CenturyLink Technology Solutions

**CenturyLink Technology Solutions Service Guide**

# CDN Service Guide

This Service Guide sets forth a description of the Content Delivery Network Services Portfolio offered by CenturyLink Technology Solutions ("CenturyLink"), including technical details and additional requirements or terms, if any. This guide is subject to and incorporated into the Master Service Agreement and Service Schedule between the parties. The specific details of the Service ordered by Customer will be set forth on the relevant Service Order.

**CenturyLink Technology Solutions**
www.centurylink.com/technology

Town & Country, MO 63017
Office: 314.628.7000

# Table of Contents

Content Delivery Network ……..3

Portfolio Overview. ……..3

Service Specifications and Terms ..... 3

Caching Service Description ..... 3

Streaming Service Description ..... 6

Customizable Features for Caching and Streaming Services .... 9

Origin Storage Service Description ..... 13

Administration and Reporting ..... 15

Installation..... 19

Maintenance and Support ..... 19

Charges ..... 20

Additional Requirements ..... 20

Roles and Responsibilities ..... 20

Appendix……..24

Content Freshness..... 24

Services not available everywhere. Business customers only. CenturyLink may change or cancel services or substitute similar services at its sole discretion without notice.
©2014 CenturyLink. All Rights Reserved. The CenturyLink mark, pathways logo and certain CenturyLink product names are the property of CenturyLink. All other marks are the property of their respective owners.

# Content Delivery Network

## Portfolio Overview

The CenturyLink Technology Solutions' Content Delivery Network ("CDN") Services Portfolio includes the following services for the delivery and storage of digital content distributed via the Internet:

- Caching
- Streaming
- Origin Storage

CenturyLink provides these CDN Services using the CDN infrastructure of Level 3 Communications; an international network of servers located in strategic locations at the edge of the internet ("CDN Network") to direct content requests to an optimal location on the network.

Customer subscribes to CDN Services by selecting the appropriate service(s), utilization allowance(s) and customizable feature(s) to meet its distribution needs.

## Service Specifications and Terms

Caching Service and Streaming Service consist of:

- Access to the CDN Network
- Subscriber chosen allowance
- Administration and Reporting web portal
- Customizable Features subscribed to by Customer
- 24x7 Support

Origin Storage Service consists of:

- Access to Origin Storage Platform
- Subscriber chosen allowance
- Administration and Reporting web portal
- 24x7 Support

## Caching Service Description

The Caching Service optimizes the performance of delivering web-based content; both small and large objects ("resources") by caching that content at the edge of the internet via an international network of caching servers so as to position the content closer to end-users.

The Caching Service configuration takes into account the Customer's caching and security requirements based on the content within their web site as well as the geographical location of their target audience; processing characteristics are assigned and the Caching Service is configured to address individual Customer needs.

### Delivery Models

The Caching Service supports the following models for content delivery:

| Delivery Model | Description |
|---|---|
| Object Delivery | The most common method to deliver popular content such as video, games, multimedia, patches, and file downloads for large audiences. Objects can be tagged for control over delivery, authentication, and content freshness. |
| Whole Site Delivery | To improve overall site performance the Caching Service can be configured to route all traffic for a particular domain name through the CDN. |
| Secure Delivery | Applicable to both Object and Whole Site Delivery; for the delivery of HTTPS content, implemented using either a Shared or Private SSL certificate. |

### Content Origin

The Caching Service supports the following content origin options:

| Option | Description |
|---|---|
| Customer Origin | Customer maintains their own origin infrastructure to store their web content which in turn feeds the CDN. |
| CDN Origin Storage | Customer subscribes to Origin Storage Service and uploads its popular content to the Origin Storage Platform which in turn feeds the CDN. |

For more information on CDN Origin Storage see the Origin Storage Service Description later in this document.

### Content Population

Content is populated to the CDN upon the initial request by a user viewing or accessing the Customer's website, where it is retrieved from the origin server and delivered to the requestor and cached for future requests. Subsequent requests are then served the cached copy.

### Caching Regions

Customer subscribes to one or more regions to cache their content, with a chosen allowance for each, depending on the geographic location of their end-user audience.

The Caching Service is offered in the following regions:

- North America/Europe
- Asia
- South America
- Middle East and Africa

End-user requests received from unsubscribed regions are delivered from a cache location within a subscribed region that is closest to the requestor.

To view a map of the CDN Network, access the Level 3 Interactive Network Map at http://maps.level3.com.

### Secure Delivery

The Caching Service supports the delivery of HTTPS content for both Object and Whole Site delivery models. Secure delivery requires a SSL Certificate. The following types of certificates are supported:

| Type | Description |
|---|---|
| Shared Certificate | SSL Certificate administered by Level 3 Communications. With Shared SSL Customer receives a secure URL similar to https://secure.footprint.net/yourname/ |
| Private Certificate | Customer-owned SSL Certificate; support for single site, wildcard, Extended Validation (EV) and SAN certificates. With Private SSL Customer receives a secure URL similar to https://secure.yourname.com/<br>In the event customer chooses to purchase a new SSL Certificate, a Certificate Signing Request ("CSR") can be provided to Customer which in turn is provided to their Certificate Authority.<br>The following details are necessary to prepare the CSR:<br>• Domain = (example: *.customer.com)<br>• Subject Alternative Name (only if desired) = (example: images.customerstage.com)<br>• L = (example: Los Angeles<br>• ST = (example: CA)<br>• C = (example: US)<br>• O = (example: Customer, Inc.) |

Implementing a Private Certificate requires additional steps in the configuration process to facilitate the receipt of the certificate which can occur in one of the following two ways:

| Key Option | Process |
|---|---|
| Existing Key | Customer will provide, in a secure fashion, their SSL certificate, private key, and pass phrase to decrypt. Upon receipt the SSL certificate and key is installed on the CDN network. |
| New Key | Customer provides their SSL certificate and a private key is generated locally. The SSL certificate and key is installed on the CDN network. |

### Customizable Features

There is several security and analytics related options available for the Caching Service. For a detailed description of these features see the Customizable Features for Caching and Streaming Services section later in this document.

