy.config.ldap.proc.ldap.server.bind_pwd</code>	STRING	NULL	Specifies a password for the user identified by the <b>proxy.config.ldap.proc.ldap.server.bind_dn</b> variable.

## RADIUS authentication

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.radius.auth.enabled</code>	INT	0	Enables (1) or disables (0) RADIUS proxy authentication.
<code>proxy.config.radius.proc.radius.primary_server.name</code>	STRING	NULL	Specifies the hostname or IP address of the primary RADIUS authentication server.
<code>proxy.config.radius.proc.radius.primary_server.auth_port</code>	INT	1812	Specifies the RADIUS server port that Content Gateway uses to communicate with the RADIUS server.
<code>proxy.config.radius.proc.radius.primary_server.shared_key</code>	STRING	NULL	Specifies the key used for encoding with the first RADIUS authentication server.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.radius. proc.radius. secondary_server. name</code>	STRING	NULL	Specifies the hostname or IP address of the secondary RADIUS authentication server.
<code>proxy.config.radius. proc.radius. secondary_server. auth_port</code>	INT	1812	Specifies the port that the proxy uses to communicate with the secondary RADIUS authentication server.
<code>proxy.config.radius. proc.radius. secondary_server. shared_key</code>	STRING	NULL	Specifies the key used for encoding with the secondary RADIUS authentication server.
<code>proxy.config.radius. auth.min_timeout</code>	INT	10	Specifies the amount of time the connection to the RADIUS server can remain idle before Content Gateway closes the connection.
<code>proxy.config.radius. auth.max_retries</code>	INT	10	Specifies the maximum number of times Content Gateway tries to connect to the RADIUS server.
<code>proxy.config.radius. cache.size</code>	INT	1000	Specifies the number of entries allowed in the RADIUS cache.  The minimum value is 256 entries.
<code>proxy.config.radius. cache.storage_size</code>	INT	15728640	Specifies the maximum amount of space that the RADIUS cache can occupy on disk.  This value must be at least one hundred times the number of entries. It is recommended that you provide the maximum amount of disk space possible.
<code>proxy.config.radius. auth.ttl_value</code>	INT	60	Specifies the number of minutes that Content Gateway stores username and password entries in the RADIUS cache.

## NTLM

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.ntlm.auth.enabled</code>	INT	0	Enables (1) or disables (0) NTLM proxy authentication.
<code>proxy.config.ntlm.dc.list</code>	STRING	NULL	<p>Specifies the hostnames of the domain controllers. You must separate each entry with a comma. The format is:</p> <pre>host_name[:port] [%netbios_name]</pre> <p>or</p> <pre>IP_address[:port] [%netbios_name]</pre> <p>If you are using Active Directory 2008, you must include the <b>netbios_name</b> or use SMB port 445.</p>
<code>proxy.config.ntlm.dc.load_balance</code>	INT	0	<p>Enables (1) or disables (0) load balancing. When enabled, Content Gateway balances the load when sending authentication requests to the domain controllers.</p> <p><b>Note:</b> When multiple domain controllers are specified, even if load balancing is disabled, when the load on the primary domain controller reaches the maximum number of connections allowed, new requests are sent to a secondary domain controller as a short-term failover provision, until such time that the primary domain controller can accept new connections.</p>
<code>proxy.config.ntlm.dc.max_connections</code>	INT	10	Specifies the maximum number of connections Content Gateway can have open to the domain controller.



Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.ntlm.cache.enabled</code>	INT	1	Enables (1) or disables (0) the NTLM cache. Applies only when Content Gateway is an explicit proxy. When disabled, Content Gateway does not store any credentials in the NTLM cache for future use. Content Gateway always sends the credentials to the domain server to be validated.
<code>proxy.config.ntlm.cache.ttl_value</code>	INT	900	Specifies the number of seconds that Content Gateway stores entries in the NTLM cache. The supported range of values is 300 to 86400 seconds.
<code>proxy.config.ntlm.cache.size</code>	INT	5000	Specifies the number of entries allowed in the NTLM cache.
<code>proxy.config.ntlm.cache.storage_size</code>	INT	15728640	Specifies the maximum amount of space that the NTLM cache can occupy on disk. This value should be proportionate to number of entries in the NTLM cache. For example, if each entry in the NTLM cache is approximately 128 bytes and the number of entries allowed in the NTLM cache is 5000, the cache storage size should be at least 64000 bytes.
<code>proxy.config.ntlm.cache_exception.list</code>	STRING	NULL	Holds the list of IP addresses and IP address ranges that will not be cached. This variable gets its value from the Content Gateway Manager NTLM Multi-Host IP addresses field.
<code>proxy.config.ntlm.fail_open</code>	INT	1	Enables (1) or disables (0) whether client requests are allowed to proceed when authentication fails due to: <ul style="list-style-type: none"> <li>no response from the domain controller</li> <li>badly formed messages from the client</li> <li>invalid SMB responses</li> </ul> <b>Note:</b> Password authentication failures are always failures.

## Integrated Windows Authentication

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.winauth.enabled</code>	INT	0	Enables (1) or disables (0) Integrated Windows Authentication (Kerberos).
<code>proxy.config.winauth.realm</code>	STRING	NULL	Specifies the name of the Windows Active Directory domain. By entering “*”, all domain controllers found in the DNS SRV records will be used.
<code>proxy.config.winauth.log_denied_requests</code>	INT	1	Enables (1) or disables (0) logging of denied authentication requests.

## Transparent authentication

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.transparent_auth_hostname</code>	STRING	NULL	Specify an alternate hostname for the proxy that can be resolved for all clients via DNS. This is needed if the regular hostname of the Content Gateway machine cannot be resolved for all users via DNS.  For additional information, see <a href="#">Transparent proxy authentication settings</a> , page 165.
<code>proxy.config.http.transparent_auth_type</code>	INT	1	Specify: <ul style="list-style-type: none"> <li>• 0 to associate a session ID with the username after the user session is authenticated. This setting is required to uniquely identify users who share a single IP address, such as in proxy-chaining or network address translation.</li> <li>• 1 to associate a client IP address with a username after the user session is authenticated.</li> </ul> In either mode, the length of time before a client must re-authenticate is determined by the value of <b>proxy.config.http.transparent_auth_session_time</b> .
<code>proxy.config.http.transparent_auth_session_time</code>	INT	15	Specify the length of time (in minutes) before the browser must re-authenticate. This value is used in both IP and cookie modes.

## HTTP engine

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.server_port</code>	INT	8080	Specifies the port that Content Gateway uses when acting as a Web proxy server for Web traffic or when serving Web traffic transparently.
<code>proxy.config.http.server_port_attr</code>	STRING	X	Specifies the server port options. You can specify one of the following: <ul style="list-style-type: none"> <li>• C=SERVER_PORT_COMPRESSED</li> <li>• X=SERVER_PORT_DEFAULT</li> <li>• T=SERVER_PORT_BLIND_TUNNEL</li> </ul>
<code>proxy.config.http.server_other_ports</code>	STRING	NULL	Specifies the ports other than the port specified by the variable <b>proxy.config.http.server_port</b> to bind for incoming HTTP requests.
<code>proxy.config.http.ssl_ports</code>	STRING	443 563 8081 8071 9443 9444	Specifies the ports used for tunneling. This is a space-separated list that can also include ranges of ports, e.g. 1-65535.  Content Gateway allows tunnels only to the specified ports.
<code>proxy.config.http.insert_request_via_str</code>	INT	1	Specify one of the following: <ul style="list-style-type: none"> <li>• 0 = no extra information is added to the string.</li> <li>• 1 = all extra information is added.</li> <li>• 2 = some extra information is added.</li> </ul>
<code>proxy.config.http.insert_response_via_str</code>	INT	1	Specify one of the following: <ul style="list-style-type: none"> <li>• 0 = no extra information is added to the string.</li> <li>• 1 = all extra information is added.</li> <li>• 2 = some extra information is added.</li> </ul>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.enable_url_expandomatic</code>	INT	1	Enables (1) or disables (0) <b>.com</b> domain expansion, which configures Content Gateway to attempt to resolve unqualified hostnames by redirecting them to the expanded address, prepended with <b>www.</b> and appended with <b>.com</b> ; for example, if a client makes a request to <b>host</b> , Content Gateway redirects the request to <b>www.host.com</b> .
<code>proxy.config.http.no_dns_just_forward_to_parent</code>	INT	0	When enabled (1), and if HTTP parent caching is enabled, Content Gateway does no DNS lookups on request hostnames.
<code>proxy.config.http.uncacheable_requests_bypass_parent</code>	INT	0	When enabled (1), Content Gateway bypasses the parent proxy for a request that is not cacheable.
<code>proxy.config.http.keep_alive_enabled</code>	INT	1	Enables (1) or disables (0) the use of keep-alive connections to either origin servers or clients.
<code>proxy.config.http.chunking_enabled</code>	INT	1	Specifies whether Content Gateway will generate a chunked response: <ul style="list-style-type: none"> <li>• 0 = Never</li> <li>• 1 = Always</li> </ul>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.send_http11_requests</code>	INT	3	<p>Configures Content Gateway to use HTTP Version 1.1 when communicating with origin servers. You can specify one of the following values:</p> <ul style="list-style-type: none"> <li>• 0 = Never use HTTP 1.1 when communicating with origin servers.</li> <li>• 1 = Always use HTTP 1.1 when communicating with origin servers.</li> <li>• 2 = Use HTTP 1.1 if the origin server has previously used HTTP 1.1.</li> <li>• 3 = Use HTTP 1.1 if the client request is HTTP 1.1 and the origin server has previously used HTTP 1.1.</li> </ul> <p>Note: If HTTP 1.1 is used, Content Gateway can use keep-alive connections with pipelining to origin servers. If HTTP 0.9 is used, Content Gateway does not use keep-alive connections to origin servers. If HTTP 1.0 is used, a Content Gateway can use keep-alive connections without pipelining to origin servers.</p>
<code>proxy.config.http.send_http11_asfirstrequest</code>	INT	1	<p>When enabled (1), specifies that Content Gateway send HTTP 1.1 in the first request to server. Otherwise, the default behavior is specified by <b>proxy.config.http.send_http11_requests</b>.</p>
<code>proxy.config.http.share_server_sessions</code>	INT	1	<p>Enables (1) or disables (0) the re-use of server sessions.</p> <p>Note: When IP spoofing is enabled, Content Gateway automatically disables this variable.</p>
<code>proxy.config.http.ftp_enabled</code>	INT	1	<p>Enables (1) or disables (0) Content Gateway from serving FTP requests sent via HTTP.</p>
<code>proxy.config.http.record_heartbeat</code>	INT	0	<p>Enables (1) or disables (0) <b>content_cop</b> heartbeat logging.</p>
<code>proxy.config.http.large_file_support</code>	INT	1	<p>When enabled (1), Content Gateway supports downloading of files larger than 2 GB.</p>

## Parent proxy configuration

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.parent_proxy_routing_enable</code>	INT	0	Enables (1) or disables (0) the HTTP parent caching option. See <a href="#">Hierarchical Caching</a> , page 77.
<code>proxy.config.http.parent_proxy_retry_time</code>	INT	300	Specifies the amount of time allowed between connection retries to a parent cache that is unavailable.
<code>proxy.config.http.parent_proxy.fail_threshold</code>	INT	10	Specifies the number of times the connection to the parent cache can fail before Content Gateway considers the parent unavailable.
<code>proxy.config.http.parent_proxy.total_connect_attempts</code>	INT	4	Specifies the total number of connection attempts allowed to a parent cache before Content Gateway bypasses the parent or fails the request (depending on the <b>go_direct</b> option in the <b>bypass.config</b> file).
<code>proxy.config.http.parent_proxy.per_parent_connect_attempts</code>	INT	2	Specifies the total number of connection attempts allowed per parent if multiple parents are used.
<code>proxy.config.http.parent_proxy.connect_attempts_timeout</code>	INT	30	Specifies the timeout value, in seconds, for parent cache connection attempts.
<code>proxy.config.http.forward.proxy_auth_to_parent</code>	INT	0	When enabled (1), the Proxy-Authorization header is <i>not</i> stripped from requests sent to a parent proxy. Enable this when Content Gateway is a child proxy and the parent proxy performs authentication.
<code>proxy.config.http.child_proxy.read_auth_from_header</code>	INT	0	When Content Gateway is the parent proxy, read X-Authenticated-User and X-Forwarded-For fields from incoming request headers. 1 = enabled 0 = disabled

Configuration Variable	Data Type	Default Value	Description
<code>proxy.local.http.parent_proxy.disable_ssl_connect_tunneling</code>	INT	0	When enabled (1), HTTPS requests bypass the parent proxy.
<code>proxy.local.http.parent_proxy.disable_unknown_connect_tunneling</code>	INT	0	When enabled (1), non-HTTPS tunnel requests bypass the parent proxy.

## HTTP connection timeouts (secs)

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.keep_alive_no_activity_timeout_in</code>	INT	60	Specifies how long Content Gateway keeps connections to clients open for a subsequent request after a transaction ends.
<code>proxy.config.http.keep_alive_no_activity_timeout_out</code>	INT	60	Specifies how long Content Gateway keeps connections to origin servers open for a subsequent transfer of data after a transaction ends.
<code>proxy.config.http.transaction_no_activity_timeout_in</code>	INT	120	Specifies how long Content Gateway keeps connections to clients open if a transaction stalls.
<code>proxy.config.http.transaction_no_activity_timeout_out</code>	INT	120	Specifies how long Content Gateway keeps connections to origin servers open if the transaction stalls.
<code>proxy.config.http.transaction_active_timeout_in</code>	INT	0	Specifies how long Content Gateway remains connected to a client. If the transfer to the client is not complete before this timeout expires, Content Gateway closes the connection. The default value of 0 specifies that there is no timeout.



Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.transaction_active_timeout_out</code>	INT	0	Specifies how long Content Gateway waits for fulfillment of a connection request to an origin server. If Content Gateway does not complete the transfer to the origin server before this timeout expires, the connection request is terminated.  The default value of 0 specifies that there is no timeout.
<code>proxy.config.http.accept_no_activity_timeout</code>	INT	120	Specifies the timeout interval in seconds before Content Gateway closes a connection that has no activity.
<code>proxy.config.http.background_fill_active_timeout</code>	INT	60	Specifies how long Content Gateway continues a background fill before giving up and dropping the origin server connection.
<code>proxy.config.http.background_fill_completed_threshold</code>	FLOAT	0.50000	Specifies the proportion of total document size already transferred when a client aborts at which the proxy continues fetching the document from the origin server to get it into the cache (a <i>background fill</i> ).

## Origin server connection attempts

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.connect_attempts_max_retries</code>	INT	6	Specifies the maximum number of connection retries Content Gateway makes when the origin server is not responding.
<code>proxy.config.http.connect_attempts_max_retries_dead_server</code>	INT	2	Specifies the maximum number of connection retries Content Gateway makes when the origin server is unavailable.
<code>proxy.config.http.connect_attempts_rr_retries</code>	INT	2	Specifies the maximum number of failed connection attempts allowed before a round-robin entry is marked as down if a server has round-robin DNS entries.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.connect_attempts_timeout</code>	INT	60	Specifies the timeout value in seconds for an origin server connection.
<code>proxy.config.http.streaming_connect_attempts_timeout</code>	INT	1800	Specifies the timeout value in seconds for a streaming content connection.
<code>proxy.config.http.down_server.cache_time</code>	INT	30	Specifies how long in seconds Content Gateway remembers that an origin server was unreachable.
<code>proxy.config.http.down_server.abort_threshold</code>	INT	10	Specifies the number of seconds before Content Gateway marks an origin server as unavailable when a client abandons a request because the origin server was too slow in sending the response header.

## Negative response caching

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.negative_caching_enabled</code>	INT	0	<p>When enabled (1), Content Gateway caches negative responses, such as <i>404 Not Found</i>, if a requested page does not exist. The next time a client requests the same page, Content Gateway serves the negative response from the cache.</p> <p>Content Gateway caches the following negative responses:</p> <ul style="list-style-type: none"> <li>204 No Content</li> <li>305 Use Proxy</li> <li>400 Bad Request</li> <li>403 Forbidden</li> <li>404 Not Found</li> <li>405 Method Not Allowed</li> <li>500 Internal Server Error</li> <li>501 Not Implemented</li> <li>502 Bad Gateway</li> <li>503 Service Unavailable</li> <li>504 Gateway Timeout</li> </ul>
<code>proxy.config.http.negative_caching_lifetime</code>	INT	1800	Specifies how long Content Gateway keeps the negative responses as valid in cache.

## Proxy users variables

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.anonymize_remove_from</code>	INT	0	When enabled (1), Content Gateway removes the <b>From</b> header that accompanies transactions to protect the privacy of your users.
<code>proxy.config.http.anonymize_remove_referer</code>	INT	0	When enabled (1), Content Gateway removes the <b>Referer</b> header that accompanies transactions to protect the privacy of your site and users.

