ERICSSON UNIFIED DELIVERY NETWORK

Content Provider Portal User's Guide

Product Version 1.0.2
Document Number D1002

Legal Information

Disclaimer

No part of this document may be reproduced in any form without the written permission of the copyright owner.

The contents of this document are subject to revision without notice due to continued progress in methodology, design and manufacturing. Ericsson shall have no liability for any error or damage of any kind resulting from the use of this document.

Ericsson is the trademark or registered trademark of Telefonaktiebolaget LM Ericsson. All other product or service names mentioned in this manual are trademarks of their respective companies.All other trademarks and registered trademarks are the property of their respective holders.

Contents

Figures

Tables

Chapter 1
UDN Overview

Ericsson's Unified Delivery Network (UDN) is a content distribution solution designed to benefit both content providers and service providers. UDN's network overlay uses intelligent caching, server load balancing, dynamic request routing to optimize the user experience. UDN enables content providers to connect with last-mile service providers and place content caches in the access network. Rather than focusing on content delivery optimization through points of presence outside the last mile, UDN keeps content close to the edge of the network for rapid, high-quality content delivery.

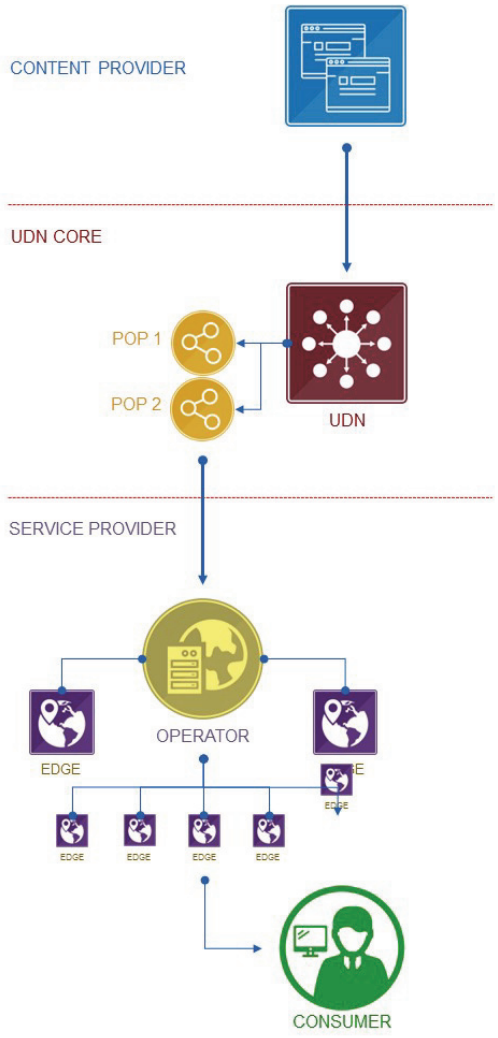
Ericsson continuously monitors UDN performance across the entire infrastructure, providing load balancing for optimized performance. UDN offers targeted, content-centric analytics focusing on content distribution and delivery data to support tuning of service offerings, which provide transparency into UDN operations and delivery. Service providers can harness real-time analytics to optimize caching, network usage, and end-user experience.

This chapter contains the following sections:

High-Level View of UDN

UDN consists of two delivery networks: the UDN Core network, located at the Internet's backbone with PoPs at strategic exchange points, and UDN partners' "last mile" network at the Service Provider edge.

Figure 1-1: High-Level UDN Overview



UDN System Components

The following sections describe the components that comprise the UDN System.

The UDN Portal

The UDN Portal provides a customized experience to each of the three primary users: Content Providers, Service Providers, and Service Administrators.

UDN Administrators can view and manage Customer Accounts, Groups, and Properties, view reports on content sources and content distribution, and manage content caching.

Content Providers can view and manage Groups and the Properties that belong to them, view reports on content sources and content delivery, and manage content caching.

Service Providers can view and manage Service Provider settings, and view reports on content delivery for both on-net and off-net traffic.

Edge Delivery Nodes

Edge delivery nodes are responsible for UDN streaming content delivery. Edge delivery nodes are optimized for streaming rather than storage. They are located as close to the consumer as possible to provide geo-optimized delivery of popular content. Whenever an asset or live stream reaches a certain popularity threshold, it is automatically replicated to the appropriate number of edge delivery nodes in the desired geographical location.

Analytics

UDN System analytics provides operators with the ability to understand both the composition and the volume of their content delivery. Data is collected, aggregated, and analyzed on an ongoing basis from numerous sources within the CDN environment. Reports provide historical and current information which can help enable operators to tailor content caching and delivery as well as empowering them to make informed business decisions.

Analytics also feed billing systems across multiple revenue types. Designated billing information can be generated and delivered to Content Providers and Service Providers.

Monitoring and Availability

The UDN System uses persistent connections, intelligent content management, and both multi-site and multi-server database redundancy to provide additional layers of protection for system operation. UDN continuously and systematically monitors system and server health and availability.

Additional protection features on-the-fly failover, and can include load balancing and clustering where additional capabilities in redundancy and fault tolerance are required. The UDN system is designed to accommodate flash events where a surge due to an event causes a dramatic increase in system loads, which might ordinarily strain a CDN system. Built-in congestion and overflow handling capabilities prevent bottlenecks and ensure continuous content delivery.

UDN Core Cache

The Core Cache is a dynamically optimized, geographically distributed, extensible caching platform. It is the primary component of the UDN Service. Strategic location at highly-connected Internet Points-of-Presence (PoPs) reduces bandwidth costs, ensures global availability, and speeds content delivery to end users.

Universal Cache Technology

Universal Cache technology enables a highly scalable Content Delivery Network (CDN) that efficiently delivers both its own managed content as well as OTT services from a common caching infrastructure. The front end of this system stores the metadata of published assets and interfaces with a storage system that hosts these assets. In addition, media

upload, download, and processing, is performed by a system that communicates job processing and status information with external asset management systems.

This technology is comprised of two main components: the conductor and the provisioner.

The conductor accepts HTTP traffic, parses it, decides how to fulfill the request, and returns a result. The conductor process is responsible for discovering content regardless of its current location. In response to an HTTP request from the client, the conductor may either deliver the requested content directly from its local storage or forward the request to another node in the network acting as a caching proxy server.

The provisioner is the service that tracks content location within the Universal Cache, and manages purging and invalidation of cached content.

Content Acquisition Optimization

At frequent intervals, a PoP cluster in the UDN Core will send out HTTP requests to all ingest paths. The speed of each response is used to create a rotating optimize path selection group for content acquisition. Path information is stored along with other route selection criteria to ensure that content acquired from the origin is retrieved as quickly as possible.

Global and Local Load Balancing

UDN's global and local load balancing system determines the fastest and closest location from which to serve content to consumers. Continuous testing of performance and latency ensures optimized content delivery. Policy-driven routing decisions are based on geography, network and server load, and business rules. Load balancing is performed globally, at the UDN Core, and locally, at Service Provider sites. The goal is to match Content Providers' needs to the CDN's needs while ensuring high availability, high performance, and low cost.

Secure Customer-Controlled Caching

Cache management via the UDN Portal enables content management personnel to specify policies for content caching and purge/invalidate content once it is no longer available to users. Secure system multi-tenancy ensures that content generated by different Content Providers can only be accessed by its owner.

UDN Benefits

On top of the delivery and management system technology, UDN serves a central contracting role for global content delivery with Content Provider and Service Provider partners worldwide. Collaboration between Ericsson, Content Providers, and Service Providers increases quality of service while decreasing delivery cost.

UDN's secure multi-tenant architecture provides a hierarchy to support different roles and permissions, enabling data security at all levels for secure visibility by Content Providers and Service Providers, and their subsidiaries, resellers, and partners.

For Content Providers, UDN provides the best quality of service for the lowest cost. Detailed data on end-user access and consumption patterns provide detailed, customized performance reports. With UDN, Ericsson removes the need to manage separate contracts with dozens of Service Providers, providing a centralized contracting organization with a global reach.

For Service Providers, UDN enables strategic placement of core and edge servers to increase capacity and lower delivery costs. In addition, Service Providers can use the UDN Portal to control how content is delivered through their network, and optimize their content delivery profits. Performance data from the content delivery platform is gathered and stored for on-demand analytics that provide dynamic, detailed information on end user access and consumption patterns.

UDN and Content Providers

The UDN is a partnership that links content providers with the optimal Service Provider (SP) Edge delivery platform to transport media from Content Providers to end-users. UDN is designed to deliver content from a location as close to the end user as possible. Ideally, content is delivered from a local cache at the SP site. If content is cached in the UDN Core, when requested, it can be retrieved and delivered from there. In other cases, content is retrieved from the Content Provider origin, and is then delivered through the Service Provider edge delivery platform to the end user.

As a UDN partner at the Service Provider edge, you operate a content delivery platform called the SP Edge within your network. This platform consists of one or more servers, networking equipment and software.

In order to expedite media delivery, the Ericsson UDN selectively stores a subset of the most popular content provider media on SP Edge servers. When your end-users make requests to websites that Ericsson has a contract to deliver, the UDN will steer your end-users to the servers that are the most appropriate to serve them. In most cases, the request will be sent to the Service Provider Edge content delivery platform within your network. In return, as a UDN partner, you will receive a share of the revenue based on your Ericsson delivery contract (known as a rev share).

By positioning the SP Edge close to end-users within your network, the SP Edge servers are located where there is the most bandwidth available to end-users at the lowest latency. This combination of low latency and high bandwidth provides end users rapid content delivery at a high quality of service.

Chapter 2
Getting Started with the Content Provider Portal

The UDN Content Provider Portal is a Graphical User Interface (GUI) web application that serves as the management application for UDN management, configuration, and monitoring.

This chapter introduces you to the Portal, its main features, and how to use it.

This chapter contains the following sections:

Accessing and Exploring the Portal

The Portal is a web-based interface that enables you to view and manage settings associated with UDN Services.

When you log into the Portal for the first time, you will be presented with a visual representation of UDN traffic in the form of a Starburst. The Starburst feature is used to represent information associated with an entity, whether that entity is an Account (the highest level managed entity), a Group, or a Property (the lowest level managed entity).

To access the Portal:

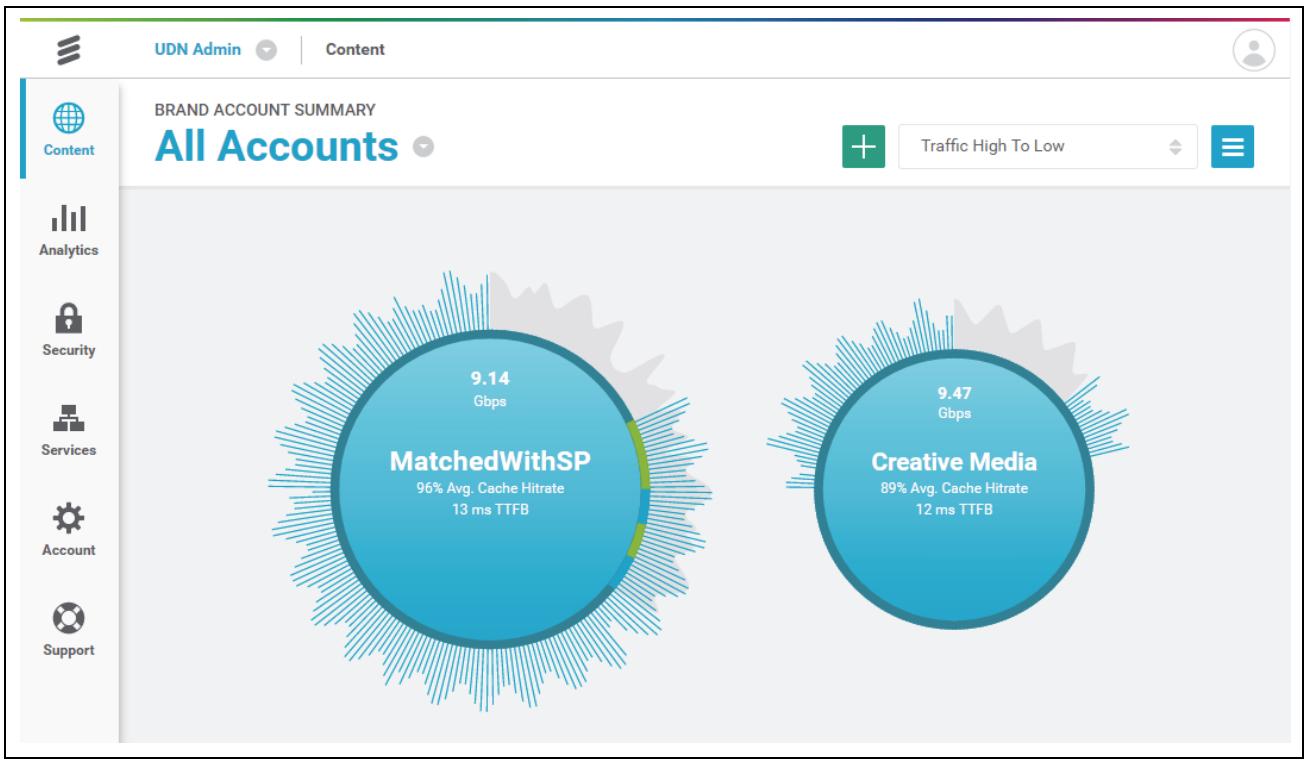
1. Open the browser of your choice. The following browsers are supported for Portal access at this time:
   - Chrome Version 48 or later
   - Internet Explore Version 11 or later
   - Safari Version 9 or later
   - Firefox Version 45 or later
2. To access the Portal, navigate to:

   `https://portal.ericssonudn.com`
3. To log in to the Portal, enter your username and password.

   NOTE

   Username entry is not case sensitive.
4. The main window of the UDN Administrator Portal displays (Figure 2-1).

Figure 2-1: Administrator Portal Main Window



NOTE

For security reasons, if you leave the Portal interface idle for too long, you will automatically be logged out.

5. At the top left corner is an icon (the Ericsson logo, as shown in Table 2-1) that will bring you to highest level view.

   To the right of that is a drop-down selector which enables you to choose different entities to view.

   To the right of the selector, you will find a breadcrumb trail of clickable links.

   Note that this breadcrumb path displays the direct path from the top-level Accounts page to the current item you are viewing, rather than the path you followed to get to the current view. The links that comprise this path enable you to quickly move up the navigation hierarchy to a higher level page.

6. At the upper right is a User avatar icon. Click here to access a modal window that displays user-specific settings including the company and the role associated with this user. You can also specify the UI Theme you want to view (Ericsson Light Theme and Ericsson Dark Theme), based on your preference.

   Note that the User Role specifies permissions for viewing and modifying various Portal configuration settings. Different roles are granted permission to view different features in the Portal. For more information, see the section titled ""Understanding User Roles and Permissions".

7. Down the left side of the screen, you will view a number of icons you can click to access the main features of the Portal. These icons are described in Table 2-1.

   Note that clicking any icon will bring you to a context-specific page associated with the icon's action. For example, if you are viewing a Group, clicking the Analytics icon will display reports for the traffic data associated with that Group.

Table 2-1: Navigation Icons

Icon	Name	Use
	Home	From any view, clicking the Home icon brings you to the highest level Portal page.
	Content	Clicking the Content icon brings you to the Content Summary page which displays information for entities associated with Content Providers.
	Analytics	Clicking the Analytics icon brings you to the Analytics page where you can view charts and generate reports. For more information on generating reports, see Chapter 3, "Generating Reports".

Table 2-1: Navigation Icons *(Continued)*

Icon	Name	Use
	Security	The Security feature enables you to load SSL certificates.
	Support	Clicking the Support icon brings you to a page where you can file and track support tickets, access support tools, and view documentation. For more information, see Chapter 9, "Accessing Support Resources".

NOTE

Features associated with the Services icon will be available in a future release.

The main (working) area of each screen displays information in the form of Starbursts. Each Starburst represents a managed entity in the form of an Account, a Group, or a Property.

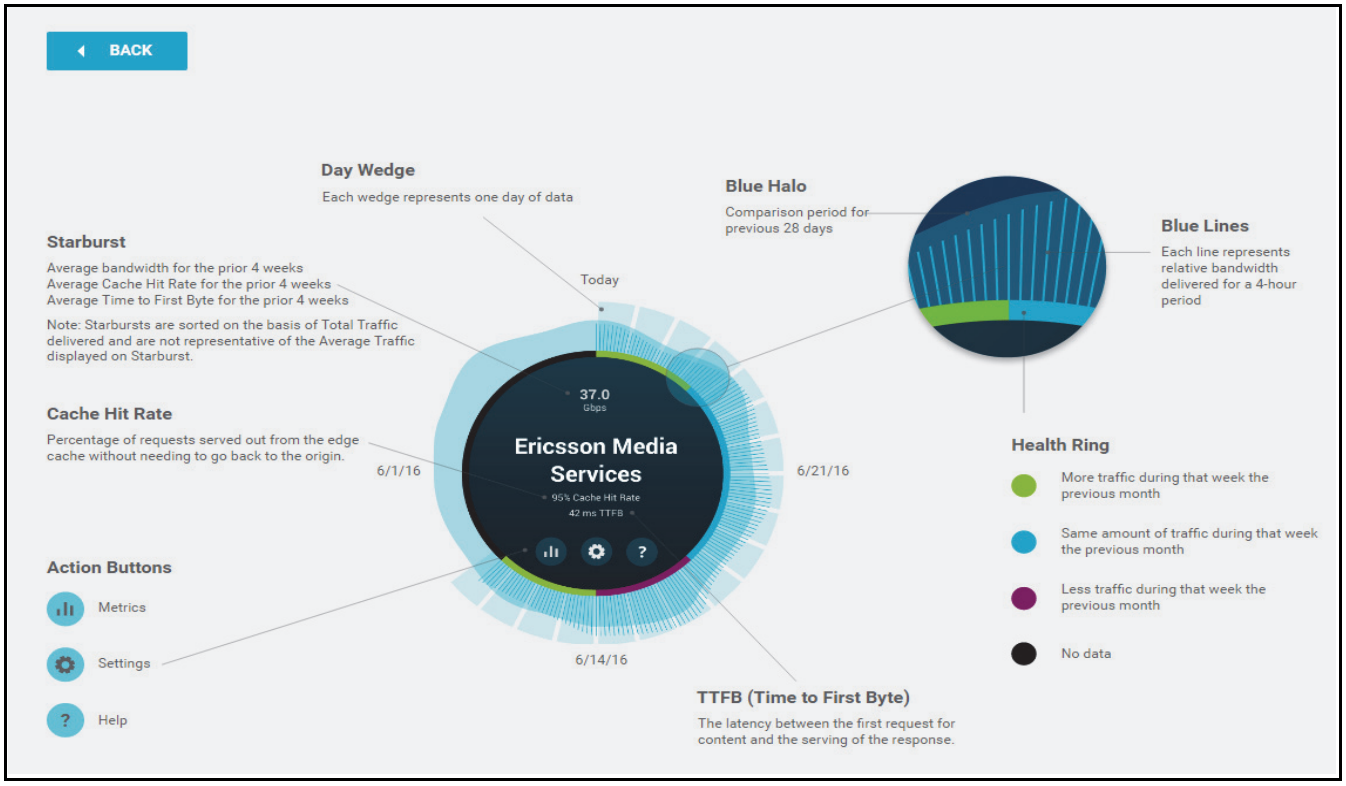
See "Exploring Starbursts" for a detailed explanation of Starbursts.

Exploring Starbursts

The Portal is used to manage and generate reports on three different levels of entity: Accounts, Groups, and Properties. Each Account contains one or more Groups, and each Group contains one or more Properties. Analytics information for an entity is an aggregation of the data for all entities below it.

Within the Portal, each entity is graphically represented as a Starburst. You can view a Help page in the Portal (Figure 2-2) by hovering over any Starburst and clicking the "?" icon that displays in its center.

Figure 2-2: Starburst Help



Following is an overview of the rich collection of information that the Starburst data visualization provides.

Viewing Data Over Time

The Starburst represents the last 28 days of traffic activity for an Account, Group, or Property.

If you picture each Starburst (all Starbursts have the same layout regardless of whether they represent an Account, Group, or Property) as the circular face of a clock:

- The 12:00 position at the top of the Starburst represents today.
- The quarter-circle section between 12:00 and 3:00 represents the past week (the past 7 days).
- The quarter-circle section between 3:00 and 6:00 represents 2 weeks ago (the time between 14 days ago and 7 days ago).
- The quarter-circle section between 6:00 and 9:00 represents 3 weeks ago (the time between 21 days ago and 14 days ago).

- The quarter-circle section between 9:00 and 12:00 represents 4 weeks ago (the time between 28 days ago and 21 days ago).

You will notice a solid ring, called the Health ring, around the inner edge of each Starburst. For each week of traffic in the outer halo, you will find the color of the inner ring represents how that week's traffic compares to traffic during the same time period four weeks earlier. When you hover over any point on the Health ring, a color key displays, enabling you to easily interpret the colored segments of the ring.

There is a halo of lines, or rays, radiating out from the edge of each Starburst. Each line represents the relative bandwidth delivered over a 4-hour period. Longer lines represent higher levels of traffic and shorter lines represent lower levels over the time period. You will typically notice a natural variation in bandwidth use over the course of a day (represented by 6 adjacent lines), but can also note other data trends as they appear.

As you mouse over the halo, the hover text shows the date and specific metrics for a particular day. For Property Starbursts, the rays for each day have a wedge, or slice, highlighting the day's boundaries.

Clicking on a particular wedge brings up the Property summary showing a bandwidth graph for the date of the wedge you selected.

Key Performance Indicators

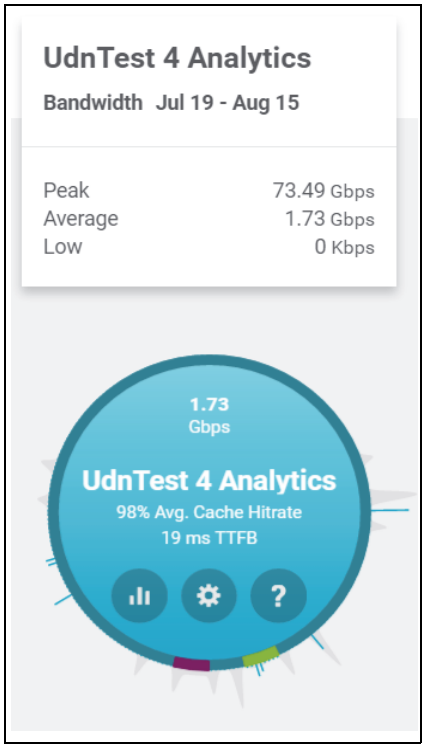
When the Starburst for an entity (Account, Group, or Property) displays, key performance indicators display automatically in the middle of the Starburst. In addition to the name of the entity, information averaged over the past month displays, including:

- The average bandwidth (in Gbps)
- The average cache hit rate for the past 28 days (as a percentage)
- The average time to first byte (TTFB) in milliseconds for the past 28 days

A Starburst display provides access to additional information when you hover over different areas:

- When you hover over any point in the center of the Starburst, you can view the Peak, Average, and Low bandwidth for the most recent 28-day period (Figure 2-3).
- When you hover over any area on the solid-color health ring at the perimeter of the circle, a color key displays to assist you in interpreting the ring colors displayed.
- When you hover over any section on the halo (rays) outside the center circle, you can view the Peak, Average, and Low bandwidth for the date represented by that halo section.

Figure 2-3: Key Performance Indicators Display



Note that all metrics for an individual Starburst are an aggregate of any entities beneath that Starburst:

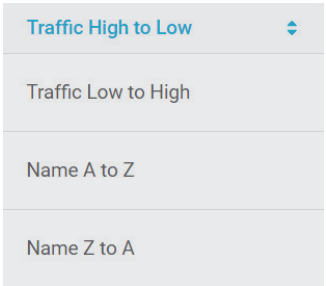
- An Account Starburst displays an aggregate of the data for all of the Groups that belong to that Account.
- A Group Starburst displays an aggregate of the data for all of the Properties belonging to that Group.
- A Property is the smallest entity available on the Portal.

Sorting Displayed Entities

At the top of any page, to the right of the title of the entity you are viewing (Account, Group, or Property), there is a drop-down which enables you to sort the information you are displaying. You can sort based on traffic (Traffic High to Low or Traffic Low to High), or you can sort alphabetically (Name A to Z or Name Z to A).

Note that when you sort by traffic, the sorting is performed based on the total transfer rate but the starbursts display the average transfer rate.