### Administration and Reporting

Administration and reporting capabilities for the Caching Service are provided via a web-based CDN Portal. See the Administration and Reporting section later in this document for a detail description.

### Content Freshness

For information on Content Freshness, see the Content Freshness section in the Appendix of this document.

## Streaming Service Description

The Streaming Service delivers video and audio content encoded by Customer in a supported streaming format ("Steaming Media") via a network of streaming cache servers on the Internet.

The following Streaming Service configurations are supported:

| Configuration | Description |
|---|---|
| On-Demand Streaming | Enables Customer to distribute archived Streaming Media for viewing upon end-user request, where the content can be viewed at any time. |
| Live Streaming: Single Event | Enables Customer to distribute Streaming Media for live viewing during a single event (as such event is specified in the Customer Service Order with CenturyLink). |
| Live Streaming: Event Series | Enables Customer to distribute Streaming Media for live viewing during a series of Events scheduled by Customer during the Service Term. |
| Live Streaming: Always On | Enables Customer to distribute Streaming Media continuously for viewing for the duration of the Service Term; where the ingest point is always available. |

All Streaming Media delivered by Customer shall be delivered in the supported encoding format(s) selected by Customer in the Customer Order.

Customer shall be responsible for maintaining any master or back-up copies of Streaming Media or other Customer provided content. CenturyLink shall not be responsible for and shall have no liability for any claims relating to the destruction, loss or corruption of Streaming Media or other Customer provided content.

### Streaming Regions

Customer subscribes to one or more regions to steam their content, with a chosen allowance for each, depending on the geographic location of their end-user audience.

The Streaming Service is offered in the following regions:

- North America/Europe
- Asia
- Middle East and Africa

## Content Accessibility

Content is made accessible to the streaming platform in the following manner:

| Delivery Type | Accessibility |
|---|---|
| On-Demand Streaming | Content is made accessible via Customer's HTTP web server, or alternatively the Origin Storage Platform, where the media files are hosted. Upon initial end-user request of a media file ("asset"), the streaming cache server fetches the content via an HTTP request and draws the content onto the streaming platform. Subsequent requests for the content will serve the cached copy to the requestors. |
| Live Streaming | Customer provides access to live content via their encoder which captures, converts, and transmit the live signal to the CDN, or via server that receives the live signal from the encoder prior to connection with the CDN. |

## Media Players

There are pre-built media player applications available for Adobe® Flash®, Microsoft® Silverlight® and HTML5 content that provide common playback functionality in the user's browser. A Media Player Customization Tool is also available which provides a simple, automated approach to customizing and deploying the HTML code required to use the Media Players.

The players include the following features:

| Delivery Type | Adobe Flash | Microsoft Silverlight | HTML5 |
|---|---|---|---|
| On-Demand Content Delivery | • VP6-encoded content and H.264-encoded content<br>• Streaming<br>– Single bit rate<br>– Multiple bit rate (dynamic streaming)<br>– Progressive download (PDL) | • VC1-encoded content and H.264-encoded content<br>• Smooth Streaming<br>– Single bit rate<br>– Multiple bit rate | • HTTP adaptive bit rate (ABR) streaming: Apple HLS on iOS devices using the Safari web browser<br>• HTTP Progressive download (support for each format below varies by operating system and web browser)<br>– MP4 (using H.264 and AAC codecs)<br>– WEBM (using VP8 and Vorbis codecs)<br>– OGG (using Theora and Vorbis codecs) |
| Live Content Delivery | • VP6-encoded content and H.264-encoded content<br>• Streaming<br>– Single bit rate<br>– Multiple bit rate (dynamic streaming) | • VC1-encoded content and H.264-encoded content<br>• Smooth Streaming<br>– Single bit rate<br>– Multiple bit rate<br>– DVR | • HTTP adaptive bit rate (ABR) streaming: Apple HLS on iOS devices using the Safari web browser |

The players are compatible with:

| | Adobe Flash | Microsoft Silverlight | HTML5 |
|---|---|---|---|
| Operating Systems | Microsoft Windows XP SP3, Windows 7, Apple OS X, and Linux | Microsoft Windows XP SP3, Windows 7, Apple OS X, and Linux | MicrosoftWindows XP SP3, Windows 7, Apple OS X, Linux, iOS, Android, Windows Phone 7.5 |
| Browsers | Microsoft Internet Explorer version 8 and higher, Mozilla Firefox 4.0 and higher, Google Chrome, and Apple Safari 5 and higher | Microsoft Internet Explorer version 8 and higher, Mozilla Firefox 4.0 and higher, Google Chrome, and Apple Safari 5 and higher | Microsoft Internet Explorer version 9 and higher, Mozilla Firefox 7.0 and higher, Google Chrome 15 and higher, and Apple Safari 5 and higher, Opera 11.5 |
| Plugin Version | Adobe Flash 10.1 and higher | Microsoft Silverlight 3.0 and higher | Not Required |

Flash: Supported Containers and Codecs by Delivery Method

| Delivery Method | Supported Containers | Codec |
|---|---|---|
| Progressive Download | • FLV - Flash Video is a container file format used to deliver video over the Internet using Adobe Flash Player versions 6–10<br>• F4V - Based on the ISO base media file format and is supported starting with Flash Player 9 update 3<br>• MP4 - Multimedia container format standard specified as a part of MPEG-4<br>• F4M - Adobe Dynamic Streaming Configuration File<br>• SMIL – Dynamic Streaming Configuration File | • H.264<br>• VP6 |