Configuration Variable	Data Type	Default Value	Description
proxy.config.http.anonymize_remove_user_agent	INT	0	When enabled (1), Content Gateway removes the <b>User-agent</b> header that accompanies transactions to protect the privacy of your site and users.
proxy.config.http.anonymize_remove_cookie	INT	0	When enabled (1), Content Gateway removes the <b>Cookie</b> header that accompanies transactions to protect the privacy of your site and users.
proxy.config.http.anonymize_remove_client_ip	INT	1	When enabled (1), Content Gateway removes <b>Client-IP</b> headers for more privacy.
proxy.config.http.anonymize_insert_client_ip	INT	0	When enabled (1), Content Gateway inserts <b>Client-IP</b> headers to retain the client's IP address.
proxy.config.http.append_xforwards_header	INT	0	When enabled (1), Content Gateway appends <b>X-Forwards</b> headers to outgoing requests.
proxy.config.http.anonymize_other_header_list	STRING	NULL	Specifies the headers that Content Gateway will remove from outgoing requests.
proxy.config.http.snarf_username_from_authorization	INT	0	When enabled (1), Content Gateway takes the username and password from the authorization header for LDAP if the authorization scheme is <i>Basic</i> .
proxy.config.http.insert_squid_x_forwarded_for	INT	0	When enabled (1), Content Gateway adds the client IP address to the <b>X-Forwarded-For</b> header.
proxy.config.http.insert_x_authenticated_user	INT	0	When enabled (1), Content Gateway inserts the <b>X-Authenticated-User</b> header to advertise the proxy authenticated user.

## Security

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.push_method_enabled</code>	INT	0	When enabled (1), <b>filter.config</b> rules can be used to push content directly into the cache without a user request. You must add a filtering rule with the PUSH action to ensure that only known source IP addresses implement PUSH requests to the cache. This variable must be enabled before PUSH is available in the Method drop down list in the configuration file editor.

## Cache control

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.cache.http</code>	INT	1	Enables (1) or disables (0) caching of HTTP requests.
<code>proxy.config.http.cache.ftp</code>	INT	1	Enables (1) or disables (0) caching of FTP requests sent via HTTP.
<code>proxy.config.http.cache.ignore_client_no_cache</code>	INT	0	When enabled (1), Content Gateway ignores client requests to bypass the cache.
<code>proxy.config.http.cache.ims_on_client_no_cache</code>	INT	0	When enabled (1), Content Gateway issues a conditional request to the origin server if an incoming request has a <b>no-cache</b> header.
<code>proxy.config.http.cache.ignore_server_no_cache</code>	INT	0	When enabled (1), Content Gateway ignores origin server requests to bypass the cache.
<code>proxy.config.http.cache.cache_responses_to_cookies</code>	INT	3	Specifies how cookies are cached: <ul style="list-style-type: none"> <li>• 0 = do not cache any responses to cookies</li> <li>• 1 = cache for any content-type</li> <li>• 2 = cache only for image types</li> <li>• 3 = cache for all but text content-types</li> </ul>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.cache.ignore_authentication</code>	INT	0	When enabled (1), Content Gateway ignores <b>WWW-Authentication</b> headers in responses. <b>WWW-Authentication</b> headers are removed and not cached.
<code>proxy.config.http.cache.cache_urls_that_look_dynamic</code>	INT	0	Enables (1) or disables (0) caching of URLs that look dynamic.
<code>proxy.config.http.cache.enable_default_vary_headers</code>	INT	0	Enables (1) or disables (0) caching of alternate versions of HTTP objects that do not contain the <b>Vary</b> header.
<code>proxy.config.http.cache.when_to_revalidate</code>	INT	0	Specifies when to revalidate content: <ul style="list-style-type: none"> <li>• 0 = Use cache directives or heuristic (the default value).</li> <li>• 1 = Stale if heuristic.</li> <li>• 2 = Always stale (always revalidate).</li> <li>• 3 = Never stale.</li> <li>• 4 = Use cache directives or heuristic (0) unless the request has an <b>If-Modified-Since</b> header. If the request has an <b>If-Modified-Since</b> header, Content Gateway always revalidates the cached content and uses the client's <b>If-Modified-Since</b> header for the proxy request.</li> </ul>
<code>proxy.config.http.cache.when_to_add_no_cache_to_msie_requests</code>	INT	0	Specifies when to add <b>no-cache</b> directives to Microsoft Internet Explorer requests. You can specify the following: <ul style="list-style-type: none"> <li>• 0 = <b>no-cache</b> not added to MSIE requests.</li> <li>• 1 = <b>no-cache</b> added to IMS MSIE requests.</li> <li>• 2 = <b>no-cache</b> added to all MSIE requests.</li> </ul>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.cache.required_headers</code>	INT	0	Specifies the type of headers required in a request for the request to be cacheable. <ul style="list-style-type: none"> <li>• 0 = no required headers to make document cacheable.</li> <li>• 1 = at least <b>Last-Modified</b> header required.</li> <li>• 2 = explicit lifetime required, <b>Expires</b> or <b>Cache-Control</b>.</li> </ul>
<code>proxy.config.http.cache.max_stale_age</code>	INT	604800	Specifies the maximum age allowed for a stale response before it cannot be cached.
<code>proxy.config.http.cache.range.lookup</code>	INT	1	When enabled (1), Content Gateway looks up range requests in the cache.
<code>proxy.config.http.cache.cache_301_responses</code>	INT	0	Enables (1) or disables (0) caching of “301” response pages.

## Heuristic expiration

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.cache.heuristic_min_lifetime</code>	INT	3600	Specifies the minimum amount of time that a document in the cache can be considered fresh.
<code>proxy.config.http.cache.heuristic_max_lifetime</code>	INT	86400	Specifies the maximum amount of time that a document in the cache can be considered fresh.
<code>proxy.config.http.cache.heuristic_lm_factor</code>	FLOAT	0.10000	Specifies the aging factor for freshness computations.
<code>proxy.config.http.cache.fuzz.time</code>	INT	240	Specifies the interval in seconds before the document stale time that the proxy checks for an early refresh.
<code>proxy.config.http.cache.fuzz.probability</code>	FLOAT	0.00500	Specifies the probability that a refresh is made on a document during the specified fuzz time.

## Dynamic content and content negotiation

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.cache.vary_default_text</code>	STRING	NULL	Specifies the header on which Content Gateway varies for text documents; for example, if you specify <b>user-agent</b> , the proxy caches all the different user-agent versions of documents it encounters.
<code>proxy.config.http.cache.vary_default_images</code>	STRING	NULL	Specifies the header on which Content Gateway varies for images.
<code>proxy.config.http.cache.vary_default_other</code>	STRING	NULL	Specifies the header on which Content Gateway varies for anything other than text and images.

## Anonymous FTP password

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.ftp.anonymous_passwd</code>	STRING	<i>the value of the administrator's email as supplied during installation</i>	Specifies the anonymous password for FTP servers that require a password for access. Content Gateway uses the Content Gateway user account name as the default value for this variable.

## Cached FTP document lifetime

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.ftp.cache.document_lifetime</code>	INT	259200	Specifies the maximum amount of time that an FTP document can stay in the cache.



## FTP transfer mode

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.http.ftp.binary_transfer_only</code>	INT	0	<p>When enabled (1), all FTP documents requested from HTTP clients are transferred in binary mode only.</p> <p>When disabled (0), FTP documents requested from HTTP clients are transferred in ASCII or binary mode, depending on the document type.</p>

## Customizable user response pages

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.body_factory.enable_customizations</code>	INT	0	<p>Specifies whether customizable response pages are enabled or disabled and which response pages are used:</p> <ul style="list-style-type: none"> <li>• 0 = disable customizable user response pages</li> <li>• 1 = enable customizable user response pages in the default directory only</li> <li>• 2 = enable language-targeted user response pages</li> </ul>
<code>proxy.config.body_factory.enable_logging</code>	INT	0	<p>Enables (1) or disables (0) logging for customizable response pages. When enabled, Content Gateway records a message in the error log each time a customized response page is used or modified.</p>
<code>proxy.config.body_factory.template_sets_dir</code>	STRING	<code>config/body_factory</code>	Specifies the customizable response page default directory.
<code>proxy.config.body_factory.response_suppression_mode</code>	INT	0	<p>Specifies when Content Gateway suppresses generated response pages:</p> <ul style="list-style-type: none"> <li>• 0 = never suppress generated response pages</li> <li>• 1 = always suppress generated response pages</li> <li>• 2 = suppress response pages only for intercepted traffic</li> </ul>

## FTP engine

Configuration Variable	Data Type	Default Value	Description
<b>FTP over HTTP</b>			
proxy.config.ftp.data_connection_mode	INT	1	Specifies the FTP connection mode: <ul style="list-style-type: none"> <li>• 1 = PASV then PORT</li> <li>• 2 = PORT only</li> <li>• 3 = PASV only</li> </ul>
proxy.config.ftp.control_connection_timeout	INT	300	Specifies how long Content Gateway waits for a response from the FTP server.
proxy.config.ftp.rc_to_switch_to_PORT	STRING	NULL	Specifies the response codes for which Content Gateway automatically fails over to the PORT command when PASV fails if the configuration variable <b>proxy.config.ftp.data_connection_mode</b> is set to 1. This variable is used for FTP requests from HTTP clients only.
<b>FTP Proxy</b>			
proxy.config.ftp.ftp_enabled	INT	0	Enables (1) or disables (0) processing of FTP requests from FTP clients.
proxy.config.ftp.logging_enabled	INT	1	Enables (1) or disables (0) logging of FTP transactions.
proxy.config.ftp.proxy_server_port	INT	2121	Specifies the port used for FTP connections.
proxy.config.ftp.open_lisn_port_mode	INT	1	Specifies how FTP opens a listening port for a data transfer: <ul style="list-style-type: none"> <li>• 1 = The operating system chooses an available port. Content Gateway sends 0 and retrieves the new port number if the listen succeeds.</li> <li>• 2 = The listening port is determined by the range of ports specified by the Content Gateway variables <b>proxy.config.ftp.min_lisn_port</b> and <b>proxy.config.ftp.max_lisn_port</b>, described below.</li> </ul>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.ftp.min_lisn_port</code>	INT	32768	Specifies the lowest port in the range of listening ports used by Content Gateway for data connections when the FTP client sends a PASV or Content Gateway sends a PORT to the FTP server.
<code>proxy.config.ftp.max_lisn_port</code>	INT	65535	Specifies the highest port in the range of listening ports used by Content Gateway for data connections when the FTP client sends a PASV or Content Gateway sends a PORT to the FTP server.
<code>proxy.config.ftp.server_data_default_pasv</code>	INT	1	<p>Specifies the default method used to set up server side data connections:</p> <ul style="list-style-type: none"> <li>• 1 = Content Gateway sends a PASV to the FTP server and lets the FTP server open a listening port.</li> <li>• 0 = Content Gateway tries PORT first (sets up a listening port on the proxy side of the connection).</li> </ul>
<code>proxy.config.ftp.different_client_port_ip_allowed</code>	INT	0	<p>When enabled (1), Content Gateway can connect to a machine other than the one on which the FTP client is running to establish a data connection.</p> <p>The FTP client uses PORT to set up a listening port on its side and allows Content Gateway to connect to that port to establish the data connection (used to transfer files). When setting up the listening port, an FTP client specifies the IP address and port number for the listening port. If this variable is set to 0 (zero), Content Gateway cannot connect to the FTP client if the IP address sent by the client is different from the IP address of the machine running the FTP client.</p>
<code>proxy.config.ftp.try_pasv_times</code>	INT	1024	Specifies the number of times Content Gateway can try to open a listening port when the FTP client sends a PASV.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.ftp.try_port_times</code>	INT	1024	Specifies the maximum number of times Content Gateway can try to open a listening port when sending a PORT to the FTP server.
<code>proxy.config.ftp.try_server_ctrl_connect_times</code>	INT	6	Specifies the maximum number of times Content Gateway can try to connect to the FTP server's control listening port.
<code>proxy.config.ftp.try_server_data_connect_times</code>	INT	3	Specifies the maximum number of times Content Gateway can try to connect to the FTP server's data listening port when it sends a PASV to the FTP server and gets the IP/listening port information.
<code>proxy.config.ftp.try_client_data_connect_times</code>	INT	3	Specifies the maximum number of times Content Gateway can try to connect to the FTP client's data listening port when the FTP client sends a PORT with the IP/listening port information.
<code>proxy.config.ftp.client_ctrl_no_activity_timeout</code>	INT	900	Specifies the inactivity timeout, in seconds, for the FTP client control connection.
<code>proxy.config.ftp.client_ctrl_active_timeout</code>	INT	14400	Specifies the active timeout, in seconds, for the FTP client control connection.
<code>proxy.config.ftp.server_ctrl_no_activity_timeout</code>	INT	120	Specifies the inactivity timeout, in seconds, for the FTP server control connection.
<code>proxy.config.ftp.server_ctrl_active_timeout</code>	INT	14400	Specifies the active timeout, in seconds, for the FTP server control connection.
<code>proxy.config.ftp.client_data_no_activity_timeout</code>	INT	120	Specifies the maximum time, in seconds, that a client FTP data transfer connection can be idle before it is aborted.
<code>proxy.config.ftp.client_data_active_timeout</code>	INT	14400	Specifies the maximum time, in seconds, of an FTP data transfer connection from a client.
<code>proxy.config.ftp.server_data_no_activity_timeout</code>	INT	120	Specifies the maximum time, in seconds, that a server FTP data transfer connection can be idle before it is aborted.
<code>proxy.config.ftp.server_data_active_timeout</code>	INT	14400	Specifies the maximum time, in seconds, of an FTP data transfer connection from a server.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.ftp.pasv_accept_timeout</code>	INT	120	Specifies the timeout value for a listening data port in Content Gateway (for PASV, the client data connection).
<code>proxy.config.ftp.port_accept_timeout</code>	INT	120	Specifies the timeout value for a listening data port in Content Gateway (for PORT, the server data connection).
<code>proxy.config.ftp.share_ftp_server_ctrl_enabled</code>	INT	1	Enables (1) or disables (0) sharing the server control connections among multiple anonymous FTP clients.
<code>proxy.config.ftp.share_only_after_session_end</code>	INT	1	Specifies how an FTP server control connection is shared between different FTP client sessions: <ul style="list-style-type: none"> <li>• 1 = the FTP server control connection can be used by another FTP client session <i>only</i> when the FTP client session is complete (typically, when the FTP client sends out a QUIT command).</li> <li>• 0 = the FTP server control connection can be used by another FTP client session <i>only</i> if the FTP client session is not actively using the FTP server connection: for example, if the request is a cache hit or during an idle session.</li> </ul>
<code>proxy.config.ftp.server_ctrl_keep_alive_no_activity_timeout</code>	INT	90	Specifies the timeout value when the FTP server control connection is not used by any FTP clients.
<code>proxy.config.ftp.reverse_ftp_enabled</code>	INT	0	Not supported.
<code>proxy.config.ftp.login_info_fresh_in_cache_time</code>	INT	604800	Specifies how long the 220/230 responses (login messages) can stay fresh in the cache.
<code>proxy.config.ftp.data_source_port_20_enabled</code>	INT	0	When enabled (1), bind to source port 20 for outgoing data transfer connections to Active mode FTP clients.

## SOCKS processor

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.socks.socks_needed</code>	INT	0	Enables (1) or disables (0) the SOCKS option. <i>See <a href="#">Configuring SOCKS firewall integration</a>, page 159.</i>
<code>proxy.config.socks.socks_version</code>	INT	4	Specifies the SOCKS version.
<code>proxy.config.socks.default_servers</code>	STRING	<code>s1.example.com:1080;socks2:4080</code>	Specifies the names and ports of the SOCKS servers with which Content Gateway communicates.
<code>proxy.config.socks.accept_enabled</code>	INT	0	Enables (1) or disables (0) the SOCKS proxy option. As a SOCKS proxy, Content Gateway receives SOCKS traffic (usually on port 1080) and forwards all requests directly to the SOCKS server.
<code>proxy.config.socks.accept_port</code>	INT	1080	Specifies the port on which Content Gateway accepts SOCKS traffic.

## Net subsystem

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.net.connections_throttle</code>	INT	45000	Specifies the maximum number of connections that Content Gateway can handle. If Content Gateway receives additional client requests, they are queued until existing requests are served. Do not set this variable below 100.

## Cluster subsystem

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.cluster.cluster_port</code>	INT	8086	Specifies the port used for cluster communication.
<code>proxy.config.cluster.ethernet_interface</code>	STRING	<i>your_interface</i>	Specifies the network interface used for cluster traffic. All nodes in a cluster must use the same network interface.

## Cache

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.cache.permit.pinning</code>	INT	0	Enables (1) or disables (0) the cache pinning option, which lets you keep objects in the cache for a specified time. You set cache pinning rules in the <b>cache.config</b> file (see <a href="#">cache.config</a> , page 324).
<code>proxy.config.cache.ram_cache.size</code>	INT	-1	Specifies the size of the RAM cache, in bytes. -1 means that the RAM cache is automatically sized at approximately 1 MB per GB of disk.
<code>proxy.config.cache.limits.http.max_alts</code>	INT	3	Specifies the maximum number of HTTP alternates that Content Gateway can cache.
<code>proxy.config.cache.max_doc_size</code>	INT	0	Specifies the maximum size of documents in the cache (in bytes): 0 = there is no size limit.

