FILEBURST GLOBAL CDN

TOKEN AUTHENTICATION USER GUIDE

v1.5

01/28/2010

Table of Contents

Overview

Fileburst Global CDN supports token-based authentication for clients who require security for their content. This feature allows an encrypted token to set access to particular content. Security options include expiration time (TTL), IP address, country block, referrer, and much more. These parameters are passed via the end of a URL string in an encrypted fashion to specify for how long a link is valid, which IP address has access to that link, which countries are blocked from accessing the link, and which referring URL is allowed to access the content. Fileburst offers token authentication across all of its platforms (HTTP, Windows, and Flash). In this document, "HTTP" includes both HTTP Large Object and HTTP Small Object platforms.

Encryption Key

Through an encryption key that is shared between the customer and Fileburst, the optional security parameters are passed through an encrypted URL token that is appended to the end of the URL string of an object. An example of what this encrypted URL may look like is:

```
http://www.domain.com/content.mov?a4fbc3710fd3449a7c99984d1b86603c22be1006d830b
```

The encryption key you provide will be used to create a secure URL token used for authentication. Our servers will use the key to decrypt the token and authenticate the file.

Primary Key and Backup Key

HTTP platforms currently have the functionality of setting a backup key in addition to the primary key. The backup key can be used to smoothly transition from using one key to another. If a backup key is provided, then our servers will also attempt to use this key to authenticate the request if authentication fails with the primary key. For example, the process to transition from key "A" to key "B" in the Media Control Center would be the following:

1) The primary key is set to "A" and all of your URLs are using tokens created with key "A".
2) Enter "A" for the backup key, and "B" for the primary key, and click on the "Update" button.
3) Allow at least one hour for the config changes to propagate to our servers.
4) Update all of your URLs to use tokens created with key "B". Note that tokens created with either key "A" or key "B" will authenticate during this time.
5) Enter "B" for the primary key, clear the backup key so that it is an empty string, and click on the "Update" button.
6) Allow at least one hour for the config changes to propagate to our servers.
7) Now, key "A" will no longer be valid and only key "B" will be used. Any existing URLs with tokens generated by key "A" will now be rejected by our servers.

Directories to Authenticate

Certain directories are flagged to be protected by token-based authentication. The directories that are specified will be valid for Fileburst origin and customer origin storage. For example, if you specify that you want "/secure_folder" to be protected, then the content under both "/Fileburstcdn.net/000003/secure_folder" and "/800003/customerorigin.com/secure_folder" will be protected. The setup of both the encryption key and the protected directories can be configured in the Media Control Center.

Custom Denial Handling

When access to content is denied, the default behavior is a server response code of 403. For HTTP platforms, you may set a customized response code with header information below.

301 - Moved Permanently - yields a redirect when combined with a Location header containing the URL of the redirect target
302 - Found (used as a temporary redirect) - yields a redirect when combined with a Location header containing the URL of the redirect target
307 - Temporary Redirect - yields a redirect when combined with a Location header containing the URL of the redirect target
403 - Forbidden
404 - File Not Found

For example, to redirect users whose request is rejected by token auth to a user-friendly error page, the recommended approach is as follows:

1) Choose "302" for the response code.
2) Choose "Location" as the added response header.
3) Set the header value to the full URL of your error page, for example http://yourdomain.com/error.php. The error page URL can reside on any domain, whether hosted by Fileburst or not.
4) Click "Update" and allow an hour for all changes to take effect.

Implementation

Clients who would like to implement token-based authentication need to download the binary token-generator file, "ec_encrypt.exe" (Windows) or "ec_encrypt" (Linux) used to create the

encrypted tokens. In the customer web application, the call to the executable takes two parameters and returns the token. The first parameter is the encryption key. The second parameter is the list of security parameters and their values.

A sample call to the .exe file using all the parameters would look like:

```
ec_encrypt.exe mykey
“ec_expire=1185943200&ec_ip=111.11.111.11&ec_country_allow=US&ec_ref_allow=ec
1.com”
```

The result of this call would return a token like:

```
a4fbc3710fd3449a7c99984d1b86603c22be1006d830b
```

The client would then append the token as a query string to the end of the URL path to the file.

```
http://www.domain.com/content.mov?a4fbc3710fd3449a7c99984d1b86603c22be1006d83
0b
```

Parameters

ec_expire

Platforms: HTTP, Flash, Windows

Description: This value sets the expiration of the token. The value is the number of seconds since Epoch (1970-01-01 00:00:00), and is based on GMT time. In this example, the value represents 2007-08-01 04:40:00

Example: 1185943200

ec_clientip

Platforms: HTTP, Flash, Windows

Description: This value is the IP address of the client requesting the content.