Figure 2-4: Sorting Displayed Entities



Displaying the Table View

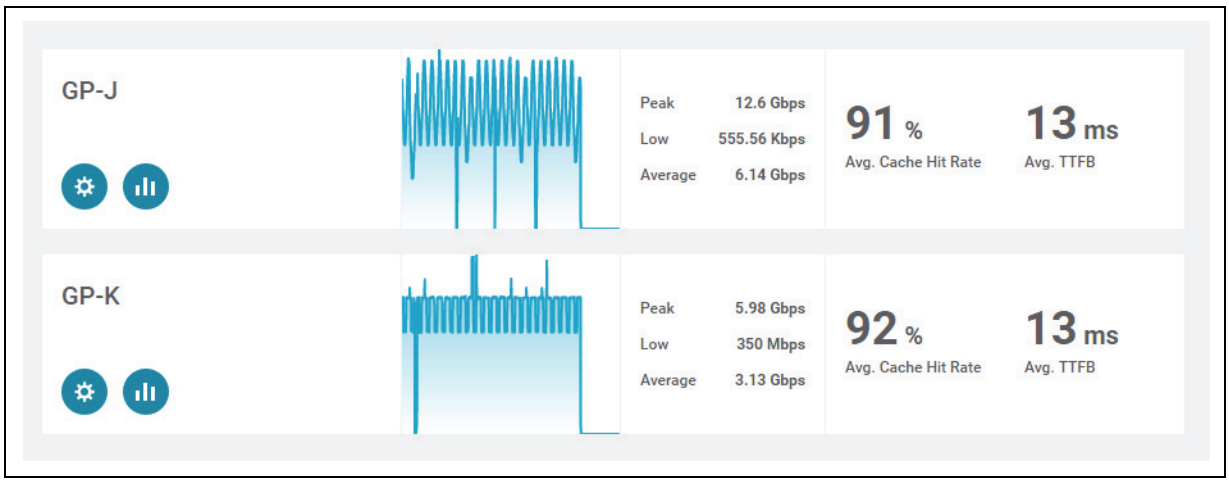
As an alternative to the Starburst view, you can choose to display the same information as a series of rows in a table.

To display the Table View, click the Table View icon at the top right of the page:

To return to the Starburst view at any time, click the Starburst View icon:

Sample rows from the Table View are shown in Figure 2-5.

Figure 2-5: Entity Table View



The Table View displays the following information for a rolling 4-week period:

- The name of the entity (Account, Group, or Property).
- The last time the entity was modified, and the user who modified it.
- A chart indicating the daily bit rate over the past 28 days. Note that you can hover over the chart for detailed information.
- The Peak, Lowest, and Average bit rate for traffic over the past 28 days.
- The average cache hit rate for the past 28 days.
- The average Time to First Byte (TTFB), in milliseconds, for the past 28 days.

The Table View also provides the following icons:

- To configure settings for the displayed entity, click the Configure icon.
- To view analytics for the displayed entity, click the Analytics icon.

Navigating Between Accounts, Groups, and Properties

There are several ways you can navigate between entities (Accounts, Groups and Properties) in the Portal: Breadcrumb navigation, Starburst navigation, and Drop-down navigation.

Starburst Navigation

To navigate to a lower-level entity in the Portal, click on a Starburst. Clicking on a Starburst brings you to a display that shows a Starburst for each of the entities it contains:

- Clicking on an Account Starburst brings you to a page that displays a Starburst for each of the Groups belonging to that Account.
- Clicking on a Group Starburst brings you to a page that displays a Starburst for each of the Properties belonging to that Group.

Breadcrumb Navigation

To navigate to a higher-level entity in the Portal hierarchy, you can traverse back up the path you used to navigate to your current view by clicking any item in the breadcrumb trail of links at the top of the page.

Figure 2-6: Breadcrumb Navigation

You can navigate to the highest level view by clicking the Ericsson logo in the upper left corner.

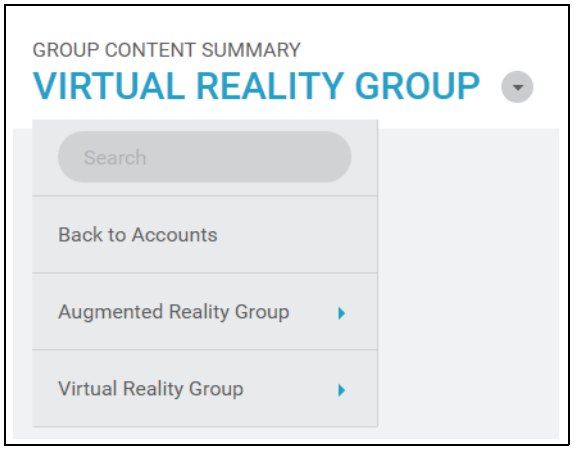
Drop-down Navigation

The Portal also provides a drop-down selector that enables you to navigate either one level up from your current location, or to choose from other entities at the same level as the one you are currently viewing (Figure 2-7).

For example, if you are viewing a Group, the drop-down selector at the top of the page enables you to navigate up one level to view Accounts, or to choose to view a different Group belonging to the same Account as the Group you are viewing.

In addition, you can search for an entity using the Search field. Note that search terms are not case sensitive.

Figure 2-7: Drop-down Navigation Menu



Changing your User Information or Password

In order to access the portal, you must have a User account. In order to create this account, information about you has been entered into the UDN Service by an administrator. The Portal enables you to modify this information.

To modify your user profile settings:

1. Click the user avatar at the upper right of the page. The User Profile modal window displays.
2. Choose Edit Profile.
3. Enter your name and your contact information.
4. If desired, you may change your password.

NOTE

If you change your password, you will need to log back into the system.

Chapter 3
Generating Reports

UDN analytics enable you to monitor crucial metrics that directly affect the success of your business, helping you to make timely decisions regarding content management, storage, and delivery. UDN reports are design to provide actionable and relevant information for Portal users and their management.

UDN reports provide detailed information on bandwidth delivered by provider, by time, and by geography. You can identify which URLs are most popular and which URLs are suffering content delivery failures. You can also view information on how frequently cached content is being served, to identify opportunities for cache optimization.

This chapter contains the following sections:

Viewing Reports

The Portal enables you to dynamically generate a number of predefined report types, specifying the desired date range for the data you want displayed.

When you click the Analytics icon, the Portal will display reporting information associated with the currently selected entity (Account, Group, or Property) associated with that page. If you select the Analytics icon for a Property Starburst or Summary, the report will reflect the data available for that Property. If you select the Analytics icon for a Group Starburst or Summary, the report will include aggregated data from all Properties belonging to that Group. Likewise, reporting for an Account displays a total of all data for all Properties belonging to all Groups within that Account.

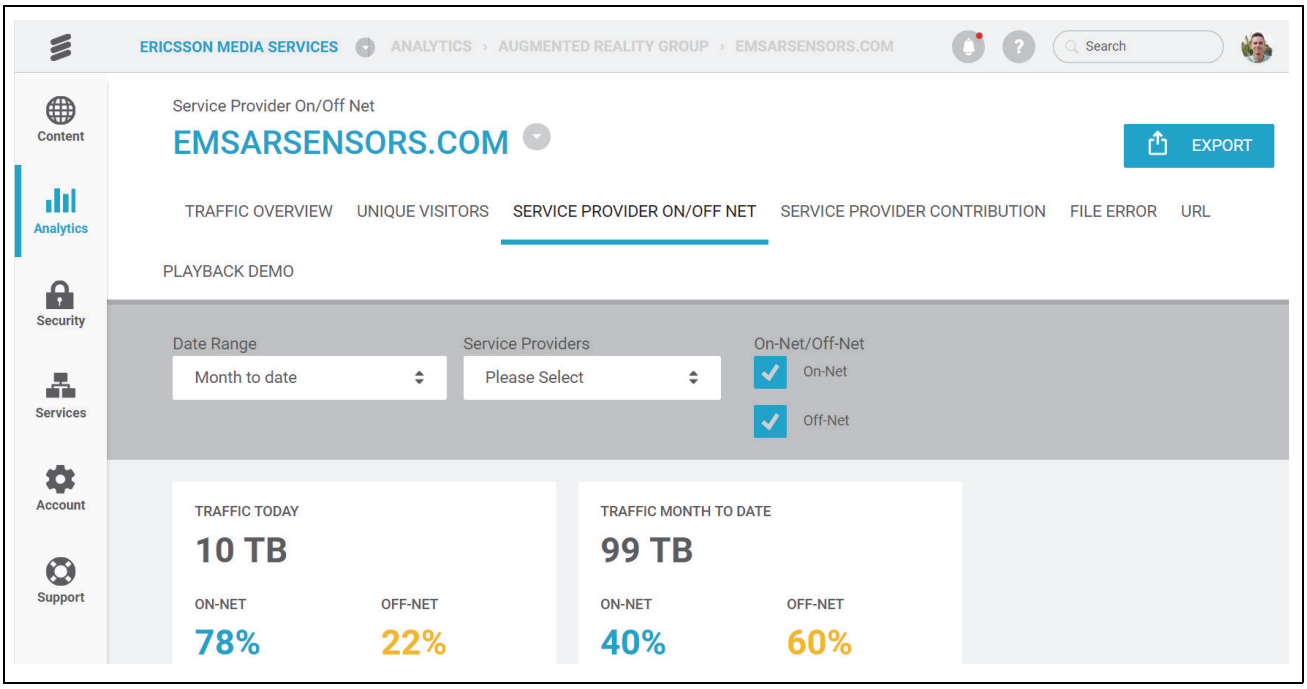
To view a report:

1. Navigate to the entity (Account, Group, or Property) whose data you want to view.
2. Doing one of the following:
   - Click the Analytics icon on the left navigation bar. 

   - Click the Analytics icon inside any Starburst. 
     Note that you need to hover the cursor in the center of the Starburst in order for this icon to display.
   - Click the Analytics icon on any Summary page. 

   A Report page displays for the selected entity (Account, Group, or Property).
3. You can select different types of reports by choosing the tabs that display above the report. Figure 3-1 shows an example of the Service Provider On/Off Net Report.

Figure 3-1: Service Provider On/Off Net Report



4. Each report has a specified date range. By default, each report type shows data for the Month to Date.

   You can modify this setting by selecting from a predefined list of options (Last Month, Last Week, and so forth), or you can specify a Custom Date Range.

   When you specify a date range that spans multiple days, the data displays in daily increments. When you specify a single day, the data displays in hourly increments.

   NOTE

   Each report type offers settings that allow you to generate more customized reports. Detailed information about each report type is available in the following sections.

5. When information is displayed in chart form, you can hover your cursor over separate parts of the graph in order to view more detailed information.
6. When information is displayed in table form, you will see a small triangle appear next to some column headings. You can sort the table rows in ascending or descending order based on the column content by clicking these headings.
7. You can Export a displayed report to a CSV (comma separated variable) file format by clicking the Export button. The resulting csv file name includes the report type and the entity (Account, Group, or Property) for which data is included.
8. Once you have generated a report, you can select a different entity from the selector at the top of the page.

   When you do so, if the report is availability for the entity type (Account, Group, or Property), the same report type will display for the selected entity. If it is not available, a report type that is available for that entity will display.

Traffic Overview Report

The Traffic Overview Report shows detailed bandwidth usage information for the Account, Group, or Property selected. This report provides a general view of the traffic being carried by the UDN service. This report summarizes general information by traffic type and data type for a given date range.

Scope

This report is available to users who have been assigned either the UDN_Admin, CP_Admin, or CP_User role. You can generate this type of report for an Account, Group, or Property.

Settings

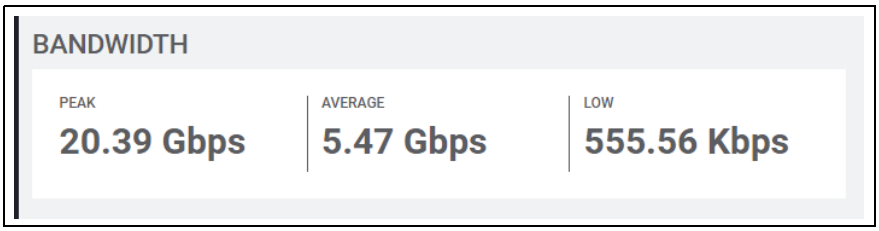
You can specify the following settings for this report:

- Date Range
- Traffic type: select HTTP traffic, HTTPS traffic, or both.
- Data type: select Bandwidth or Requests.

Content

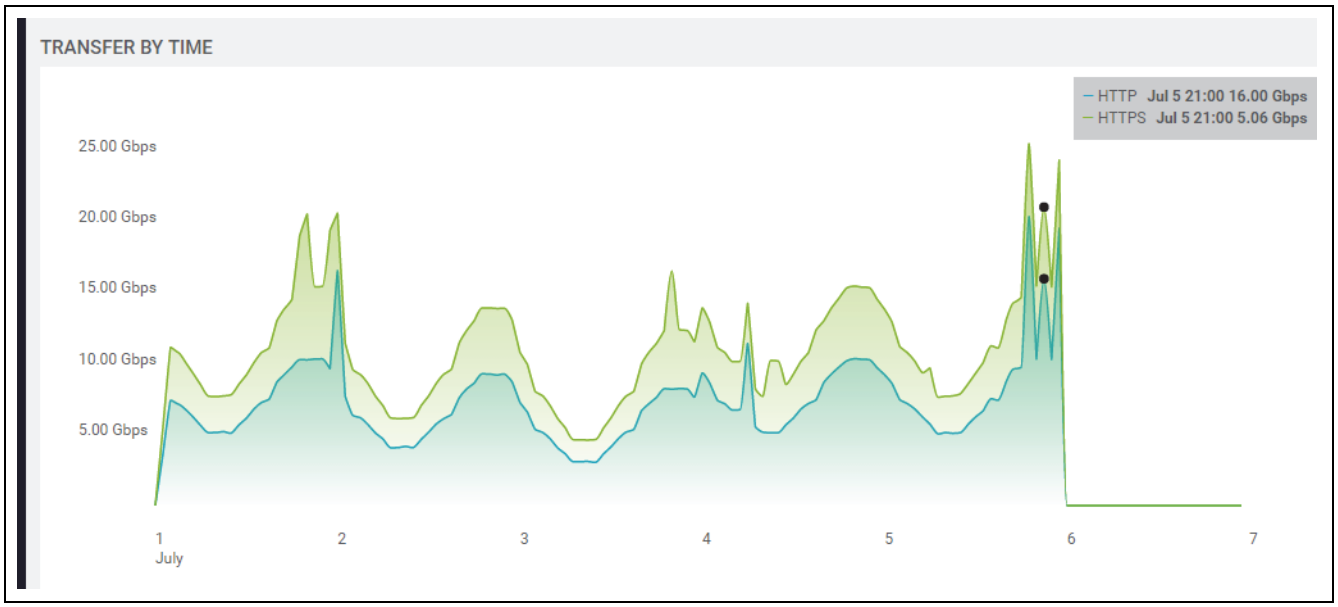
When viewing the Traffic Overview report, the Bandwidth area at the top (Figure 3-2) displays Peak, Average, and Low bandwidth values over the total date range. If you select Requests, Peak, Average, and Low values will display.

Figure 3-2: Traffic Overview Report: Bandwidth Area



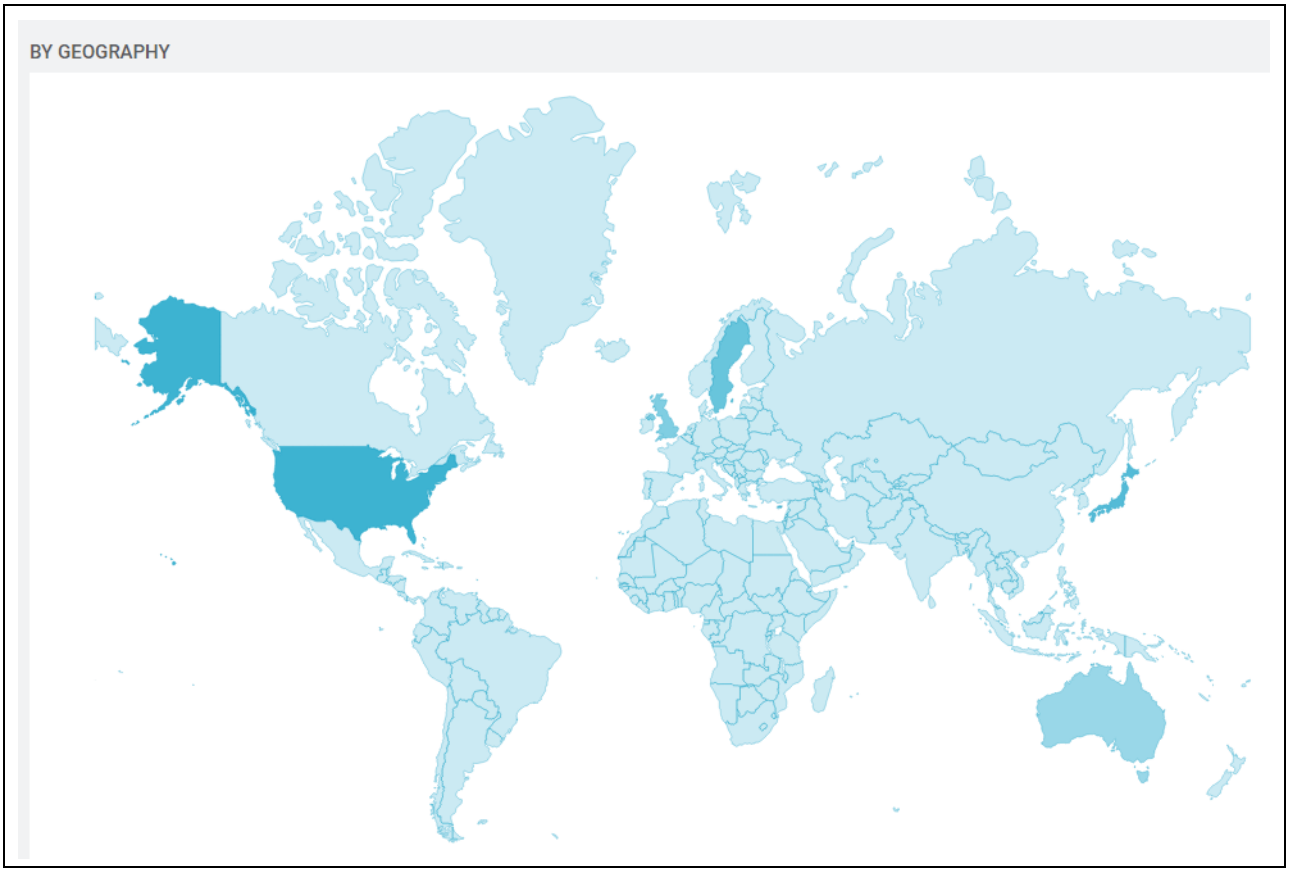
The Transfer by Time area (Figure 3-3) displays a graph showing the volume of data transferred over the dates specified.

Figure 3-3: Traffic Overview Report: Transfer by Time Area



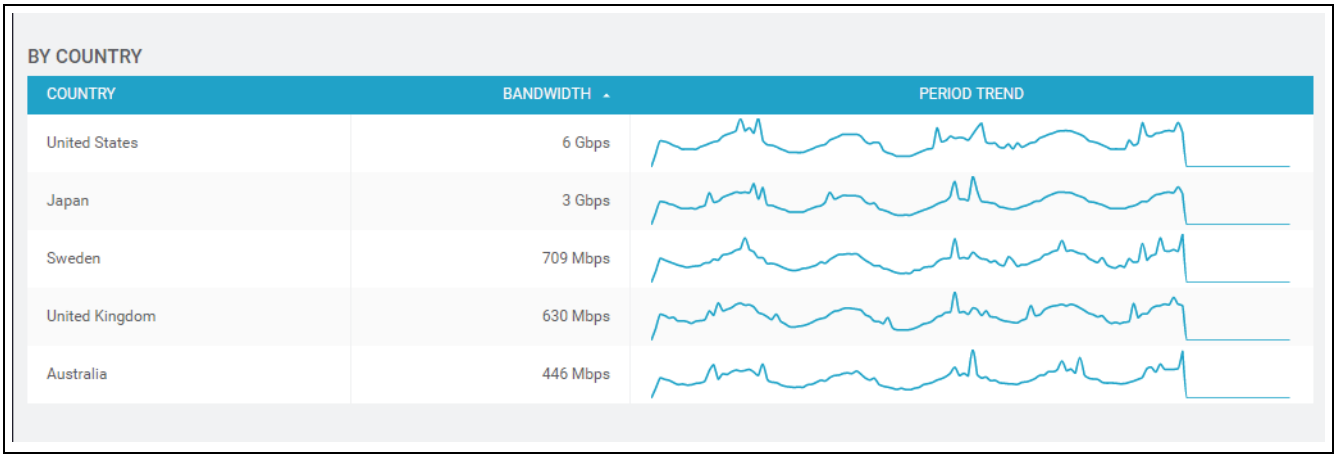
The By Geography area (Figure 3-4) displays traffic information in the form of a world map. Darker areas indicate more traffic. Hovering over a specific country displays the total traffic in that country over the specified data range.

Figure 3-4: Traffic Overview Report: By Geography Area



The By Country area at the bottom of the report (Figure 3-5) shows bandwidth volume information and a chart line indicating traffic trends for the specified time period for the top five countries.

Figure 3-5: Traffic Overview Report: By Country Area



Cache Hit Rate Report

The Cache Hit Report shows the percentage of traffic served from cache for each day over a specified date range. The percentage of traffic served from the cache is called the offload rate, because this data is not retrieved from the origin, or from anywhere outside the UDN network. The operator goal is to optimize cache usage, while taking into consideration that there are types that are not appropriate to cache (non-cacheable content or long tail content).

Scope

This report is available to users who have been assigned either the UDN_Admin, CP_Admin, or CP_User role. You can generate this type of report for an Account, Group, or Property.

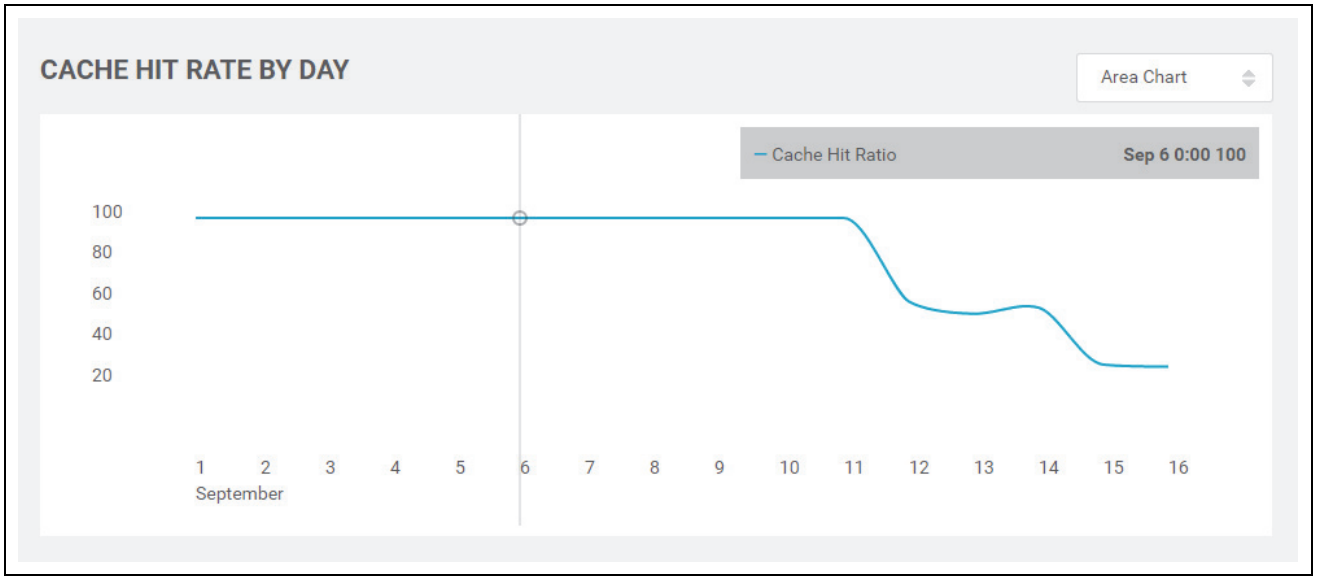
Settings

You can specify the date range for this report.