## DNS

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.dns.search_default_domains</code>	INT	1	Enables (1) or disables (0) local domain expansion so that Content Gateway can attempt to resolve unqualified hostnames by expanding to the local domain; for example, if a client makes a request to an unqualified host named <b>host_x</b> , and if the Content Gateway local domain is <b>y.com</b> , Content Gateway expands the hostname to <b>host_x.y.com</b> .
<code>proxy.config.dns.splitDNS.enabled</code>	INT	0	Enables (1) or disables (0) DNS server selection. When enabled, Content Gateway refers to the <b>splitdns.config</b> file for the selection specification. See <a href="#">Using the Split DNS option, page 161</a>
<code>proxy.config.dns.splitdns.def_domain</code>	STRING	NULL	Specifies the default domain for split DNS requests. This value is appended automatically to the hostname if it does not include a domain before split DNS determines which DNS server to use.
<code>proxy.config.dns.url_expansions</code>	STRING	NULL	Specifies a list of hostname extensions that are automatically added to the hostname after a failed lookup; for example, if you want Content Gateway to add the hostname extension <b>.org</b> , specify <b>org</b> as the value for this variable (Content Gateway automatically adds the dot (.).)  Note: If the variable <b>proxy.config.http.enable_url_expandomatic</b> is set to 1 (the default value), you do not have to add <b>www.</b> and <b>.com</b> to this list; Content Gateway tries <b>www.</b> and <b>.com</b> automatically after trying the values you specify.



Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.dns.lookup_timeout</code>	INT	20	Specifies the DNS lookup timeout duration in seconds. When the timeout period expires, the lookup attempt is terminated.
<code>proxy.config.dns.retries</code>	INT	5	Specifies the number of times a DNS lookup is retried before giving up.

## DNS proxy

Configuration Variable Data Type	Data Type	Default Value	Description
<code>proxy.config.dns.proxy.enabled</code>	INT	0	Enables (1) or disables (0) the DNS proxy caching option that lets you resolve DNS requests on behalf of clients. This option off-loads remote DNS servers and reduces response time for DNS lookups. See <a href="#">DNS Proxy Caching</a> , page 91.
<code>proxy.config.dns.proxy_port</code>	INT	5353	Specifies the port that Content Gateway uses for DNS traffic.

## HostDB

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.hostdb.size</code>	INT	200000	Specifies the maximum number of entries allowed in the host database.
<code>proxy.config.hostdb.ttl_mode</code>	INT	0	Specifies the host database time to live mode. You can specify one of the following: <ul style="list-style-type: none"> <li>• 0 = obey</li> <li>• 1 = ignore</li> <li>• 2 = min(X,ttl)</li> <li>• 3 = max(X,ttl)</li> </ul>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.hostdb.timeout</code>	INT	86400	Specifies the foreground timeout, in seconds.
<code>proxy.config.hostdb.strict_round_robin</code>	INT	0	When disabled (0), Content Gateway always uses the same origin server for the same client as long as the origin server is available.

## Logging configuration

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.log2.logging_enabled</code>	INT	1	Enables and disables event logging: <ul style="list-style-type: none"> <li>• 0 = logging disabled</li> <li>• 1 = log errors only</li> <li>• 2 = log transactions only</li> <li>• 3 = full logging (errors + transactions)</li> </ul> See <a href="#">Working With Log Files</a> , page 195.
<code>proxy.config.log2.max_secs_per_buffer</code>	INT	5	Specifies the maximum amount of time before data in the buffer is flushed to disk.
<code>proxy.config.log2.max_space_mb_for_logs</code>	INT	20480	Specifies the amount of space allocated to the logging directory, in megabytes.
<code>proxy.config.log2.max_space_mb_for_orphan_logs</code>	INT	25	Specifies the amount of space allocated to the logging directory, in megabytes, if this node is acting as a collation client.
<code>proxy.config.log2.max_space_mb_headroom</code>	INT	100	Specifies the tolerance for the log space limit in bytes. If the variable <b>proxy.config.log2.auto_delete_rolled_file</b> is set to 1 (enabled), auto-deletion of log files is triggered when the amount of free space available in the logging directory is less than the value specified here.
<code>proxy.config.log2.hostname</code>	STRING	localhost	Specifies the hostname of the machine running Content Gateway.

Configuration Variable	Data Type	Default Value	Description
proxy.config.log2.logfile_dir	STRING	/opt/WCG/logs	Specifies the full path to the logging directory.
proxy.config.log2.logfile_perm	STRING	rw-r--r--	<p>Specifies the log file permissions. The standard UNIX file permissions are used (owner, group, other). Valid values are:</p> <ul style="list-style-type: none"> <li>• - = no permission</li> <li>• r = read permission</li> <li>• w = write permission</li> <li>• x = execute permission</li> </ul> <p>Permissions are subject to the umask settings for the Content Gateway process. This means that a umask setting of 002 will not allow write permission for others, even if specified in the configuration file.</p> <p>Permissions for existing log files are not changed when the configuration is changed.</p> <p>Linux only.</p>
proxy.config.log2.custom_logs_enabled	INT	0	<p>When enabled (1), supports the definition and generation of custom log files according to the specifications in <b>logs_xml.config</b>.</p> <p>See <a href="#">logs_xml.config</a>, page 335.</p>
proxy.config.log2.xml_logs_config	INT	1	<p>Specifies the size, in MB, which when reached causes the log files to roll. See <a href="#">Rolling event log files</a>, page 204.</p>
proxy.config.log2.squid_log_enabled	INT	0	<p>Enables (1) or disables (0) the squid log file format.</p>
proxy.config.log2.squid_log_is_ascii	INT	1	<p>Specifies the squid log file type:</p> <ul style="list-style-type: none"> <li>• 1 = ASCII</li> <li>• 0 = binary</li> </ul>
proxy.config.log2.squid_log_name	STRING	squid	Specifies the squid log filename.
proxy.config.log2.squid_log_header	STRING	NULL	Specifies the squid log file header text.
proxy.config.log2.common_log_enabled	INT	0	<p>Enables (1) or disables (0) the Netscape common log file format.</p>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.log2.common_log_is_ascii</code>	INT	1	Specifies the Netscape common log file type: <ul style="list-style-type: none"> <li>• 1 = ASCII</li> <li>• 0 = binary</li> </ul>
<code>proxy.config.log2.common_log_name</code>	STRING	common	Specifies the Netscape common log filename.
<code>proxy.config.log2.common_log_header</code>	STRING	NULL	Specifies the Netscape common log file header text.
<code>proxy.config.log2.extended_log_enabled</code>	INT	1	Enables (1) or disables (0) the Netscape extended log file format.
<code>proxy.config.log2.extended_log_is_ascii</code>	INT	1	Specifies the Netscape extended log file type: <ul style="list-style-type: none"> <li>• 1 = ASCII</li> <li>• 0 = binary</li> </ul>
<code>proxy.config.log2.extended_log_name</code>	STRING	extended	Specifies the Netscape extended log filename.
<code>proxy.config.log2.extended_log_header</code>	STRING	NULL	Specifies the Netscape extended log file header text.
<code>proxy.config.log2.extended2_log_enabled</code>	INT	0	Enables (1) or disables (0) the Netscape Extended-2 log file format.
<code>proxy.config.log2.extended2_log_is_ascii</code>	INT	1	Specifies the Netscape Extended-2 log file type: <ul style="list-style-type: none"> <li>• 1 = ASCII</li> <li>• 0 = binary</li> </ul>
<code>proxy.config.log2.extended2_log_name</code>	STRING	extended2	Specifies the Netscape Extended-2 log filename.
<code>proxy.config.log2.extended2_log_header</code>	STRING	NULL	Specifies the Netscape Extended-2 log file header text.
<code>proxy.config.log2.separate_host_logs</code>	INT	0	When enabled (1), configures Content Gateway to create a separate log file for HTTP/FTP transactions for each origin server listed in the <b>log_hosts.config</b> file (see <a href="#">HTTP host log splitting</a> , page 207).

Configuration Variable	Data Type	Default Value	Description
<code>proxy.local.log2.collation_mode</code>	INT	0	Specifies the log collation mode: <ul style="list-style-type: none"> <li>• 0 = Collation disabled.</li> <li>• 1 = This host is a log collation server.</li> <li>• 2 = This host is a collation client and sends entries using standard formats to the collation server.</li> </ul> For information on sending XML-based custom formats to the collation server, see <a href="#">logs_xml.config</a> , page 335.
<code>proxy.config.log2.collation_host</code>	STRING	NULL	Specifies the hostname of the log collation server.
<code>proxy.config.log2.collation_port</code>	INT	8085	Specifies the port used for communication between the collation server and client.
<code>proxy.config.log2.collation_secret</code>	STRING	foobar	Specifies the password used to validate logging data and prevent the exchange of unauthorized information when a collation server is being used.
<code>proxy.config.log2.collation_host_tagged</code>	INT	0	When enabled (1), configures Content Gateway to include the hostname of the collation client that generated the log entry in each entry.
<code>proxy.config.log2.collation_retry_sec</code>	INT	5	Specifies the number of seconds between collation server connection retries.
<code>proxy.config.log2.rolling_enabled</code>	INT	1	Enables (1) or disables (0) log file rolling. See <a href="#">Rolling event log files</a> , page 204.
<code>proxy.config.log2.rolling_interval_sec</code>	INT	21600	Specifies the log file rolling interval, in seconds. The minimum value is 300 (5 minutes). The maximum value is 86400 seconds (one day).
<code>proxy.config.log2.rolling_offset_hr</code>	INT	0	Specifies the file rolling offset hour. The hour of the day that starts the log rolling period.
<code>proxy.config.log2.rolling_size_mb</code>	INT	10	Specifies the size, in megabytes, which when reached causes the current file to be closed and a new file to be created.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.log2.auto_delete_rolled_files</code>	INT	1	Enables (1) or disables (0) automatic deletion of rolled files.
<code>proxy.config.log2.sampling_frequency</code>	INT	1	Configures Content Gateway to log only a sample of transactions rather than every transaction. You can specify the following values: <ul style="list-style-type: none"><li>• 1 = log every transaction</li><li>• 2 = log every second transaction</li><li>• 3 = log every third transaction and so on...</li></ul>

## URL remap rules

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.url_remap.default_to_server_pac</code>	INT	0	<p>Enables (1) or disables (0) requests for a PAC file on the proxy service port (8080 by default) to be redirected to the PAC port.</p> <p>For this type of redirection to work, the variable <code>proxy.config.reverse_proxy.enabled</code> must be set to 1.</p>
<code>proxy.config.url_remap.default_to_server_pac_port</code>	INT	-1	<p>Sets the PAC port so that PAC requests made to the Content Gateway proxy service port are redirected to this port.</p> <p><b>-1</b> specifies that the PAC port will be set to the autoconfiguration port (the default autoconfiguration port is 8083). This is the default setting.</p> <p>This variable can be used together with the <b><code>proxy.config.url_remap.default_to_server_pac</code></b> variable to get a PAC file from a different port. You must create and run a process that serves a PAC file on this port; for example, if you create a Perl script that listens on port 9000 and writes a PAC file in response to any request, you can set this variable to 9000, and browsers that request the PAC file from a proxy server on port 8080 will get the PAC file served by the Perl script.</p>
<code>proxy.config.url_remap.remap_required</code>	INT	0	<p>Set this variable to 1 if you want Content Gateway to serve requests only from origin servers listed in the mapping rules of the <code>remap.config</code> file. If a request does not match, the browser will receive an error.</p>
<code>proxy.config.url_remap.pristine_host_hdr</code>	INT	0	<p>Set this variable to 1 if you want to retain the client host header in a request during remapping.</p>

## Scheduled update configuration

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.update.enabled</code>	INT	0	Enables (1) or disables (0) the Scheduled Update option.
<code>proxy.config.update.force</code>	INT	0	Enables (1) or disables (0) a force immediate update. When enabled, Content Gateway overrides the scheduling expiration time for all scheduled update entries and initiates updates until this option is disabled.
<code>proxy.config.update.retry_count</code>	INT	10	Specifies the number of times Content Gateway retries the scheduled update of a URL in the event of failure.
<code>proxy.config.update.retry_interval</code>	INT	2	Specifies the delay in seconds between each scheduled update retry for a URL in the event of failure.
<code>proxy.config.update.concurrent_updates</code>	INT	100	Specifies the maximum simultaneous update requests allowed at any time. This option prevents the scheduled update process from overburdening the host.

## WCCP configuration

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.wccp.enabled</code>	INT	0	Enables (1) or disables (0) WCCP.
<code>proxy.local.wccp2.ethernet_interface</code>	STRING	<i>your_interface</i>	Specifies the ethernet interface used to talk to the WCCP v2 router.  Note: The Content Gateway installation script detects your Ethernet interface and sets this variable appropriately. If your system has multiple network interfaces, check that this variable specifies the correct interface.



## SSL Decryption



### Note

All SSL decryption setting should be made in the Content Gateway Manager. None of the variables in the table below should be modified directly in records.config.

Configuration Variable	Data Type	Default Value	Description
proxy.config.ssl_decryption.use_decryption	INT	0	When enabled (1), Content Gateway performs SSL decryption.
proxy.config.ssl_decryption_ports	INT	443	Specifies the HTTPS ports. Content Gateway allows SSL decryption and policy lookup only to the specified ports.
proxy.config.ssl_decryption.ui_enabled	INT	0	When enabled (1), the SSL configuration tab is displayed in the Content Gateway Manager.
proxy.config.ssl_management_port	INT	8071	The management port on which the SSL Manager listens.
proxy.config.ssl_inbound_port	INT	8070	The port on which SSL Manager listens for inbound (client-facing) traffic.
proxy.config.ssl_outbound_port	INT	8090	The port SSL Manager uses for outbound (Internet-facing) traffic.
proxy.config.ssl_outbound_ip	STRING	127.0.0.1	The IP address of the SSL Manager inbound and outbound proxy.
proxy.config.ssl_forward_to_inbound	INT	1	Do not change. When SSL Manager is enabled, causes SSL traffic to be forwarded to the correct proxy port.
proxy.config.administrator_id	STRING	NULL	Do not change. Holds the encrypted administrator ID. The variable is used by SSL Manager.

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.ssl_decryption.tunnel_skype</code>	INT	0	When enabled (1), Content Gateway identifies and tunnels Skype traffic (explicit proxy deployments only). User policies must be adjusted accordingly. See the configuration information in <a href="#">Enabling SSL Manager</a> , page 124.
<code>proxy.config.ssl_decryption.master_cas</code>	STRING	127.0.0.1	Do not change. The value is automatically set when <b>SSL Manager Configuration Server</b> is specified in the UI. A value of 127.0.0.1 means the SSL master configuration server is the local host.

## ICAP

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.icap.enabled</code>	INT	0	Enables (1) or disables (0) ICAP support with Websense Data Security Suite (DSS). See <a href="#">Working With Websense Data Security</a> , page 113.
<code>proxy.config.icap.ICAPUri</code>	STRING	NULL	<p>Specifies the Uniform Resource Identifier for the ICAP service. A backup server can be specified in a comma-separated list.</p> <p>Obtain the identifier from your DSS administrator. Enter the URI in the following format:</p> <pre>icap://hostname:port/path</pre> <p>For <i>hostname</i>, enter the IP address or hostname of the DSS Protector appliance.</p> <p>The default ICAP port is 1344.</p> <p><i>Path</i> is the path of the ICAP service on the host machine.</p> <p>For example:</p> <pre>icap://   ICAP_machine:1344/opt/   icap_services</pre> <p>You do not need to specify the port if you are using the default ICAP port 1344.</p>

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.icap.FailOpen</code>	INT	1	Set to: <ul style="list-style-type: none"> <li>• 1 to allow traffic when the ICAP server(s) is down</li> <li>• 0 to send a block page if the ICAP server(s) is down</li> </ul>
<code>proxy.config.icap.BlockHugeContent</code>	INT	0	Set to: <ul style="list-style-type: none"> <li>• 0 to send a block page if a file larger than the size limit specified by Data Security Suite is sent. The default size limit in DSS is 12 MB.</li> <li>• 1 to allow traffic</li> </ul>
<code>proxy.config.icap.AnalyzeSecureContent</code>	INT	1	Set to: <ul style="list-style-type: none"> <li>• 0 if decrypted traffic should be sent directly to its destination.</li> <li>• 1 if decrypted traffic should be sent to Data Security Suite for analysis.</li> </ul>
<code>proxy.config.icap.AnalyzeFTP</code>	INT	1	When enabled (1), send native FTP upload file transfers to ICAP server for analysis.
<code>proxy.config.icap.ActiveTimeout</code>	INT	5	The read/response timeout in seconds. The activity is considered a failure if the timeout is exceeded.
<code>proxy.config.icap.RetryTime</code>	INT	5	The recovery interval, in seconds, to test whether a down server is back up.
<code>proxy.config.icap.LoadBalance</code>	INT	1	When to ICAP servers are specified, set to: <ul style="list-style-type: none"> <li>• 1 to distribute requests to all available servers</li> <li>• 0 to distribute requests to only the primary server.</li> </ul>

## Data Security

Configuration Variable	Data Type	Default Value	Description
<code>proxy.config.dss.enabled</code>	INT	0	Enables (1) or disables (0) support for on-box Data Security. See <a href="#">Working With Websense Data Security</a> , page 113.
<code>proxy.config.dss.AnalyzeFTP</code>	INT	1	When enabled (1), send native FTP upload file transfers to the on-box Data Security policy engine for analysis.
<code>proxy.config.dss.AnalyzeSecureContent</code>	INT	1	Set to: <ul style="list-style-type: none"> <li>• 0 if decrypted traffic should be sent directly to its destination.</li> <li>• 1 if decrypted traffic should be sent to Data Security Suite for analysis.</li> </ul>
<code>proxy.config.dss.analysis_timeout</code>	INT	10000	Specifies the maximum length of time, in milliseconds, that a single file analysis can take before analysis is aborted.

