Quick Reference

EDGECAST
LOS ANGELES, CA

SEP 2021
VER 1.6

Protect

Token-Based Authentication

Best Practices

General Security

Perform general administrative security tasks on a regular basis, such as:

- Remove old user accounts.
- Change passwords on a regular basis.
- Remind users to use complex passwords.

Primary and Backup Key

Take the following precautions to secure the primary and backup key:

- Ensure that these keys are never shared outside of your organization.
- Periodically rotate the primary key.
- Remove the backup key upon transitioning to a new primary key.

PARAMETERS

Parameter	Description
Allow Client IP Address (ec_clientip)	Limits connections to requests originating from a specific IP address. This parameter uses standard IPv4 notation.
Allow Country (ec_country_allow)	Defines the set of countries for which content delivery will be allowed. Set this parameter to a comma-delimited list of the desired countries (ISO 3166 country codes).
Deny Country (ec_country_deny)	Defines the set of countries for which content delivery will be denied. Set this parameter to a comma-delimited list of the desired countries (ISO 3166 country codes).
Expiration Date (ec_expire)	Defines a token value's expiration date and time (GMT). Set this parameter to the number of seconds that must pass between the start of Unix time and the desired expiration date/time.
Allow Host (ec_host_allow)	Defines a set of hostnames through which content delivery will be allowed. Set this parameter to a comma-delimited list of hosts. A comparison will be made against the value specified in the Host request header.
Deny Host (ec_host_deny)	Defines a set of hostnames through which content delivery will be denied. Set this parameter to a comma-delimited list of hosts. A comparison will be made against the value specified in the Host request header.
Allow Referrer (ec_ref_allow)	Defines a set of referrers through which content delivery will be allowed. Set this parameter to a comma-delimited list of referrers. A comparison will be made against the value specified in the Referer request header. A match is found when the Referer request header starts with a value specified by this parameter.
Deny Referrer (ec_ref_deny)	Defines a set of referrers through which content delivery will be denied. Set this parameter to a comma-delimited list of referrers. A comparison will be made against the value specified in the Referer request header. A match is found when the Referer request header starts with a value specified by this parameter.
Allow Protocol (ec_proto_allow)	Defines a protocol through which content delivery will be allowed. Acceptable values for this parameter are "http" and "https.“
Deny Protocol (ec_proto_deny)	Defines a protocol through which content delivery will be allowed. Acceptable values for this parameter are "http" and "https.“
Allow URL (ec_url_allow)	Defines a relative URL path for valid requests. Only requests that start with the specified URL path will be allowed access. This parameter should not include the protocol and domain portions of the desired URL (e.g., http://www.domain.com).

Authentication Directory Configuration

- Specify a relative path that starts with a forward
- slash (/).
- Add the root folder (/) as an authentication directory to require authentication for all requests on the current platform.
  The comparison of an authentication directory to a request starts after the base URL. Please refer to the table directly to the right to find out the base URL for each request type.

SECURED DIRECTORY COMPARISON

Origin	URL Type	Starts After (Base URL)
Customer Origin	CDN & Edge CNAME URL	http://<Domain>/80xxxx https://<Domain>/80xxxx
CDN Origin	CDN URL	http://<Domain>/00xxxx
CDN Origin	Edge CNAME URL	http://<Domain> https://<Domain>