Example: 111.11.111.11

ec_country_deny

Platforms: HTTP, Flash, Windows

Description: This value is the two-letter ISO 3166 country code. The country specified will be *blocked* from accessing the content. Multiple country codes may be specified in this parameter by separating them with a comma. All other countries will be allowed. "ec_country_allow" takes precedence over "ec_country_deny" in the case that both are present. For a list of country codes, see end of document.

Example: US

ec_country_allow

Platforms: HTTP, Flash, Windows

Description: This value is the two-letter ISO 3166 country code. The country specified will be *allowed* to access the content. Multiple country codes may be specified in this parameter by separating them with a comma. All other countries will be blocked. "ec_country_allow" takes precedence over "ec_country_deny" in the case that both are present. For a list of country codes, see end of document.

Example: US

ec_ref_deny

Platforms: HTTP, Flash

Description: This value is a comma-separated list of referrers that will be denied access. The Referer header that is received will first have any leading "protocol://" stripped. The resulting Referer will then be tested against each item in the "ec_ref_deny" list. If any "ec_ref_deny" item matches the Referer, or matches the initial characters of the Referer, then access is denied.

For http platforms only, the ec_ref_deny value may optionally begin with a single '*', which will match zero or more initial non-"/" characters of the received Referer header to allow wildcard subdomain matching. If no Referer is given, or if the Referer does not match any of the "ec_ref_deny" items, then access is allowed. If both "ec_ref_allow" and "ec_ref_deny" are given, then "ec_ref_deny" is ignored.

Example: sample: ec_ref_deny=server1.com/file1,server2.com

DENIED: Referer=http://server1.com/file1
DENIED: Referer=http://server1.com/file1.htm
DENIED: Referer=http://server1.com/file1.swf
DENIED: Referer=http://server1.com/file1/file2.htm
DENIED: Referer=http://server2.com/dir1/

ALLOWED: Referer= (empty or not given)
ALLOWED: Referer=http://server1.com
ALLOWED: Referer=http://server1.com/file2
ALLOWED: Referer=http://images.server2.com
ALLOWED: Referer=http://server3.com

For http platforms only:

sample: ec_ref_deny=*.domain.com/folder/

DENIED: Referer=http://sub.domain.com/folder/
DENIED: Referer=http://sub.domain.com/folder/file1
DENIED: Referer=http://sub.sub.domain.com/folder/
DENIED: Referer=http://sub.sub.domain.com/folder/file1

ALLOWED: Referer=http://sub.domain.com/ ("/folder/" path did not match)
ALLOWED: Referer=http://domain.com/folder/ ("." after "*" did not match)
ALLOWED: Referer=http://subdomain.com/folder/ ("." after "*" did not match)
ALLOWED: Referer=http://other.com/sub.domain.com/folder/ ("*" only matches non-"/" characters)

ec_ref_allow

Platforms: HTTP, Flash

Description: This value is a comma-separated list of referrers that will be allowed access. The Referer header that is received will first have any leading "protocol://" stripped. The resulting Referer will then be tested against each item in the "ec_ref_allow" list. If any "ec_ref_allow" item matches the Referer, or matches the initial characters of the Referer, then access is allowed.

For http platforms only, the ec_ref_allow value may optionally begin with a single '*', which will match zero or more initial non-"/" characters of the received Referer header to allow wildcard subdomain matching. If no Referer is given, or if the Referer does not match any of the "ec_ref_allow" items, then access is denied. If both "ec_ref_allow" and "ec_ref_deny" are given, then "ec_ref_deny" is ignored.