## Connectivity, analysis, and boundary conditions

Configuration Variable	Data Type	Default Value	Description
<code>wtg.config.subscription_key</code>	STRING	NULL	Holds the Websense Security Gateway or Websense Security Gateway Anywhere subscription key value.
<code>wtg.config.download_server_ip</code>	STRING	<code>download.websense.com</code>	Holds the hostname or IP address of the Websense download server.
<code>wtg.config.download_server_port</code>	INT	80	Holds the port number of the Websense download server.
<code>wtg.config.policy_server_ip</code>	STRING		Holds the IP address of the Websense Policy Server.
<code>wtg.config.policy_server_port</code>	INT	55806	Holds the port number of the Websense Policy Server.
<code>wtg.config.wse_server_ip</code>	STRING		Holds the IP address of the Websense Filtering Service.

Configuration Variable	Data Type	Default Value	Description
<code>wtg.config.wse_server_port</code>	INT	15868	Holds the port number of the Websense Filtering Service WISP interface.
<code>wtg.config.ssl_bypassed_categories</code>	STRING	NULL	<p>This variable takes a list of category identifiers that will bypass SSL decryption.</p> <p><b>Do not change the value of this variable.</b> It is included strictly as a troubleshooting aid.</p> <p>Use the Web Security Manager to specify categories to bypass SSL decryption.</p>
<code>wtg.config.ssl_decryption_bypass_ip_based</code>	INT	0	<p>Specifies that the SSL category bypass process use only the IP address (not the hostname) when performing a category lookup.</p> <p>0 = disabled 1 = enabled</p>
<code>wtg.config.fail_open</code>	INT	1	<p>Specifies whether Content Gateway will permit or block the request when Websense Web filtering (Filtering Service) is unavailable.</p> <p>Set to:</p> <ul style="list-style-type: none"> <li>• 0 to send a block page</li> <li>• 1 to permit the request</li> </ul>
<code>wtg.config.fail_open_low_memory</code>	INT	0	<p>Specifies whether Content Gateway will permit or block traffic when there is a system low memory condition.</p> <p>Set to:</p> <ul style="list-style-type: none"> <li>• 0 to block traffic</li> <li>• 1 to permit traffic, bypassing scanning</li> </ul>
<code>wtg.config.fail_open_analytic_scan</code>	INT	1	<p>Specifies how Content Gateway behaves should analytic scanning become non-functional.</p> <p>Set to:</p> <ul style="list-style-type: none"> <li>• 0 to block traffic</li> <li>• 1 to perform a lookup in the URL master database and apply policy</li> </ul> <p><b>Note:</b> An alarm is raised whenever analytics scanning becomes non-functional.</p>

Configuration Variable	Data Type	Default Value	Description
<code>wtg.config.archive_depth</code>	INT	5	Specifies the maximum depth of analysis performed on archive files.
<code>wtg.config.max_decompressions</code>	INT	10	Specifies the maximum number of total decompressions to be performed on archive files (per transaction). The value should not exceed 25.
<code>wtg.config.max_subsamples</code>	INT	10000	Specifies the maximum number of discrete files within an archive file that Content Gateway may decompress and analyze to classify a given transaction.
<code>wtg.config.zipbomb_action</code>	INT	1	For internal use. Indicates zip bomb analysis status. <b>Do not change the value of this variable.</b>
<code>wtg.config.min_mem_avail</code>	INT	100	Specifies in megabytes, the minimum amount of available memory which when reached causes Content Gateway to request more memory from the system.
<code>wtg.config.max_mem_allowed</code>	INT	0	Specifies in megabytes, the maximum amount of memory, which when consumed, causes Content Gateway to perform more extensive memory monitoring.
<code>wtg.config.ip_ranges_not_to_scan</code>	STRING	10.0.0.0-10.255.255.255, 172.16.0.0-172.31.255.255, 192.168.0.0-192.168.255.255	Specifies internal IP address ranges not to scan. By default, the list is the standard private non-routable IP addresses. Address ranges are hyphenated with each range separated by a comma.  This is especially helpful in explicit proxy deployments in which a PAC file is not used and you want to exclude the standard internal IP addresses from being scanned.
<code>wtg.config.scan_ip_ranges</code>	INT	1	Enables (1) or disables (0) bypass of the internal IP address ranges specified in <code>wtg.config.ip_ranges_not_to_scan</code> . See above.

## remap.config

The `remap.config` file contains mapping rules that Websense Content Gateway uses to redirect HTTP requests permanently or temporarily without Content Gateway having to contact any origin server:



### Important

After you modify this file, run `content_line -x` from the Content Gateway **bin** directory (`/opt/WCG/bin`) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

## Format

Each line in the **remap.config** file must contain a mapping rule. Content Gateway recognizes three space-delimited fields: type, target, and replacement. The following table describes the format of each field.

Field	Description
<i>type</i>	Enter one of the following: <ul style="list-style-type: none"> <li><code>redirect</code>—redirects HTTP requests permanently without having to contact the origin server. Permanent redirects notify the browser of the URL change (by returning an HTTP status code 301) so that the browser can update bookmarks.</li> <li><code>redirect_temporary</code>—redirects HTTP requests temporarily without having to contact the origin server. Temporary redirects notify the browser of the URL change for the current request only (by returning an HTTP status code 307).</li> </ul>
<i>target</i>	Enter the origin or <i>from</i> URL. You can enter up to four components: <i>scheme://host:port/path_prefix</i> <i>scheme</i> can be <code>http</code> , <code>https</code> , or <code>ftp</code> .
<i>replacement</i>	Enter the destination or <i>to</i> URL. You can enter up to four components: <i>scheme://host:port/path_prefix</i> <i>scheme</i> can be <code>http</code> , <code>https</code> , or <code>ftp</code> .



### Note

The scheme type (HTTP, HTTPS, FTP) of the target and replacement must match.

## Examples

The following section shows example mapping rules in the **remap.config** file.

### Redirect mapping rules

The following rule *permanently* redirects all HTTP requests for `www.company.com` to `www.company2.com`:

```
redirect http://www.company.com http://www.company2.com
```

The following rule *temporarily* redirects all HTTP requests for `www.company1.com` to `www.company2.com`:

```
redirect_temporary http://www.company1.com http://  
www.company2.com
```

## socks.config

---

The **socks.config** file specifies the following information:

- ◆ The SOCKS servers that Websense Content Gateway passes through to access specific origin servers, and the order in which the proxy goes through the SOCKS server list



#### Note

You can specify your *default* SOCKS servers in the Content Gateway Manager or by editing the configuration variable:

```
proxy.config.socks.socks.default_servers
```

However, the **socks.config** file lets you perform additional SOCKS configuration; you can send requests to specific origin servers through specific SOCKS servers.

- ◆ The origin servers you want Content Gateway to access directly *without* going through the SOCKS server
- ◆ The user name and password that Content Gateway uses to connect to a SOCKS server (SOCKS version 5 only)



#### Important

After you modify this file, you must restart the proxy.

## Format

To specify the SOCKS servers Content Gateway must go through to reach specific origin servers, you must add a rule to the **socks.config** file with the following format:



```
dest_ip=ipaddress parent=server_name:port  
[round_robin=value]
```

where:

*ipaddress* is the origin server IP address or range of IP addresses separated by - or /.

*server\_name* is the hostname of the SOCKS server.

*port* is the port number through which the proxy communicates with the SOCKS server.

*value* is either *strict* if you want Content Gateway to try the SOCKS servers one by one, or *false* if you do not want round-robin selection to occur.

To specify the origin servers you want Content Gateway to access directly *without* going through the SOCKS server, enter a rule in the `socks.config` file in the following format:

```
no_socks ipaddress
```

where *ipaddress* is a comma-separated list of the IP addresses or IP address ranges associated with the origin servers you want Content Gateway to access directly. Do not specify the all networks broadcast address: 255.255.255.255.

To specify the user name and password Content Gateway uses for authentication with the SOCKS version 5 server, enter a rule in the `socks.config` file in the following format:

```
auth u username password
```

where *username* is the user name, and *password* is the password used for authentication.

**Note**

Each rule in the **socks.config** file can consist of a maximum of 400 characters. The order of the rules in the **socks.config** file is not significant.

---

## Examples

The following example configures the proxy to send requests to the origin servers associated with the range of IP addresses 123.15.17.1 - 123.14.17.4 through the SOCKS server `socks1` on port 1080 and `socks2` on port 4080. Because the optional specifier `round_robin` is set to *strict*, the proxy sends the first request to `socks1`, the second request to `socks2`, the third request to `socks1`, and so on.

```
dest_ip=123.14.15.1 - 123.14.17.4  
parent=socks1:1080;socks2:4080 round_robin=strict
```

The following example configures the proxy to access the origin server associated with the IP address 11.11.11.1 directly *without* going through the SOCKS server:

```
no_socks 11.11.11.1
```

The following example configures Content Gateway to access the origin servers associated with the range of IP addresses 123.14.15.1 - 123.14.17.4 and the IP address 113.14.18.2 directly *without* going through the SOCKS server:

```
no_socks 123.14.15.1 - 123.14.17.4, 113.14.18.2
```

The following example configures Content Gateway to use the user name `content_gateway` and the password `secret` for authentication with the SOCKS version 5 server:

```
auth u content_gateway secret
```

## **splitdns.config**

---

The **splitdns.config** file enables you to specify the DNS server that Content Gateway should use for resolving hosts under specific conditions.

To specify a DNS server, you must supply the following information in each active line within the file:

- ◆ A primary destination specifier in the form of a destination domain, a destination host, or a URL regular expression
- ◆ A set of server directives, listing one or more DNS servers with corresponding port numbers

You can also include the following optional information with each DNS server specification:

- ◆ A default domain for resolving hosts
- ◆ A search list specifying the domain search order when multiple domains are specified

For more information, see [Using the Split DNS option](#), page 161.



### **Important**

After you modify this file, run `content_line -x` from the Content Gateway **bin** directory (`/opt/WCG/bin`) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

---

## **Format**

Each line in the **splitdns.config** file uses one of the following formats:

```
dest_domain=dest_domain | dest_host | url_regex  
named=dns_server  
def_domain=def_domain search_list=search_list
```

The following table describes each field.

Field	Allowed Value
<i>dest_domain</i>	A valid domain name. This specifies that the DNS server selection be based on the destination domain. You can prefix the domain with an exclamation mark (!) to indicate the NOT logical operator.
<i>dest_host</i>	A valid hostname. This specifies that the DNS server selection be based on the destination host. You can prefix the host with an exclamation mark (!) to indicate the NOT logical operator.
<i>url_regex</i>	A valid URL regular expression. This specifies that the DNS server selection be based on a regular expression.
<i>dns_server</i>	This is a required directive. It identifies the DNS server for Content Gateway to use with the destination specifier. You can specify a port using a colon (:). If you do not specify a port, 53 is used. You can specify multiple DNS servers separated by spaces or by semicolons (;). You must specify the domains using IP addresses in dot notation.
<i>def_domain</i>	A valid domain name. This optional directive specifies the default domain name to use for resolving hosts. Only one entry is allowed. If you do not provide the default domain, the system determines its value from <b>/etc/resolv.conf</b> .
<i>search_list</i>	A list of domains separated by spaces or semicolons (;). This specifies the domain search order. If you do not provide the search list, the system determines the value from <b>/etc/resolv.conf</b> .

## Examples

Consider the following DNS server selection specifications:

```
dest_domain=internal.company.com named=255.255.255.255:212
255.255.255.254 def_domain=company.com
search_list=company.com company1.com
dest_domain=!internal.company.com named=255.255.255.253
```

Now consider the following two requests:

- ◆ `http://minstar.internal.company.com`  
This request matches the first line and select DNS server 255.255.255.255 on port 212. All resolver requests will use **company.com** as the default domain, and **company.com** and **company1.com** as the set of domains to search first.
- ◆ `http://www.microsoft.com`  
This request will match the second line. Therefore, Content Gateway selects DNS server 255.255.255.253. No **def\_domain** or **search\_list** was supplied, so Content Gateway retrieves this information from **/etc/resolv.conf**.

## storage.config

---

The **storage.config** file lists all the files, directories, or hard disk partitions that make up the cache.



---

**Important**

After you modify this file, you must restart the proxy.

---

## Format

The format of the **storage.config** file is:

*pathname size*

where *pathname* is the name of a partition, directory, or file, and *size* is the size of the named partition, directory, or file, in bytes. You must specify a size for directories or files. For raw partitions, size specification is optional.

You can use any partition of any size. For best performance, the following guidelines are recommended:

- ◆ Use raw disk partitions.
- ◆ For each disk, make all partitions the same size.
- ◆ For each node, use the same number of partitions on all disks.

Specify pathnames according to your operating system requirements. See the following examples.



---

**Important**

In the **storage.config** file, a formatted or raw disk must be at least 2 GB. The recommended disk cache size is 147 GB.

---

## update.config

---

The **update.config** file controls how Websense Content Gateway performs a scheduled update of specific local cache content. The file contains a list of URLs specifying objects that you want to schedule for update.

A scheduled update performs a local HTTP GET on the objects at the specific time or interval. You can control the following parameters for each specified object:

- ◆ The URL
- ◆ URL-specific request headers, which overrides the default
- ◆ The update time and interval

- ◆ The recursion depth



### Important

After you modify this file, run `content_line -x` from the Content Gateway **bin** directory (`/opt/WCG/bin`) to apply the changes. When you apply the changes to a node in a cluster, Content Gateway applies the changes to all nodes in the cluster.

Scheduled update supports the following tag/attribute pairs when performing recursive URL updates:

- ◆ `<a href="">`
- ◆ `<img src="">`
- ◆ `<img href="">`
- ◆ `<body background="">`
- ◆ `<frame src="">`
- ◆ `<iframe src="">`
- ◆ `<fig src="">`
- ◆ `<overlay src="">`
- ◆ `<applet code="">`
- ◆ `<script src="">`
- ◆ `<embed src="">`
- ◆ `<bgsound src="">`
- ◆ `<area href="">`
- ◆ `<base href="">`
- ◆ `<meta content="">`

Scheduled update is designed to operate on URL sets consisting of hundreds of input URLs (expanded to thousands when recursive URLs are included); it is *not* intended to operate on massively large URL sets, such as those used by Internet crawlers.

## Format

Each line in the `update.config` file uses the following format:

```
URL\request_headers\offset_hour\interval\recursion_depth\
```

The following table describes each field.

Field	Allowed Inputs
<i>URL</i>	HTTP and FTP-based URLs.
<i>request_headers</i>	(Optional.) A list of headers (separated by semi-colons) passed in each GET request. You can define any request header that conforms to the HTTP specification. The default is no request header.
<i>offset_hour</i>	The base hour used to derive the update periods. The range is 00-23 hours.
<i>interval</i>	The interval, in seconds, at which updates should occur, starting at offset hour.
<i>recursion_depth</i>	The depth to which referenced URLs are recursively updated, starting at the given URL.

## Examples

The following example illustrates an HTTP scheduled update:

```
http://www.company.com\User-Agent: noname user  
agent\13\3600\5\
```

This example specifies the URL and request headers, an offset hour of 13 (1 p.m.), an interval of one hour, and a recursion depth of 5. This would result in updates at 13:00, 14:00, 15:00, and so on. To schedule for an update to occur only once a day, use an interval value of 24 hours x 60 minutes x 60 seconds = 86400.

The following example illustrates an FTP scheduled update:

```
ftp://anonymous@ftp.company.com/pub/misc/  
test_file.cc\18\120\0\
```

This example specifies the FTP request, an offset hour of 18 (6 p.m.), and an interval of every two minutes. The user must be *anonymous* and the password must be specified by the variable *proxy.config.http.ftp.anonymous\_passwd* in the **records.config** file.

## wccp.config

---

The **wccp.config** file stores the WCCP configuration information and service group settings. When WCCP is enabled on the **Configure > MyProxy > Basic** page, WCCP service group settings can be configured on the **Configure > Networking > WCCP > General** page. Service groups must be defined if WCCP is to be used for transparent redirection to Content Gateway. For more information, see [Transparent interception with WCCP v2 devices](#), page 46.







# F

## Error Messages

### Websense Content Gateway error messages

---

The following table lists messages that can appear in system log files. This list is not exhaustive; it describes warning messages that can occur and might require your attention. For information about warning messages not included in the list below, go to [www.websense.com](http://www.websense.com) and then navigate to Support and Knowledge Base.