Content

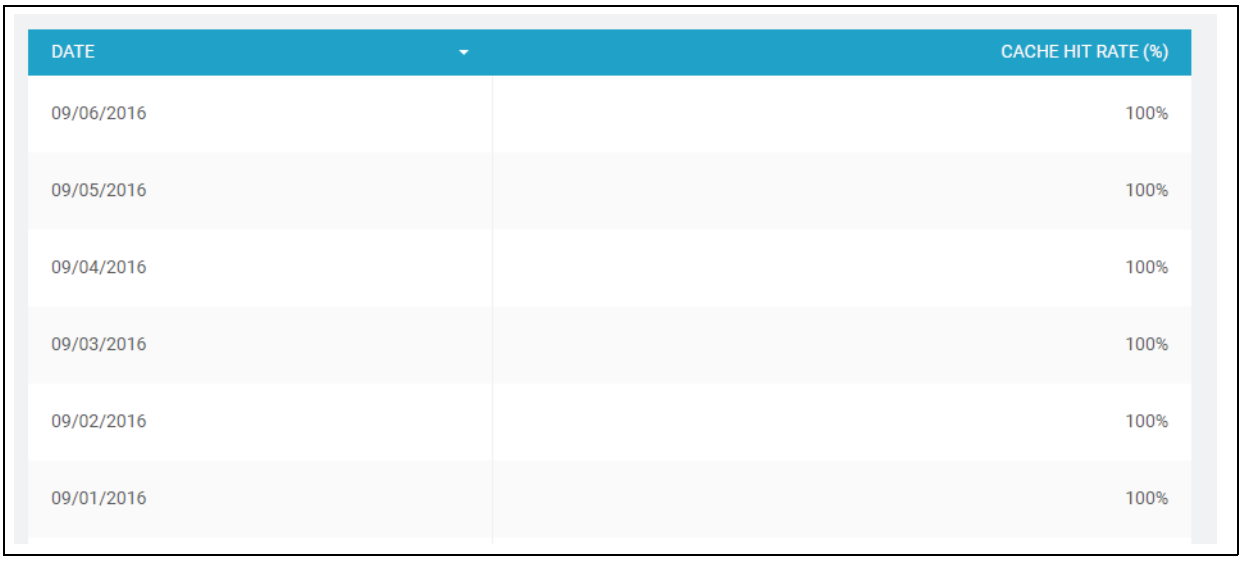
When viewing the Cache Hit Overview report, the chart at the top of the report (Figure 3-6) displays the cache hit rate as a percentage for each day in the specified date range. Note that you can select whether you want the data displayed in the form of an Area Chart or a Column Chart.

Figure 3-6: Cache Hit Rate Report: Chart Area



The bottom of the Cache Hit Rate report displays the same information in table form ().

Figure 3-7: Cache Hit Rate Report: Table Area



DATE	CACHE HIT RATE (%)
09/06/2016	100%
09/05/2016	100%
09/04/2016	100%
09/03/2016	100%
09/02/2016	100%
09/01/2016	100%

Unique Visitors Report

The Unique Visitors Report shows the number of unique visitors to a particular URL. A unique visitor is defined as a visitor that has consumed content for a given Property from a given device one or more times. An increase in unique visitors indicates that more end users are requesting UDN content.

Tracking for unique visitors is done via a UDN cookie. For those visitors that disable or disallow cookies the IP address and User Agent are used as a proxy.

Scope

This report is available to users who have been assigned either the UDN_Admin, CP_Admin, or CP_User role. You can generate this type of report for an Account, Group, or Property.

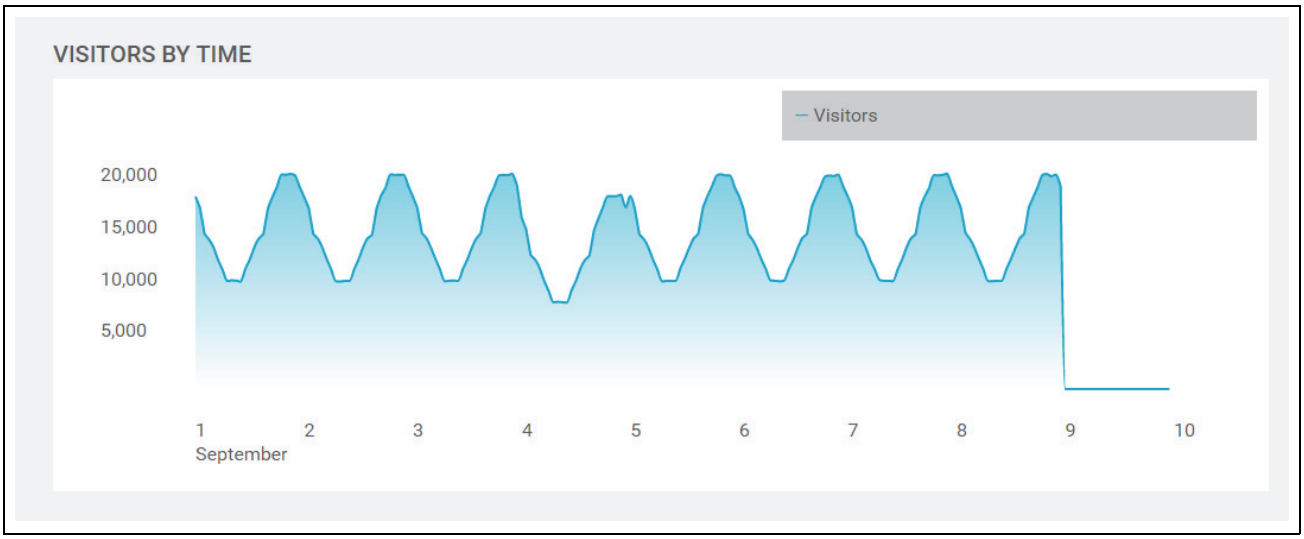
Settings

This report enables you to modify the Date Range for the data displayed.

Content

When viewing the Unique Visitors report, the Visitors by Time area at the top (Figure 3-8) displays the number of unique visitors over the specified time period.

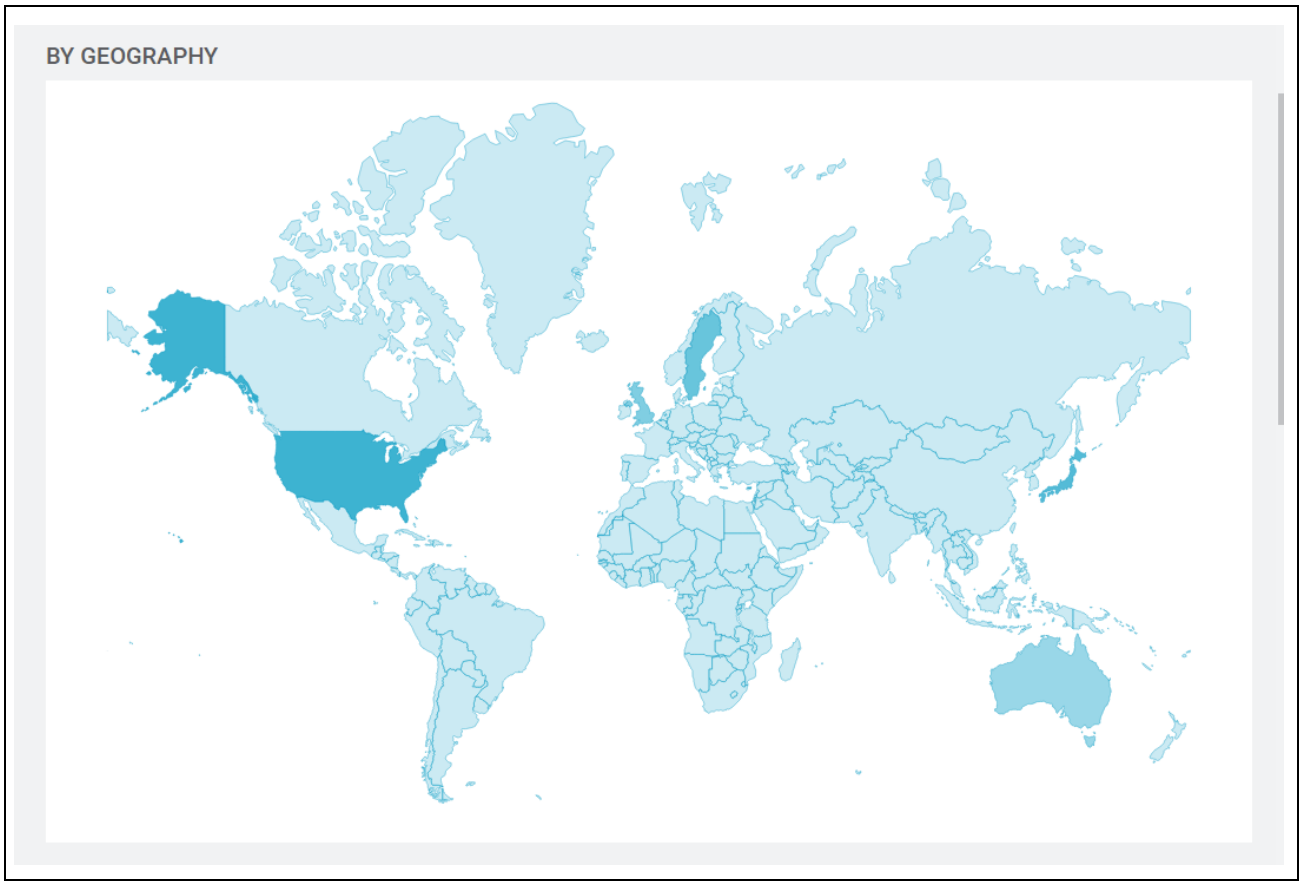
Figure 3-8: Unique Visitors Report: Visitors by Time Area



The By Geography area displays visitor information in the form of a world map (Figure 3-9). Hovering over a specific country displays the total number of unique visitors for that country over the specified data range. Darker areas indicate more traffic.

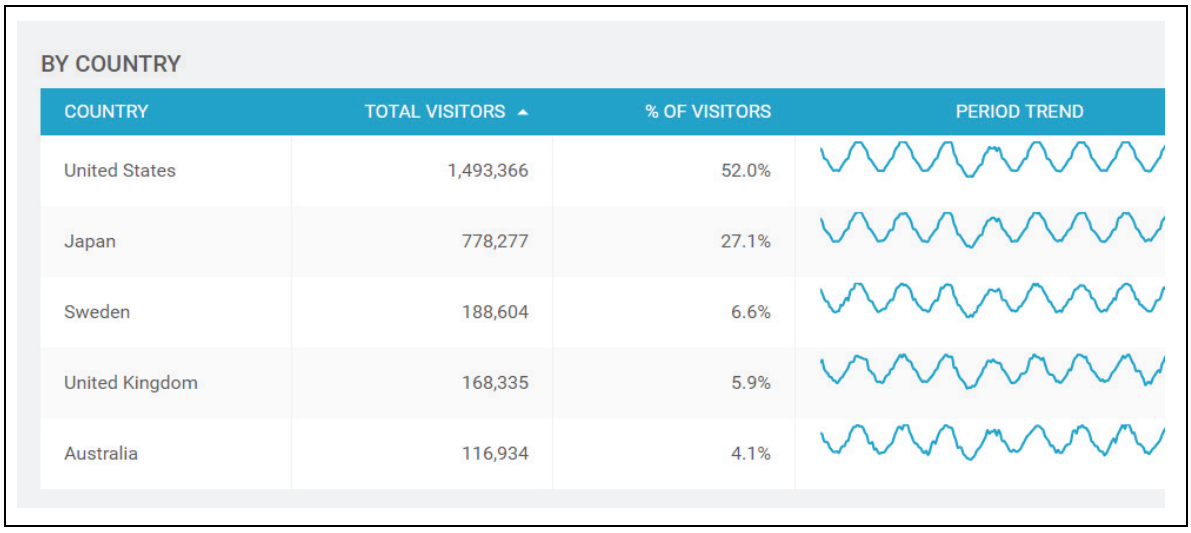
Note that the Unique Visitor geographical breakdown is ranking countries by the number of unique visitors for that country. This is different than the Traffic Overview geographical breakdown which ranks the countries by the amount of traffic consumed, so it is possible a country that has the highest number of unique visitors is one of the lower countries relative to traffic consumption, and conversely a country with a low number of unique visitors may be consuming the most traffic.

Figure 3-9: Unique Visitors Report: Visitors by Geography Area



The next section displays unique visitor information By Country (Figure 3-10). This section displays the top five countries by volume, the total number of unique visitors in that country over the date range, the percent of visitors in that country, a period trend chart, and the percent change from the start of the date range to the end. You can hover over any portion of the Period Trend charts to display information for a specific date.

Figure 3-10: Unique Visitors Report: Visitors by Country

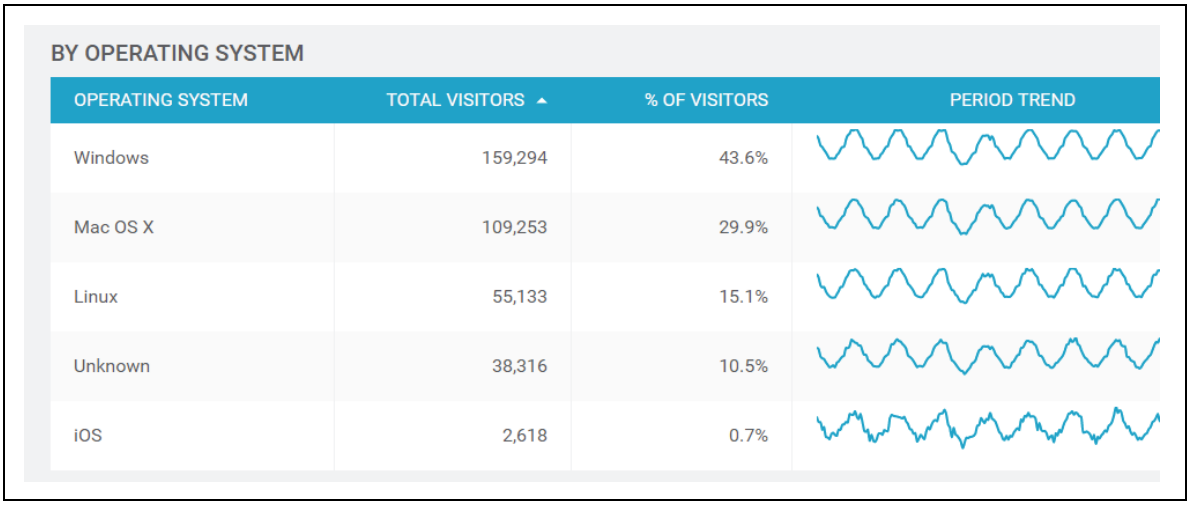


The next section displays unique visitor information By Browser (Figure 3-11). This section displays the top five browsers by volume, the total number of unique visitors using each browser over the date range, the percent of visitors with that browser, a period trend chart, and the percent change from the start of the date range to the end. You can hover over any portion of the Period Trend charts to display information for a specific date.

Figure 3-11: Unique Visitors Report: Visitors by Browser

The next section displays unique visitor information By Operating System (Figure 3-12). The section displays the top five operating systems in use by unique visitors, the total number of unique visitors over the date range, the percent of visitors with that operating system, a period trend chart, and the percent change from the start of the date range to the end. You can hover over any portion of the Period Trend charts to display information for a specific date.

Figure 3-12: Unique Visitors Report: Visitors by Operating System



BY OPERATING SYSTEM

OPERATING SYSTEM	TOTAL VISITORS ▲	% OF VISITORS	PERIOD TREND
Windows	159,294	43.6%	
Mac OS X	109,253	29.9%	
Linux	55,133	15.1%	
Unknown	38,316	10.5%	
iOS	2,618	0.7%	

Service Provider On / Off Net Report

The Service Provider (SP) On/Off Net Report allows Service Provider partners to see how much traffic to their subscribers is being served to end-users directly from the UDN network (On Net). On-Net traffic provides the best end user experience due to the location of UDN SP edge servers in the SP delivery network.

Off-Net traffic is defined is content that has been served from the Service Provider cache to another Service Provider's end-user.

Why might traffic be served off-net? This could happen for a number of reasons. A request from a subscriber might be routed to either outside the UDN Edge or to another Service Provider for a variety of reasons including:

- A lack of server availability for the SP that owns the subscriber
- The SP network edge's inability to satisfy the request due to issues such as SSL delivery problems or a lack of SSL service
- Advanced cache control requirements that cannot be properly identified by the SP network
- Network saturation/volume

Availability is determined based on the health or load of the SP Edge servers. If there are no healthy servers to route the request to, or if the load for the SP Edge Servers is too high, routing will bring this subscriber to the UDN Edge or another SP in order to obtain the content. SP Partners are given incentive to maintain enough capacity to minimize any Off Net routing because they get more revenue share for serving their subscribers directly.

Scope

This report is available to users who have been assigned either the UDN_Admin, SP_Admin, or SP_User role. You can generate this type of report for an Account, Group, or Property.

Settings

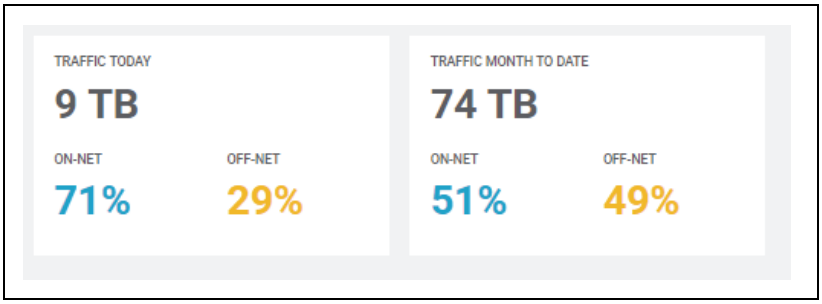
You can specify the following settings for this report:

- Date range
- Traffic type: select On-Net traffic, Off-Net traffic, or both

Content

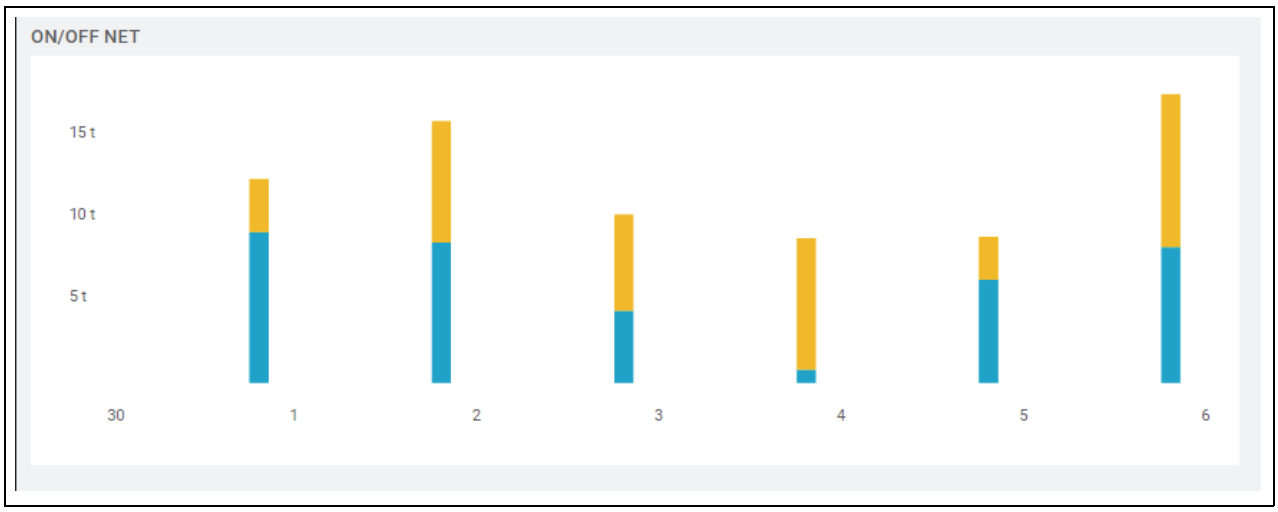
When viewing the SP On/Off Net report, the area at the top displays traffic information for both the current date and the specified date range (Figure 3-13).

Figure 3-13: SP On/Off Net Report: Traffic Overview



The next section of the report (Figure 3-14) shows the traffic volume both On and Off Net for each day in the range specified.

Figure 3-14: SP On/Off Net Report: Volume Chart



The last section of the report (Figure 3-15) displays a table with specific data for each date in the range specified.

Figure 3-15: SP On/Off Net Report: Data Table

DATE	ON NET (BYTES)	ON NET (%)	OFF NET (BYTES)	OFF NET (%)	TOTAL (BYTES)
07/05/2016	8 TB	47%	9 TB	53%	18 TB
07/04/2016	6 TB	70%	3 TB	30%	9 TB
07/03/2016	817 GB	9%	8 TB	91%	9 TB
07/02/2016	4 TB	43%	6 TB	57%	10 TB
07/01/2016	9 TB	54%	7 TB	46%	16 TB
06/30/2016	9 TB	74%	3 TB	26%	12 TB

Contribution Report

The Contribution Report provides detailed traffic information for each Service Provider (SP) or Content Provider (CP) that supported the content delivery of a particular Account, Group, and/or Property. Information is broken down by geography.

Scope

This report is available to all users. You can generate this type of report for an Account, Group, or Property.

Settings

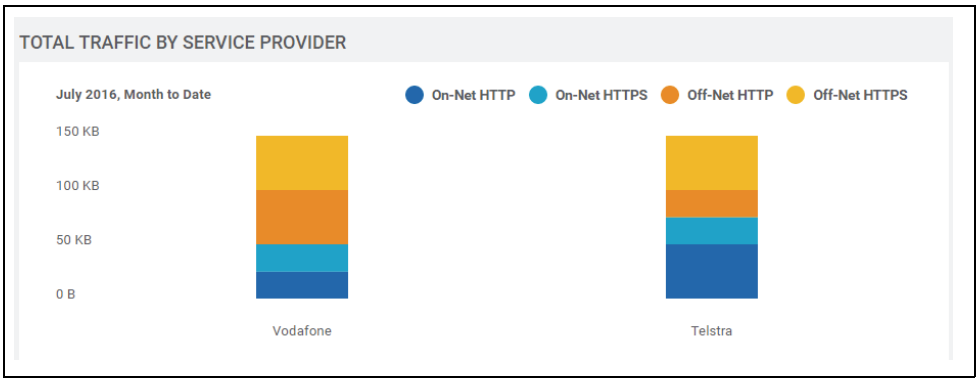
This report allows you to specify the following settings:

- Date range
- Providers and provider groups for whom data is available
- Delivery type: select On-Net, Off-Net, or both
- Service type: select HTTP, HTTPS, or both.

Content

The top of the report displays a chart that shows traffic volume per Provider for each traffic type (based on your settings). Figure 3-16 shows an example of a Contribution Report generated for a Service Provider.

Figure 3-16: Contribution Report: Traffic Chart



The following section (Figure 3-17) provides the same information in table form.

Figure 3-17: Contribution Report: Traffic Table

SERVICE PROVIDER	COUNTRY	TRAFFIC	% OF TRAFFIC ▲
Vodafone	Germany	150 KB	35%
Telstra	Australia	150 KB	30%
Vodafone	France	150 KB	20%

File Error Report

The File Error Report shows requests for an asset that resulted in a 4xx or 5xx (error) response. The results are sorted and the top 15 assets are displayed.

This report does not describe why a particular error occurred, primarily because the causes for a specific error type are many and varied. For example, a 404 error (file not found) could be caused by a requested file being moved, renamed, or deleted, or the file may be temporarily unavailable.

Scope

This report is available to users who have been assigned either the UDN_Admin, CP_Admin, or CP_User role. You can only generate this type of report for a Property, not for a Group or an Account.