Example: sample: ec_ref_allow=server1.com/file1,server2.com

ALLOWED: Referer=http://server1.com/file1
ALLOWED: Referer=http://server1.com/file1.htm
ALLOWED: Referer=http://server1.com/file1.swf
ALLOWED: Referer=http://server1.com/file1/file2.htm
ALLOWED: Referer=http://server2.com/dir1/

DENIED: Referer= (empty or not given)
DENIED: Referer=http://server1.com
DENIED: Referer=http://server1.com/file2
DENIED: Referer=http://images.server2.com
DENIED: Referer=http://server3.com

For http platforms only:

sample: ec_ref_allow=*.domain.com/folder/

ALLOWED: Referer=http://sub.domain.com/folder/

ALLOWED: Referer=http://sub.domain.com/folder/file1
ALLOWED: Referer=http://sub.sub.domain.com/folder/
ALLOWED: Referer=http://sub.sub.domain.com/folder/file1

DENIED: Referer=http://sub.domain.com/ ("/folder/" path did not match)
DENIED: Referer=http://domain.com/folder/ ("." after "*" did not match)
DENIED: Referer=http://subdomain.com/folder/ ("." after "*" did not match)
DENIED: Referer=http://other.com/sub.domain.com/folder/ ("*" only matches non-"/" characters)

ec_url_allow

Platforms: HTTP, Flash

Description: This value is a comma-separated list of page URLs that will be allowed access with the given token. This field can be used to restrict token auth strings to individual files, preventing a token auth string from being reused with a different file inside the same directory. The requested URL will first have any leading "protocol://hostname.com" stripped. The resulting URL will then be tested against each item in the "ec_url_allow" list. If any "ec_url_allow" item matches the URL, or matches the initial characters of the URL, then access is allowed. If the URL does not match any of the "ec_url_allow" items, then access is denied.

The path begins from the directory right after the hostname; so if using CNAMES, it will NOT include the AN portion of the URL, and if not using CNAMES, it WILL include the AN portion of the URL.

Example: sample: ec_url_allow=/dir1/movie1,/dir2

ALLOWED: http://server.com/dir1/movie1.flv
ALLOWED: http://server.com/dir1/movie1.mpg
ALLOWED: http://server.com/dir1/movie1/index.htm
ALLOWED: http://server.com/dir2/movie123.mpg

DENIED: http://server.com/dir1/movie2.flv
DENIED: http://server.com/dir3

ec_proto_deny

Platforms: HTTP

Description: This value is a comma-separated list of protocols that will be denied access with the given token. Protocols not explicitly listed will be allowed. Known protocols are "http" and "https". If both "ec_proto_allow" and "ec_proto_deny" are given, then "ec_proto_deny" is ignored.

Example: sample: ec_proto_deny=https

DENIED: https://host.com/file
ALLOWED: http://host.com/file

ec_proto_allow

Platforms: HTTP

Description: This value is a comma-separated list of protocols that will be allowed access with the given token. Protocols not explicitly listed will be denied. Known protocols are "http" and "https". If both "ec_proto_allow" and "ec_proto_deny" are given, then "ec_proto_deny" is ignored.

Example: sample: ec_proto_allow=https

ALLOWED: https://host.com/file
DENIED: https://host.com/file

ISO 3166 Country Codes

AF	Afghanistan
AL	Albania
DZ	Algeria
AS	American Samoa
AD	Andorra
AO	Angola
AI	Anguilla
AQ	Antarctica
AG	Antigua and Barbuda
AR	Argentina
AM	Armenia
AW	Aruba
AP	Asia/Pacific Region
AU	Australia
AT	Austria
AZ	Azerbaijan
BS	Bahamas
BH	Bahrain
BD	Bangladesh
BB	Barbados
BY	Belarus
BE	Belgium
BZ	Belize
BJ	Benin
BM	Bermuda
BT	Bhutan
BO	Bolivia
BA	Bosnia and Herzegovina
BW	Botswana
BV	Bouvet Island
BR	Brazil
IO	British Indian Ocean Territory
BN	Brunei Darussalam
BG	Bulgaria
BF	Burkina Faso
BI	Burundi
KH	Cambodia
CM	Cameroon
CA	Canada
CV	Cape Verde
KY	Cayman Islands
CF	Central African Republic
TD	Chad
CL	Chile
CN	China