#### Process fatal errors

Message	Description
Accept port is not between 1 and 65535. Please check configuration.	The port specified in the records.config file that accepts incoming HTTP requests is not valid.
Ftp accept port is not between 1 and 65535.	The port specified in the records.config file that accepts incoming FTP requests is not valid.
Self loop is detected in parent proxy configuration.	The name and port of the parent proxy are the same as that of Content Gateway. This creates a loop when Content Gateway attempts to send requests to the parent proxy.
Could not open the ARM device	ARM failed to load. The most common reason for this is that the host system has an incompatible system kernel. To see if ARM is loaded, run: <code>/sbin/lsmmod   grep arm</code>
content_manager failed to set cluster IP address	The content_manager process could not set the cluster IP address. Check the cluster IP address. Make sure that it is not already used by another device in the network.
Unable to initialize storage. (Re)Configuration required.	Cache initialization failed during startup. The cache configuration should be checked and configured or reconfigured.

## Warnings

Message	Description
<i>Logfile error: error_number</i>	Generic logging error.
Bad cluster major version range <i>version1-version2</i> for node <i>IP address</i> connect failed	Incompatible software versions causing a problem.
can't open config file <i>filename</i> for reading custom formats	Custom logging is enabled, but Content Gateway cannot find the <b>logs.config</b> file.
connect by disallowed client <i>IP address</i> , closing connection	The specified client is not allowed to connect to Content Gateway. The client IP address is not listed in the <b>ip_allow.config</b> file.
Could not rename log <i>filename</i> to <i>rolled filename</i>	System error when renaming log file during roll.
Did <i>this_amount</i> of backup still to do <i>remaining_amount</i>	Congestion is approaching.
Different clustering minor versions <i>version 1</i> , <i>version 2</i> for node <i>IP address</i> continuing	Incompatible software versions causing a problem.
log format symbol <i>symbol_name</i> not found	Custom log format references a field symbol that does not exist. See <a href="#">Event Logging Formats</a> , page 309.
missing field for field marker	Error reading a log buffer.
Unable to accept cluster connections on port: <i>cluster_port_number</i>	Contact Websense Technical Support. Go to <a href="http://www.websense.com/support/">www.websense.com/support/</a> for Technical Support contact information
Unable to open log file <i>filename</i> , errno= <i>error_number</i>	Cannot open the log file.
Error accessing disk <i>disk_name</i>	Content Gateway might have a cache read problem. You might have to replace the disk.
Too many errors accessing disk <i>disk_name</i> : declaring disk bad	Content Gateway is not using the cache disk because it encountered too many errors. The disk might be corrupt and might have to be replaced.
No cache disks specified in <b>storage.config</b> file: cache disabled	The Content Gateway <b>storage.config</b> file does not list any cache disks. Content Gateway is running in proxy-only mode. You must add the disks you want to use for the cache to the <b>storage.config</b> file (see <a href="#">storage.config</a> , page 406).
All disks are bad, cache disabled	There is a problem with the cache disk(s) and caching has been disabled. Please verify that the cache disks are working and have been properly formatted for caching. See <a href="#">Configuring the Cache</a> , page 81.

Message	Description
Missing DC parameter <missing_param> on auth.profile line	A required parameter was not specified. Please provide a value for the missing parameter.
Bad DC parameter <bad_param> - <dc_name>	A specified Domain Controller parameter is invalid. Please enter a valid value for the cited parameter.
[ParentSelection] <error_description> for default parent proxy	Proxy chaining is not working due to misconfiguration of the parent proxy in the child proxy. Please check the chaining configuration of parent proxy values in the child proxy.
WCCP2: Cannot find Interface name. Please check that the variable proxy.local.wccp2. ethernet_interface is set correctly	No value is specified for the WCCP interface. In Content Gateway Manager check <b>Configure &gt; Networking &gt; WCCP &gt; General</b> . Or assign a value to proxy.local.wccp2.ethernet_interface in <b>records.config</b> .
ARMManager: Unable to read network interface configuration	There is a format or configuration error in <b>ipnat.conf</b> . In Content Gateway Manager, go to <b>Configure &gt; Networking &gt; ARM &gt; General</b> and click <b>Edit File</b> to view and correct <b>ipnat.conf</b> .

## Alarm messages

The following table describes alarm messages that you may see in Content Gateway Manager.

Message	Description/Solution
The Content Gateway subscription has expired.	Please contact your Websense customer service representative or Technical Support for assistance.
Content Gateway subscription download failed.	Content Gateway was unable to connect to the download server to verify the subscription information. Please check your connection to the download server.
After several attempts, Content Gateway failed to connect to the Websense Database Download Service. Please troubleshoot the connection.	Verify that Content Gateway is able to access the Internet. Check firewall and upstream proxy server settings that might prevent Content Gateway from connecting to the download server.

Message	Description/Solution
After several attempts, Content Gateway failed to connect to the Policy Server. Please troubleshoot the connection.	Verify that there is network connectivity between Content Gateway and Web Security. Sometimes firewall settings block connectivity. Also confirm that the Policy Server service is running on the Web Security host.
After several attempts, Content Gateway failed to connect to the Policy Broker. Please troubleshoot the connection.	Verify that there is network connectivity between Content Gateway and Web Security. Sometimes firewall settings block connectivity. Also confirm that the Policy Broker service is running on the Web Security host.
After several attempts, Content Gateway failed to connect to the Filter service. Please troubleshoot the connection.	Verify that there is network connectivity between Content Gateway and Web Security. Sometimes firewall settings block connectivity. Also confirm that the Filter Service process is running on the Web Security host.
Communication with the analytics engine has failed. Please restart Content Gateway.	Restart Content Gateway.
SSL decryption has been disabled due to an internal error, please restart Content Gateway.	There was a fatal error in the SSL Manager module. Please restart Content Gateway.
[Rollback::Rollback] Config file is read-only: <i>filename</i>	Go to the Content Gateway <b>config</b> directory (default location is <b>/opt/WCG/config</b> ) and check the indicated file permissions; change them if necessary.
[Rollback::Rollback] Unable to read or write config file <i>filename</i>	Go to the Content Gateway <b>config</b> directory and make sure the indicated file exists. Check its permissions and change them if necessary.
[Content Gateway Manager] Configuration File Update Failed <i>error_number</i>	Go to the Content Gateway <b>config</b> directory and check the indicated file permissions; change them if necessary.
Access logging suspended - configured space allocation exhausted.	The space allocated to the event log files is full. You must either increase the space or delete some log files to enable access logging to continue. To prevent this from happening, consider rolling log files more frequently and enabling the autodelete feature. See <a href="#">Rolling event log files</a> , page 204.
Access logging suspended - no more space on the logging partition.	The entire partition containing the event logs is full. You must delete or move some log files to enable access logging to continue. To prevent this from happening, consider rolling log files more frequently and enabling the autodelete feature. See <a href="#">Rolling event log files</a> , page 204.

Message	Description/Solution
Created zero length place holder for config file <i>filename</i>	Go to the Content Gateway <b>config</b> directory and check the indicated file. If it is indeed zero in length, use a backup copy of the configuration file.
Content Gateway can't open <i>filename</i> for reading custom formats	Make sure that the <i>proxy.config.log2.config_file</i> variable in the <b>records.config</b> file contains the correct path to the custom log configuration file (the default is <b>logging/logs.config</b> ).
Content Gateway could not open logfile <i>filename</i>	Check permissions for the indicated file and the logging directory.
Content Gateway failed to parse line <i>line_number</i> of the logging config file <i>filename</i>	Check your custom log configuration file. There may be syntax errors. See <a href="#">Custom logging fields, page 309</a> , for correct custom log format fields.
vip_config binary is not setuid root, manager will be unable to enable virtual ip addresses	The <b>content_manager</b> process is not able to set virtual IP addresses. You must setuid root for the <b>vip_config</b> file in the Content Gateway <b>bin</b> directory.
Content Gateway cannot parse the ICAP URI. Please ensure that the URI is entered correctly in Content Gateway Manager or in the <i>proxy.config.icap.ICAPUri</i> configuration variable.	The Universal Resource Identifier (URI) is not in the correct format. Enter the URI as follows:  icap://hostname:port/path  See <a href="#">Working With Websense Data Security, page 113</a> for additional details on the format of the URI.
The specified ICAP server does not have a DNS entry. Please ensure that a valid DSS hostname is entered correctly in Content Gateway Manager or in the <i>proxy.config.icap.ICAPUri</i> configuration variable.	The hostname in the <b>records.config</b> file does not match any entries in the DNS. Ensure that the name of a valid Websense Data Security Suite server is entered correctly in Content Gateway Manager.  See <a href="#">Working With Websense Data Security, page 113</a> for information on the format of the URI.
Content Gateway is not able to communicate with the DSS server. Please try again.	Ensure that the Websense Data Security Suite server is up and running, and accepting connections on the port specified in the <i>proxy.config.icap.ICAPUri</i> variable. Contact your Websense Data Security Suite administrator if this message persists.
Domain controller <i>domain_controller_name:port</i> is down.	The named NTLM domain controller is not responding to requests and has been marked as down. Investigation the status of the domain controller.

## HTML messages sent to clients

Websense Content Gateway returns detailed error messages to browser clients when there are problems with the HTTP transactions requested by the browser. These response messages correspond to standard HTTP response codes, but provide more information. A list of the more frequently encountered HTTP response codes is provided in [Standard HTTP response messages, page 419](#). You can customize the response messages.

The following table lists the Content Gateway hard-coded HTTP messages, their corresponding HTTP response codes, and their corresponding customizable files.

Title	HTTP Code	Description	Customizable Filename
Access Denied	403	You are not allowed to access the document at location <i>URL</i> .	access#denied
Bad HTTP request for FTP Object	400	Bad HTTP request for FTP object.	ftp#bad_request
Cache Read Error	500	Error reading from cache. Please retry request.	cache#read_error
Connection Timed Out	504	Server has not sent any data for too long a time.	timeout#inactivity
Content Length Required	400	Could not process this request because no Content-Length was specified.	request#no_content_length
Cycle Detected	400	Your request is prohibited because it would cause an HTTP proxy cycle.	request#cycle_detected
Forbidden	403	<i>port_number</i> is not an allowed port for SSL connections. (You have made a request for a secure SSL connection to a forbidden port number.)	access#ssl_forbidden
FTP Authentication Required	401	You need to specify a correct user name and password to access the requested FTP document <i>URL</i> .	ftp#auth_required
FTP Connection Failed	502	Could not connect to the server <i>server_name</i> .	connect#failed_connect
FTP Error	502	The FTP server <i>server_name</i> returned an error. The request for document <i>URL</i> failed.	ftp#error

Title	HTTP Code	Description	Customizable Filename
Host Header Required	400	An attempt was made to transparently proxy your request, but this attempt failed because your browser did not send an HTTP <code>Host</code> header. Manually configure your browser to use <code>https://proxy_name:proxy_port</code> as an HTTP proxy. See your browser's documentation for details.  Alternatively, end users can upgrade to a browser that supports the HTTP <code>Host</code> header field.	interception#no_host
Host Header Required	400	Your browser did not send a <code>Host</code> HTTP header field and therefore the virtual host being requested could not be determined. To access this Web site correctly, you will need to upgrade to a browser that supports the HTTP <code>Host</code> header field.	request#no_host
HTTP Version Not Supported	505	The origin server <i>server_name</i> is using an unsupported version of the HTTP protocol.	response#bad_version
Invalid HTTP Request	400	Could not process this <i>client_request</i> HTTP method request for <i>URL</i> .	request#syntax_error
Invalid HTTP Response	502	The host <i>server_name</i> did not return the document <i>URL</i> correctly.	response#bad_response
Malformed Server Response	502	The host <i>server_name</i> did not return the document <i>URL</i> correctly.	response#bad_response
Malformed Server Response Status	502	The host <i>server_name</i> did not return the document <i>URL</i> correctly.	response#bad_response
Maximum Transaction Time exceeded	504	Too much time has passed transmitting document <i>URL</i> .	timeout#activity
No Response Header From Server	502	The host <i>server_name</i> did not return the document <i>URL</i> correctly.	response#bad_response

Title	HTTP Code	Description	Customizable Filename
Not Cached	504	This document was not available in the cache, and you (the client) accept cached copies only.	cache#not_in_cache
Not Found on Accelerator	404	The request for <i>URL</i> on host <i>server_name</i> was not found. Check the location and try again.	urlrouting#no_mapping
NULL	502	The host <i>hostname</i> did not return the document <i>URL</i> correctly.	response#bad_response
Proxy Authentication Required	407	Please log in with user name and password.	access#proxy_auth_required
Server Hangup	502	The server <i>hostname</i> closed the connection before the transaction was completed.	connect#hangup
Temporarily Moved	302	The document you requested, <i>URL</i> , has moved to a new location. The new location is <i>new_URL</i> .	redirect#moved_temporarily
Transcoding Not Available	406	Unable to provide the document <i>URL</i> in the format requested by your browser.	transcoding#unsupported
Tunnel Connection Failed	502	Could not connect to the server <i>hostname</i> .	connect#failed_connect
Unknown Error	502	The host <i>hostname</i> did not return the document <i>URL</i> correctly.	response#bad_response
Unknown Host	500	Unable to locate the server named <i>hostname</i> . The server does not have a DNS entry. Perhaps there is a misspelling in the server name or the server no longer exists. Double-check the name and try again.	connect#dns_failed
Unsupported URL Scheme	400	Cannot perform your request for the document <i>URL</i> because the protocol scheme is unknown.	request#scheme_unsupported



## Standard HTTP response messages

---

The following standard HTTP response messages are provided for your information. For a more complete list, see the *Hypertext Transfer Protocol — HTTP/1.1 Specification*.

Message	Description
200	OK
202	Accepted
204	No Content
206	Partial Content
300	Multiple Choices
301	Moved Permanently
302	Found
303	See Other
304	Not Modified
400	Bad Request
401	Unauthorized; retry
403	Forbidden
404	Not Found
405	Method Not Allowed
406	Not acceptable
408	Request Timeout
500	Internal server error
501	Not Implemented
502	Bad Gateway
504	Gateway Timeout



# G

## The req\_ca.cnf File

Create a **req\_ca.cnf** file and copy the code below into that file. See [Creating a subordinate CA](#), page 128 for information on the **req\_ca.cnf** file.

```
#
# Configuration file for generating a CA Request
#
HOME = .
RANDFILE = $ENV::HOME/.rnd
#
[ policy_match ]
countryName = match
stateOrProvinceName = match
organizationName = match
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
#
[ policy_anything ]
countryName = optional
stateOrProvinceName = optional
localityName = optional
organizationName = optional
organizationalUnitName = optional
commonName = supplied
emailAddress = optional
#####
#
[ req ]
default_bits = 1024
default_keyfile = privkey.pem
distinguished_name = req_distinguished_name
string_mask = nombstr
req_extensions = v3_req # The extensions to add to a certificate
request
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
countryName_default = US
countryName_min = 2
countryName_max = 2
stateOrProvinceName = State or Province Name (full name)
stateOrProvinceName_default = Some-State
localityName = Locality Name (eg, city)
0.organizationName = Organization Name (eg, company)
0.organizationName_default = Internet Widgits Pty Ltd
#organizationalUnitName = Organizational Unit Name (eg, section)
```

```
#organizationalUnitName_default =
commonName = Common Name (Name of Sub-CA)
commonName_max = 64
emailAddress = Email Address
emailAddress_max = 64
[ v3_req ]
# Extensions to add to a certificate request to make it a CA
basicConstraints=CA:TRUE
nsCertType = sslCA
keyUsage = cRLSign, keyCertSign
```

## Frequently Asked Questions (FAQs)

---

- ◆ *How do disk I/O errors affect the cache and what does Content Gateway do when a cache disk fails?*, page 423
- ◆ *If a client disconnects during the time that Content Gateway is downloading a large object, is any of the object saved in the cache?*, page 424
- ◆ *Can Content Gateway cache Java applets, JavaScript programs, or other application files like VBScript?*, page 424
- ◆ *How do you access Content Gateway Manager if you forget the master administrator password?*, page 424
- ◆ *How do you apply changes to the logs\_xml.config file to all nodes in a cluster?*, page 425
- ◆ *In Squid- and Netscape-format log files, what do the cache result codes mean?*, page 425
- ◆ *What does the cctx field record in a custom log file?*, page 427
- ◆ *Does Content Gateway refresh entries in its host database after a certain period of time if they have not been used?*, page 427
- ◆ *Can you improve the look of your custom response pages by using images, animated gifs, and Java applets?*, page 427
- ◆ *How do you configure Content Gateway to serve only transparent requests?*, page 428

See *Troubleshooting tips*, page 429 for additional information.

## How do disk I/O errors affect the cache and what does Content Gateway do when a cache disk fails?

If a disk drive fails five successive I/O operations, Content Gateway considers the drive inaccessible and removes the whole disk from the cache. Normal cache operation continues on all other Content Gateway disk drives.

## If a client disconnects during the time that Content Gateway is downloading a large object, is any of the object saved in the cache?

When a client disconnects during an HTTP or FTP operation, Content Gateway continues to download the object from the origin server for up to 10 seconds. If the transfer from the origin server completes successfully within 10 seconds after the client disconnect, Content Gateway stores the object in the cache. If the origin server download does not complete successfully within 10 seconds, Content Gateway disconnects from the origin server and deletes the object from the cache. Content Gateway does not store partial documents in the cache.

## Can Content Gateway cache Java applets, JavaScript programs, or other application files like VBScript?

Content Gateway can store and serve Java applets, JavaScript programs, VBScripts, and other executable objects from its cache according to the freshness and cacheability rules for HTTP objects.