Settings

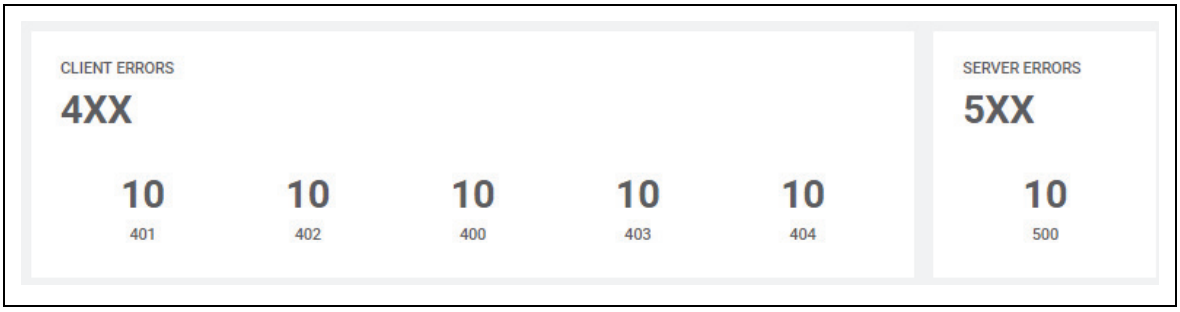
This report enables you to specify the following settings:

- Date range
- Service types: select HTTP, HTTPS, or both
- Status codes: select one, some, or all

Content

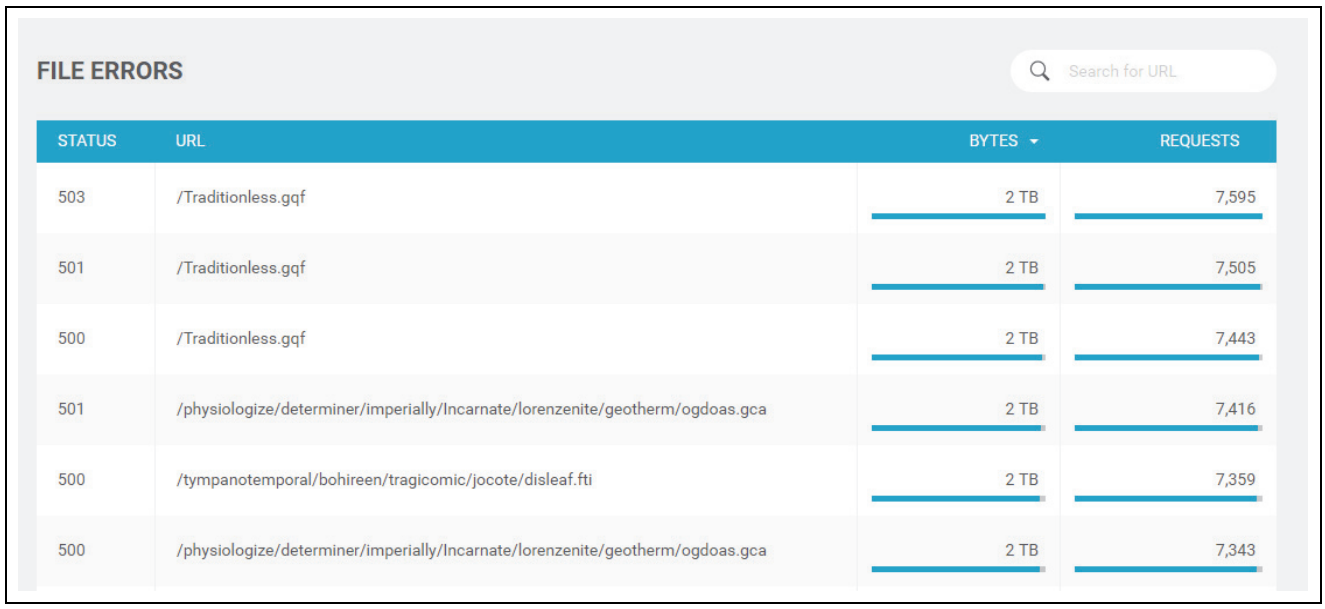
The top of the report (Figure 3-18) displays the number of Client Errors (listed by error type), and Server Errors for the dates specified. The report lists error information for redirection errors (3XX), client errors (4XX), and server errors (5XX).

Figure 3-18: File Error Report: Client Errors



The rest of the report (Figure 3-19) lists Byte and Request volumes for URLs associated with errors.

Figure 3-19: File Error Report: Byte and Request Volumes



URL Report

The URL Report shows all accelerated assets ranked by traffic volume (GB delivered) over the specified date range.

Scope

This report is available to users who have been assigned either the UDN_Admin, CP_Admin, or CP_User role. You can only generate this type of report for a Property, not for an Account or a Group.

Settings

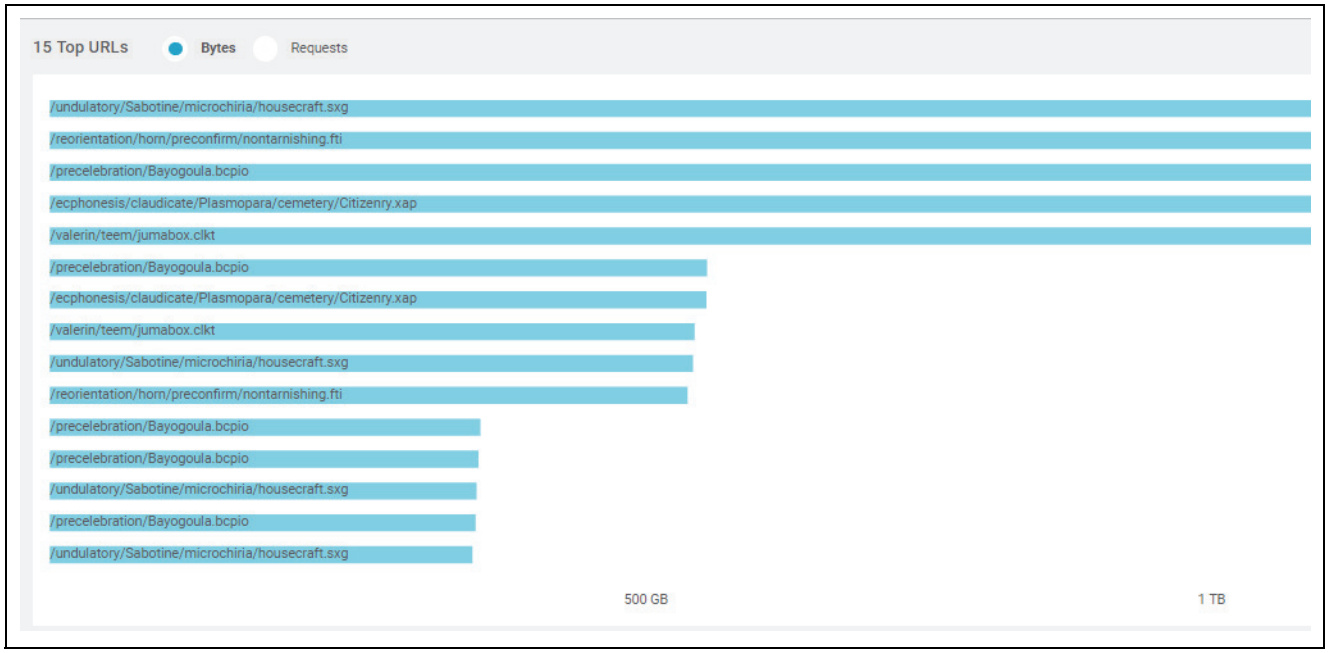
This report enables you to specify the following settings:

- Date range
- Service type: select HTTP, HTTPS, or both
- Status codes: select one, several, or all

Content

The top of the report (Figure 3-20) displays a chart that shows the relative volume of traffic associated with different URLs. You can choose whether to display data associated with Bytes or Requests.

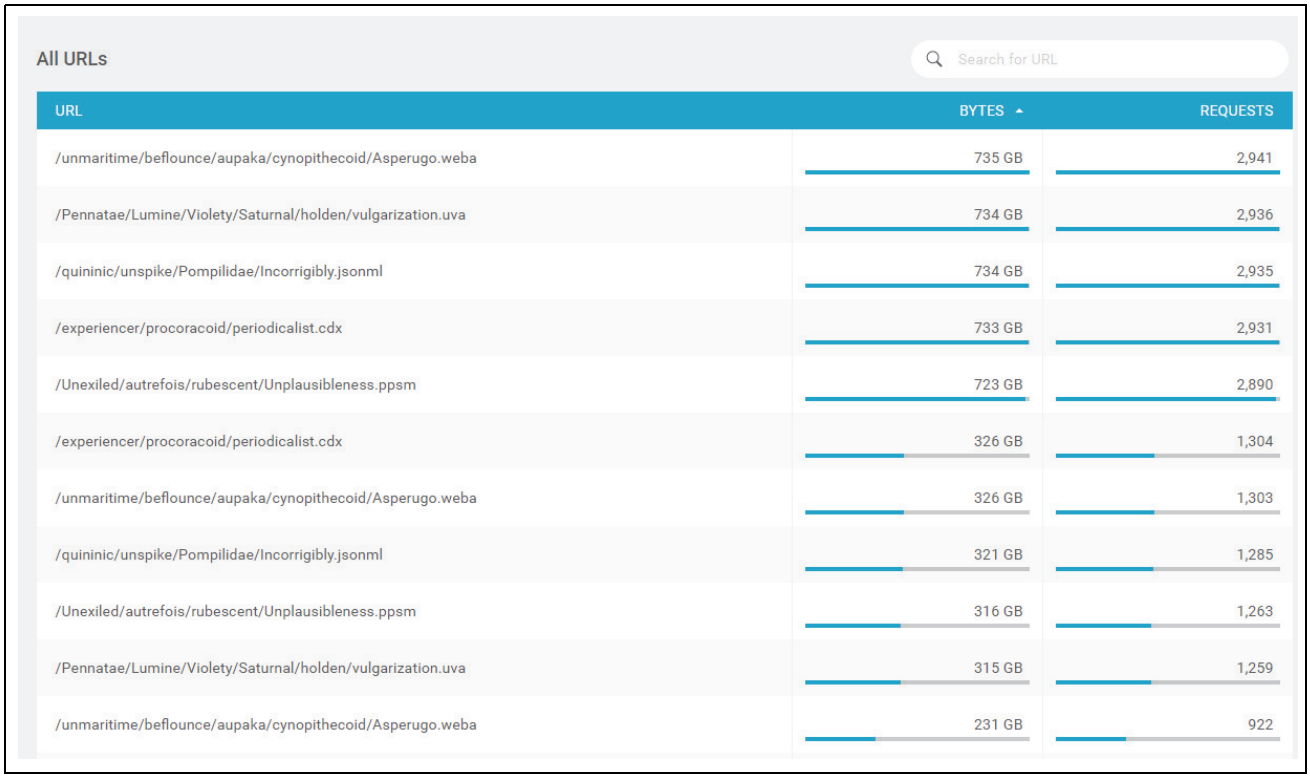
Figure 3-20: URL Report: Top URLs



The bottom of the report (Figure 3-21) lists header information. Each URL is listed with its associated Bytes and Requests volume.

Above this table and to the right, you will find a Search field where you can enter a URL. The search field acts as a filter for the list below, and displays partial and full matches depending on the URL information you enter. Note that search terms are not case sensitive.

Figure 3-21: URL Report: All URLs



Chapter 4
Working with Users

The Portal can only be accessed by people who have been added as Portal users. Each user is associated with a specific Portal Account. When a Portal user is added, they are assigned a user role which grants them permission to access specific Portal features.

This chapter contains the following sections:

Understanding User Roles and Permissions

In order to access the Portal, people must be added to the Portal as users, and when a User is created, they are given a User Role chosen from those predefined in the Portal.

Roles fall under one of two categories: Administrator or User. In addition to the ability to view information in the Portal, users who have been assigned an Administrator role can also create, modify, and delete items through the Portal interface. Those with a User role can view items in the Portal interface, but cannot create, modify, or delete them.

Each role provides specific permission to access different features of the UDN Admin Portal, as shown in Table 4-1.

NOTE

For users associated with Content Provider accounts, there are two types of user roles: CP Admin and CP User. CP Administrators can view, create, and modify settings for those features they have permission to access. CP Users can only view settings associated with those features.

Table 4-1: Predefined Portal Role Permissions

Portal Feature	Content Provider
Account	X
Analytics	X
Analytics - Daily Cache Hit Rate Report	X
Analytics - File Error Report	X
Analytics - Contribution Report	X
Analytics - SP On/Off Net Report	X
Analytics - Traffic Overview Report	X
Analytics - Unique Visitors Report	X
Analytics - URL Report	X
Configuration	X
Content	X
DNS	
Security	X
Services	X
Support	X

NOTE

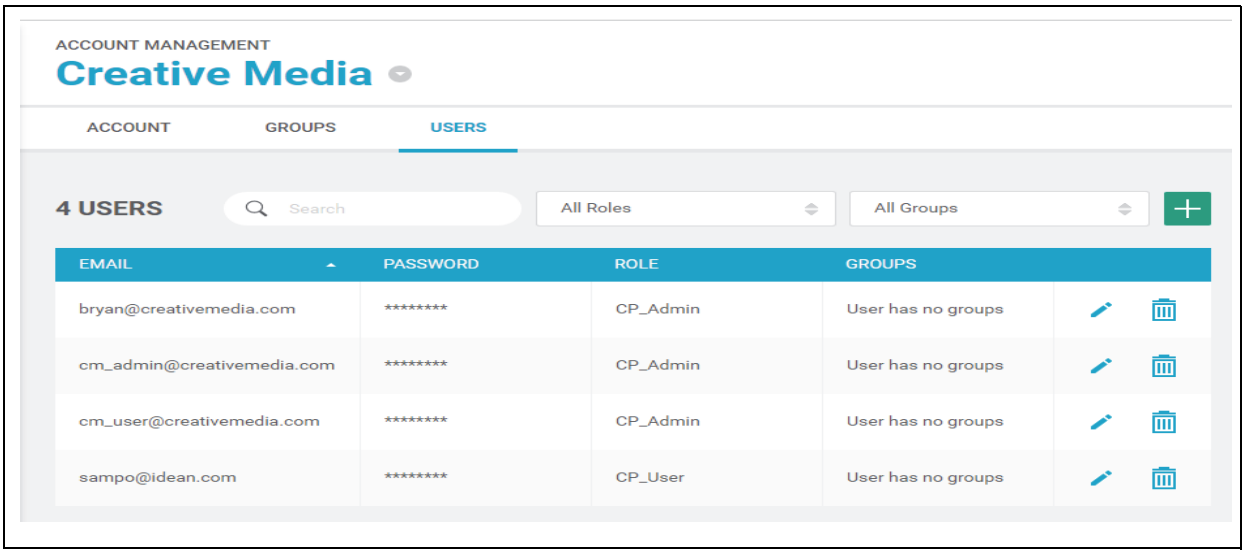
If a user attempts to access a feature that their role does not grant permission to access, a message indicating this will display.

Viewing and Managing Users

To view User information:

1. Navigate to the summary page for the desired Account.
2. Click the Users tab. A list of all current Users displays. For each User, the table lists their Email (which is also their user name), Password, Role, and any Groups they belong to.

Figure 4-1: Account Management: Users Tab



3. To search for a specific user, enter information in the Search area. Note that search terms are not case sensitive.
4. To view users with specific Roles, select the desired option in the Role drop-down list.

> NOTE
>
> Users are not assigned to Groups in this release, so searching for Users in the Groups drop-down will yield no results.

5. To add a user, click the Add (+) icon.

> NOTE
>
> Only Users with Admin permissions can add other Users. For more information on User Roles see "Understanding User Roles and Permissions".

   a. Specify the user's email (which acts as their username).
   b. Specify and confirm the user's password. Passwords must meet the following requirements:
      - Between 8-15 characters long
      - Contain at least one uppercase letter
      - Contain at least one lowercase letter
      - Contain at least one number
      - Contain at least one special character (non-alphanumeric characters)

c. Select the user's Role.

d. Click Save to save your changes, or click X to cancel the operation.

6. To edit a user, locate the row associated with that user in the table, and click EDIT.

> NOTE
>
> Only Users with an Admin Role can edit users. For more information on User Roles see "Understanding User Roles and Permissions".

Specify the information associated with this user by entering:

- Their email (which acts as their username)
- Their first name
- Their last name
- Their phone number
- Their password
- Their user role.

7. When finished, click Save to save your changes, or click Cancel to cancel the operation.

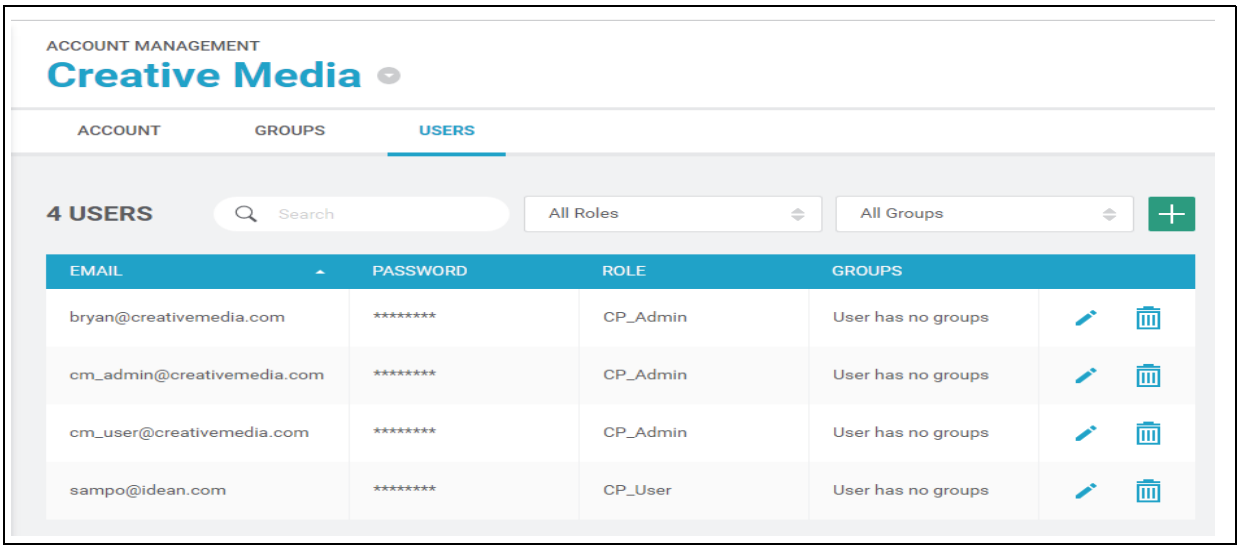
Deleting a User

Only Users with Admin permissions can delete users. For more information on Roles see “Understanding User Roles and Permissions”.

To delete a User:

1. Navigate to the summary page for the desired Account.
2. Click the Users tab.

Figure 4-2: Accounts Page: Users Tab



3. Locate the row associated with the user in the table, and click the Delete (trash) icon on that row.
4. Confirm the deletion to complete the operation.

Chapter 5
Working with Groups

The UDN Administrator Portal is a Graphical User Interface (GUI) web application that serves as the management application for UDN administration, configuration, and monitoring.

Groups are defined as collections Properties associated with a specific Account. Groups also include a collection of Users who have permission to access that Group.

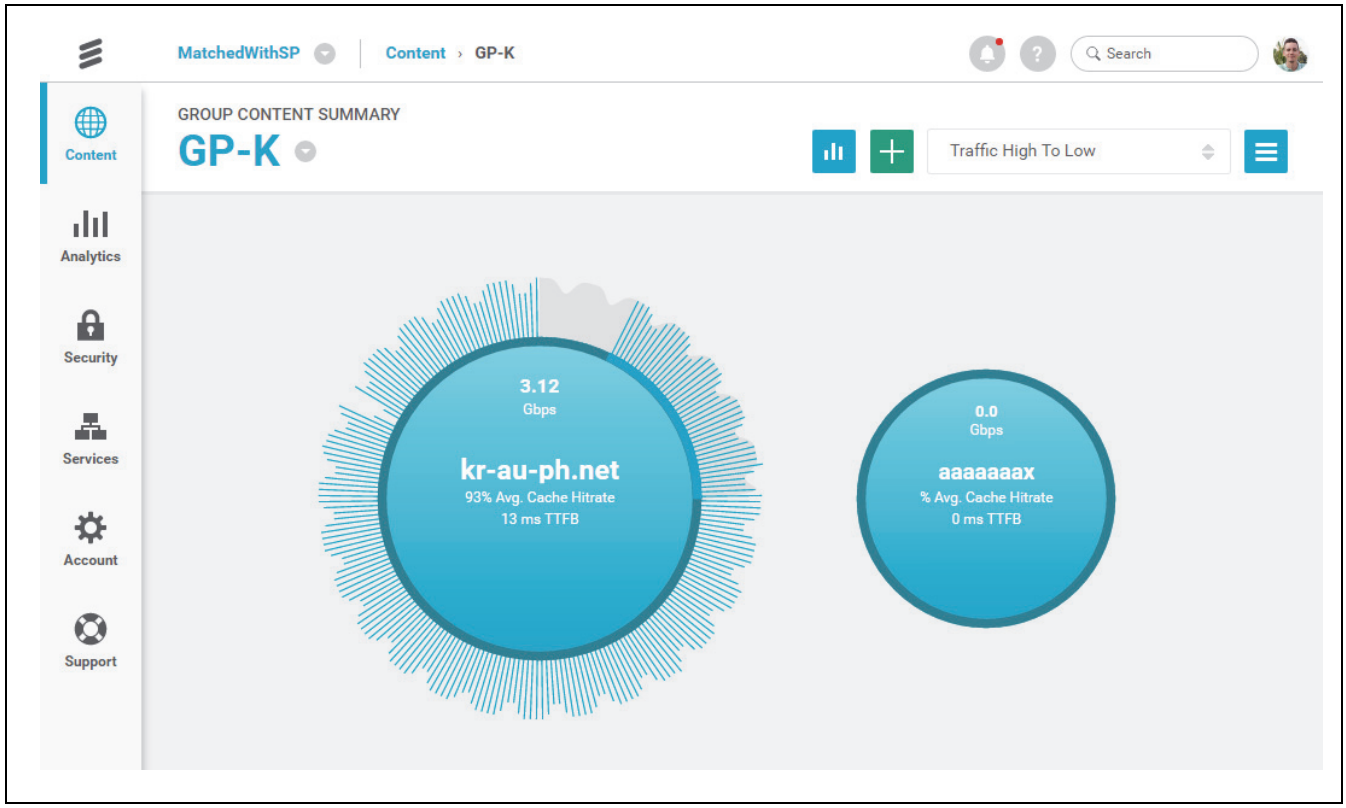
This chapter contains the following sections:

Viewing and Managing Groups

To view and manage Groups:

1. Navigate to the summary page for the desired Account.
2. Select a Group by doing one of the following:
   - Click the selection icon to choose from a drop-down list of Groups.
   - Click the desired Group Starburst to display additional information for that Group.
3. Information for the selected Group displays on the Group Content Summary page (Figure 5-1). This page displays a Starburst for each Property that belongs to the Group.

Figure 5-1: Group Content Summary Page

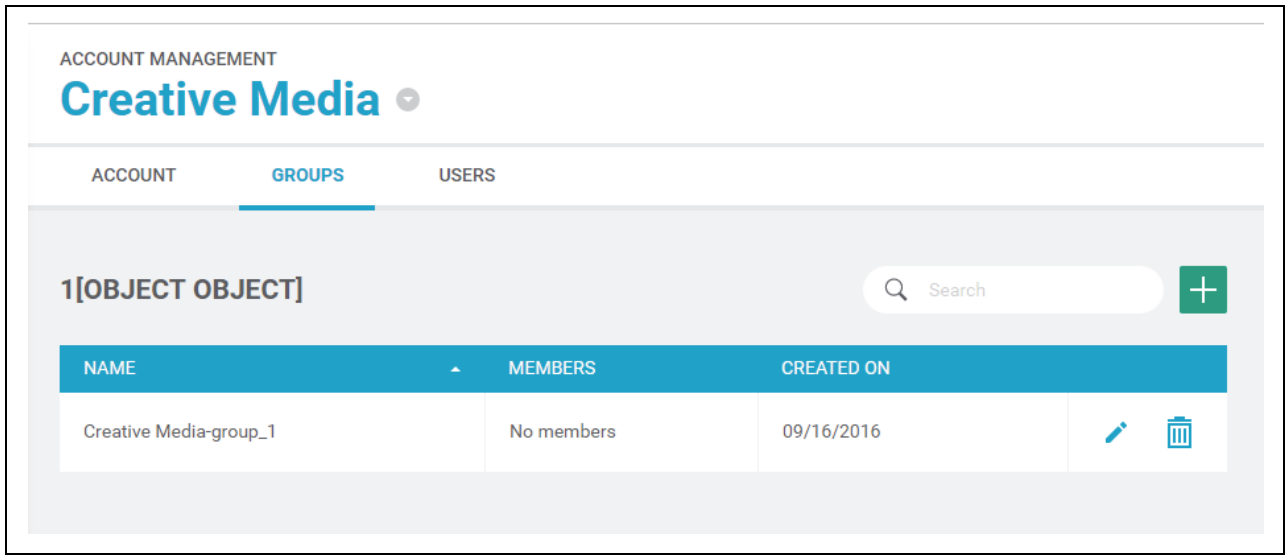


NOTE

If you wish to add or modify the Properties associated with this Group, refer to Chapter 6, "Working with Properties" for further information.

4. Click the Account icon in the left navigation bar. The Account Management page displays.
5. Click the Groups tab (Figure 5-2) to view information about all existing Groups associated with this Account.

Figure 5-2: Account Management: Groups Tab



6. To add a Group:

   NOTE

   Only Users with Admin permissions can add Groups. For more information on User Roles see "Understanding User Roles and Permissions".

   a. Click the Add (+) icon.
   b. Enter the Name of the Group
   c. Click Save to save your changes, or click X to cancel the operation.

7. To edit a Group:

   NOTE

   Only Users with an Admin Role can edit Groups. For more information on User Roles see "Understanding User Roles and Permissions".

   a. Locate the row associated with that Group in the table.
   b. Click the Edit (pencil) icon at the end of that row.
   c. Edit the Name of the Group.
   d. Click Save to save your changes, or click X to cancel the operation.

Deleting a Group

The Portal allows users with the appropriate privileges to delete Groups. Note that when you delete a Group, any Properties associated with that Group are also deleted.

CAUTION

Delete with caution: you cannot restore a deleted Group.