Silverlight: Supported Containers by Delivery Method

| Delivery Method | Supported Containers |
|---|---|
| Progressive Download | Windows Media, MP4, MP3, ASX |
| Windows Media Streaming over HTTP | Windows Media, Server Side Play List (SSPL) |
| Smooth Streaming (Specific type of MediaStreamSource) | fMP4 |
| ASX | Windows Media, MP4, ASX |
| PlayReady DRM | MP4 |
| Server Side Playlist | Windows Media |
| MediaStreamSource | MediaStreamSource gives the developer complete control over the container. Any container can be used as long as the developer writes or uses a parser for it. |

SilverLight: Support Codec by Container

| Container | Codec |
|---|---|
| Windows Media | • "353" - Microsoft Windows Media Audio v7 v8 and v9.x Standard (WMA Standard)<br>• "354" - Microsoft Windows Media Audio v9.x and v10 Professional (WMA Professional)<br>• WMV1 (Windows Media Video 7)<br>• WMV2 (Windows Media Video 8) |

| | |
|---|---|
| | • WMV3 (Windows Media Video 9) |
| MP4 | H.264 (ITU-T H.264 / ISO MPEG-4 AVC), AAC-LC |
| MP3 | "85" - ISO MPEG-1 Layer III (MP3) |

HTML5: Supported Containers and Codecs by Delivery Method

| Delivery Method | Containers | Codec |
|---|---|---|
| Progressive Download | MP4 | H.264 (ITU-T H.264 / ISO MPEG-4 AVC), AAC-LC |
| | Ogg | • Theora<br>• Vorbis |
| | WebM | Vorbis |

### Content Freshness

Customer may apply cache control headers as a means to control when content should be expired off of the streaming platform. The streaming cache servers will honor cache control header values as long as they are delineated in seconds. If no cache control header is present a cache control of 1 hour is applied.

In cases where content needs to be removed from the streaming platform ahead of its expiration, Customer may perform active content invalidation via the CDN Portal. For information see the Content Freshness section in the Appendix of this document.

### Customizable Features

There is several security and analytics related options available for the Streaming Service. For a detailed description of these features see the Customizable Features for Caching and Streaming Services section later in this document.

### Administration and Reporting

Administration and Reporting capabilities for the Streaming Service are provided via a web-based CDN Portal. See the Administration and Reporting section later in this document for a detail description.

## Customizable Features for Caching and Streaming Services

### Security Related Features

The implementation of the following security related features are supported through CDN Rulebase settings as part of the service configuration. Certain features are offered as standard options while others are subscription-based.

| Feature | Description | Service and Option Type | |
|---|---|---|---|
| | | Caching | Streaming |
| IP Blocking | The CDN may be configured to block end-user requests from specified IP addresses or Classless Inter-Domain Routing Blocks (CIDR). Any requestors | Standard | |

| | | | |
|---|---|---|---|
| | whose IP address matches those specified will be banned from accessing resources. | | |
| Referrer Blocking | The Referrer Blocking feature enables the capability to control resource access so as to block referrals (cross links) that are not from authorized locations. The *Referrer:* header attached to the request is compared to a list of approved hostnames and the request blocked if a match is not found. It is possible to exempt specific resources from the *Referrer:* header check to allow access to resources that may be legitimately linked to from search engines or other external sources. | Standard | |
| Geo Intelligence | The Geo Intelligence feature enables the Customer to selectively target its end-user delivery based on location for the purpose of localizing content and/or distribution rights enforcement. The CDN has incorporated a geographic database that allows the Customer to anonymously identify an end-user's physical location on the Internet based on their IP address location and does not require the use of cookies or behavioral profiling.<br>This feature offers a variety of geographic and network attributes that can be used to tailor the end-user experience; ranging from basic country level policy management or complex delivery policies based on multiple geographic and network attributes simultaneously.<br>Data attributes include Continent, Country, State, City, MSA, DMA, Zip, Device Type, Network, and Bandwidth. | Subscription | Subscription |
| Token Authentication | The Token Authentication feature provides Customer with protection from URL tampering or re-use by providing the ability to:<br>• publish resources with URL embedded tokens that will affect the validity of the request<br>• encode/sign the URL in such a way as to allow the CDN to verify is authenticity and integrity<br>• perform certain validation determinations without contacting the customer's environment for authentication<br>Using Token Authentication prevents hyper distribution of resources by verifying the token of each end-user request. Because each token has a short time-to-live, it prevents end-users from accessing the file in perpetuity and forces end-users to request a new token | Subscription | Subscription |

| | | | |
|---|---|---|---|
| | from the customer once the current token has expired. This allows the customer to perform credential checks to ensure that the end-user is still entitled to receive the resource — all the while providing high performance quality of service to the end-user by using edge authentication. | | |

### Analytics Related Features

The analytics related features are made available to Customer via the CDN Portal. Certain features are offered as standard options while others are subscription-based. There are analytics features available for both Caching and Streaming Services.

#### Content Analytics

Content Analytics, available for Caching and On-Demand Streaming services, is a powerful feature that provides data on a wide variety of customer-defined traffic measures. The power in the Content Analytics feature arises through the Customer's ability to define how the data is collected plus the tool's numerous ways to analyze the data.

How the process works:

1. Customer defines a data collection via the CDN Portal. A collection is a subset of the URLs delivered by the CDN, and specified with simple string matches, custom fields or query string parameters. The collection definition is then distributed to data-collecting servers at the edge of the CDN.

2. As end-users request traffic, any URL that fits the pattern or query string defined is collected as part of the current month's data set and stored in a database by the collection.