Content Gateway does not execute the applets, scripts, or programs. These objects run only when the client system that sent the request loads them.

## How do you access Content Gateway Manager if you forget the master administrator password?

During installation, you can specify an administrator password. The installer automatically encrypts the password and stores the encryptions in the `records.config` file. Each time you change passwords in Content Gateway Manager, Content Gateway updates the **records.config** file.

If you forget the administrator password and cannot access Content Gateway Manager, you can clear the current password in the **records.config** file (set the value of the configuration variable to NULL) and then enter a new password in Content Gateway Manager. You cannot set passwords in the **records.config** file because the password variables can contain only password encryptions or the value NULL.

1. Open the **records.config** file in `/opt/WCG/config`.
2. Set the variable `proxy.config.admin.admin_password` to NULL to leave the password blank.



### Note

Ensure that there are no trailing spaces after the word NULL.

---

3. Save and close the file.

4. From the Content Gateway **bin** directory (**/opt/WCG/bin**), run `content_line -x` to apply the changes.
5. Log on to Content Gateway Manager. When prompted for the user name and password, enter the administrator ID and leave the password entry blank.  
Because you have already cleared the password in the **records.config** file, you do not need a password to log on as the administrator.
6. Navigate to the **Configure > My Proxy > UI Setup > Login** tab.
7. In the **Administrator** section, leave the Old Password field empty. Type the new password in the **New Password** field, and then retype the new password in the **New Password (Retype)** field.
8. Click **Apply**.  
The next time you access Content Gateway Manager, you must use the new password.

## How do you apply changes to the `logs_xml.config` file to all nodes in a cluster?

After you modify the `logs_xml.config` file on one Content Gateway node, enter the following command from the Content Gateway **bin** directory (**/opt/WCG/bin**):

```
content_line -x
```

Content Gateway applies the changes to all nodes in the cluster. The changes take effect immediately.

## In Squid- and Netscape-format log files, what do the cache result codes mean?

The following table describes the cache result codes in the Squid and Netscape log files.

Cache Result Code	Description
TCP_HIT	Indicates that a valid copy of the requested object was in the cache and that the proxy sent the object to the client.
TCP_MISS	Indicates that the requested object was not in the cache and that the proxy retrieved the object from the origin server or from a parent proxy and sent it to the client.
TCP_REFRESH_HIT	Indicates that the object was in the cache but was stale. Content Gateway made an <code>if-modified-since</code> request to the origin server and the origin server sent a <code>304 not-modified</code> response. The proxy sent the cached object to the client.

Cache Result Code	Description
TCP_REF_FAIL_HIT	Indicates that the object was in the cache but was stale. Content Gateway made an <code>if-modified-since</code> request to the origin server but the server did not respond. The proxy sent the cached object to the client.
TCP_REFRESH_MISS	Indicates that the object was in the cache but was stale. Content Gateway made an <code>if-modified-since</code> request to the origin server and the server returned a new object. The proxy served the new object to the client.
TCP_CLIENT_REFRESH	Indicates that the client issued a request with a <code>no-cache</code> header. The proxy obtained the requested object from the origin server and sent a copy to the client. Content Gateway deletes any previous copy of the object from the cache.
TCP_IMS_HIT	Indicates that the client issued an <code>if-modified-since</code> request and the object was in the cache and fresher than the IMS date, or an <code>if-modified-since</code> to the origin server found that the cache object was fresh. The proxy served the cached object to the client.
TCP_IMS_MISS	Indicates that the client issued an <code>if-modified-since</code> request and the object was either not in cache or was stale in cache. The proxy sent an <code>if-modified-since</code> request to the origin server and received the new object. The proxy sent the updated object to the client.
TCP_SWAPFAIL	Indicates that the object was in the cache but could not be accessed. The client did not receive the object.
ERR_CLIENT_ABORT	Indicates that the client disconnected before the complete object was sent.
ERR_CONNECT_FAIL	Indicates that Content Gateway could not reach the origin server.
ERR_DNS_FAIL	Indicates that the Domain Name Server could not resolve the origin server name, or that no Domain Name Server could be reached.
ERR_INVALID_REQ	Indicates that the client HTTP request was invalid. Content Gateway forwards requests with unknown methods to the origin server.
ERR_READ_TIMEOUT	Indicates that the origin server did not respond to the Content Gateway request within the timeout interval.
ERR_PROXY_DENIED	Indicates that client service was denied by access control configuration.
ERR_UNKNOWN	Indicates that the client connected but subsequently disconnected without sending a request.



## What does the `cqtx` field record in a custom log file?

The `cqtx` field records the complete client request text (minus headers) in the log file. For example, `get http://www.company.com HTTP/1.0`.

## Does Content Gateway refresh entries in its host database after a certain period of time if they have not been used?

By default, the Content Gateway host database observes the time-to-live (ttl) values set by name servers. You can reconfigure Content Gateway to a different value.

1. Open the **records.config** file located in **/opt/WCG/config**.
2. Edit the following variable:

Variable	Description
<code>proxy.config.hostdb.ttl_mode</code>	<p>Set to</p> <p><b>0</b> - to obey the ttl values set by the name servers</p> <p><b>1</b> - to ignore the ttl values set by name servers and use the value set by the Content Gateway configuration variable <b>proxy.config.hostdb.timeout</b>. Set this variable to a value appropriate for your environment.</p> <p><b>2</b> - to use the lower of the two values (the one set by the name server or the one set by Content Gateway)</p> <p><b>3</b> - to use the higher of the two values (the one set by the name server or the one set by Content Gateway)</p>

3. Save and close the file.
4. From the Content Gateway **bin** directory (**/opt/WCG/bin**), run `content_line -x` to apply the configuration changes.

## Can you improve the look of your custom response pages by using images, animated gifs, and Java applets?

Content Gateway can respond to clients only with a single text or HTML document. However, you can provide references on your custom response pages to images, animated gifs, Java applets, or objects other than text that are located on a Web server.

Add links in the **body\_factory** template files in the same way you do for any image in an HTML document, with the full URL in the SRC attribute.

It is recommended that you do not run the Web server and Content Gateway on the same system, to prevent both programs from trying to serve documents on the same port number.

## How do you configure Content Gateway to serve only transparent requests?

You can configure Content Gateway to serve *only* transparent requests and prevent explicit proxy requests from being served in the following ways:

- ◆ You can control client access to Content Gateway from the **ip\_allow.config** file by specifying ranges of IP addresses that are allowed to use Content Gateway. If Content Gateway receives a request from an IP address not listed in a range specified in the file, it discards the request. See [ip\\_allow.config](#), page 332.
- ◆ If you do not know the ranges of client IP addresses allowed to access Content Gateway, you can add rules to the **ipnat.conf** file so that only requests that have been redirected by your Layer 4 switch or WCCP router reach the proxy port. To make a transparent-only Content Gateway server, add rules in the **ipnat.conf** file before the normal redirect service rule to redirect explicit proxy traffic to a port on which no service is listening. For example, if you want Content Gateway to ignore explicit HTTP requests, add rules above the normal HTTP redirect rule in the **ipnat.conf** file as shown below (where *ipaddress* is the IP address of your Content Gateway system and *port\_number* is a port number on which no service is listening):

```
rdr hme0 ipaddress port 80 -> ipaddress port port_number tcp
rdr hme0 ipaddress port 8080 -> ipaddress port port_number tcp
rdr hme0 0.0.0.0/0 port 80 -> ipaddress port 8080 tcp
```

Add equivalent rules to the **ipnat.conf** file for each protocol service port or separate network interface to be served. After you make changes to the **ipnat.conf** file, you must restart the proxy.

- ◆ If your Content Gateway system has multiple network interfaces or if you configure the Content Gateway operating system to use virtual IP addresses, you can give Content Gateway two IP addresses. One address must be the *real* address that the proxy uses to communicate with origin servers and the other a private IP address (for example 10.0.0.1) for WCCP or switch redirection. After you configure the IP addresses, you must add the following variables to the end of the **records.config** file. Replace *private\_ipaddress* with the private IP address used for WCCP or switch redirection and *real\_ipaddress* with the IP address the proxy uses to communicate with origin servers.

```
LOCAL proxy.local.incoming_ip_to_bind STRING
private_ipaddress
LOCAL proxy.local.outgoing_ip_to_bind STRING
real_ipaddress
```

## Troubleshooting tips

---

- ◆ [The throughput statistic is inaccurate in Content Gateway Manager, page 429](#)
- ◆ [You are unable to execute Content Gateway commands, page 429](#)
- ◆ [You observe inconsistent behavior when one node obtains an object from another node in the cluster, page 430](#)
- ◆ [Web browsers may display an error document with a data missing message, page 430](#)
- ◆ [Content Gateway does not resolve any Web sites, page 431](#)
- ◆ [Maximum document size exceeded message in the system log file, page 431](#)
- ◆ [DrainIncomingChannel message in the system log file, page 431](#)
- ◆ [No cop file message in the system log file, page 432](#)
- ◆ [Warning in system log file when editing vaddrs.config \(Linux\), page 432](#)
- ◆ [Non transparent requests fail after enabling always\\_query\\_destination, page 433](#)
- ◆ [Content Gateway is running but no log files are created, page 433](#)
- ◆ [Content Gateway error indicates too many network connections, page 434](#)
- ◆ [Low memory symptoms, page 434](#)
- ◆ [Connection timeouts with the origin server, page 435](#)
- ◆ [IBM Web servers do not work with Content Gateway, page 435](#)
- ◆ [Content Gateway does not start \(or stop\), page 435](#)

### The throughput statistic is inaccurate in Content Gateway Manager

Content Gateway updates the throughput statistic after it has transferred an entire object. For larger files, the byte count increases sharply at the end of a transfer. The complete number of bytes transferred is attributed to the last 10-second interval, although it can take several minutes to transfer the object.

This inaccuracy is more noticeable with a light load. A heavier load yields a more accurate statistic.

### You are unable to execute Content Gateway commands

Commands do not execute under the following conditions:

- ◆ If the `content_manager` process is not running.  
Check if the `content_manager` process is running by entering the following command:  

```
ps aux | grep content_manager
```

  
or

```
./WCGAdmin status
```

If the `content_manager` process is not running, enter the following command from the Content Gateway **bin** directory (**/opt/WCG/bin**) to start it:

```
./content_manager
```

**Important**

If you must stop Content Gateway, it is recommended that you restart it using **./WCGAdmin**. Stop it with **./WCGAdmin stop** and start it with **./WCGAdmin start** to ensure that all the processes stop and start correctly. See [Getting Started](#), page 11.

---

- ◆ If you are not executing the command from **\$WCGHome/bin**.  
If the Content Gateway **bin** directory is not in your path, prepend the commands with `./` (for example, `./content_line -h`).
- ◆ If multiple Content Gateway installations are present and you are not executing the command from the active path specified in **/etc/content\_gateway**.

Always change to the correct directory by issuing the command:

```
cd `cat /etc/content_gateway`/bin
```

## You observe inconsistent behavior when one node obtains an object from another node in the cluster

As part of the system preparation process, you must synchronize the clocks on all the nodes in your cluster. Minor time differences cause no problems, but differences of more than a few minutes can affect Content Gateway operation.

It is recommended that you run a clock synchronization daemon such as `xntpd`. You can obtain the latest version of `xntpd` from the following URL:

<http://www.ntp.org>

## Web browsers may display an error document with a data missing message

A message similar to the following displays in Web browsers:

```
Data Missing
```

```
This document resulted from a POST operation and has  
expired from the cache. If you wish you can repost the  
form data to re-create the document by pressing the  
reload button.
```

Web browsers maintain their local cache in memory and/or disk on the client system. Browser messages about documents that have expired from cache see the browser local cache, *not* the Content Gateway cache. There is no Content Gateway message or condition that can cause such messages to appear in a Web browser.

For information about browser cache options and effects, see the browser documentation.

## Content Gateway does not resolve any Web sites

The browser indicates that it is contacting the host and then times out with the following message:

```
The document contains no data; Try again later, or contact
the server's Administrator....
```

Make sure that the system is configured correctly and that Content Gateway can read the name resolution file:

- ◆ Check if the server can resolve DNS lookups by issuing the `nslookup` command. For example:

```
nslookup www.myhost.com
```
- ◆ Check if the `/etc/resolv.conf` file contains the valid IP address of your DNS server(s).
- ◆ On some systems, if the `/etc/resolv.conf` file is unreadable or has no name server entry, the operating system will use localhost as a name server. However, Content Gateway does not use this convention. If you want to use localhost as a name server, you must add a name server entry for 127.0.0.1 or 0.0.0.0 in the `/etc/resolv.conf` file.
- ◆ Check that the Content Gateway user account has permission to read the `/etc/resolv.conf` file. Change the file permissions to `rw-r--r-- (644)`.



### Important

If the IP addresses in `/etc/resolv.conf` change, Content Gateway must be restarted.

---

## Maximum document size exceeded message in the system log file

The following message appears in the system log file.

```
WARNING: Maximum document size exceeded
```

A requested object was larger than the maximum size allowed in the proxy cache. Content Gateway provided proxy service for the oversized object but did not cache it.

You can set the object size limit for the cache by modifying the **Maximum Object Size** field on the **Configure > Subsystems > Cache > General** tab. If you do not want to limit the size of objects in the cache, set the document size to 0 (zero).

## DrainIncomingChannel message in the system log file

The following messages appear in the system log file:

```
Feb 20 23:53:40 louis content_manager[4414]: ERROR ==>
[drainIncomingChannel] Unknown message: 'GET http://
www.telechamada.pt/ HTTP/1.0'
Feb 20 23:53:46 louis last message repeated 1 time
Feb 20 23:53:58 louis content_manager[4414]: ERROR ==>
[drainIncomingChannel] Unknown message: 'GET http://
www.ip.pt/ HTTP/1.0'
```

These error messages indicate that a browser is sending HTTP requests to one of the Content Gateway cluster ports, either `rsport` (default port 8087) or `mcport` (default port 8088). Content Gateway discards the request. This error does not cause any Content Gateway problems. The browser must be reconfigured to use the correct proxy port.



---

**Note**

Content Gateway clusters work best when configured to use a separate network interface and cluster on a private subnet so that client machines have no access to the cluster ports.

---

## No cop file message in the system log file

The following message appears repeatedly in the system log file:

```
content_cop[16056]: encountered "config/internal/no_cop"
file...exiting
```

The file **config/internal/no\_cop** acts as an administrative control that instructs the `content_cop` process to exit immediately without starting `content_manager` or performing any health checks. The **no\_cop** file prevents the proxy from starting automatically when it has been stopped with the `./WCGAdmin stop` or the `stop_content_gateway` commands. Without such a static control, Content Gateway would restart automatically upon system reboot. The `no_cop` control keeps Content Gateway off until it is restarted with the `./WCGAdmin start` or the `start_content_gateway` command.

The Content Gateway installation script creates a **no\_cop** file so that Content Gateway does not start automatically. After you have completed installation and configuration, and have rebooted the operating system, use the `./WCGAdmin start` or the `start_content_gateway` command to start Content Gateway. See [Getting Started, page 11](#), for information on starting and stopping Content Gateway.

## Warning in system log file when editing vaddrs.config (Linux)

If you edit the `vaddrs.config` file on a Linux system as a non-root user, Content Gateway issues a warning message in the system log file similar to the following:

```
WARNING: interface is ignored: Operation not permitted.
```

You can ignore this message. Content Gateway does apply your configuration edits.



---

**Important**

It is recommended that you always configure virtual IP addresses from Content Gateway Manager. Editing the **vaddrs.config** file can lead to unpredictable results.

---

## Non transparent requests fail after enabling `always_query_destination`

The variable `proxy.config.arm.always_query_dest` in the `records.config` file configures Content Gateway in transparent mode to ignore host headers and always ask for the IP address of the origin server. When you enable this variable, Content Gateway obtains the origin server's IP address from the existing NAT map list rather than trying to resolve the destination host name with a DNS lookup. As a result, logged URLs contain only IP addresses, not host names. To log domain names, set `proxy.config.arm.always_query_dest` to 0. However, setting `proxy.config.arm.always_query_dest` to 0 does not reduce the number of DNS lookups.

However, explicit requests (non transparent requests, including requests on port 80) fail, as there is no matching map in the NAT list.



---

**Note**

The `always_query_destination` option works only on the primary proxy port.

---

## Content Gateway is running but no log files are created

Content Gateway writes event log files only when there is information to record. If Content Gateway is idle, there may be no log files.

Ensure that you are looking in the correct directory. By default, Content Gateway creates log files in its **logs** directory. Check the location of the log files in Content Gateway Manager by examining the **Log Directory** field on the **Configure > Subsystems > Logging > General** tab. Alternatively, you can check the value of the variable `proxy.config.log2.logfile_dir` in the **records.config** file.

Check that the log directory has read/write permissions for the Content Gateway user account. If the log directory does not have the correct permissions, the `content_gateway` process is unable to open or create log files.

Check that logging is enabled. In Content Gateway Manager, examine the **Logging** area on the **Configure > Subsystems > Logging > General** tab. Alternatively, you can check the value of the variable `proxy.config.log2.logging_enabled` in the **records.config** file.