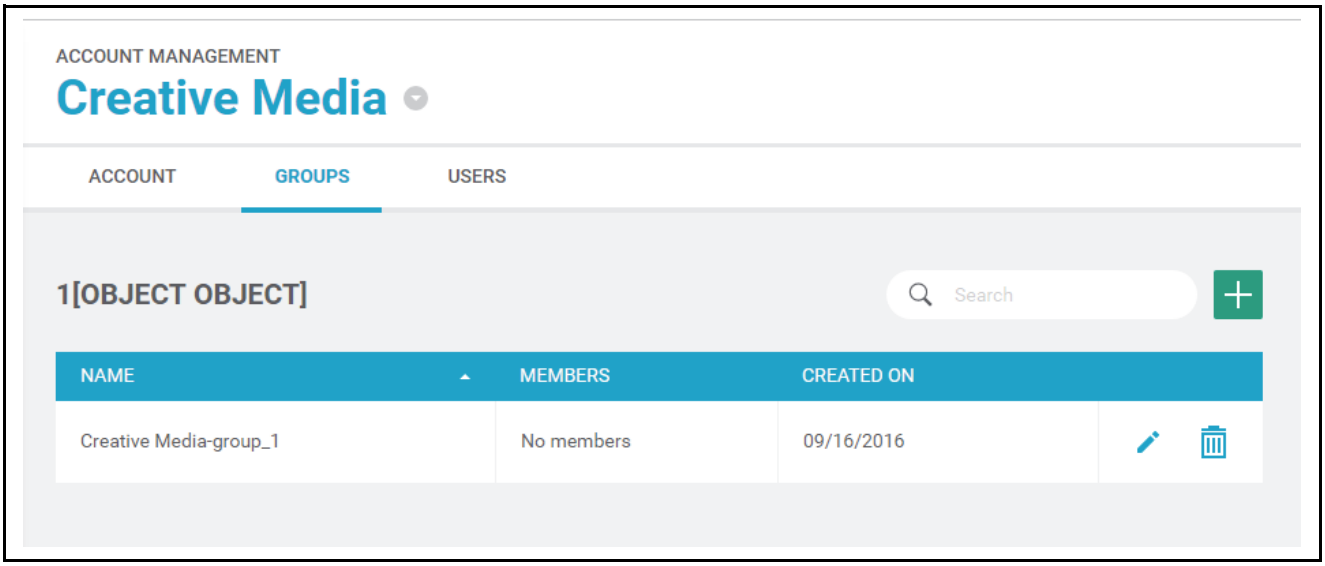
NOTE

Only Users with an Admin Role can delete Groups. For more information on User Roles see "Understanding User Roles and Permissions".

To delete a Group:

1. Navigate to the summary page for the desired Account.
2. Click the Account icon in the left navigation bar. The Account Management page displays.
3. Click the Groups tab.

Figure 5-3: Account Management: Groups Tab



1. Locate the row associated with that Group in the table.
2. Click the Delete (trash) icon at the end of that row.
3. Confirm your action to complete the operation.

Chapter 6
Working with Properties

The UDN Administrator Portal is a Graphical User Interface (GUI) web application that serves as the management application for UDN administration, configuration, and monitoring.

Each UDN Property represents a Content Provider's published host name, or the URL of the actual asset to be accelerated. The Portal provides a rich collection of settings to enable you to specify the unique parameters associated with each Content Provider's Property.

> NOTE
>
> If you want to specify caching polices, see Chapter 7, "Managing Cache Content" for detailed instructions.

This chapter contains the following sections:

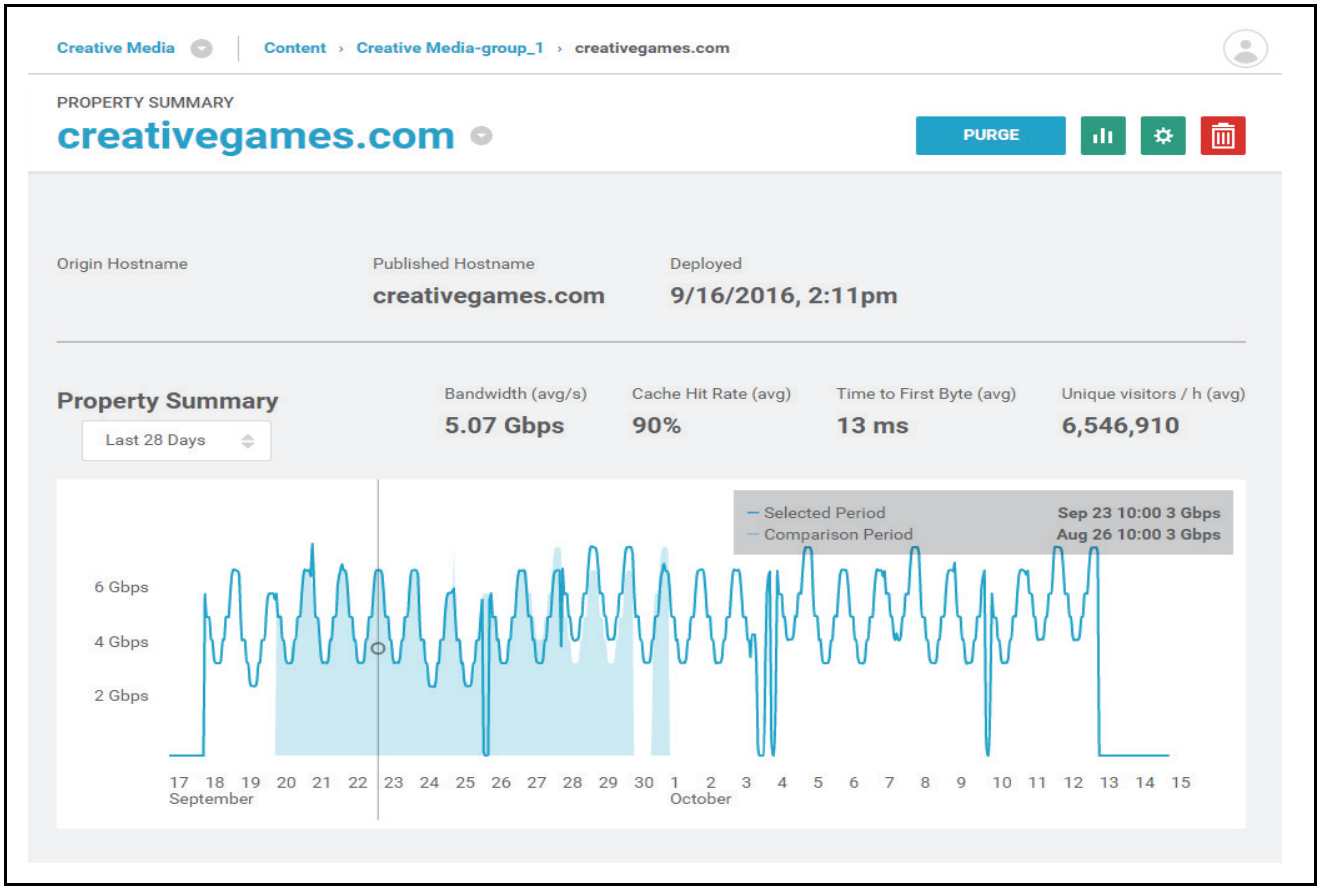
Viewing Properties

To view and manage a Property:

1. Navigate to the summary page for the desired Account.
2. Navigate to the Group to which the desired Property belongs by doing one of the following:
   - Click the selection icon to choose from a drop-down list of Groups.
   - Click the desired Group Starburst to display information for that Group.
3. Navigate to the desired Property by doing one of the following:
   - Click the selection icon to choose from a drop-down list of Properties.
   - Click the desired Property Starburst to display information for that Property.

   The Property Summary page displays (Figure 6-1).

Figure 6-1: Property Summary Page

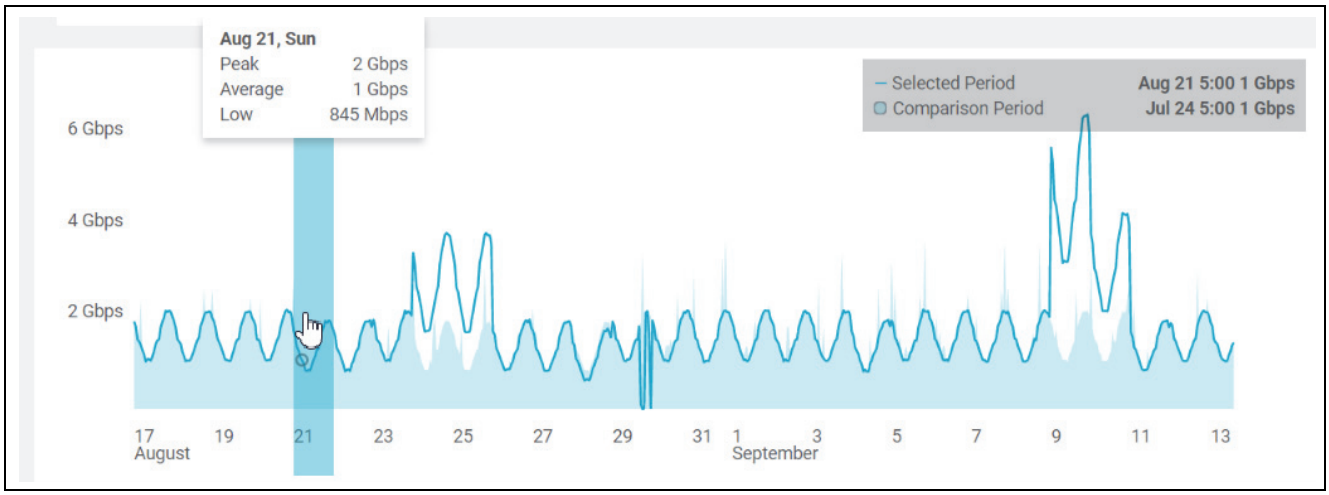


At the top of the summary, the Portal displays the Origin Hostname, the Published Hostname, and the date the Property was deployed.

Below that is a drop-down selector that enables you to choose the period of time for which you want to display data.

4. The chart at the top of the summary page provides additional detail on a specific day when you hover over any portion of the graph (Figure 6-2).

Figure 6-2: Property Summary Graph



NOTE

When you hover over a specific date, then click on it, the graph will zoom in to show data for that day.

The Property Summary page displays the following information about the Property:

Table 6-1: Property Summary Information

Information	Description
Property Name	The name of the Property, followed by a drop-down icon that enables you to select any other Property in that Group.
Origin Hostname	The URL of the origin associated with the Property.
Published Hostname	The hostname associated with the Property.
Current Version	The current version of the Property configuration.
Deployed date	The date of this Property's configuration deployment.
Property Summary date range selector	Enables you to specify the date range to display in the chart below. You can choose to view data for the Last 28 Days, or to specify a Custom Date Range.
Bandwidth (avg/s)	The average bandwidth over the specified date range.
Cache Hit Rate (avg)	The average cache hit rate for this Property over the specified date range.
Time to First Byte (avg)	The average TTFB over the specified date range.
Unique Visitors / hour (avg)	The average number of unique visitors per hour over the specified date range.

5. There are icons at the upper right which enable you to access other Portal features, enabling you to:
   - Purge content from the Property, as described in "Purging Cache Content" in Chapter 7.
   - Generate reports for traffic associated with this property, as described in Chapter 3, "Generating Reports"

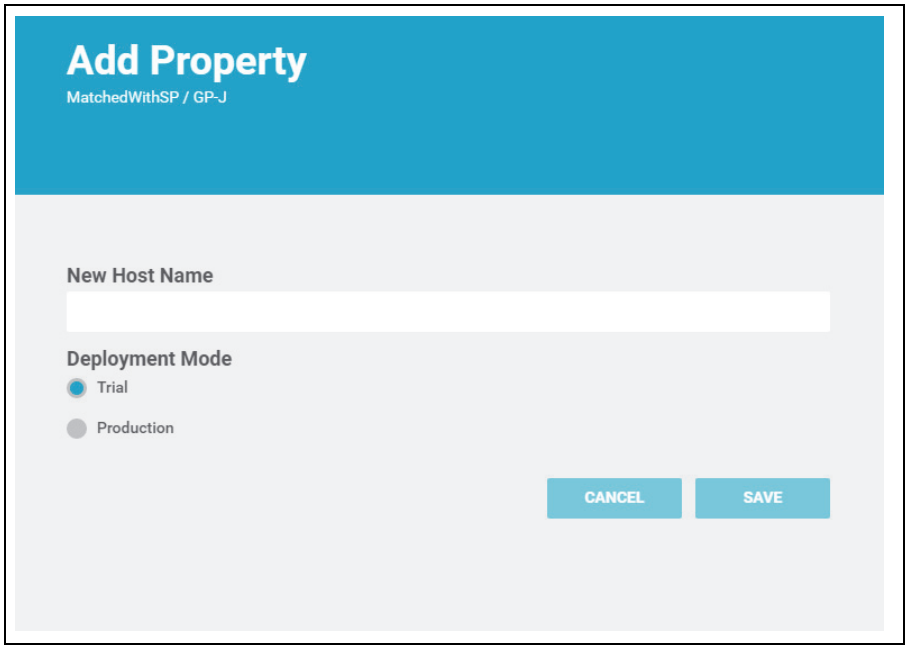
Adding a Property

Only Users with an Admin Role can add Properties. For more information on User Roles see “Understanding User Roles and Permissions”.

To add a Property:

1. Navigate to the Group to which you want to add the Property.
2. At the upper left of the Group Summary page, click the Add (+) icon.
3. The Add Property page displays ().

Figure 6-3: Add Property



4. Enter the Host Name for the new Property.
5. Select the Deployment Mode for this Property.
6. Click Save.
7. Once you have created your Property, you can customize its settings. For detailed information, see “Modifying Property Hostname Settings”.

Modifying Property Hostname Settings

When initially configuring a property, or modifying an existing property, you can modify hostname settings. These settings enable you to specify origin, host header, and hostname information.

NOTE

Only Users with an Admin Role can modify Properties. For more information on User Roles see "Understanding User Roles and Permissions".

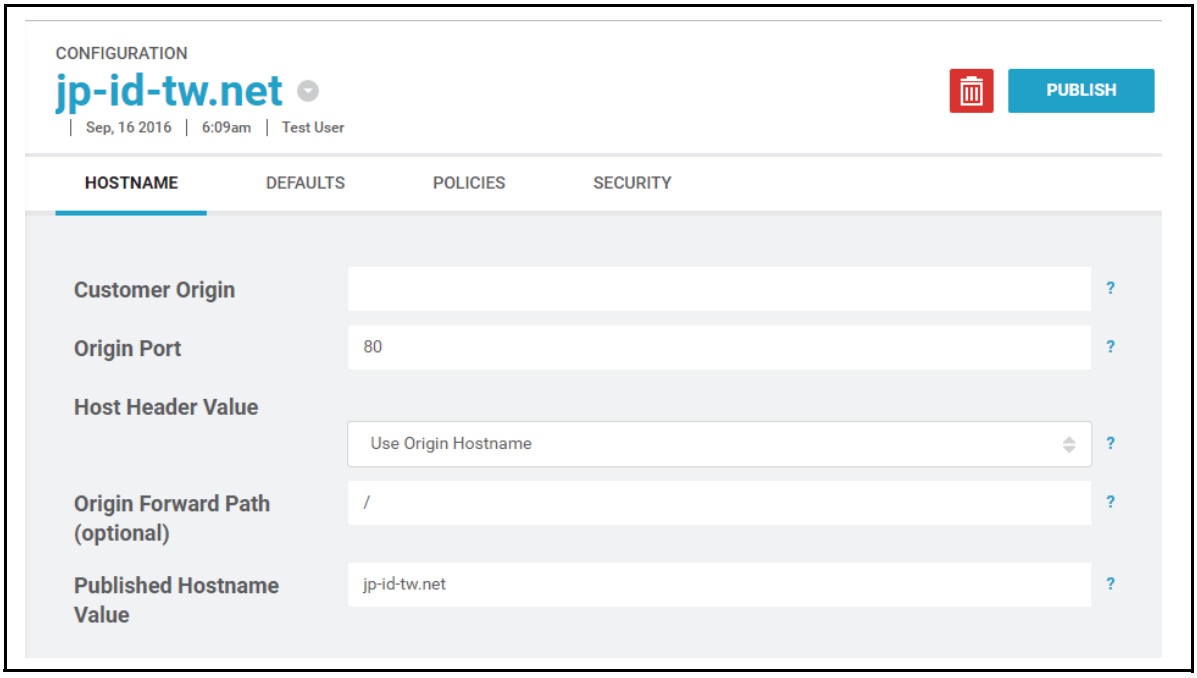
To modify Property hostname settings:

1. Navigate to the Group to which the Property belongs.
2. Locate the desired Property, then click the Configure icon.

   You can find this icon on the Table View row for a specific Property, or at the top of a Property Summary page. To access this icon on a Starburst page, hover over the center of the Starburst for that Property until the Configure icon displays.

3. Click the Hostname tab in order to view Hostname settings for this Property (Figure 6-4).

Figure 6-4: Property Configuration Page: Hostname Tab



4. Specify the URL for the Customer Origin, which is the web server that holds the CP content.

   The Customer Origin is the publicly addressable location of the web server from which the UDN platform will retrieve content for delivery to end users.

   This address can be either a fully qualified domain name or an IP address. Typically, the customer origin is a subdomain of the delivery domain such as origin.example-domain.com.

5. Specify the Origin Port.

   By default, the UDN platform will use port 80 to fetch HTTP content and port 443 to fetch HTTPS content.

6. Specify the Host Header Value, which is the value that the UDN caching server will use for the origin host name.

   You can choose from three options:

   - Select Use Other Hostname Value in order to specify a custom value, which you do in the field that displays after you select this option.
   - Select Use Origin Hostname in order to use the Customer Origin specified on this tab as your Host Header Value.
   - Select Use Published Hostname in order to use the Published Hostname Value on this tab as your Host Header Value.

7. The Origin Forward Path is an optional setting that should only be used if the content on the origin does not use the same request path as the end user request path.

   By default, the Origin Forward Path will be set to the path of the end user URL request.

   If you want to specify a separate request path, do so here.

8. The Published Hostname Value is the hostname used to deliver content to the end users (sometimes called a Vanity Hostname). This Published Hostname must be a sub-domain value.

   NOTE

   The Published Hostname Value cannot be modified in this version of the Portal.

9. When finished, click Save.

Modifying Property Default Settings

When initially configuring a property, or modifying an existing property, you need to modify default settings associated with cache control.

NOTE

Only Users with an Admin Role can modify Properties. For more information on User Roles see "Understanding User Roles and Permissions".

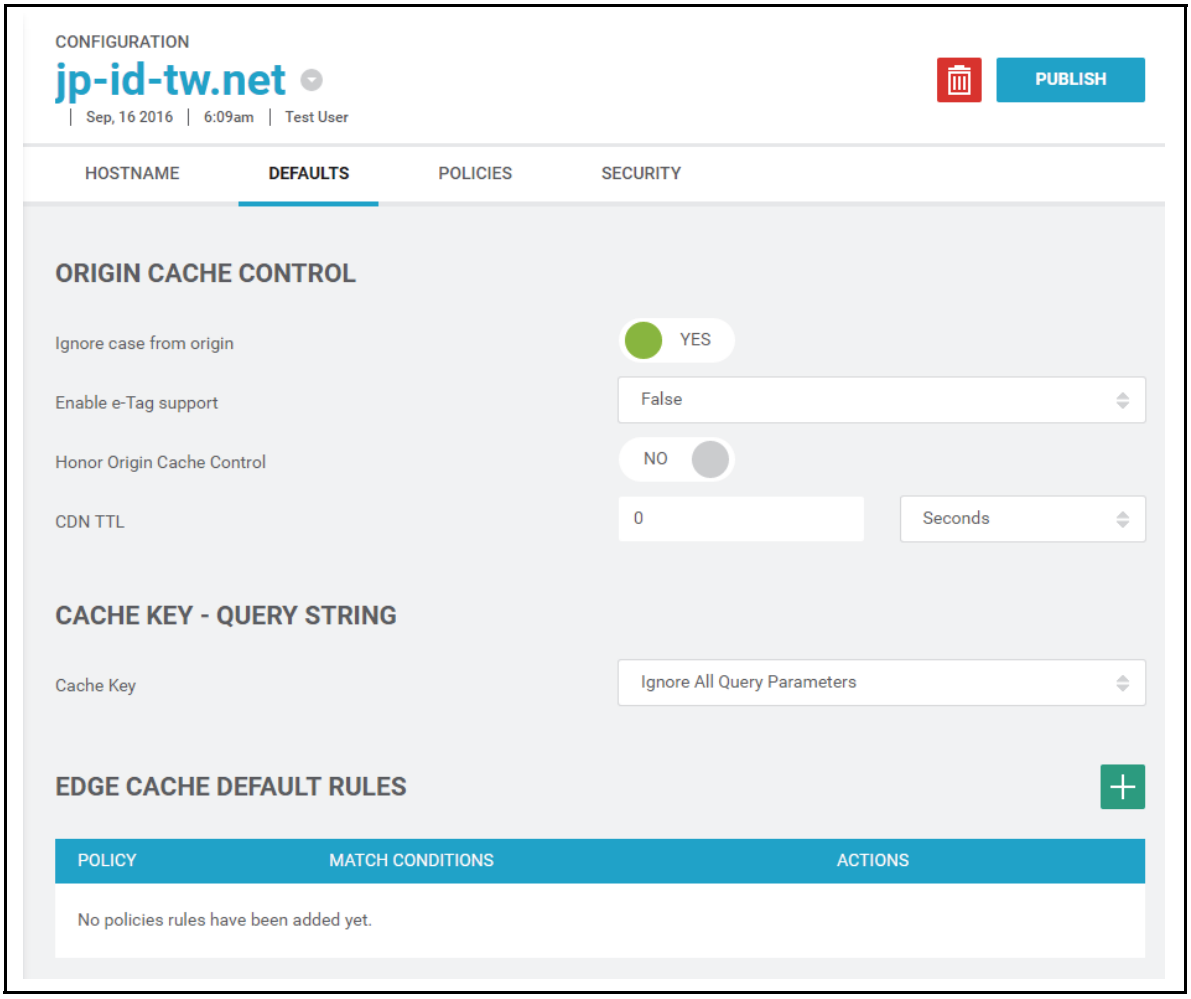
To modify Property hostname settings:

1. Navigate to the Group to which the Property belongs.
2. Locate the desired Property, then click the Configure icon.

   You can find this icon on the Table View row for a specific Property, or at the top of a Property Summary page. To access this icon on a Starburst page, hover over the center of the Starburst for that Property until the Configure icon displays.

3. To Configure Property Default settings, click the Defaults tab (Figure 6-5).

Figure 6-5: Property Configuration: Defaults Tab



4. Set “Ignore Case from Origin” to either Yes or No.

   This setting provides support for situations where content received from the origin is case sensitive.

5. Set the type of e-tag Support for the origin cache.

   This setting specifies whether the origin supports entity tags in the HTTP header. E-tag usage is one of several mechanisms that HTTP provides for web cache validation, which allows a client to make conditional requests. This allows caches to be more efficient, and saves bandwidth, as a web server does not need to send a full response if the content has not changed.

   You can choose from the following settings:

   - Strong
   - Weak
   - False

6. Specify whether or not to Honor Origin Cache Control.

   This setting determines whether cache control settings in the HTTP header, which affect control of the cache from the origin, are to be honored.

   In some cases, the Origin is used for multiple purposes, not just as a caching origin, and these values may not apply to UDN usage.

7. Specify the CDN Time To Live (TTL) value:

   This TTL setting specifies the period of time (specified in seconds, minutes, hours, or days) that the cached object will remain valid in the cache. Once a cached object is no longer valid, that object will be fetched from the origin when it is next requested.

   If no cache rule match is found in the configuration, or if UDN is instructed to use the Origin's cache control policy and there is no explicit maximum age value, the CDN Time-to-Live (TTL) value will be applied.

8. The middle section of the Defaults tab enables you to specify cache key settings to modify caching behavior. By default, the entire query string value, along with the URL path, is utilized as the cache key value.

   To specify the cache key query string, select the appropriate cache key control:

   - Include all query parameters
   - Ignore all query parameters
   - Include some parameters

   If you choose “Include Some Parameters”, specify one or more Query names (parameters) associated with this caching behavior.