3. The Content Analytics tools in the CDN Portal are used to browse and analyze the collected data.

Content Analytics can provide sampled or un-sampled data. A sampling rate is configurable by property. There are two feature levels available for Content Analytics: Basic and Premium. Basic is made available to Customer free of charge and includes up to 20 collections with high-level results in certain reports. Premium is a subscription-based option, includes up to 100 collections and provides more detailed information for all available reports. The following table lists the data available:

| Data displayed | Basic | Premium | Description |
|---|---|---|---|
| By Collection | ● | ● | Trends for the collection at the aggregate level, by Requests or Bytes, with comparisons available between collections within the property |
| By Status Code | ● | ● | Statistics for each status code within the collection at the aggregate level, in Requests and Megabytes |
| URLs per status code | | ● | Click any row in the list to see all URLs with traffic in that code, plus a mini-chart and links to a larger chart |

| Data displayed | Basic | Premium | Description |
|---|---|---|---|
| By URL Detail | | Up to 20 | URL detail, by requests or megabytes, in list and chart form |
| By Custom Field | Up to 4 | Up to 20 | Results based on the contents of the defined collection statistics at an aggregate level |
| By Referrer | | • | Summary: Requests from the first 500 referring domains in list form<br>Detail: Click a referrer line to see a chart of the number of requests |
| By Server Status | • | • | Summary: Specific categories, in list form<br>Detail: Click a category to see its charted activity |
| By Region | • | • | Summary: Lists requestor data by geographic region to the country level<br>Detail: Regional information for requestors and servers in table, chart and map form |
| By AS Number | | Up to 20 | View traffic through ASNs, determined by the IP address in requests, ranked by volume |

### Client Side Statistics

Client Side Statistics, available for both Live and On-Demand Streaming Services, provides CDN performance monitoring. The measures within the CDN Portal are presented in two types of metrics: Audience and Quality. The metrics are presented for both real-time and historical data.

There are three feature levels available for Client Side Statistics: Audience, Quality and Both. All are subscription-based options.

| Measure | Audience | Quality |
|---|---|---|
| Metrics: | All can be defined by scope and functionality including cities, countries, content and platform:<br>• Concurrent viewers – real-time statistic<br>• Peak Concurrent Views (PCV)<br>• Total Views information<br>• Unique Viewers<br>• Minutes per view and per viewer<br>• Total Viewer Minutes | • Average bit rate<br>• Buffering ratio – current, real-time<br>• Quality impacted views and viewers<br>• Minutes per quality-impacted view and viewer<br>• Play start failures<br>• Abandoned views<br>• Streaming and connection errors (stream errors)<br>• Time to first byte |

| Measure | Audience | Quality |
|---|---|---|
| Content Scopes (filters) | • Geography<br>• VoD<br>• Live<br>• Whole site<br>• Object/Asset title<br>• Stream | • Whole site<br>• Per CDN (Level3 and other CDNs)<br>• All/VoD/Live |
| Metrics History | • Available for one year<br>• Top 50 cities and countries<br>• Top 50 objects by concurrent views | • Available for one year<br>• Top 50 cities and countries |

Data is collected for content played through Adobe® Flash, Microsoft® Silverlight and HTML5 broadband content, as well as on the Apple® iPhone® or iPad®. As part of configuration, Customer adds a plugin to their content players.

### Log Retrieval

Customer may retrieve standard log data for analysis and archival with the Advanced Log Retrieval Tool ("ALR"). The ARL is available for installation on Windows, Unix and Solaris. Logs are aggregated at scheduled intervals and prepared for download.

In addition to standard HTTP status codes, Extended Status Codes are added to log entries, providing additional information about each request and increased visibility into the behavior and efficiency of CDN features and functions.

Raw log data is in a proprietary format and may be converted to Common Log Format, Extended Common Log Format, Microsoft IIS Log Format, W3C Extended Log Format or a custom format as required by reporting requirements or the analysis tool to be utilized.

The ALR Tool is available free of charge to all Customers.

## Origin Storage Service Description

The Origin Storage Service is a highly redundant and scalable Origin Storage Platform ("OSP") designed specifically to store content for the CDN; including images, audio and video files, software and other content to be delivered to end-users via the Internet taking advantage of CenturyLink' Caching Service and/or Streaming Service.

There are four Origin Storage nodes; located in Los Angeles, New York, Frankfurt and London. The nodes in Los Angeles and New York store content for the North American region, and the nodes in London and Frankfurt store content for the European region. Content to be served out of Asia and South America can also be stored in the North America region.

Customer, based on their requirements, is assigned a primary upload site. The site serves as the upload location and the primary serving origin to the CDN for the Customer's content. Once content is uploaded into the primary site it is automatically replicated to the secondary site within that region. Content is not

automatically replicated between regions; Customer must upload its content into one location in each region if it requires its content be stored in both regions.

If an end-user request is made for content that is not already cached on the CDN, then the request for that content is redirected to the primary serving origin. Should the content not be available at the primary origin, the request is redirected to the secondary origin within the region before redirecting requests back to the customer's origin.

New content added to the OSP is available to the CDN after upload and replicated within minutes. Changes to or deletions of content require a certain amount of time for the changes to be completely propagated throughout the entire CDN. Deletions will also be dependent on the specific "time to live" (TTL) parameters set for the content which may require a separate content invalidation action.

### Content Upload

Access to the OSP is made available for content upload via DNS information (i.e., customer.ingest.cdn.level3.net) and using credentials that are supplied to the Customer at time of service activation. Customer may choose to upload content into one of two directories on the OSP with their account:

1. **Published Directory:** (/published) where content is quickly available to serve through the CDN.

2. **Staging Directory:** (/home/<customer>) where content will be staged" until Customer determines that it should be available to serve through the CDN, at which time it must be moved to the Published Directory.

Customer can determine and maintain their file structure on the OSP; a balanced directory hierarchy using a two- or three-tiered structure is recommended.

### Upload Methods

Content may be uploaded to the OSP using the following methods:

| Upload Method | Description |
|---|---|
| FTP | A non-encrypted, standard file transport protocol. Active and Passive FTP modes are supported. |
| FTPS | An extension to FTP that adds support for the Transport Layer Security (TLS) and the Secure Sockets Layer (SSL) cryptographic protocols. |
| SSH | Supported through Secure Copy (SCP), Secure FTP (SFTP) and rsync (content management and movement application for Unix system). |

### Content Security

Reasonable steps have been taken to prevent unauthorized access to content on the OSP. Access to any Origin Storage account requires specific credentials to view, load, or access content on the account. Additionally, the OSP is protected from DDoS or other types of digital attacks that could somehow negatively impact service.