CX	Christmas Island
CC	Cocos (Keeling) Islands
CO	Colombia
KM	Comoros
CG	Congo
CD	Congo, The Democratic Republic of the
CK	Cook Islands
CR	Costa Rica
CI	Cote d'Ivoire
HR	Croatia
CU	Cuba
CY	Cyprus
CZ	Czech Republic
DK	Denmark
DJ	Djibouti
DM	Dominica
DO	Dominican Republic
EC	Ecuador
EG	Egypt
SV	El Salvador
GQ	Equatorial Guinea
ER	Eritrea
EE	Estonia
ET	Ethiopia
EU	Europe
FK	Falkland Islands (Malvinas)
FO	Faroe Islands
FJ	Fiji
FI	Finland
FR	France
GF	French Guiana
PF	French Polynesia
TF	French Southern Territories
GA	Gabon
GM	Gambia
GE	Georgia
DE	Germany
GH	Ghana
GI	Gibraltar
GR	Greece
GL	Greenland
GD	Grenada
GP	Guadeloupe
GU	Guam
GT	Guatemala
GN	Guinea

GW	Guinea-Bissau
GY	Guyana
HT	Haiti
HM	Heard Island and McDonald Islands
VA	Holy See (Vatican City State)
HN	Honduras
HK	Hong Kong
HU	Hungary
IS	Iceland
IN	India
ID	Indonesia
IR	Iran, Islamic Republic of
IQ	Iraq
IE	Ireland
IL	Israel
IT	Italy
JM	Jamaica
JP	Japan
JO	Jordan
KZ	Kazakhstan
KE	Kenya
KI	Kiribati
KP	Korea, Democratic People's Republic of
KR	Korea, Republic of
KW	Kuwait
KG	Kyrgyzstan
LA	Lao People's Democratic Republic
LV	Latvia
LB	Lebanon
LS	Lesotho
LR	Liberia
LY	Libyan Arab Jamahiriya
LI	Liechtenstein
LT	Lithuania
LU	Luxembourg
MO	Macao
MK	Macedonia
MG	Madagascar
MW	Malawi
MY	Malaysia
MV	Maldives
ML	Mali
MT	Malta
MH	Marshall Islands
MQ	Martinique
MR	Mauritania

MU	Mauritius
YT	Mayotte
MX	Mexico
FM	Micronesia, Federated States of
MD	Moldova, Republic of
MC	Monaco
MN	Mongolia
ME	Montenegro
MS	Montserrat
MA	Morocco
MZ	Mozambique
MM	Myanmar
NA	Namibia
NR	Nauru
NP	Nepal
NL	Netherlands
AN	Netherlands Antilles
NC	New Caledonia
NZ	New Zealand
NI	Nicaragua
NE	Niger
NG	Nigeria
NU	Niue
NF	Norfolk Island
MP	Northern Mariana Islands
NO	Norway
OM	Oman
PK	Pakistan
PW	Palau
PS	Palestinian Territory
PA	Panama
PG	Papua New Guinea
PY	Paraguay
PE	Peru
PH	Philippines
PL	Poland
PT	Portugal
PR	Puerto Rico
QA	Qatar
RE	Reunion
RO	Romania
RU	Russian Federation
RW	Rwanda
SH	Saint Helena
KN	Saint Kitts and Nevis
LC	Saint Lucia

PM	Saint Pierre and Miquelon
VC	Saint Vincent and the Grenadines
WS	Samoa
SM	San Marino
ST	Sao Tome and Principe
SA	Saudi Arabia
SN	Senegal
RS	Serbia
SC	Seychelles
SL	Sierra Leone
SG	Singapore
SK	Slovakia
SI	Slovenia
SB	Solomon Islands
SO	Somalia
ZA	South Africa
GS	South Georgia and the South Sandwich Islands
ES	Spain
LK	Sri Lanka
SD	Sudan
SR	Suriname
SJ	Svalbard and Jan Mayen
SZ	Swaziland
SE	Sweden
CH	Switzerland
SY	Syrian Arab Republic
TW	Taiwan
TJ	Tajikistan
TZ	Tanzania, United Republic of
TH	Thailand
TG	Togo
TK	Tokelau
TO	Tonga
TT	Trinidad and Tobago
TN	Tunisia
TR	Turkey
TM	Turkmenistan
TC	Turks and Caicos Islands
TV	Tuvalu
UG	Uganda
UA	Ukraine
AE	United Arab Emirates
GB	United Kingdom
US	United States
UM	United States Minor Outlying Islands
UY	Uruguay

UZ	Uzbekistan
VU	Vanuatu
VE	Venezuela
VN	Vietnam
VG	Virgin Islands, British
VI	Virgin Islands, U.S.
WF	Wallis and Futuna
EH	Western Sahara
YE	Yemen
ZM	Zambia
ZW	Zimbabwe