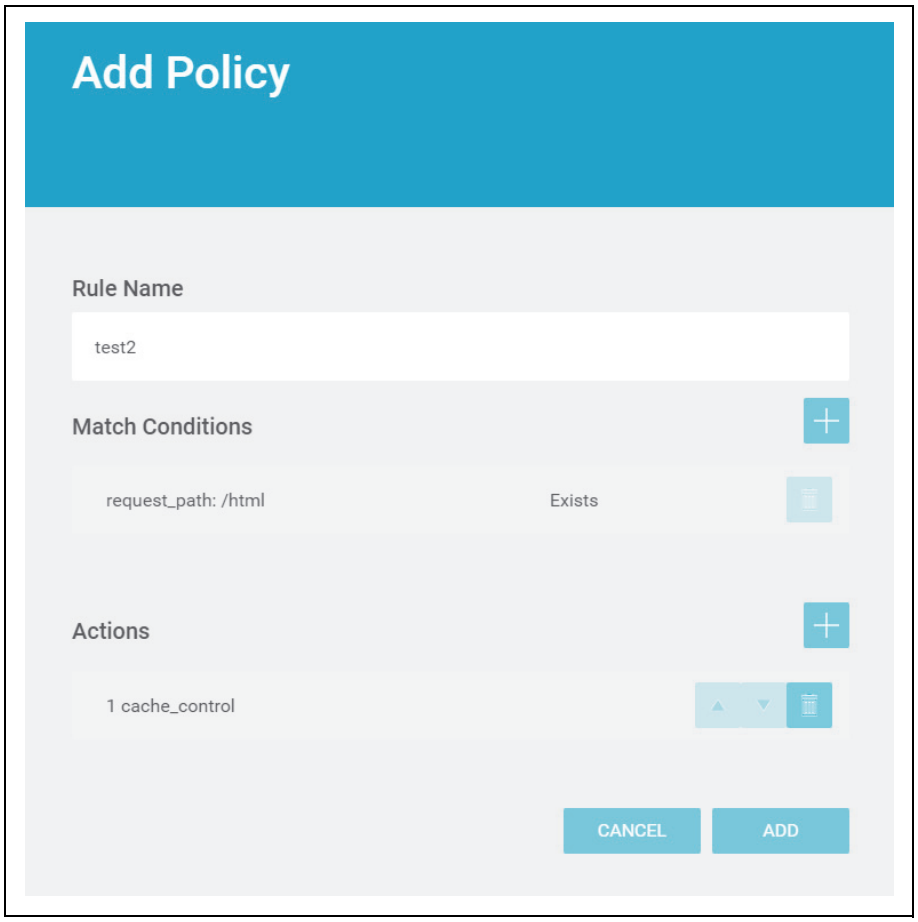
9. Finally, on the Defaults tab, specify Edge Cache Default Rules (policies).

   To manage Edge Cache Default Rules:

   a. Do one of the following:
      - To add a new policy, click the Add (+) icon.
      - To modify an existing policy, locate the policy in the table and click Edit on that row.

      The Add or Edit Policy dialog box displays.

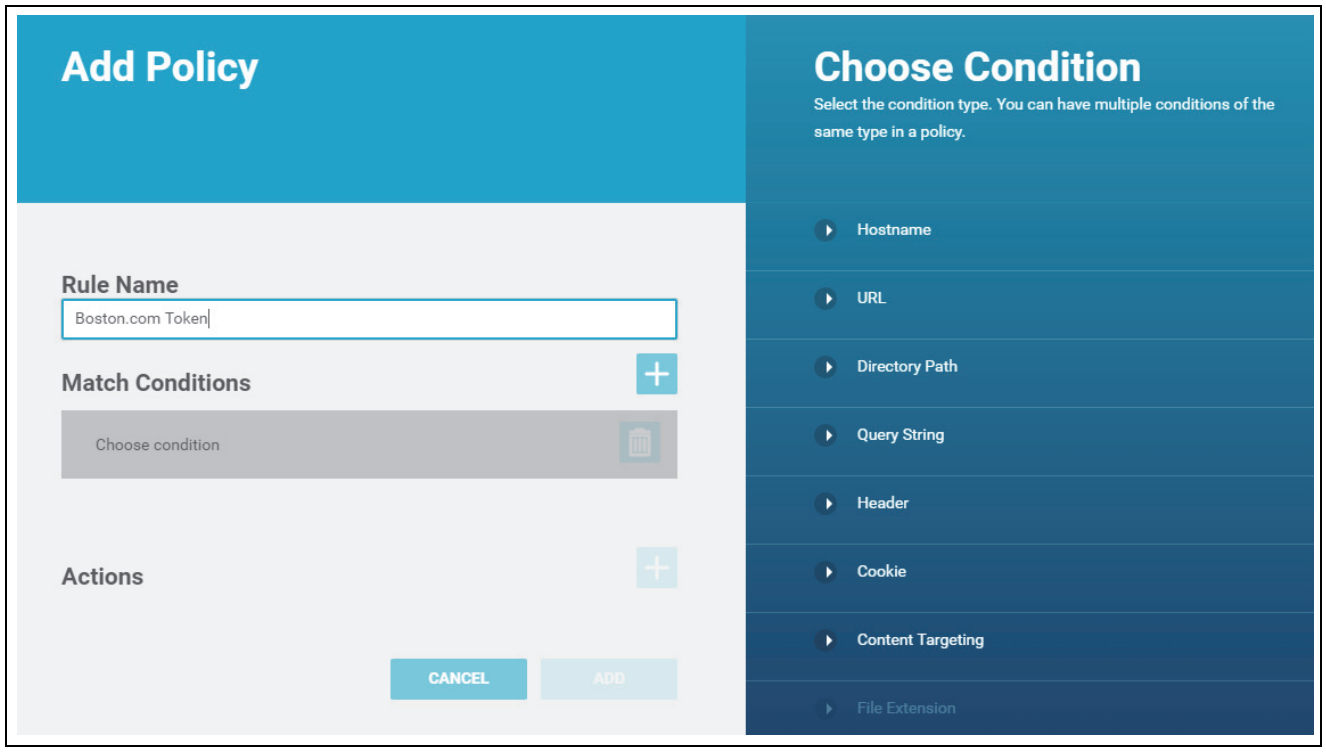
Figure 6-6: Add Policy Screen



b. Specify a name for the Rule you are adding to the Policy. Consider adopting a meaningful naming convention that lets you uniquely identify rules based solely on their name.

c. If the Choose Condition modal window is not already showing, click the Add (+) icon to the right of the Match Conditions label. The Choose Condition modal window displays (Figure 6-7). Now you must specify the first Match Condition associated with your Policy.

Figure 6-7: Add Policy: Choose Condition Modal Window



Click to select the condition you want associated with this rule. You can specify conditions associated with a Hostname, Directory Path, Query String, Header, Cookie, or Content Targeting.

When you define a condition, for each condition type, you must indicate the text the system will search for within the content request, and under what conditions you want the system to trigger the policy. For example, you could choose to have a policy apply only when a specific directory path does not exist in the content request. Or you could choose to have a policy apply only when a content request contains a specified query string. The available conditions are listed in Table 6-2.

Table 6-2: Specifying Policy Match Conditions

Condition Type	Condition Text	Match Types (Choose One)
Hostname	Enter the host name.	• Exists • Does Not Exist
URL	Enter the URL.	The policy applies when the specified URL matches the content URL.
Directory Path	Enter the directory path.	• Exists • Does Not Exist
Query String	Enter the query string.	• Exists • Does Not Exist • Contains • Does Not Contain

Table 6-2: Specifying Policy Match Conditions *(Continued)*

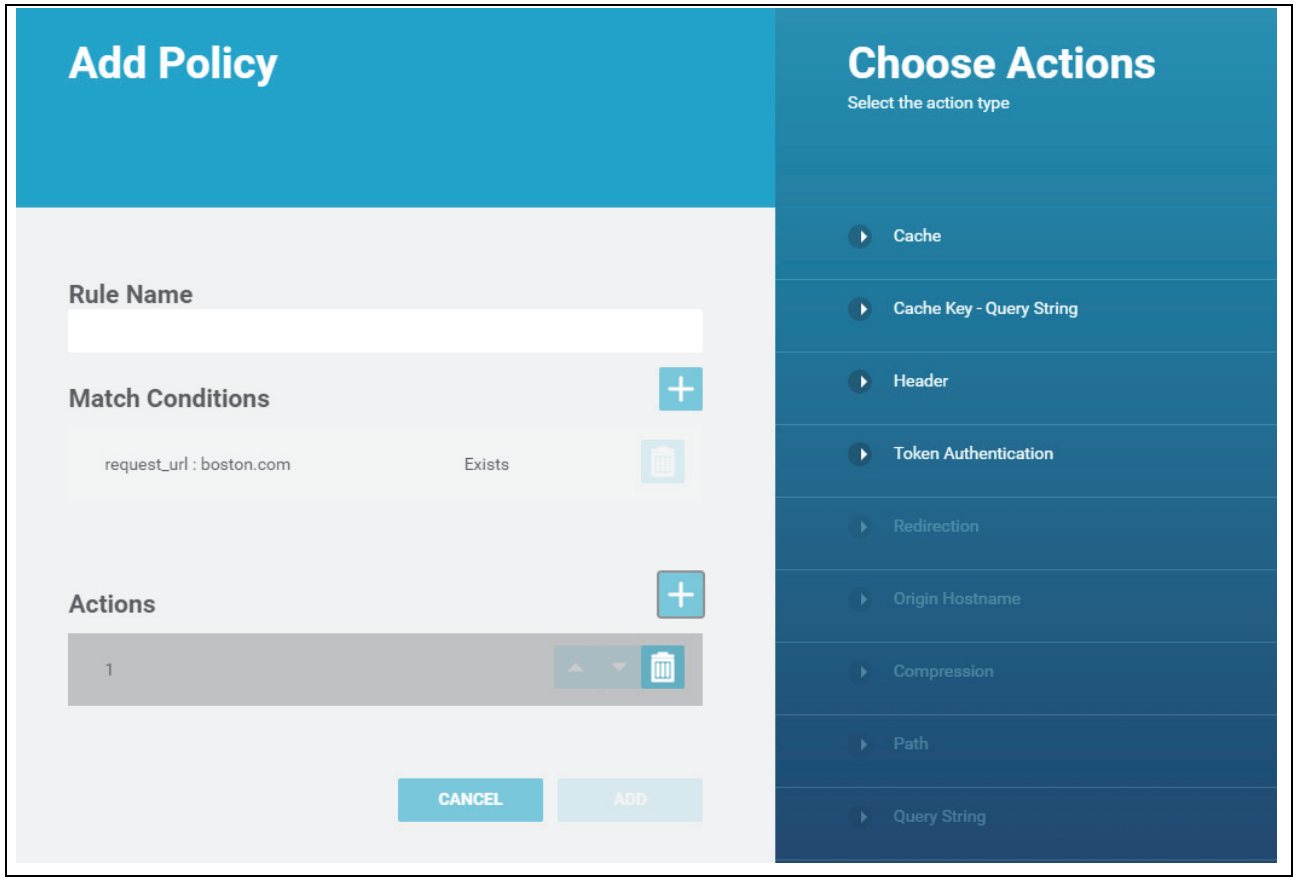
Condition Type	Condition Text	Match Types (Choose One)
Header	Enter the header.	• Exists • Does Not Exist • Contains • Does Not Contain
Cookie	Enter the name of the cookie.	• Exists • Does Not Exist • Contains • Does Not Contain
Content Targeting	Enter a list of areas to include in the policy, separated by commas. Enter a list of areas to exclude from the policy, separated by commas.	The policy applies to content being requested from areas included in the policy. The policy is not applied to content being requested from areas excluded from the policy.

- When finished, click Save Match.
- Create additional matches, if needed, for this Policy Rule.

d. To specify the Action the system will take when the match condition is met:

- Click the Add (+) icon to the right of the Actions label. The Choose Action modal window displays.

Figure 6-8: Policy Rule: Choose Action Modal Window

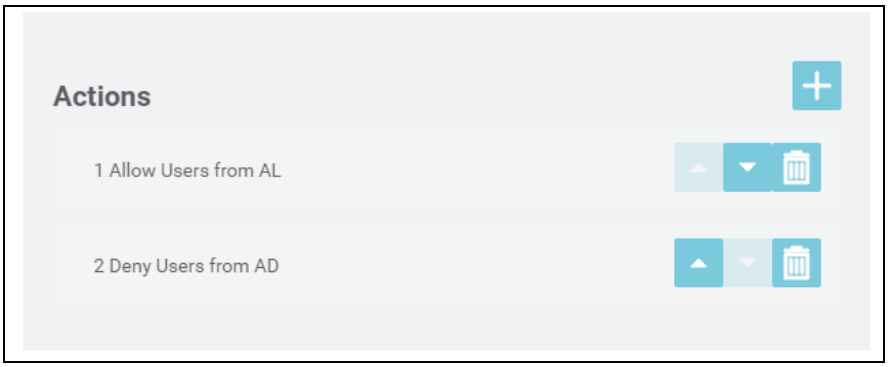


- Select the Action Type you want associated with this rule. This selection specifies the type of action you want the UDN system to take when the match conditions are met. You can select Cache, Cache Key - Query String, or Header.
- Enter the caching action you want taken.
- When finished click Save Action.
- If you wish, you may specify additional actions that will trigger when this Policy Rule applies.

10. Once you have finished specifying Match Conditions and Actions for this rule, you may want to change the priority in which they're applied.

    Use the up and down arrows (triangles) to the right of the available Actions or Conditions to organize them in the desired order (Figure 6-9).

Figure 6-9: Ordering Match Conditions



e. When finished specifying information for this Policy Rule, click Add.

Modifying Property Security Settings

If you plan to use UDN to deliver HTTPS Content, you will need to configure Security settings.

NOTE

Only Users with an Admin Role can modify Properties. For more information on User Roles see "Understanding User Roles and Permissions".

To modify Property security settings:

1. Navigate to the Group to which the Property belongs.
2. Locate the desired Property, then click the Configure icon. 

   You can find this icon on the Table View row for a specific Property, or at the top of a Property Summary page. To access this icon on a Starburst page, hover over the center of the Starburst for that Property until the Configure icon displays.

3. To enable HTTPS:
   a. Change the Enable HTTP selector from NO to YES.
   b. Select the appropriate SSL certificate.
   c. Click Save.

NOTE

For information on how to load an SSL Certificate, refer to Chapter 8, "Managing Security Settings".

Publishing Property Settings

Property configuration settings are delivered to UDN Properties by publishing them. By disconnecting the process of modifying and reviewing Property settings from the process of delivering those settings so they take affect, the Portal enables you to modify and review Property settings at your leisure. Note that publishing property settings will not disrupt current content delivery.

NOTE

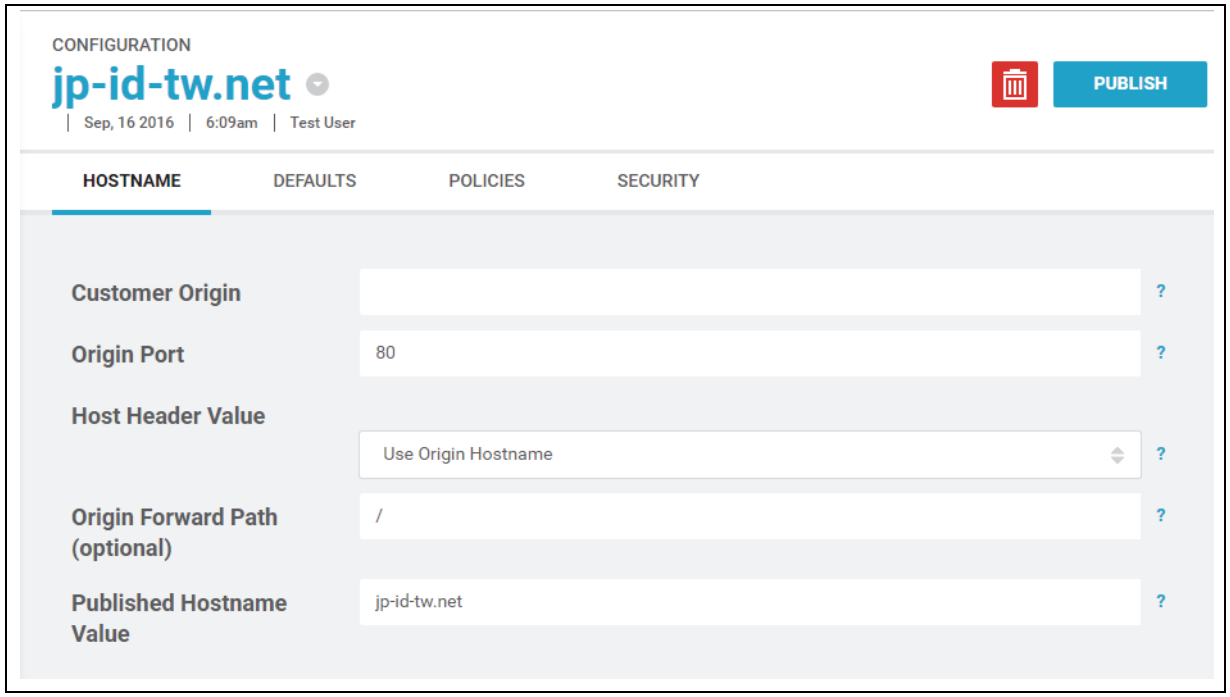
Publish with caution, as there is no current way to roll back publication to a previous configuration.

To publish Property settings:

1. Navigate to the summary page for the desired Property.
2. In the upper right corner of the Property Summary page, click the Configure icon. 

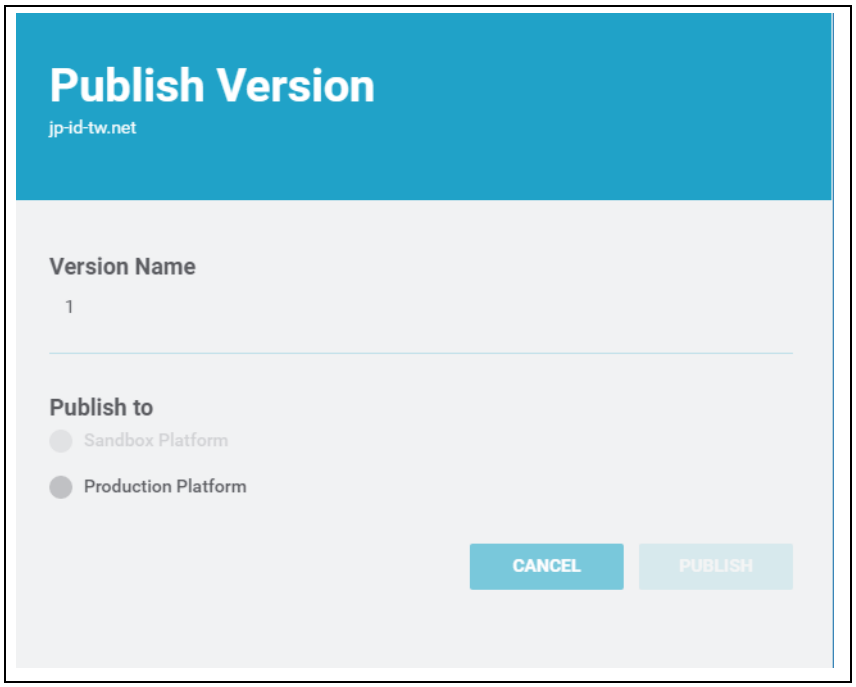
   The Property Configuration page displays (Figure 6-10).

Figure 6-10: Property Configuration



3. Click Publish. The Publish Version page displays (Figure 6-11).

Figure 6-11: Property Settings: Publish Version



4. Select the option to publish to the Production Platform.

   NOTE

   For this version, you can only publish to the Production Platform.

5. Click Publish.

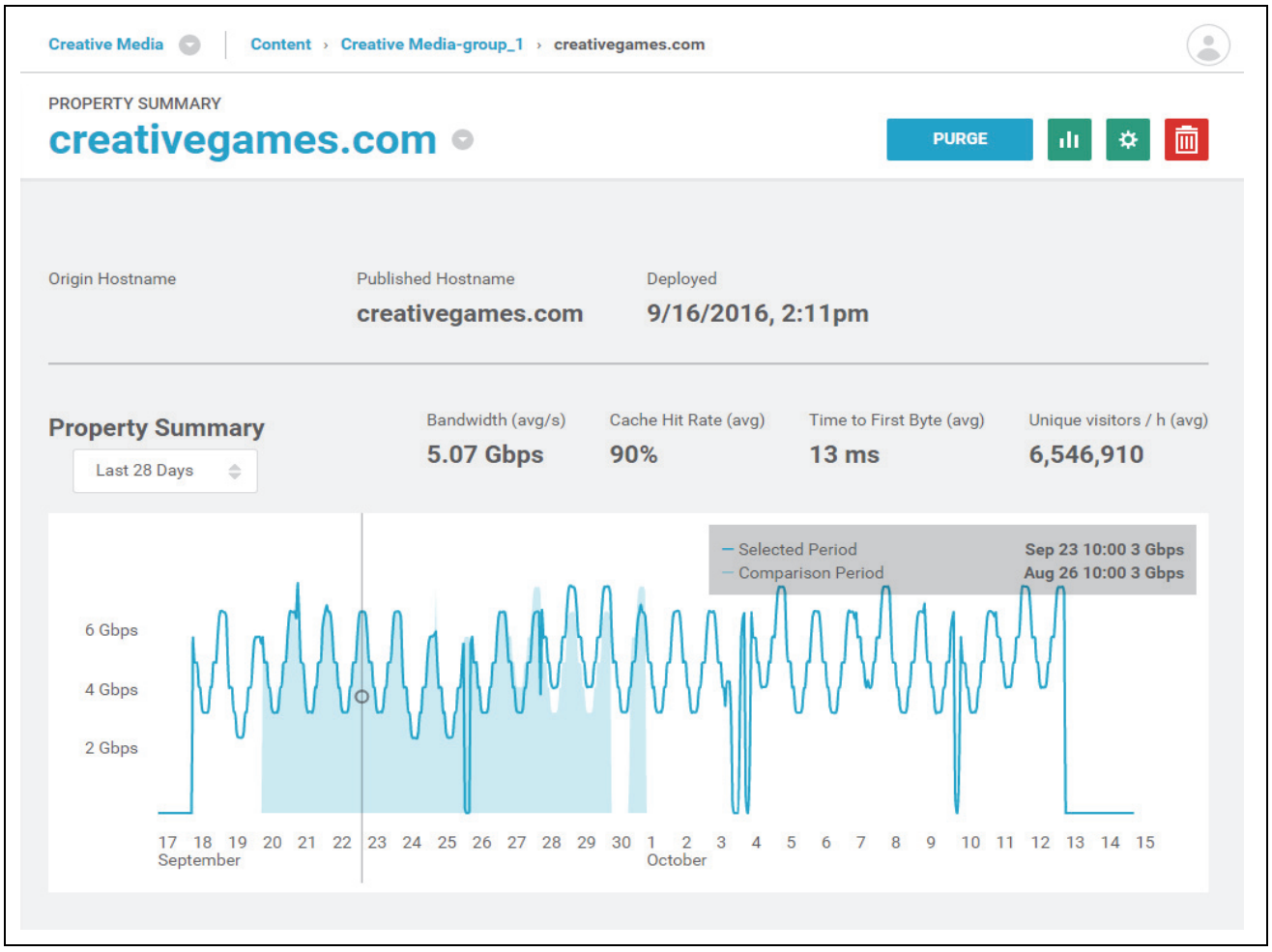
Deleting a Property

Only Users with an Admin Role can delete Properties. For more information on User Roles see “Understanding User Roles and Permissions”.

To delete a Property.

1. Navigate to a page where you can view the desired Property.
2. Click the Configure (gear) icon for the Property. The Property Summary page displays (Figure 6-12).

Figure 6-12: Property Summary Page



3. Click the Delete (trash) icon.
4. Confirm your selection to complete the operation.

Chapter 7
Managing Cache Content

Once an object is cached, ordinarily it remains in the cache until it expires or is remove to make room for new content. At times, you will want to remove content from the cache prior to its normal expiration time. You can choose to purge this content, removing it from the cache, or invalidate the content, by forcing it to be ignored by the cache.

Policies enable you to control content caching for a specific Property. You can specify conditions associated with Property content, and the actions you want UDN to take when those conditions are met. Cache Control rules defined in the Portal are pushed out to the UDN production environment.

This chapter contains the following sections:

Caching Policy Overview

For greater content caching control, a single Policy can include multiple match conditions and multiple actions. Note that the actions associated with a Policy Rule are not triggered unless the requested content meets ALL match conditions specified for that rule.

For example, if you wanted to perform a specific action if a query string was part of the URL for a piece of requested content, then you would specify the query string when defining the policy, and then specify that you want the policy applied when that string is found in the content request. Then you would choose the appropriate action to take when this query string is present. For example, you could specify that the cache freshness value is no-store when in the presence of a particular name-value pairing in the query string.

UDN enables users to define caching policies that are then applied to content requests as they are processed by UDN Properties. Before you configure policies, it is important to know how these policies are defined and applied.

UDN caching policies, or rules, consist of three parts: a unique name, match conditions, and actions.

When you create a policy, Each policy has one or more match conditions. Simply stated, a match condition specifies when the policy will act on a specific content request.

A match condition has three parts. The first is the type of match, which is the type of information you want the policy to act on, such as a Hostname, URL, or Query String. The second is the match string, which is a user-specified string of text that UDN searches for in each content request processed by this Property. The final part enables you to specify when you want the policy activated, such as when the match string is found in the content request, or when it is not found in the content request.