### Reporting

Origin Storage reporting capabilities are provided via a web-based CDN Portal. See the Administration and Reporting section later in this document for a detail description.

## Administration and Reporting

The CDN Service includes a web-based portal ("CDN Portal"), for administration capabilities and reporting of usage statistics for subscribed CDN Services; Caching, Streaming and Origin Storage.

The Portal can be access at: https://mediaportal.level3.com

### Key Service Identifiers

The following are key service identifiers for CDN Services within the CDN Portal:

| Identifier | Description |
|---|---|
| Access Group and Child Access Group | Access Groups are the underlying structure for grouping services and controlling how users access those services in the CDN Portal. Customer may have one or more top-level access groups, depending on their configuration, and Administrators are able to create one or more Child Access Groups under the top-level group with no limit to the number of levels. Users are associated to one or more access groups with an appropriate permission level; a single user can be associated with multiple access groups, and have different permissions for each. |
| SCID | Service Component ID (i.e., ABCD1234); a unique identifier assigned to a service configuration. Customers may have one or more SCIDs per service type depending on their specific configuration. SCIDs are assigned to Access Groups, or Child Access Groups, for access management. |
| Property | The basic element of a customer configuration for Caching Service. Content is stored in cache on a per-property basis. Properties take the form of an URL like "cdn.something.com" (HTTP) or "secure.footprint.net/something" (HTTPS). |
| Streaming ID | The basic element of a customer configuration for Streaming Service; unique for On-Demand and Live streaming media assets. Streaming IDs take the form of an alphanumeric identifier like "something-live". |
| Ingest/Hostname | The basic element of a customer configuration for Origin Storage Service; unique for each origin storage account, like "abc.origin.cdn.company.net". |

### CDN Portal Overview

Below is an overview of the functionality provided by the CDN Portal. The table below describes the functions made available under each Tab within the Portal. The functions available to each individual user will depend on their access permission.

| Function | Description |
|---|---|
| Portal Admin: | |
| Access Groups | Visibility to all existing Access Groups for the Customer with the ability to create new |

| | |
|---|---|
| | Child Access Groups, assign SCIDs and users to the groups, and invite new users for access. |
| Role Management | View permissions for standard roles and the ability to create a custom role and assign permissions. |
| API Keys | The CDN Portal API provides the ability to request data directly about the CDN Services for use in Customer's own processing. This option provides a key used in building authorization for the API requests. For more detailed information see the CDN Portal API section later in this document. |
| My Services: | |
| Service Configuration | Provides a list of the services specific to the Customer's configuration or subscription, provisioned for the Access Group. Services are listed by SCID and show the Properties/Streaming IDs/Hostnames for each. Selecting one of the SCIDs allows Customer to add new Properties, Streaming IDs or Origin Storage accounts as needed. Selecting a specific Property/Streaming ID/Hostname provides configuration details. |
| Orders: | |
| CDN Order Status | Shows the status and order details of any orders submitted for new Properties, Streaming IDs or Origin Storage accounts. |
| Reports: | |
| CDN Usage Reports | Provides both summary and detailed usage report for customer's CDN Services. |
| Content Analytics | Provides the ability to define data collection parameters and to analyze that data. For more detailed information see the Customizable Features for Caching and Streaming Services section earlier in this document. |
| Event Reports | Provides the ability to schedule a report that captures streaming data during a live streaming event to be used for later analysis. The time interval can be set to begin at a particular hour or minute while other CDN Portal reports are set at only full day boundaries. |
| Scheduled Reports | Displays any usage report that has been scheduled for automatic generation and delivery. Once a report is scheduled any modifications to the report, or deletion, can be accomplished through the Scheduled Report option. |
| Client Side Statistics | Provides CDN performance monitoring for Audience and/or Quality metrics. Metrics are presented for both real-time and historical data. For more detailed information see the Customizable Features for Caching and Streaming Services section earlier in this document. |
| Network Tools | |
| Caching Real Time Monitor | Displays a selection of data measures reported in near real-time from the caching network. Snapshots of data are gathered every five minutes and displayed in a regions table and time series chart. The display is updated every 20 seconds if new data is available. Data continues to be collected as long as the chart or map is open. |

| | |
|---|---|
| | The real-time data is not stored. |
| Streaming Real Time Monitor | Displays real-time reporting from the streaming network. Snapshots of data are gathered every 15 to 30 seconds and displayed in the stream table and time series chart. The real-time data is not stored but the contents of the table or chart after the data has been collected can be emailed or saved. |
| Content Invalidation | Provides the ability to perform active content invalidation for Caching and Streaming resources. Content invalidation takes the form of a request. Once an invalidation request is submitted the status of the request can be monitored. |
| Flash Diagnostics | A tool to help diagnose end-user Flash Streaming problems using client-side data. The data presented on the diagnostic tool is displayed directly as the stream is being delivered from the CDN to the Flash player on the client, without any calculation or manipulation. |
| Silverlight Diagnostics | A tool to help diagnose end-user Silverlight Streaming problems using client-side data. The data presented on the diagnostic tool is displayed directly as the stream is being delivered from the CDN to the Silverlight player on the client, without any calculation or manipulation. |
| Media Player Configuration | A tool that facilitates the creation of HTML code used to play content from customer's web sites. The tool provides a simple, automated approach to customizing and deploying the HTML code required to use the Media Players for Adobe® Flash®, Microsoft® Silverlight® and HTML5 content. |