Check that a log format is enabled. In Content Gateway Manager, check that a standard format is enabled on the **Configure > Subsystems > Logging > Formats** tab or that the custom format is enabled on the **Custom** tab. In the **records.config** file, you select standard formats or the custom format by editing variables in the **Logging Config** section.

## Content Gateway error indicates too many network connections

By default, Content Gateway supports 8000 network connections: half of this number is allocated for client connections and half for origin server connections. A connection throttle event occurs when client or origin server connections reach 90% of half the configured limit (3600 by default). When a connection throttle event occurs, Content Gateway continues processing all existing connections but does not accept new client connection requests until the connection count falls below the limit.

Connection throttle events can occur under the following conditions:

- ◆ If there is a *connection spike* - if thousands of client requests all reach the proxy at the same time. Such events are typically transient and require no corrective action.
- ◆ If there is a *service overload* - if client requests continuously arrive faster than the proxy can service them. Service overloads often indicate network problems between Content Gateway and origin servers or indicate that Content Gateway needs more memory, CPU, cache disks, or other resources to handle the client load.

Examine the Performance graphs to determine the nature of the connection throttle. In particular, check the Client Connections, TCP Connections, and Client Ops Per Second graphs. You can also check error messages in the system log file, error log file, or event log files.

If necessary, you can reset the maximum number of connections supported by the proxy on the **Configure > Networking > Connection Management > Throttling** tab or by editing the value of `proxy.config.net.connections_throttle` in the **records.config** file. Do not increase the connection throttle limit unless the system has adequate memory to handle the client connections required. A system with limited RAM might need a throttle limit lower than the default value.



### Important

Do not set this variable below the minimum value of 100.

---

## Low memory symptoms

Under heavy load, the Linux kernel can run out of RAM. The low memory condition can cause slow performance and a variety of system problems. RAM exhaustion can occur even if the system has plenty of free swap space.

Symptoms of extreme memory exhaustion include the following messages in the system log files (**/var/log/messages**):



```
WARNING: errno 105 is ENOBUFS (low on kernel memory),
consider a memory upgrade
kernel: eth0: can't fill rx buffer (force 0)!
kernel: recvmsg bug: copied E01BA916 seq E01BAB22
```

To avoid memory exhaustion, add more RAM to the system or reduce the load on Content Gateway.

## Connection timeouts with the origin server

Some origin servers take longer than 30 seconds to post HTTP requests, which results in proxy connection timeouts. To prevent such connection timeouts, in Content Gateway Manager go to the **Configure > Protocols > HTTP > Timeouts** tab, and in the **Active Timeout** section, change the value of **Origin Server Response** to 60 seconds or more.

## IBM Web servers do not work with Content Gateway

IBM Web servers do not support the TLS (Transport Layer Security) protocol. For IBM Web servers to work with Content Gateway, you must edit the value of a configuration variable.

1. Open the **records.config** file located in **/opt/WCG/config**.
2. Edit the following configuration variable:

Variable	Description
proxy.config.ssl.TLSv1	Set this variable to 0 (zero).

3. Save and close the file.
4. From the Content Gateway **bin** directory (**/opt/WCG/bin**), run `content_line -x` to apply the changes.

## Content Gateway does not start (or stop)

Content Gateway starts automatically upon installation. If you must stop the product, the preferred method to stop and restart Content Gateway is to use the `./WCGAdmin start` and `./WCGAdmin stop` commands.

### Starting or stopping Content Gateway

1. Become root:
 

```
su
```
2. Change to the Content Gateway **bin** directory (**/opt/WCG/bin**)
3. Start the proxy:
 

```
./WCGAdmin start
```

Stop the proxy:

```
./WCGAdmin stop
```

# Glossary

## alternates

Different versions of the same Web object. Some origin servers answer requests to the same URL with a variety of objects. The content of these objects can vary, depending on whether a server delivers content for different languages, targets different browsers with different presentation styles, or delivers variable content at different times of the day.

## ARM

Adaptive Redirection Module. Used in transparent proxy caching, ARM is a component that redirects intercepted client traffic destined for an origin server to the Content Gateway application. Before the traffic is redirected by the ARM, it is intercepted by an **L4 switch** or router.

## cache

Stores copies of frequently accessed objects close to users and serves them to users when requested. See also **object store**.

## cache hierarchy

Levels of caches that communicate with each other. All cache hierarchies recognize the concepts of **parent cache** and **child cache**.

## cache hit

An object in the cache that can be served directly to the client.

## cache miss

An object that is not in the cache or that is in the cache but no longer valid. In both cases, the proxy must get the object from the **origin server**.

## caching web proxy server

A Web proxy server with local cache storage that allows the proxy to fulfill client requests locally, using a cached copy of the origin server's previous response.

## CGI

---

Common Gateway Interface. A set of rules that describe how an origin server and another piece of software (a *CGI program*) located on the same machine communicate.

### **cgi-bin**

The most common directory name on an origin server in which **CGI** programs are stored.

### **child cache**

A cache lower in a **cache hierarchy** for which Content Gateway is a parent. See also **parent cache**.

### **cluster**

A group of Content Gateway nodes that share configuration information and can act as a single large virtual cache.

### **Configure mode**

One of two modes in **Content Gateway Manager**. Configure mode lets you configure the Content Gateway system. See also **Monitor mode**.

### **content\_cop**

A Content Gateway process that monitors the health of the **content\_gateway** and **content\_manager** processes by periodically issuing heartbeat requests to fetch synthetic Web pages.

### **content\_gateway**

A Content Gateway process that is the cache processing engine of the Content Gateway product. **content\_gateway** is responsible for accepting connections, processing requests, and serving documents from the **cache** or **origin server**.

### **Content Gateway Manager**

Content Gateway's browser-based interface consisting of a series of Web pages that enable you to monitor performance and change configuration settings.

### **content\_manager**

A Content Gateway process and the command and control facility. **content\_manager** is responsible for launching, monitoring, and reconfiguring the **content\_gateway** process. It is also responsible for the administration user interface, the proxy auto-configuration port, and the statistics interface, cluster administration, and **virtual IP failover**.

### **cookie**

A piece of information sent by an origin server to a Web browser. The browser software saves the information and sends it back to the server whenever the browser makes additional requests from the server. Cookies enable origin servers to keep track of users.

---

## DNS

Domain Name Service. Content Gateway includes a fast, asynchronous DNS resolver to streamline conversion of host names to IP addresses.

## explicit proxy caching

A Content Gateway configuration option, in which client software (typically a browser) must be specifically configured to send Web requests to the Content Gateway proxy.

## FTP

File Transfer Protocol. A protocol based on TCP/IP for reliable file transfer.

## HTTP

Hypertext Transfer Protocol. The client/server protocol upon which the World Wide Web is based.

## HTTPS

Hypertext Transfer Protocol Secure. The use of HTTP with SSL to provide a form of encrypted communication on the World Wide Web.

## IP

Internet Protocol. The lowest-layer protocol under TCP/IP responsible for end-to-end forwarding and long packet fragmentation control.

## ISP

Internet Service Provider. An organization that provides access to the Internet.

## JavaScript

A scripting language designed to give Web pages the ability to interact with the people viewing them. Examples of such interaction include performing actions in response to mouse movement or mouse clicks and validation of what has been entered into forms.

## L4 switch

An Ethernet switch that can control network traffic flow using Level 4 rules. The switch can intercept desired client protocol packets and direct them to a proxy for transparent operation.

## management clustering

A Content Gateway option in which all nodes in a cluster automatically share configuration information.

## Monitor mode

One of two modes in **Content Gateway Manager**. Monitor mode lets you view statistics about Content Gateway performance and Web traffic. See also **Configure mode**.

---

## MRTG

Multi Router Traffic Grapher. A graphing tool provided with Content Gateway that creates the Performance graphs that allow you to monitor Content Gateway performance.

## Netscape log format

A standard access log format. Using the Netscape log format, you can analyze Content Gateway access log files with off-the-shelf log analysis scripts. See also [Squid log format](#).

## object store

A custom high-speed database, on which Content Gateway stores all cached objects.

## origin server

The Web server that contains the original copy of the requested information.

## PAC file

Proxy Auto-Configuration file. A JavaScript function definition that a browser calls to determine how requests are handled.

## parent cache

A cache higher up in a [cache hierarchy](#), to which the proxy can send requests.

## proxy server

See [web proxy server](#).

## router

A device that handles the connection between two or more networks. Routers look at destination addresses of the packets passing through them and decide which route to send them on.

## SOCKS

A circuit-level proxy protocol that provides a tunneling mechanism for protocols that cannot be proxied conveniently.

## Squid log format

A standard access log format. Using the Squid log format, you can analyze Content Gateway event log files with off-the-shelf log analysis scripts. See also [Netscape log format](#).

## SSL

Secure Sockets Layer. A protocol that enables encrypted, authenticated communications across the Internet. Used mostly in communications between origin servers and Web browsers.

---

## syslog

The UNIX system logging facility.

## TCP

Transmission Control Protocol. An Internet standard transport layer protocol. TCP provides reliable end-to-end communication by using sequenced data sent by IP.

## transparent proxy caching

A configuration option that enables Content Gateway to intercept and respond to Internet requests without requiring users to reconfigure their browser settings. It does this by intercepting traffic destined for an origin server and redirecting that traffic through the proxy cache.

## URL

Uniform Resource Locator. The address that defines the route to a file on the Web or other Internet facility.

## virtual IP failover

An option available to clustered Content Gateway servers, in which WCG maintains a pool of virtual IP addresses that it assigns to the nodes of a cluster. If a node fails, the remaining nodes mask the fault and take over the failed node's virtual interface.

## WCCP

Web Cache Control Protocol. A protocol used by Cisco IOS-based routers to redirect traffic during transparent proxy caching.

## web proxy server

A proxy server that forwards client requests to **origin servers**. The proxy server may deny requests according to filter rules or security limitations.

## web server

A computer that provides World Wide Web services on the Internet. See also **origin server**.

## WPAD

Web Proxy Auto-Discovery. A protocol that allows clients to automatically locate a Web proxy, providing the benefits of a proxy without the need for explicit client configuration.





# Copyrights

**Websense® Content Gateway Online Help**

©1996-2011, Yahoo, Inc., and Websense, Inc.

All rights reserved.

10240 Sorrento Valley Rd., San Diego, CA 92121, USA

Published March 31, 2015

Printed in the United States of America

R033011760

This document contains proprietary and confidential information of Yahoo, Inc. and Websense, Inc. The contents of this document may not be disclosed to third parties, copied, or duplicated in any form, in whole or in part, without prior written permission of Websense, Inc.

Websense and ThreatSeeker are registered trademarks of Websense, Inc., in the United States and certain international markets. Websense has numerous other unregistered trademarks in the United States and internationally. All other trademarks are the property of their respective owners.

Every effort has been made to ensure the accuracy of this manual. However, Websense Inc., and Yahoo, Inc. make no warranties with respect to this documentation and disclaim any implied warranties of merchantability and fitness for a particular purpose. Websense Inc. shall not be liable for any error or for incidental or consequential damages in connection with the furnishing, performance, or use of this manual or the examples herein. The information in this documentation is subject to change without notice.

Traffic Server is a trademark or registered trademark of Yahoo! Inc. in the United States and other countries.

Red Hat is a registered trademark of Red Hat Software, Inc.

Linux is a registered trademark of Linus Torvalds.

Microsoft, Windows, Windows NT, and Active Directory are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Mozilla and Firefox are registered trademarks of the Mozilla Foundation.

Netscape and Netscape Navigator are registered trademarks of Netscape Communications Corporation in the United States and in other countries.

UNIX is a registered trademark of AT&T.

All other trademarks are property of their respective owners.

**RESTRICTED RIGHTS LEGEND**

Use, duplication, or disclosure of the technical data contained in this document by the Government is subject to restrictions as set forth in subdivision (c) (1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 52.227-7013 and/or in similar or successor clauses in the FAR, or in the DOD or NASA FAR Supplement. Unpublished rights reserved under the Copyright Laws of the United States.

Contractor/manufacturer is Websense, Inc., 10240 Sorrento Valley Parkway, San Diego, CA 92121.

Portions of Websense Content Gateway include third-party technology used under license. Notices and attribution are included below.

**Portions of Websense Content Gateway include the following technology:****OpenSSL 0.9.6**

The OpenSSL is an open source toolkit licensed under the GNU General Public License. Copyright © 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA. 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 QUAL-

---

ITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

Netscape Directory SDK 4.0 for C

Netscape Directory SDK 4.0 for C is available without license fee under the terms of the Netscape ONE SDK End User License Agreement.

Each of the Components is provided on an "AS IS" basis, without warranty of any kind, including without limitation the warranties of merchantability, fitness for a particular purpose and non-infringement. The entire risk as to the quality and performance of the Components is borne by you. Should the Components prove defective or inaccurate, as the case may be, you and not Netscape or its suppliers assume the entire cost of any service and repair. In addition, the security mechanisms, if any, implemented by the Components have inherent limitations, and you must determine that each of the Components sufficiently meets your requirements. This disclaimer of warranty constitutes an essential part of the agreement. SOME JURISDICTIONS DO NOT ALLOW EXCLUSIONS OF AN IMPLIED WARRANTY, SO THIS DISCLAIMER MAY NOT APPLY TO YOU AND YOU MAY HAVE OTHER LEGAL RIGHTS THAT VARY BY JURISDICTION.

Tcl 8.3

Tcl software is copyrighted by the Regents of the University of California, Sun Microsystems, Inc., Scriptics Corporation, and other parties. The following terms apply to all files associated with the software unless explicitly disclaimed in individual files. The authors hereby grant permission to use, copy, modify, distribute, and license this software and its documentation for any purpose, provided that existing copyright notices are retained in all copies and that this notice is included verbatim in any distributions. No written agreement, license, or royalty fee is required for any of the authorized uses. Modifications to this software may be copyrighted by their authors and need not follow the licensing terms described here, provided that the new terms are clearly indicated on the first page of each file where they apply.

IN NO EVENT SHALL THE AUTHORS OR DISTRIBUTORS BE LIABLE TO ANY PARTY FOR DIRECT, INDIRECT, SPECIAL, INCIDENTAL, OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OF THIS SOFTWARE, ITS DOCUMENTATION, OR ANY DERIVATIVES THEREOF, EVEN IF THE AUTHORS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGE. THE AUTHORS AND DISTRIBUTORS SPECIFICALLY DISCLAIM ANY WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, AND NONINFRINGEMENT. THIS SOFTWARE IS PROVIDED ON AN "AS IS" BASIS, AND THE AUTHORS AND DISTRIBUTORS HAVE NO OBLIGATION TO PROVIDE MAINTENANCE, SUPPORT, UPDATES, ENHANCEMENTS, OR MODIFICATIONS.

libdb

LIBDB Copyright © 1991, 1993 The Regents of the University of California. All rights reserved. This product includes software developed by the University of California, Berkeley and its contributors.

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 LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER ARISING 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.

INN

Copyright © 1991, 1994, 1995, 1996, 1997, 1998, 1999, 2000, 2001 The Internet Software Consortium and Rich Salz. This code is derived from software contributed to the Internet Software Consortium by Rich Salz. 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 Internet Software Consortium and its contributors. 4. Neither the name of the Internet Software Consortium 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 INTERNET SOFTWARE CONSORTIUM 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 INTERNET SOFTWARE CONSORTIUM 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 AD-

---

WARRANTY OF THE POSSIBILITY OF SUCH DAMAGE.

#### MRTG

Multi Router Traffic Grapher (MRTG) is freely available under the terms of the GNU General Public License. Copyright © 1989, 1991 Free Software Foundation, Inc. 59 Temple Place - Suite 330, Boston, MA 02111-1307, USA

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.

#### Libregx

Copyright © 1992, 1993, 1994, 1997 Henry Spencer. All rights reserved. This software is not subject to any license of the American Telephone and Telegraph Company or of the Regents of the University of California.

#### libmagic

Copyright (c) Ian F. Darwin 1986, 1987, 1989, 1990, 1991, 1992, 1994, 1995.

Software written by Ian F. Darwin and others; maintained 1994- Christos Zoulas.

This software is not subject to any export provision of the United States Department of Commerce, and may be exported to any country or planet.

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 immediately at the beginning of the file, without modification, 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 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 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.