Adding or Modifying a Caching Policy

A policy is a specific action you want the UDN system to take when it encounters a particular set of circumstances. You can define policy rules in the Portal to specify these circumstances, and what you want the cache to do when they occur.

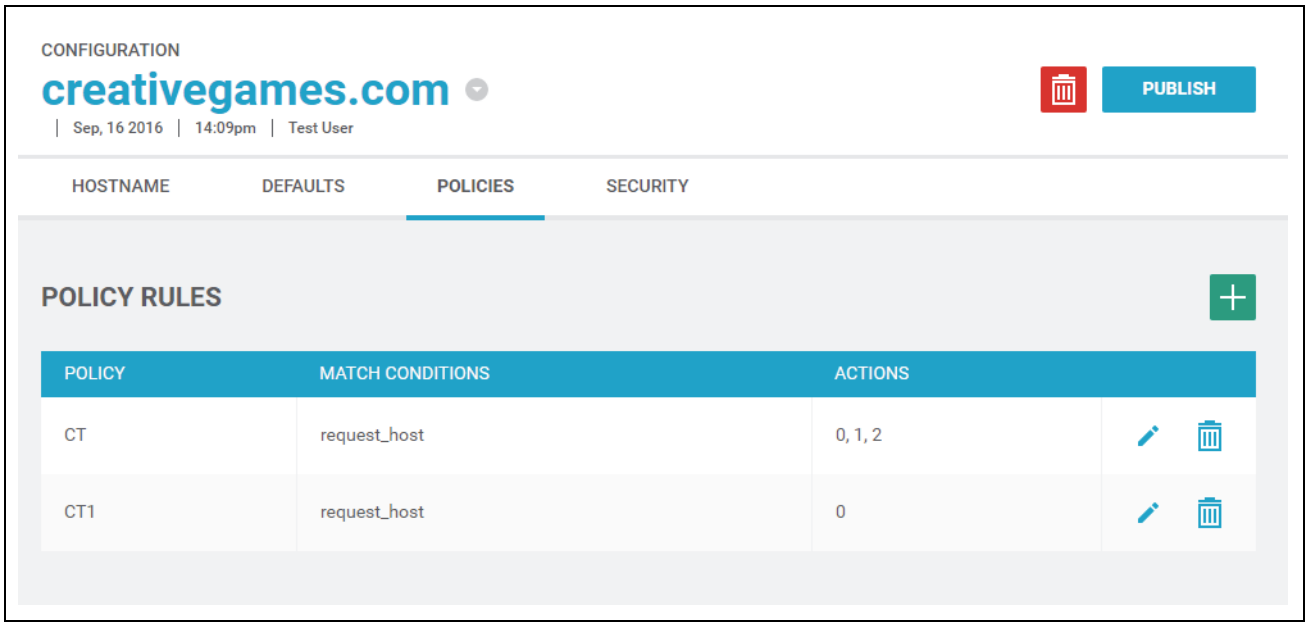
To add or change a caching policy:

1. Navigate to the summary page for the desired Property.
2. Click the Configure icon in the upper left corner of the page.

   The Property Configuration page displays.

3. Click the Policies tab. A list of current Policy Rules displays in table form.

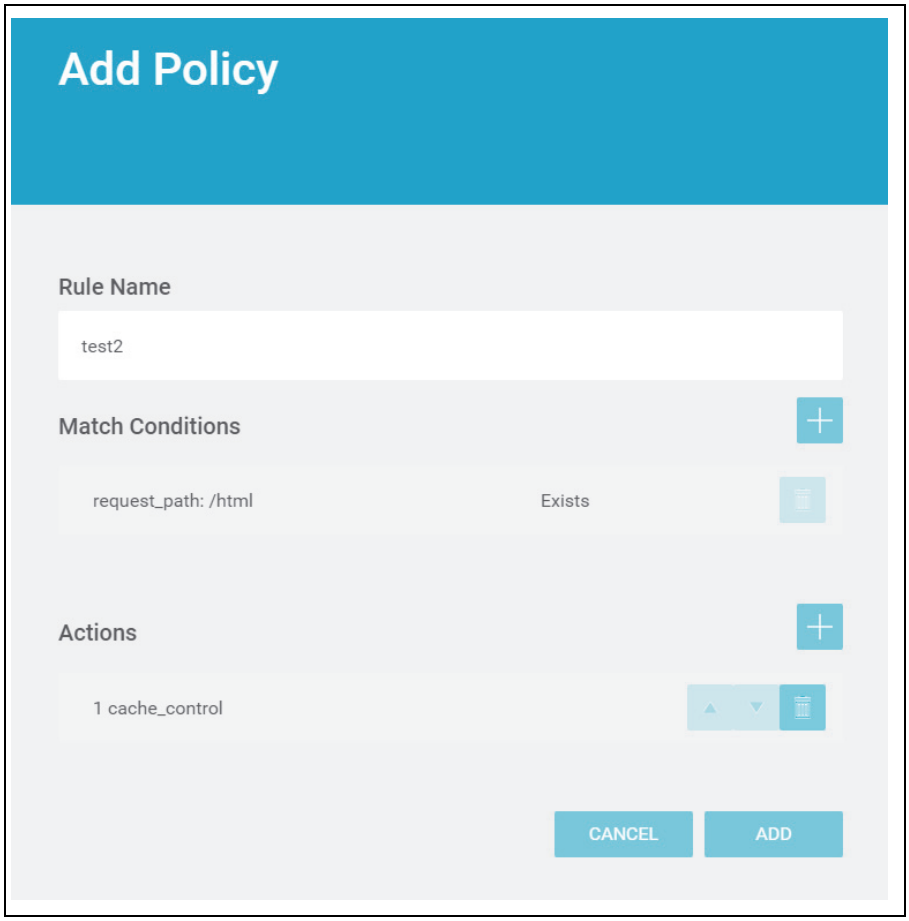
Figure 7-1: Property Configuration: Policies Tab



4. Do one of the following:
   - To add a policy, click the Add (+) icon. The Add Policy window displays.
   - To edit a policy, locate the row associated with that policy in the Policy Rules table and click the Edit (pencil) icon on that row. The Edit Policy window displays.

   The Add Policy and Edit Policy windows are very similar. Figure 7-2 shows the Add Policy window.

Figure 7-2: Add Policy Window

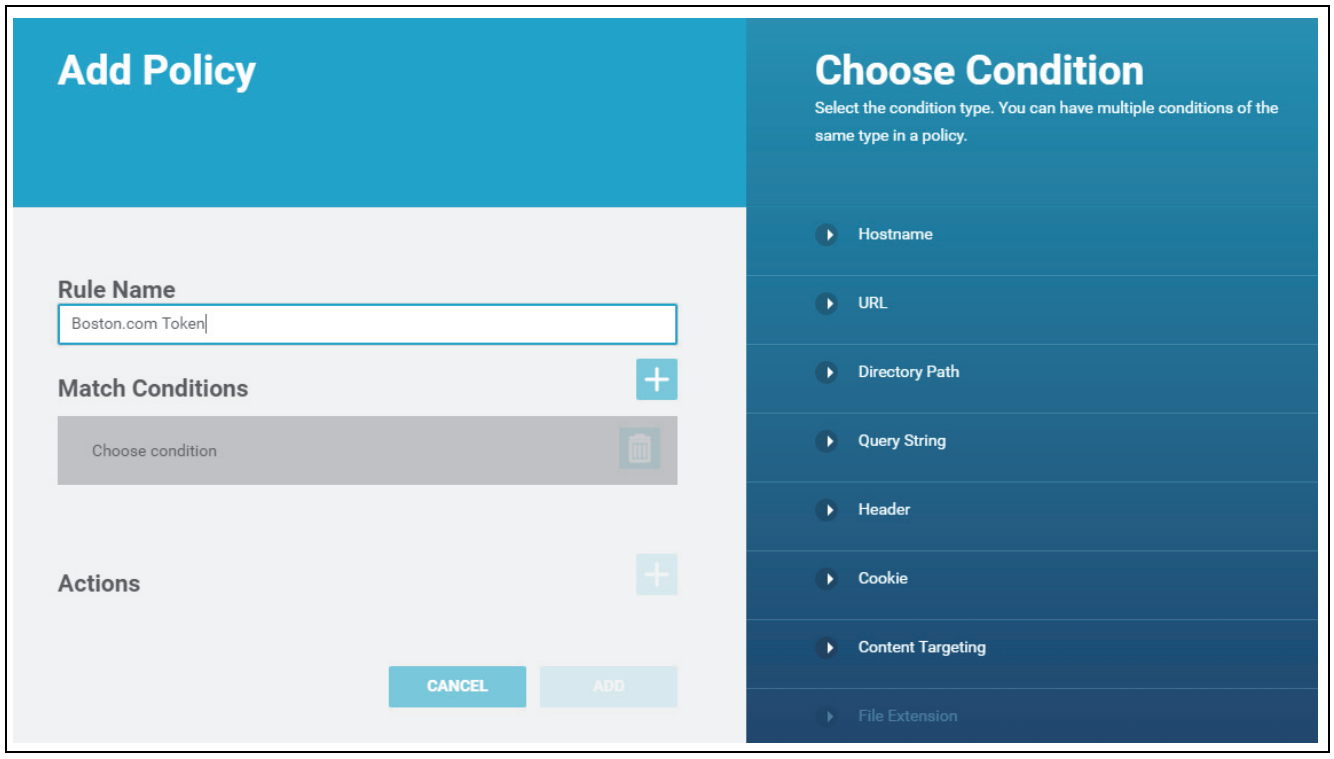


5. Specify a name for the Rule you are adding to the Policy. Consider adopting a meaningful naming convention that lets you uniquely identify rules based solely on their name.
6. Next, specify the match conditions for this rule.

   To specify Match Conditions for this Rule:

   a. Click the Add (+) icon to the right of the Match Conditions label. The Choose Condition modal window displays.

Figure 7-3: Add Policy: Choose Condition Modal Window



b. Click the condition you want associated with this rule. You can specify conditions associated with a Hostname, URL, Directory Path, Query String, Header, Cookie, or Content Targeting.

   A modal window displays that enables you to specify the condition criteria.

c. When you define a condition, for each condition type, you must indicate the text the system will search for within the content request, and under what conditions you want the system to trigger the policy. The available conditions are listed in Table 7-1.

   For example, you could choose to have a policy apply only when a specific directory path does not exist in the content request. Or you could choose to have a policy apply only when a content request contains a specified query string.

Table 7-1: Specifying Policy Match Conditions

Condition Type	Condition Text	Match Types (Choose One)
Hostname	Enter the host name.	• Exists • Does Not Exist
URL	Enter the URL.	The policy applies when the specified URL matches the content URL.
Directory Path	Enter the directory path.	• Exists • Does Not Exist

Table 7-1: Specifying Policy Match Conditions *(Continued)*

Condition Type	Condition Text	Match Types (Choose One)
Query String	Enter the query string.	• Exists • Does Not Exist • Contains • Does Not Contain
Header	Enter the header.	• Exists • Does Not Exist • Contains • Does Not Contain
Cookie	Enter the name of the cookie.	• Exists • Does Not Exist • Contains • Does Not Contain
Content Targeting	Enter a list of areas to include in the policy, separated by commas. Enter a list of areas to exclude from the policy, separated by commas.	The policy applies to content being requested from areas included in the policy. The policy is not applied to content being requested from areas excluded from the policy.

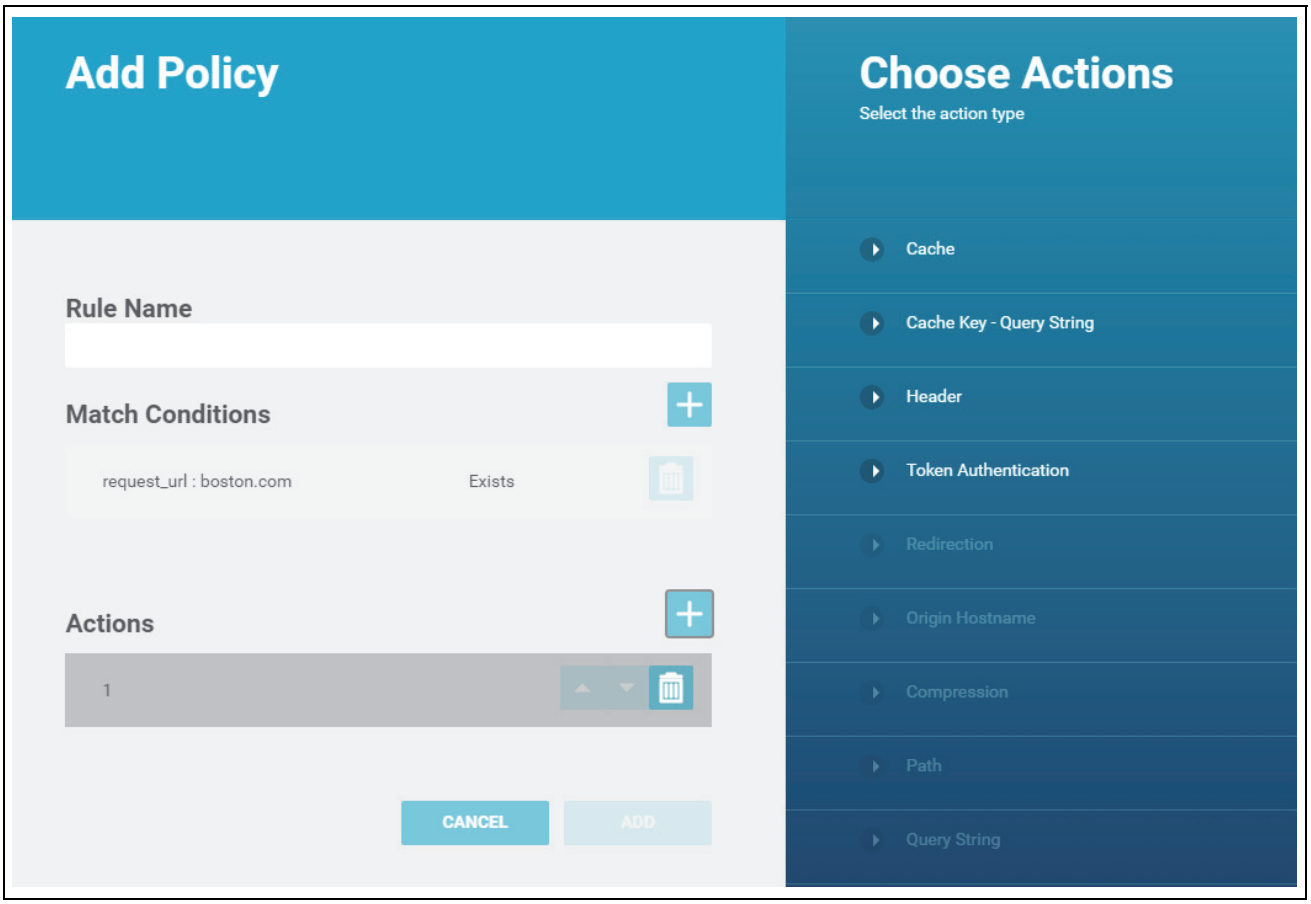
d. When finished, click Save Match.

e. Create additional matches, if needed, for this Policy Rule.

7. To specify the Action the system will take when the match condition is met:

a. Click the Add (+) icon to the right of the Actions label. The Choose Action modal window displays.

Figure 7-4: Policy Rule: Choose Action Modal Window



b. Select the Action Type you want associated with this rule. This selection specifies the type of action you want the UDN system to take when the match conditions are met. You can select Cache, Cache Key - Query String, or Header.

c. Enter the caching action you want taken.

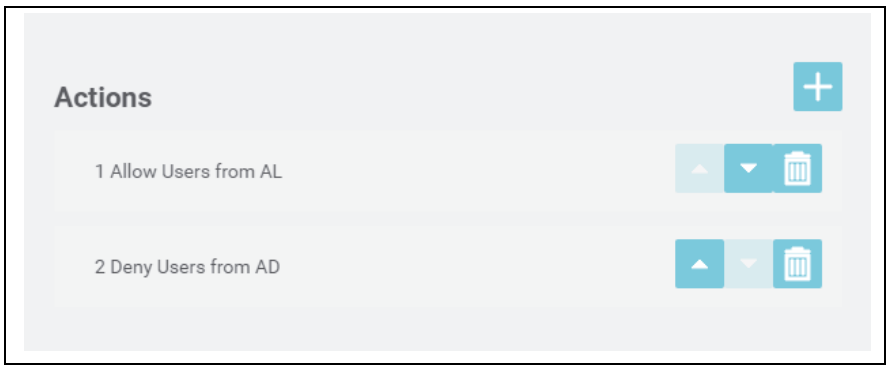
d. When finished click Save Action.

e. If you wish, you may specify additional actions that will trigger when this Policy Rule applies.

8. Once you have finished specifying Match Conditions and Actions for this rule, you may want to change the priority in which they're applied.

   Use the up and down arrows (triangles) to the right of the available Actions or Conditions to organize them in the desired order (Figure 7-5).

Figure 7-5: Ordering Match Conditions



9. When you are satisfied with the Policy Rule settings, click Add.

NOTE

Additions and changes to the list of Policies associated with a Property are not automatically applied to the Property. To apply any Policy updates you have made, you will need to Publish them. For detailed information, see "Publishing Caching Policies".

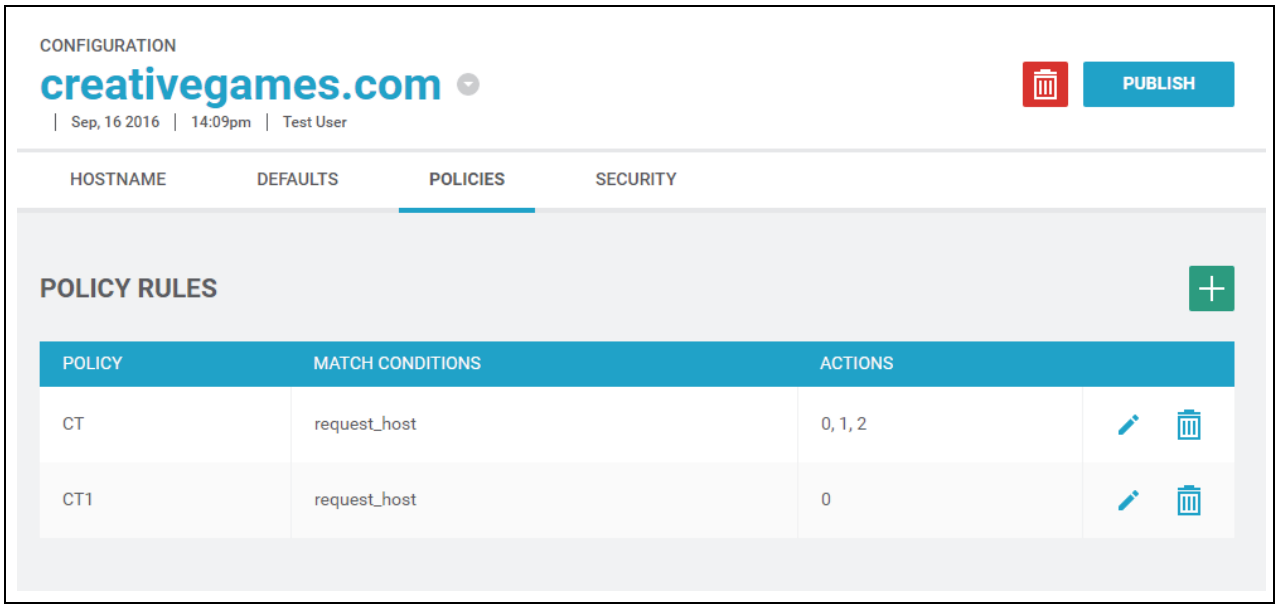
Token Authentication Policy Example

UDN Token Authentication enables content providers (CP) to apply authentication and time-based access restrictions for content acquisition to fulfill end user requests. In these cases a Content Provider creates a URL that requires a token in order to validate an incoming request.

To create a token authentication caching policy:

1. Navigate to the summary page for the desired Property.
2. In the upper right corner of the Property Summary page, click the Configure icon. The Property Configuration page displays.
3. Click the Policies tab. A list of current Policies displays in table form.

Figure 7-6: Property Configuration: Policies Tab

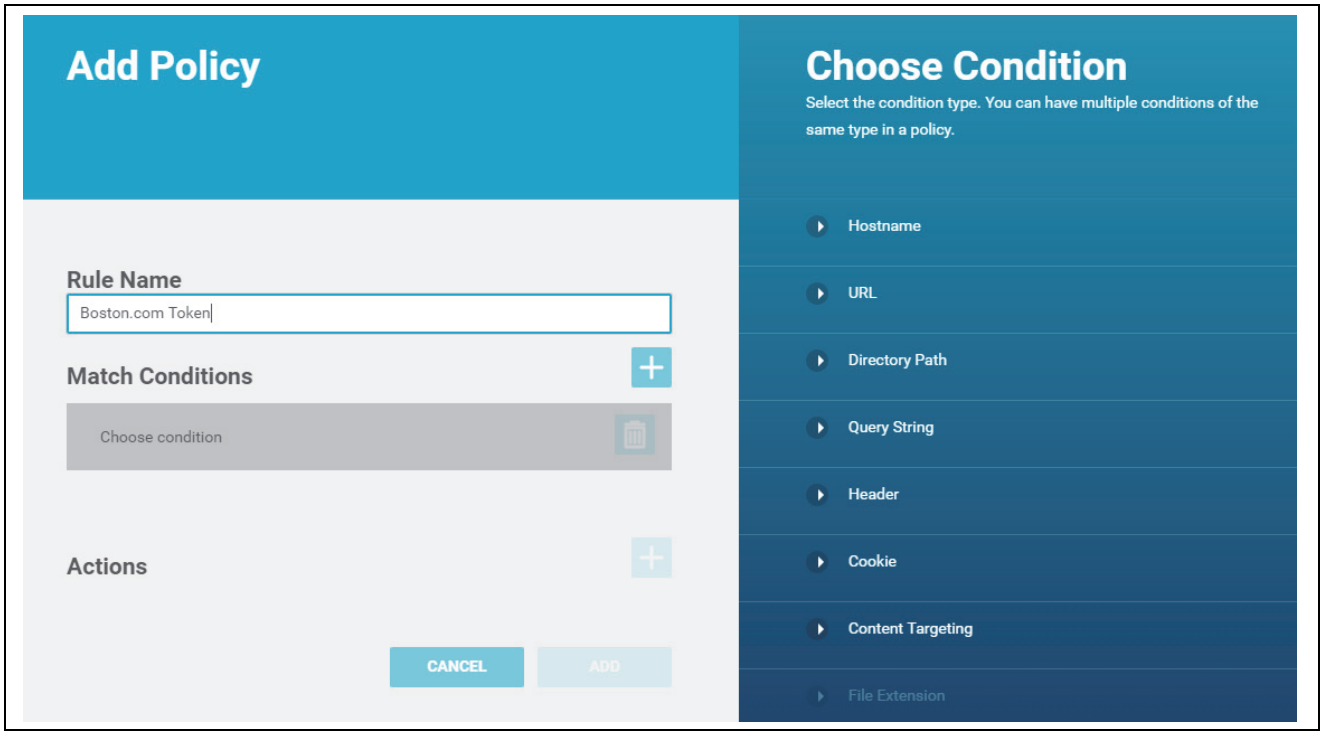


4. To add a new policy, click the Add (+) icon. The Add Policy screen displays (Figure 7-7).
5. Enter a name for the policy Rule. The name should indicate that this is a Token policy for a specific site (URL).
6. The Choose Condition modal window automatically displays when you add a Policy (Figure 7-7).
7. A token authentication policy requires that you specify a URL for the match condition. In the Choose Condition modal window, select URL.
8. Enter the URL when prompted, then click Save.