### Access Permissions

At the time of CDN Service activation CenturyLink will provide one or more users with Administrator access to the CDN Portal. User(s) with Administrator access may set up additional users and assign permissions.
The table below summarizes the available access permissions in the CDN Portal and the associated capabilities under each Tab within the Portal:

| Function | Admin + Ordering | Admin | Configuration | Reporting | View Service |
|---|---|---|---|---|---|
| Administration: | | | | | |
| Edit Access Group | ● | ● | | | |
| Add New Child Access Group | ● | ● | | | |
| Delete Child Access Group | ● | ● | | | |
| Associate SCIDs to Access Group | ● | | | | |
| Invite New Users | ● | ● | | | |
| Update User Permissions | ● | ● | | | |
| Manage API Keys | ● | ● | | | |
| View Order History | ● | | ● | | ● |
| Access Help Information | ● | ● | ● | ● | ● |
| Customize the Welcome Page | ● | ● | ● | ● | ● |

| | | | | | |
|---|---|---|---|---|---|
| Update account profile | ● | ● | ● | ● | ● |
| Reporting: | | | | | |
| View Dashboard | ● | ● | ● | ● | ● |
| View Service Specific Utilization Reports | ● | ● | ● | ● | ● |
| Generate Service Specific Utilization Reports | ● | ● | ● | ● | ● |
| Schedule Utilization Reports | ● | ● | ● | ● | ● |
| View Content Analytics Reports | ● | ● | ● | ● | ● |
| Configure Collections for Content Analytics Reporting | ● | ● | ● | ● | ● |
| View Client Side Analytics | ● | ● | ● | ● | ● |
| Configure Client Side Analytics | ● | ● | ● | ● | ● |
| View Streaming Event Reports | ● | ● | ● | ● | ● |
| Configure Streaming Event Reports | ● | ● | ● | ● | ● |
| Service Configuration: | | | | | |
| View Configuration Details | ● | | ● | | ● |
| Request New Property/Streaming ID | ● | | ● | | ● |
| Network Tools: | | | | | |
| Caching Real Time Monitoring | ● | ● | ● | ● | ● |
| Streaming Real Time Monitoring | ● | ● | ● | ● | ● |
| Request Content Invalidation | ● | ● | ● | | |
| View Status of Content Invalidation Requests | ● | ● | ● | | |
| Setup Flash Diagnostics | ● | ● | ● | ● | ● |
| View Flash Diagnostics | ● | ● | ● | ● | ● |
| Setup Silverlight Diagnostics | ● | ● | ● | ● | ● |
| View Silverlight Diagnostics | ● | ● | ● | ● | ● |
| Media Player Configuration | ● | ● | ● | ● | ● |

### Usage Reports

The CDN Portal provides a dashboard view of the current month's utilization displayed in a time series chart of aggregated total usage and a table of usage measures for each of the Customer's CDN Services. From the dashboard the Customer can select more detailed CDN Service usage reports to include a number of display formats and filter options.

Reports can be printed, exported in .csv format, or scheduled at regular intervals for delivery by email in spreadsheet format.

### CDN Portal API

The CDN Portal RESTful Application Programming Interface (API) provides the means for developers to build software that interacts directly with CDN Portal data without requiring use of the browser-based graphical user interface.

The available API interfaces include CDN Services and Access Group Hierarchy, Invalidations, Usage Reporting, Real-Time Monitoring, and Content and Client Side Analytics.

The basic steps required to use the APIs are:

1. Acquire an API Key. An API Key consists of a numeric Key ID and a Secret. Keys are created through the CDN Portal API Security Key Management screen.
2. Determine the Access Group ID. Since the Access Group name is editable, the CDN Portal assigns an Access Group ID that does not change. The Access Group ID is required as part of the scope for each API request and the Key API is used to locate this ID.

Though use of the API is free of charge to Customers, API keys are granted a monthly credit limit and each API interface has an associated cost per call. Each call made reduces the monthly call balance by the cost of the call. The API credits have no monetary value; their only use is to ensure that a reasonable use policy is maintained. The monthly allotment is 5,000,000 credits for each key. The credit balance is reset at midnight UTC on the first of each month; any remaining credits expire and are not carried over. API Keys can be disabled on an individual basis by any CDN Portal user with Administrator permission for the associated Access Group. Disabled keys may be re-enabled for later use. API keys cannot be deleted but may be re-used by generating a new Secret.

## Installation

A standard CDN Service installation has the following primary steps:

**Step 1:** Once a signed Master Service Agreement, including Service Order, is received and executed by CenturyLink, a Service Delivery Coordinator is assigned to the installation. The Customer's technical contact serves as the point of contact.
**Step 2:** The Service Delivery Coordinator validates that required configuration information has been collected with the Service Order; Technical Questionnaire (TQ), which records the configuration details, and SSL Certificate information if applicable. Once confirmed, the Service Delivery Coordinator facilitates the service configuration.
**Step 3:** Once service configuration is complete, the Service Delivery Coordinator will provide a Service Activation Notification to include service details specific to the customer's configuration.
**Step 4:** The Service Delivery Coordinator will facilitate the setup of Customer's administrator account(s) to the CDN Portal.
**Step 5:** The Service Delivery Coordinator will facilitate a hand-off discussion over the phone with Customer and CenturyLink Solutions Engineer to review configuration and CDN Portal functionality.
**Step 6:** The Customer is free to test the service configuration and implement any necessary DNS changes to begin utilizing the service.

## Maintenance and Support

### Maintenance

Scheduled Maintenance includes any foreseen, predictable need to make a change to the current state of the CDN Network, including upgrades and augments.

If scheduled maintenance is reasonably expected to produce a service interruption, advanced notification will be provided by email. The email notification will specify the date and time (GMT) of activity,

description and duration of activity, scope of event, possible effect on network, and a completion date, if needed.

Maintenance activities deemed necessary to prevent or restore network failure may occur at any time. For high-risk and service-threatening outages, Customer will be notified by email as early as possible. The notification lead time and maintenance window for these types of events vary based on the degree of customer impact.

If determined that an emergency security change is required, CenturyLink, or its underlying vendor, will make the changes deemed necessary as soon as reasonably possible and will notify the Customer of the changes as soon as practicable.

### Support

CenturyLink provides 24x7 phone and email support in English.