# Index

## A

- absolute freshness limit, setting, 19
- access log files, 149
- access web site, 143
- accessing Content Gateway Manager, 11, 155
- Adaptive Redirection Module. See ARM.
- adding certificate authorities, 134, 135
- adding nodes to a cluster, 72
- adding virtual IP addresses, 76
- admin, 2
- administration tools, 7
- administrator ID, 12
- administrator ID, changing, 154
- administrator ID, setting, 154
- administrator password, 154
- administrator password default
  - administrator ID, 12
- aging factor
  - modifying, 19
- alarm messages, 413
- alarm script file, 108
- alarms, 7, 107
  - clearing, 108
  - email notification, 108
  - viewing, 107
- Alarms button, 222
- alerts, 7
- allow certificates, 135
- allowing requests, 327
- alternates for caching, 31
- analytic\_server process, 7
- ARM, 5, 43, 63
  - bypass and WCCP, 45
  - enabling, 44
  - redirection rules, 44
  - static bypass rules, 62
- ASCII log files, 202
- ASCII\_PIPE mode, 200, 339
- auth.config file, 319
- autodeleting log files, 197

## B

- backing up certificates, 136
- backup domain controllers, 164
- binary log files, 202
- browsers to use with Content Gateway Manager, 11
- bypass rules
  - deny, 323
  - dynamic, 62
  - static, 63

- viewing, 64
- bypass.config file, 322
  - examples, 324
  - format, 323
- bypassing certificate validation, 141
- bypassing parent proxies, 78, 343

## C

- cache
  - changing capacity, 83
  - child, 77
  - clearing, 87
  - contents, 83, 406
  - hit, 18
  - miss, 18
  - partitioning, 85
  - scheduling updates to, 22, 406
  - statistics, 104
- cache affinity, 45, 47
- cache capacity, 406
- cache pinning, 24
- cache request overview, 17
- cache space
  - managing, 85, 346
- cache statistics, 222
- cache.config file, 19, 324
- cache-control headers, 20
- cached objects
  - expiration date, 18
  - freshness, 18
  - FTP, 18
  - HTTP, 18
- caching, 18
- caching alternates, 31
- caching cookied content, 30
- caching dynamic content, 30
- caching FTP objects, 32
- certificate authorities
  - adding, 134, 135
- certificate revocation lists
  - updating, 142
- certificate status, 134
- certificate validation, bypassing, 141
- certificates, 126, 135
  - allow, 135
  - backing up, 136
  - bypassing validation, 141
  - deleting, 134
  - deny, 135
  - generating, 126
  - importing, 127
  - managing, 134
  - restoring, 136
  - revocation status, 141

- sub-certificate authority, 128
- changing, 155
- changing cache capacity, 83
- changing certificate status, 134, 135
- changing records.config variables, 100
- changing size
  - RAM cache, 88
- changing status of, 135
- changing virtual IP addresses, 76
- child cache, 77
- Citrix, 168, 173, 183
- clearing alarms, 108
- clearing the cache, 87
- client access control lists, 62
- client access to proxy cache, 62, 153, 332
- client no-cache directives, 26
- clustering
  - adding nodes, 72
  - management, 70
  - management-only, 3
  - modes, 3
- collating event log files, 209
- command line interface
  - variables, 242
- command-line interface, 14
  - commands, 241
- commands
  - content\_line -h, 15
  - WCGAdmin start, 15
- configuration
  - remote, 156
- configuration files, 100
  - filter.config, 327
- configuration information, sharing, 70
- configuration options, 159
  - changing in the records.config file, 100
- configuration snapshots
  - deleting, 102
  - restoring, 102
  - taking, 101
- configuration variables (records.config), 347
- Configure mode
  - Content Gateway Manager, 95
- configuring Content Gateway, 95
- configuring user authentication
  - NTLM, 172
  - RADIUS, 177
- configuring Websense Content Gateway, 14, 100
  - via the command line, 99
- Content Gateway Manager, 104, 155
  - accessing, 11
  - alarms, 107
  - Alarms button (Monitor), 222
  - Configure mode, 12, 95

- controlling access, 154
  - logging on, 12
  - Monitor mode, 103
  - Performance button (Monitor), 106
  - starting, 11
  - starting Monitor mode, 103
  - supported browsers, 11
  - user accounts, 155
  - viewing statistics, 103, 104
- content\_cop process, 6, 7
- content\_gateway process, 6
- content\_line -h command, 15
- content\_manager process, 6
- contents, 149
- controlling
  - access to Content Gateway Manager, 154, 342
  - client access to proxy cache, 153
- controlling host access to Content Gateway Manager, 155
- controlling information leakage, 114
- cookies. See caching cookied content
- custom logging, 199
  - fields, 309
- customer support, 8

## D

- Date header, 18
- default, 12
- deleting certificates, 134
- deleting configuration snapshots, 102
- deny bypass rules, 63, 323
- deny certificates, 135
- denying requests, 327
- deployment options, 3
- directory services, user authentication, 163
- disabling
  - FTP over HTTP caching, 33
  - HTTP caching, 30
  - logging, 196
- disk usage
  - restricting, 85, 346
- displaying cache statistics, 104, 222
- DNS
  - proxy caching, 91
  - resolver, 6
- DNS servers
  - specifying, 161, 404
- dynamic bypass rules, 62
  - deny bypass, 63, 323
  - setting, 63
- dynamic bypass statistics, viewing, 63
- dynamic content
  - caching, 30

**E**

- editing virtual IP addresses, 76
- emailing alarms, 108
- encryption, 424
- error log files, 195
- error messages, 411
  - HTML, 416
- event log entries, examples, 214
- event log files
  - collating, 209
  - converting binary to ASCII, 203
  - managing, 197
  - splitting, 207
  - statistics, 212
  - summary logs, 201
- expiration date, 18
- Expires header, 18
- explicit proxy
  - HTTPS PAC file, 124
  - SSL, 123
- explicit proxy caching, 3, 17

**F**

- files
  - auth.config, 319
  - bypass.config, 322
  - cache.config, 19, 324
  - hosting.config, 330
  - ip\_allow.config, 153, 332
  - ipnat.conf, 333
  - log\_hosts.config, 208
  - logs\_xml.config, 199
  - mgmt\_allow.config, 155, 342
  - parent.config, 78, 343
  - partition.config, 85, 346
  - records.config, 19, 347
  - socks.config, 402
  - splittedns.config, 161, 404
  - storage.config, 83, 406
  - update.config, 406
  - wccp.config, 408
- filter.config file, 327
  - examples, 329
  - format, 328
- filtering rules, 327
- force immediate update option, 24
- forcing object caching, 31
- freshness computations, 19
- FTP client application, 39
- FTP objects
  - caching, 32
  - freshness, 22

**G**

- getting started, 11
- Graphs button
  - Content Gateway Manager, 104
  - statistics, 222
- Graphs button (Monitor), 222

**H**

- header requirements, 20
- headers
  - cache-control, 20
  - Expires, 18
  - Last-Modified, 18
  - max-age, 18
  - WWW-Authenticate, 29
- headroom limit (logging), 197
- health alerts, 7
- hierarchical caching, 3, 77
  - HTTP hierarchies, 77
  - parent failover, 78
- host access, 155
- host access to Content Gateway Manager, 155
- host database, 5
- host log splitting, 207
- hosting.config file, 330
- hostname length restriction with IWA, 168
- hostname, changing when using IWA user
  - authentication, 168
- HTML error messages, 416
- HTTP
  - alternates, 31
  - cache hierarchies, 77, 78, 343
  - host, separate logs, 207
- HTTP object freshness, 18
- HTTP response messages, 419

**I**

- ICAP, 114
- ICAP (Internet Content Adaptation Protocol)
  - protocols supported, 114
- ICAP Service URI, 118
- immediate update, 24
- inbound traffic
  - SSL, 137
- incidents, 143
- increasing cache capacity, 83
- information leakage, controlling, 114
- integrated windows authentication, 166
- interception strategies, 45
- internal root CA, 126
  - backup, 133
- IP spoofing, 66
- ip\_allow.config file, 153, 332



- examples, 332
- format, 332
- ipnat.conf file, 333
- IWA, 166
  - changing the domain, 169
  - configuration, 167
  - configuration summary, 166
  - finding the domain controller, 169
  - hostname length restriction, 168
  - hostname, changing, 168
  - troubleshooting, 169

## J

- Java, 11
- JavaScript, 11

## K

- keeping header information, 327
- Kerberos, 166

## L

- Last-Modified header, 18
- LDAP authentication rules, 327
- LDAP proxy authentication, 173
- listing cache contents, 83, 406
- listing commands, 15
- log collation, 209
- log collation server, 209
- log files
  - autodeleting, 197
- log files, contents, 149
- log formats, 198
- log\_hosts.config file, 208
- logcat application, 203
- LogFilter specification, 337
- LogFormat specification, 337
- logging
  - access logs, 148
  - activity logs, 148
  - aggregate summaries, 201
  - ASCII\_PIPE, 200, 339
  - choosing log file formats, 198
  - collating log files, 209
  - converting binary files to ASCII, 203
  - custom logging fields, 309
  - disabling, 196
  - example log entries, 214
  - file splitting, 207
  - headroom limit, 197
  - length of time to keep files, 149
  - managing log files, 197
  - Netscape Common formats, 313
  - Netscape Extended formats, 313

- Netscape Extended-2 formats, 314
- offset hour, 206
- rolling intervals, 206
- size of log files, 149
- Squid formats, 312
- SSL Manager, 148
- stand-alone collator (SAC), 211
- statistics, 212
- time stamps, 206
- WELF, 342
- logging on to Content Gateway Manager, 12
- LogObject specification, 338
- logs\_xml.config file, 199

## M

- management clustering, 70
- management-only clustering, 3
- manager alarms, 7
- managing certificates, 134
- max-age header, 18
- messages
  - certificate validation failure, 151
  - connection failure, 151
- mgmt\_allow.config file, 155, 342
- modifying aging factor, 19
- monitor
  - remote, 156
- Monitor mode, 103
- multiple realm user authentication, 179
  - aliases and logging, 181
  - authentication logic, 192
  - changing a rule, 188
  - configuration summary, 181
  - domains, 182
  - global options, 183
  - IWA rules, 184
  - LDAP rules, 186
  - legacy NTLM rules, 185
  - troubleshooting, 191
  - use cases, 189
- multi-user hosts, 168, 173, 183
- Multi-user IP Exclusions, 168, 173, 183
- My Proxy
  - statistics, 219
- My Proxy button
  - Monitor tab, 104

## N

- naming rolled log files, 205
- Netscape Common logging formats, 313
- Netscape Extended logging formats, 313
- Netscape Extended-2 logging formats, 314
- Networking



- statistics, 231
- Networking button
  - Content Gateway Manager Monitor tab, 106
- nodes
  - adding to a cluster, 72
- NTLM authentication rules, 327
- NTLM proxy authentication, 171, 172
- NTLMv2, 166

## O

- object caching, forcing, 31
- object freshness
  - aging factor, 19
- object store, 81
- offset hour, 206
- Online certification status protocol, 142
- origin server, 17
- orphan log files, 209
- outbound traffic
  - SSL, 137
- outgoing content, examining, 114
- overwriting dynamic bypass rules, 324

## P

- PAC file
  - HTTPS, 124
  - SSL Manager, 123
- parent cache, 77
- parent failover, 78
- parent proxies
  - bypassing, 78, 343
- parent.config file, 78, 343
- partition.config file, 85, 346
- partitioning the cache, 85
- partitions, 406
- passphrase, 128
- password, 12, 155
- password encryption, 424
- password, setting administrator, 154
- Performance graphs, 7
- pin-in-cache, 326
- print\_bypass utility, 64
- processes (Websense Content Gateway), 6
- Protocol
  - statistics, 222
- Protocols button
  - Content Gateway Manager Monitor tab, 104
- proxy cache
  - client access to, 153
  - controlling client access to, 332
- proxy caching
  - cache-control headers, 20
  - client no-cache directives, 26

- cookie content, 30
    - disabling HTTP caching, 30
    - dynamic content, 30
    - explicit, 17
    - FTP object freshness, 22
    - header requirements, 20
    - HTTP alternates, 31
    - revalidating HTTP objects, 21
    - scheduling cache updates, 22
    - server no-cache directives, 28
    - transparent, 17
    - whether to cache, 25
    - WWW-Authenticate headers, 29
- proxy user authentication, 162
- PUSH, 328

## R

- RADIUS proxy authentication, 176, 177
- RAM cache, 81, 88
- raw disk, 406
- Read authentication from child proxy, 250
- re-authentication, 165
- records.config file, 19
- records.config file, 347
- Redirect Hostname, 165
- redirecting requests (ARM), 43
- reducing cache capacity, 84
- regular expressions, 317
- remote monitoring and configuration, 156
- restoring certificates, 136
- restoring configuration snapshots, 102
- restoring Websense Content Gateway
  - configurations, 101, 102
- restricting access to Content Gateway
  - Manager, 154
- revalidation, 21
- revocation list
  - restoring, 136
- revocation status, 141
- rolled log files, 205
- rolling intervals, 206
- root CA
  - internal, 126
  - backup, 133
- routers
  - configuring, 50
- rules
  - filtering, 327

## S

- SAC (stand-alone collator), 211
- sample records.config file, 100
- saving configurations, 101

- scheduling cache updates, 22
- scheduling updates, 406
- script file for alarms, 108
- Secure Sockets Layer, 156
- Security
  - statistics, 225
- security, 153
  - Content Gateway Manager
    - access, 154
    - options, 1, 153
    - proxy user authentication, 162
    - SOCKS, 159
    - split DNS, 161
    - SSL for secure administration, 156
- Security button
  - Content Gateway Manager Monitor tab, 105
- server no-cache directives, 28
- service group ID number, 51
- service groups, 53
  - disabling WCCP processing, 53
  - enabling WCCP processing, 51
  - guidelines for configuring, 51
- setting absolute freshness limit, 19
- setting administrator ID and password, 154
- setting administrator password, 154
- sharing configuration information, 70
- snapshots
  - deleting, 102
  - restoring, 102
  - taking, 101
- SOCKS, 159
  - proxy options, 160
- SOCKS servers
  - specifying, 402
- socks.config file, 402
- split DNS, 161
- splitdns.config file, 161, 404
- splitting event log files, 207
- spoofing, 66
- Squid logging formats, 312
- SSL, 156
  - certificates, 156
  - enabling (Content Gateway Manager), 156
  - inbound traffic, 137
  - outbound traffic, 137
- SSL Manager
  - enabling, 124
- stand-alone collators, 211
- starting, 15
  - Content Gateway Manager Configure mode, 95
  - Content Gateway Manager Monitor mode, 103
- starting Content Gateway Manager, 11
- starting Websense Content Gateway, 15
- static bypass rules, 63, 324

- statistics
  - My Proxy, 219
  - Networking, 231
  - Protocol, 222
  - Subsystems, 229
  - viewing from Content Gateway Manager, 104
  - viewing from the command line, 106
  - viewing in Content Gateway Manager, 103
- status
  - changing certificate, 135
- status, certificate, 134
- storage.config file, 83, 406
  - format, 406
- stripping header information, 327
- Subsystems
  - statistics, 229
- Subsystems button
  - Content Gateway Manager Monitor tab, 105
- summary log files, 201
- Super Administrator
  - admin, 2
- system status, 7

## T

- technical support, 8
- terminal servers, 168, 173, 183
- time in cache, 18
- time stamps (log files), 205
- timeout period for user authentication, 165
- traffic analysis options, 7
- traffic graphs, see Performance graphs, 7
- transaction logging, 8
- transparent proxy
  - caching, 17
  - interception strategies, 45
- transparent proxy authentication, 165, 281
  - Authentication Mode, 165, 281
  - Redirect Hostname, 165, 281
  - Session TTL, 165, 281
- transparent proxy caching, 43
  - L4 switch, 45
  - policy-based routing, 60
  - software solutions, 60
  - WCCP, 46
- TRITON - Web Security, 2
- troubleshooting
  - Integrated Windows Authentication, 169

## U

- update.config file, 23, 406
- updates
  - scheduling, 406
- URL regular expressions, 317

- url\_regix, 317
- user accounts, 155
- user authentication, 162
  - backup domain controllers, 164
  - browser limitations, 164
  - integrated windows, 166
  - integrated windows, configuration summary, 166
  - Kerberos, 166
  - LDAP, 173
  - Multiple realm authentication, 179
    - aliases and logging, 181
    - authentication logic, 192
    - changing a rule, 188
    - configuration summary, 181
    - domains, 182
    - global options, 183
    - IWA rules, 184
    - LDAP rules, 186
    - legacy NTLM rules, 185
    - troubleshooting, 191
    - use cases, 189
  - NTLM, 171
  - NTLMv2, 166
  - RADIUS, 176
  - supported directories, 163
  - timeout period, 165
  - transparent, 163
  - transparent proxy, 165
- V**
- validation, bypassing certificate, 141
- variables
  - records.config file, 100, 347
- verifying that Websense Content Gateway is running, 14
- verifying URLs, 24
- viewing alarms, 107
- viewing bypass rules, 64
- viewing certificates
  - certificates
    - viewing, 134
- viewing dynamic bypass statistics, 63
- viewing logging statistics, 212
- viewing statistics
  - from Content Gateway Manager, 104
  - from the command line, 106
- virtual IP addresses, 75
  - adding, 76
  - editing, 76
- virtual IP failover, 3, 74
- W**
- WCCP, 46
  - enabling, 54
  - load balancing, 48
  - service groups, 53
- wccp
  - wccp.config file, 408
- WCCP 2.0
  - security, 53
- WCCP processing
  - disabling, 53
  - enabling, 51
- WCCP2 routers
  - configuring, 50
- WCGAdmin start command, 15
- Web browser authentication support limits, 164
- web proxy caching, 3, 17
- Web Security user identification, 162
- web site access, 143
- Websense Content Gateway, 15
  - verifying, 14
- Websense Content Gateway components, 5
- Websense Content Gateway configurations
  - saving, 101
- Websense Content Gateway Manager, 222
  - Monitor mode, 12
- Websense Content Gateway processes, 6
- WELF, 342
- WWW-Authenticate headers, 29
- X**
- X-Authenticated-User, 250
- X-Forwarded-For, 250
- XML custom log formats, 199, 335