CenturyLink serves as the single point of contact. CenturyLink Service Center's frontline associates will respond to Incidents and Requests with case creation and escalate promptly to the appropriate internal resource(s) or Level 3 Communications.

### Charges

The manner of billing and applicable charges shall be set forth in the applicable CenturyLink Service Order and shall remain in effect during the Service Term.

Charges for CDN Services and certain customizable features consist of three components: (1) a non-recurring installation charge; (2) a monthly recurring charge based on service level; and (3) monthly usage charges to the extent usage exceeds allowances in the service level where applicable.

### Additional Requirements

If any third party software, including any corresponding documentation, is provided to Customer by CenturyLink in connection with any of CDN Services, or features, Customer agrees to use such third party software strictly in accordance with all applicable licensing terms and conditions. CenturyLink makes no representations or warranties whatsoever with regard to such third party software.

Customer must comply with all of its responsibilities under this CenturyLink Service Guide or CenturyLink' obligation to provide this service in accordance with this CenturyLink Service Guide will be suspended until customer does so.

## Roles and Responsibilities

The following table defines a high level overview of CenturyLink' roles and responsibilities in providing CDN Services as well as those responsibilities of the customer.

| Roles and Responsibilities | CenturyLink | Customer |
|---|---|---|
| **Service Implementation** | | |
| Technical Review: Configuration Specifications and Requirements | ● | ● |
| Service Configuration and Activation | ● | |
| Initial CDN Portal Administrator Account Creation | ● | |

| Roles and Responsibilities | CenturyLink | Customer |
|---|---|---|
| Caching: | | |
| DNS change(s) to point to CDN | | ● |
| Streaming: | | |
| Encode streaming media in a supported format | | ● |
| Integrate streaming links in to the context of web site | | ● |
| Push content to Flash Media Server, if applicable | | ● |
| Origin Storage: | | |
| Storage Account Access Creation | ● | |
| Content Upload | | ● |
| Content Replication | ● | |
| **Service Management** | | |
| CDN Portal: Access Group Management | | ● |
| CDN Portal: User Management | | ● |
| Maintain master and/or backup copies of content | | ● |
| Usage Reporting | | ● |
| Active content invalidation | | ● |
| **Maintenance & Support** | | |
| Network Management, Monitoring and Repair | ● | |
| Troubleshooting Service Issues | ● | ● |
| Architecture and Software Upgrades | ● | |
| **Service Cancellation and Termination** | | |
| Notice of Service Cancellation as set forth in MSA | | ● |
| Service Deactivation | ● | |

## Glossary and Acronyms

| Term/Acronym | Definition |
|---|---|
| **ALR** | Advanced Log Retrieval Tool used to retrieve standard log data |
| **Asset** | Synonymous to a media file |
| **ASX File** | Advanced Stream Redirector File: ASX files allow customers to embed streaming links as an abstraction method rather than directly exposing the streaming links to the media player for On-Demand streaming of Windows Media content |
| **BRefresh** | Background Refresh: an optional CDN Rule base policy that will serve expired content for a limited amount of time while an asynchronous cache-fill is in progress |
| **CDN** | Content Delivery Network |
| **CDN Network** | An international network of servers located in strategic locations at the edge of the internet to direct content requests to an optimal location on the network |
| **CDN Portal** | A web-based portal for administration capabilities and reporting of usage statistics for Caching, Streaming and Origin Storage Services |
| **CDN Rulebase** | CDN internal settings as part of configuration that assign caching or processing characteristics to requests or resources |
| **CIDR** | Classless Inter-Domain Routing Blocks |
| **CSR** | Certificate Signing Request |
| **GMT** | Greenwich Mean Time |
| **MSA** | Master Service Agreement |
| **MRC** | Monthly Recurring Charges |
| **NRC** | Non-Recurring Charges |
| **OSP** | Origin Storage Platform |
| **Resources** | Synonymous to content to be cached |
| **SCID** | Service Component ID: a unique identifier assigned to a service configuration |
| **SERVICE GUIDE** | CenturyLink Service Guide |
| **Streaming Media** | Video and audio content encoded by customer in a supported streaming |

| | |
|---|---|
| | format |
| **SWF File** | An Adobe Flash file format |
| **TTL** | Time-To-Live: the time, in seconds, that a cached resource will remain current or fresh |

# Appendix

# Content Freshness

## Introduction

Content freshness and validation (“Cache Control”) are important ways that a cache works with content. Together they are the means for determining what resources are served instantly from cache and what resources may require validation and possible refresh from the origin in order to serve the most current version.

Additionally, a content freshness strategy designed around CDN utilization can provide better off-load of traffic from the hosting environment.

There are several mechanisms for controlling content freshness, both standard and proprietary, to help content publishers maintain control over the freshness of their content served through the CDN.

## Content Freshness Mechanisms

### Origin Server Policies

Specific configuration of individual HTTP servers vary.  The most modern, compliant servers offer the ability to set cache-controlling headers (Expires, Last Modified, and Cache-Control: max-age, no-cache, no-store, must-revalidate, etc.) with varying degrees of flexibility and granularity as part of the HTTP 1.1 application protocol.

The CDN does use HTTP 1.1 (RFC 2616) (“HTTP 1.1 Specification”); therefore the CDN caches will honor cache-controlling headers to expire content according to the policies established at the origin server.

Setting policies at the origin server is the suggested method for controlling the freshness of content as it provides the most flexibility and is under the direct control of the content owner.

How cache-controlling headers are implemented depends on the content within your site and its variability. The following are general Cache-Control response directives:

| Directive | Description |
|---|---|
| Cache Control: max-age | Specified in seconds, it implicitly tells the browser it may cache a resource, but must re-validate with the server if the max-age has been exceeded. A max-age of zero ensures that a resource is never served from cache, but is always re-validated against the origin server.<br>It is suggested that you use the Cache-Control max-age directive instead of the Expires header to control content freshness. |
| Cache Control: s-max-age | Similar to the max-age directive, the "s-" stands for "shared cache" which means it applies specifically to how long the CDN may cache a resource.<br>If you want resources to stay in CDN cache for a different duration than in browser cache, you can use the Cache-Control max-age and Cache-Control s-max-age directives together. |
| Cache Control: no-cache | Instructs the browser and CDN to re-validate the resource with the origin server each time it is requested; effectively the resource is not cached. |
| Cache Control: private | Permits browsers to cache the resource but not the CDN. |

Note that meta tags in HTML resources are not supported for cache control.

For more detailed information on the HTTP 1.1 Specification and other supporting documentation, see the following references:

- HTTP 1.1 Specification: http://www.ietf.org/rfc/rfc2616.txt
- Caching Tutorial for Web Authors: http://www.mnot.net/cache_docs/
- Optimize Caching from Google: https://developers.google.com/speed/docs/best-practices/caching
- http://palpapers.plynt.com/issues/2008Jul/cache-control-attributes/

### CDN Rulebase Policies

Cache control can be established at the CDN through rulebase policies; configuration settings. The Cache Control Header Override is a mechanism generally used when it is technically not possible to establish content freshness policies at the origin.

Cache Control Header Override allows for the definition of expiration criteria for resources cached in the CDN (internal) and in the local cache of the requesting browser (external). Criteria may be specified for resources or groups/classes of resources using pattern-matching designations. Specified values may be a unit of time (seconds, minutes…, years), or may indicate that the resource is not to be cached.

As the name implies, Cache Control Header Override policies override any internal policies set at the origin server if they exist, and provides flexibility when it comes to external policies to either honor or override.

In the event that no cache control header is provided by the origin server for a resource, and no Cache Control Header Override is present, the default expiration is 7 days.

An additional rulebase policy allows the CDN to serve “stale” content for a period of time in the event that the origin server is not reachable. A resource becomes stale either when its cache control policy indicates that it has expired, or as the result of an active invalidation request.

Any changes to rulebase policies are administered through a change request submitted to the Support Desk and may take up to 48 hours to implement.

### Active Invalidation

Active Invalidation capabilities are available through the CDN Portal providing on-demand content expiration for resources. This mechanism provides an override when other methods are used but content requires real-time replacement outside of defined expiration policies.

Active Invalidation is not a primary method of content freshness control and should not be used as such. Active Invalidation should only be used in conjunction with other content freshness mechanisms.

Invalidation types include:

| Type | Description |
|---|---|
| Normal | Issues a GIMS (GET with an If-Modified-Since: header) request the next time the resource is requested (assumes that the resource being invalidated has a Last-Modified: header). |
| Force | Makes an unconditional revalidation on the next request, which causes the resource to be reloaded. |

An Active Invalidation takes the form of a request which specifies the content that should be invalidated across the CDN; specified as a combination of property and path. A path can be specified as either a complete path or it can make use of one or more wildcard specifications. For instance, an invalidation request can specify all the content in a certain subdirectory or all resources with a common extension.

| Characters | Match |
|---|---|
| * | Zero or more characters |
| + | One or more, non-directory separator characters |
| ? | Any singe character, include the directory separator |
| . | The “.” Character only |
| \ | Directory separator |
| / | Directory separator |
| {n,m} | Integer value between “n” and “m” inclusive |
| [a,x-y, …] | Any character (a) or range of characters (x-y) inclusive |
| [^a,x-y, …] | Any character not matching “a” or within a specified range |

The result of an Active Invalidation is that the resource(s) in cache becomes invalid and the next request for the resource will cause the cache to revalidate the content with the origin server.

Invalidation of up to 5 Properties/Streaming IDs and path combinations is allowed at one time. Defined Properties/Streaming IDs are selectable from a drop-down list.

The CDN Portal also provides a RESTful Application Programming Interface (API) to facilitate repetitive active invalidation requirements.

### Diagnostic Tools

There are a number of diagnostics tools available that are useful for examining the cache control policy for resources for validation purposes. Here are just a few:

- http://redbot.org: an online tool that interacts with HTTP resources at a provided URL to display how the resource supports a number of HTTP features, to include Cache Control.
- http://www.websitepulse.com/help/testtools.httpheaders-test.html: another online tool that retrieves the HTTP response headers for a given URL.
- cURL: a command line tool for performing a number of URL manipulations including retrieving basic response headers to ensure a given header has been correctly set.
- Modify Headers:  a Firefox add-on that is useful for validating HTTP response headers.

For more information on these tools, access the web or refer to the link provided.

### General Practices for Building a Cache-Aware Site

No matter what content freshness strategy you deploy, there are a number of general practices that assist to make a site more cache-aware and lend support to that strategy:

| Practice | Description |
|---|---|
| Refer to objects consistently: | A golden rule of caching: If you serve the same content on different pages, to different users, or from different sites, it should use the same URL. This is the easiest and most effective way to make your site cache-friendly. For example, if you use /index.html in your HTML as a reference once, always use it that way. |
| Common Library: | Use a common library of images and other elements and refer back to them from different places. |
| Resource Classification: | As a general rule, resources, especially those that are time sensitive or likely to be updated on short-notice, should be grouped or classified to facilitate ease of policy definitions and invalidation. Those that are published on a regular schedule or require refreshed content based on external factors may be classified accordingly, and policies developed to minimize manual intervention. |
| File Renaming: | If a resource changes, especially in the case of a downloadable file, change its name. This allows you to expire the resource far in the future and still guarantee that the correct version is served; only the page that links to it needs a short expiry time. |

| | |
|---|---|
| Avoid Cookies: | Use cookies only where necessary as cookies are difficult to cache. If you must use a cookie, limit its use to dynamic pages. |
| Avoid changing files unnecessarily: | When updating a site, don't copy over the entire site; just move the files that have changed. Otherwise everything will have a falsely young Last-Modified date. |
| Resource Expiration: | Specify a far-away expiration on images and pages that don’t change often, and specify an appropriate expiration on pages that are regularly updated. |