NOTE

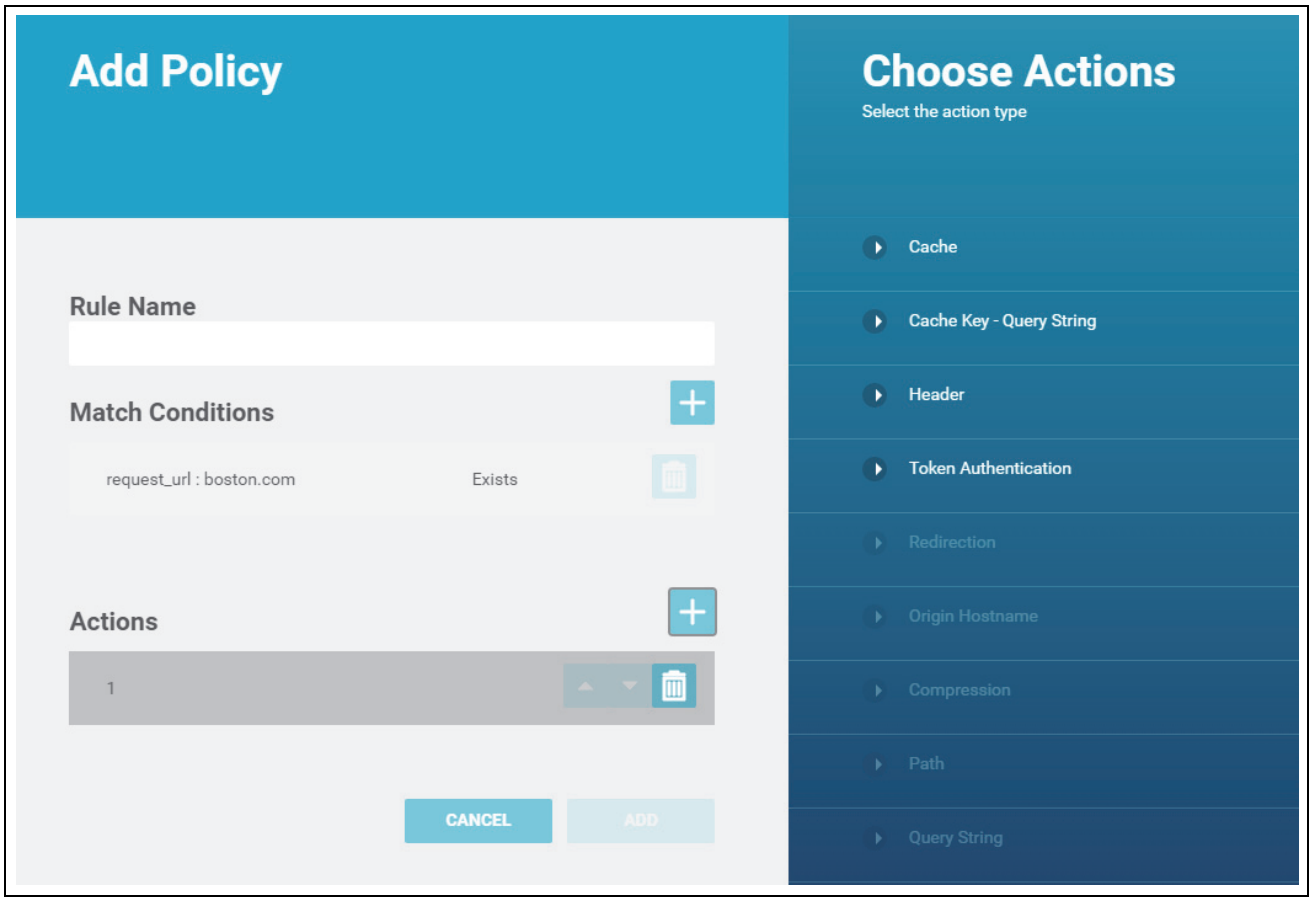
When creating a Token Authentication policy, you can only specify one Match Condition, and it must be a URL match.

Figure 7-7: Token Authentication Policy: Choose Match Condition



9. Now you must specify an Action for this policy. To do so, click the Add (+) button next to Actions. The Choose Action modal window displays (Figure 7-8).
10. On the Choose Action modal window, select Token Authentication.

Figure 7-8: Add Policy: Choose Action

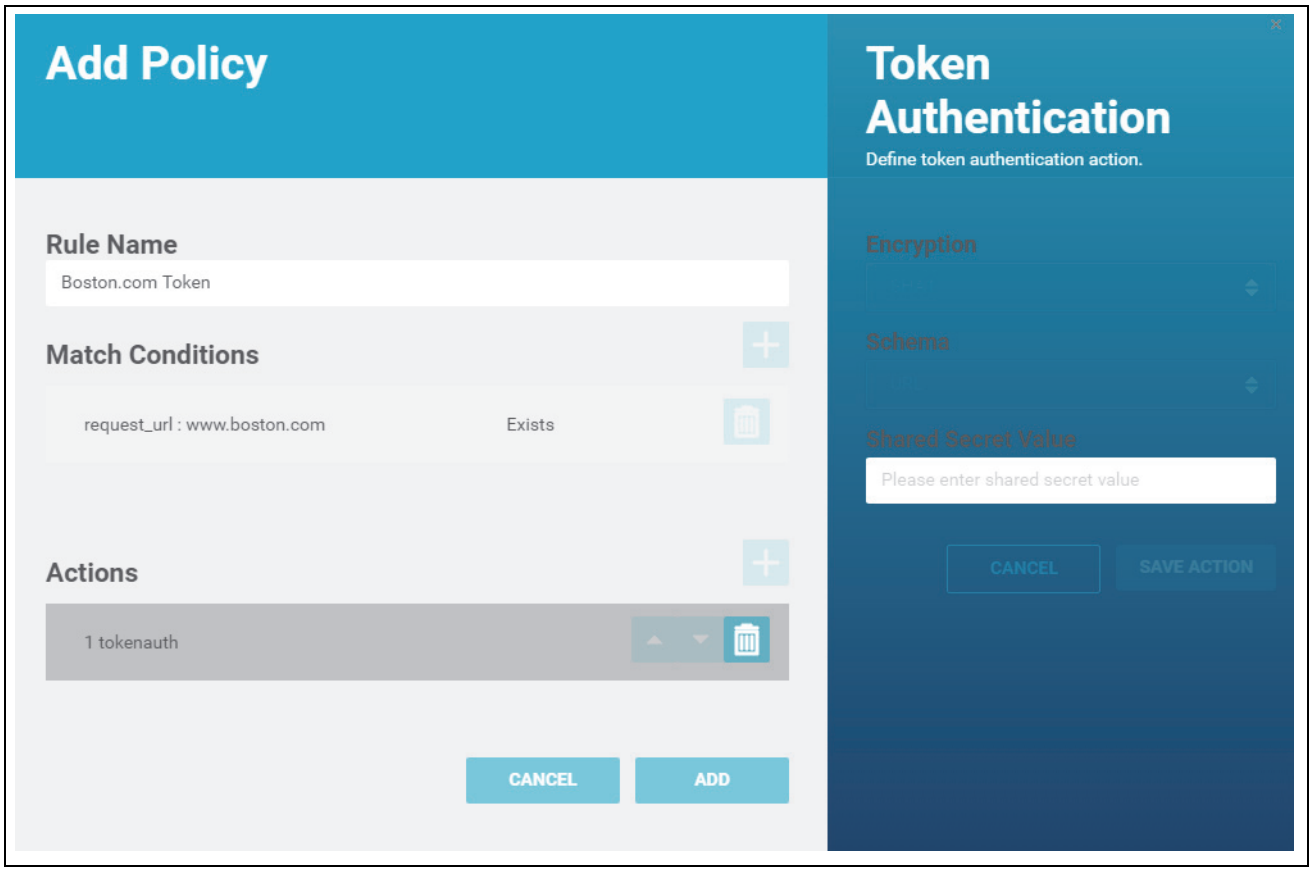


11. To enter the Token Authentication information associated with this Action, enter the Shared Secret Value for this Token, then click Save Action.(Figure 7-9). Note that the Encryption and Schema fields are set to a predetermined value in this release.

NOTE

When creating a Token Authentication policy, you can only specify one Action.

Figure 7-9: Add Policy: Token Authentication



12. When you have finished specifying Policy information, click Add at the bottom of the Add Policy window.

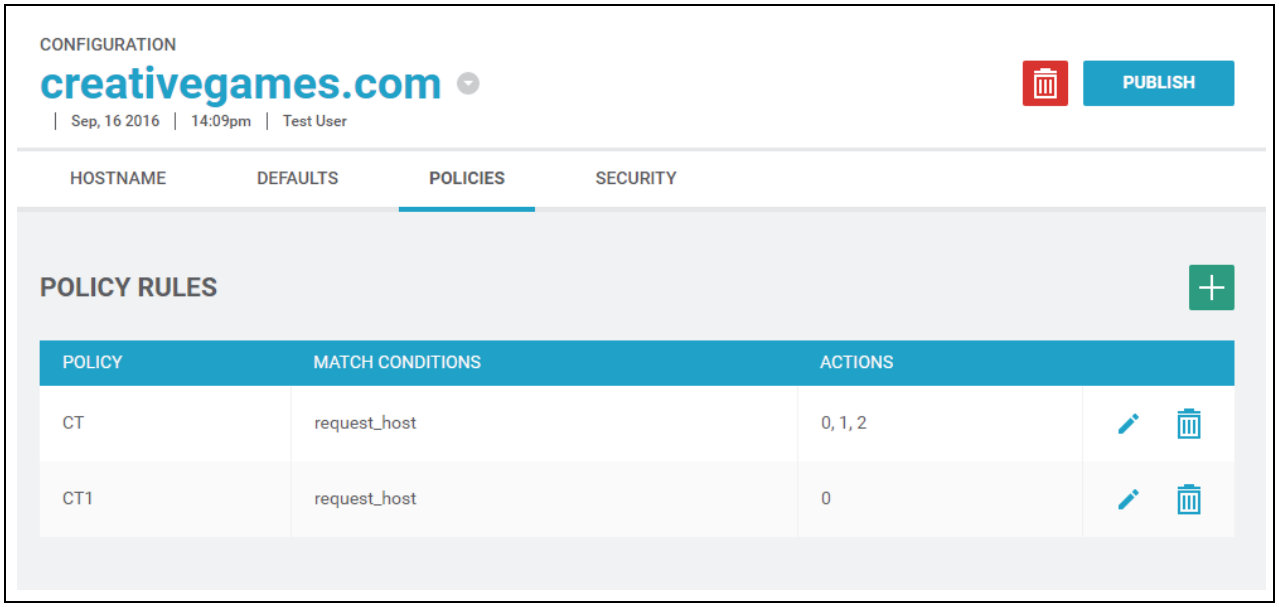
Content Targeting Policy Example

UDN Content Targeting enables Content Providers to specify where content can, and cannot, be delivered. You can configure geographic content targeting policies on a per-country basis.

To create a content targeting policy:

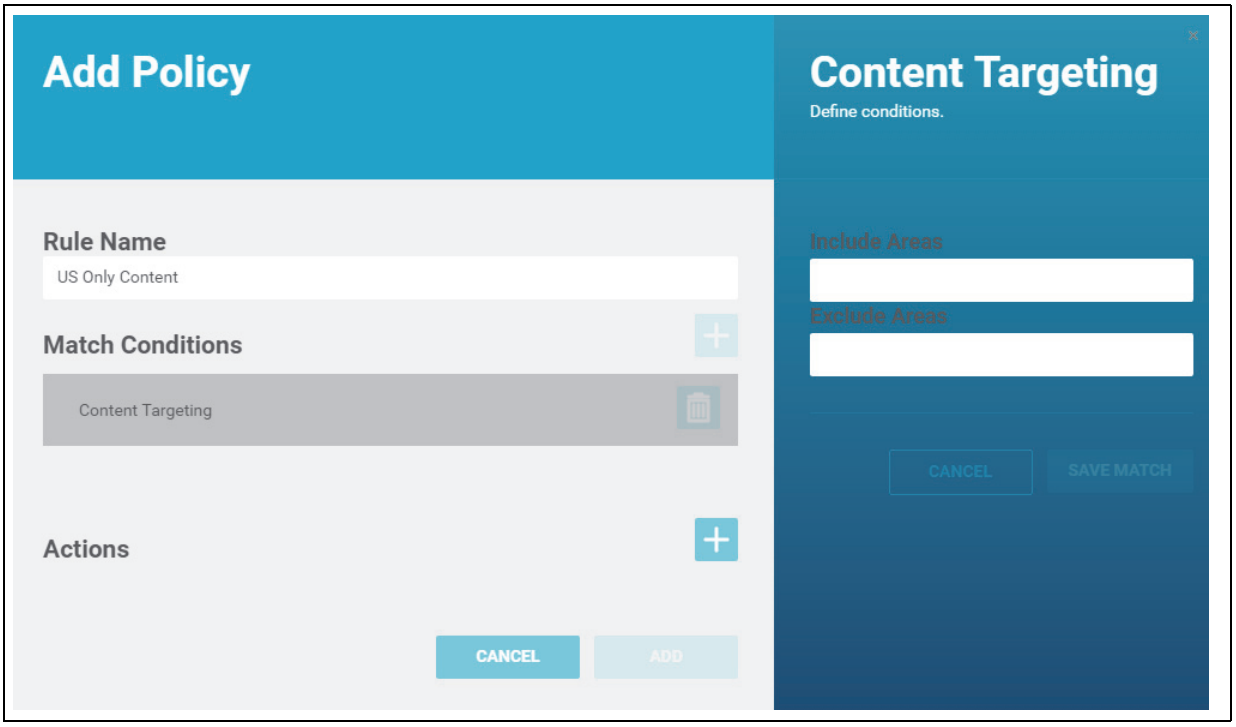
1. Navigate to the summary page for the desired Property.
2. In the upper right corner of the Property Summary page, click the Configure icon. The Property Configuration page displays.
3. Click the Policies tab. A list of current Policies displays in table form.

Figure 7-10: Property Configuration: Policies Tab



4. To add a new policy, click the Add (+) icon. The Add Policy screen displays (Figure 7-7).
5. Enter a name for the policy Rule. The name should indicate that this is a Content Targeting policy for a specific region or country.
6. The Choose Condition modal window automatically displays when you add a Policy. If it does not, click the Add (+) icon. In the Choose Condition modal window select Content Targeting. The Content Targeting actions modal window displays (Figure 7-11).
7. In the Content Targeting actions modal window, specify the countries to be included in delivery, and those to be excluded. A list of countries displays when you click in each field. Select as many countries as needed for each area. When finished, then click Save Match.

Figure 7-11: Content Targeting Policy: Content Targeting Areas



8. You can add more Content Targeting actions by clicking the Add (+) button at the top of the Actions area.

   For each Action, you specify three options:

   - Action: whether to Allow, Redirect, or Deny requests for content from the specified area.
   - Users From or Users Not From: whether you want the Action to occur when the user is from the specified area, or whether you want the Action to occur when the user is not from the specified area.
   - Location: the countries whose users you want this policy to affect.

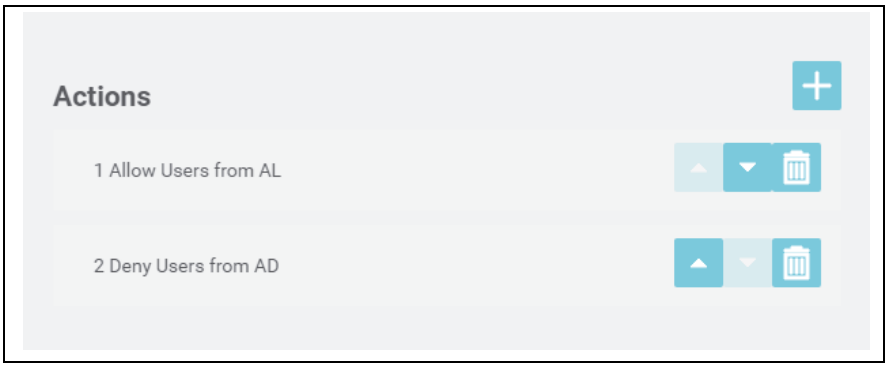
   For example, you could create a Policy that Allows requests for content from a specified group of countries in the first Action, and Denies requests from all other countries in the second action.

   When you have finished specifying the settings for an Action, click Save Action

9. Once you have finished specifying Match Conditions and Actions for this rule, you may want to change the priority in which they're applied.

   Use the up and down arrows (triangles) to the right of the available Actions or Conditions to organize them in the desired order (Figure 7-12).

Figure 7-12: Ordering Match Conditions or Actions



10. When you are satisfied with the Policy Rule settings, click Add.

NOTE

Additions and changes to the list of Policies associated with a Property are not automatically applied to the Property. To apply any Policy updates you have made, you will need to Publish them. For detailed information, see "Publishing Caching Policies".

Publishing Caching Policies

Property configuration settings, including caching policies, are delivered to UDN Properties by publishing them. By disconnecting the process of modifying and reviewing Property settings from the process of delivering those settings so they take affect, the Portal enables you to modify and review Property settings at your leisure. Note that publishing property settings will not disrupt current content delivery.

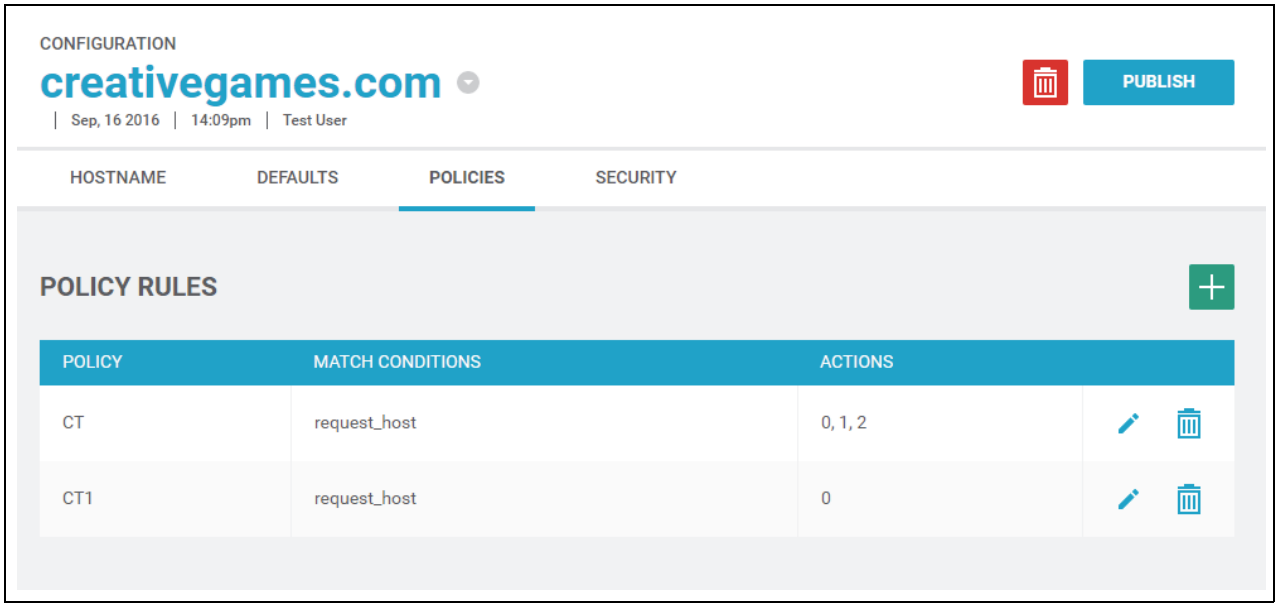
NOTE

Publish with caution, as there is no current way to roll back publication to a previous configuration.

To publish any new or modified caching policies (and other Property-specific configuration settings):

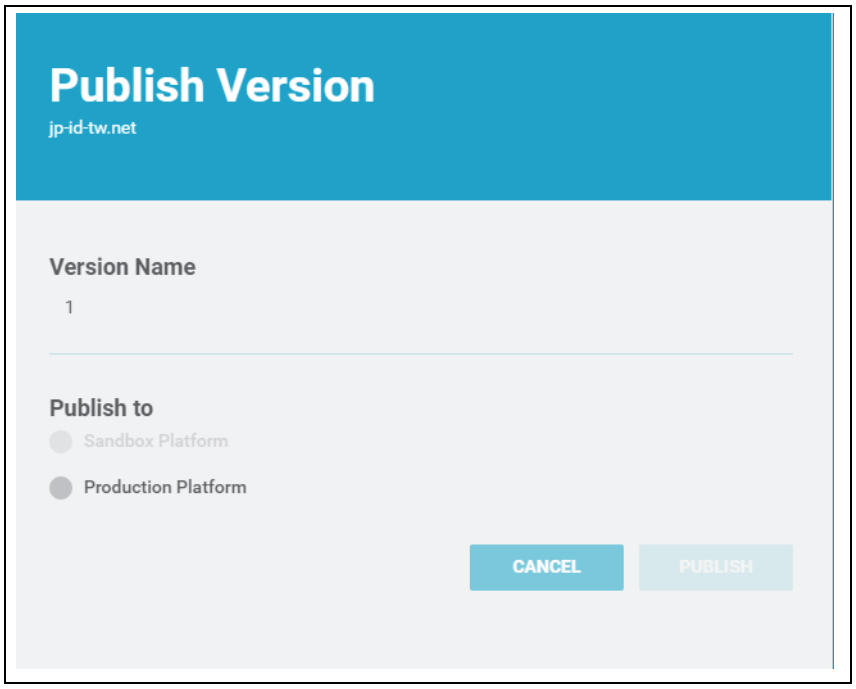
1. Navigate to the summary page for the desired Property.
2. In the upper right corner of the Property Summary page, click the Configure icon. The Property Configuration page displays.
3. Click the Policies tab. A list of current Policies displays in table form (Figure 7-13).

Figure 7-13: Property Configuration: Policies Tab



4. Review any policy changes you have made before publishing.
5. When ready, click Publish. The Publish Version page displays (Figure 7-14).

Figure 7-14: Property Settings: Publish Version



6. Select the option to publish to the Production Platform.

   NOTE

   For this version, you can only publish to the Production Platform.

7. Click Publish.

Purging Cache Content

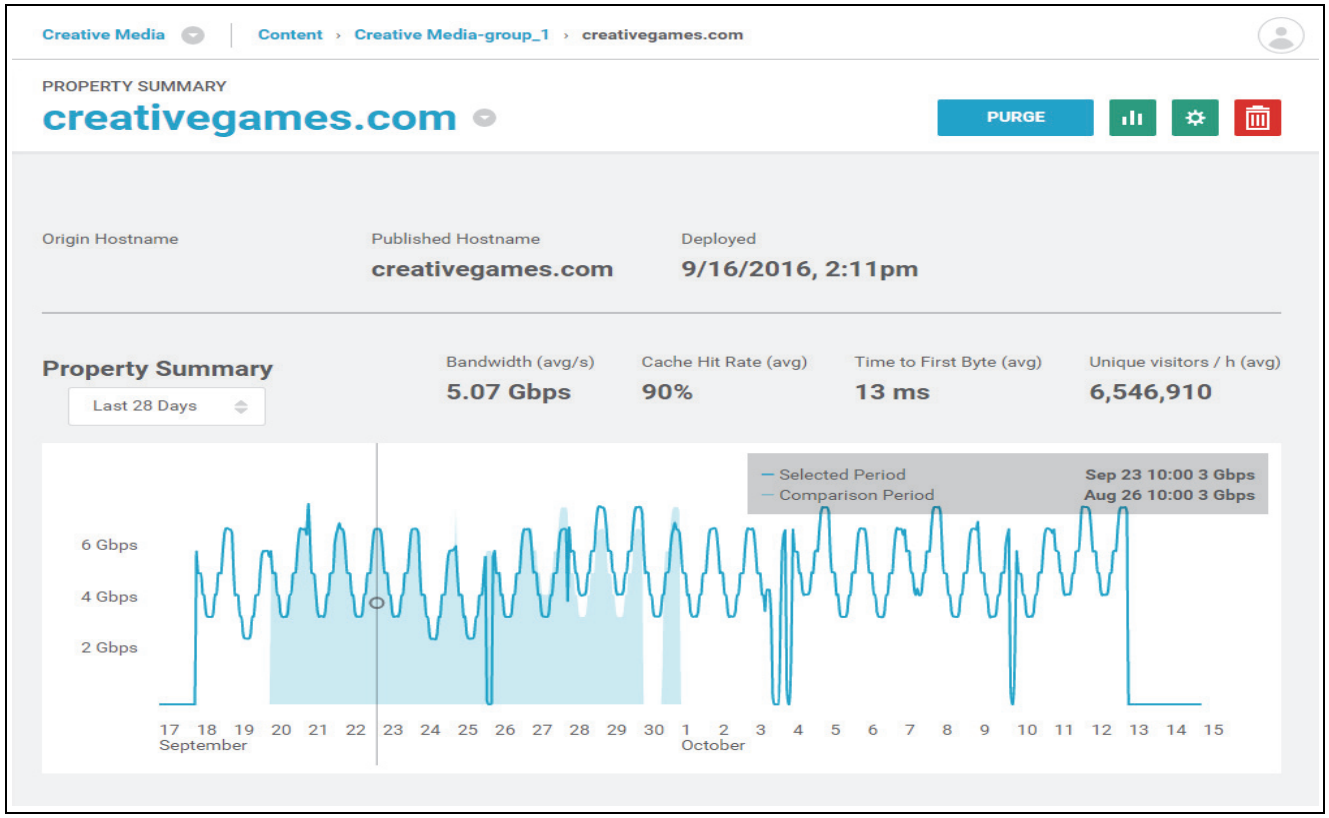
UDN will cache an asset until the asset's time-to-live (TTL) expires. After the asset's TTL expires, when a client requests the asset from the edge node, the edge node will retrieve a new version of the asset to serve the client request and refresh the cache.

Sometimes you may wish to purge cached content from a Property and force that Property to retrieve new assets. This might be due to updates to your web application, or to quickly update assets that contain incorrect information.

To purge content from a Property:

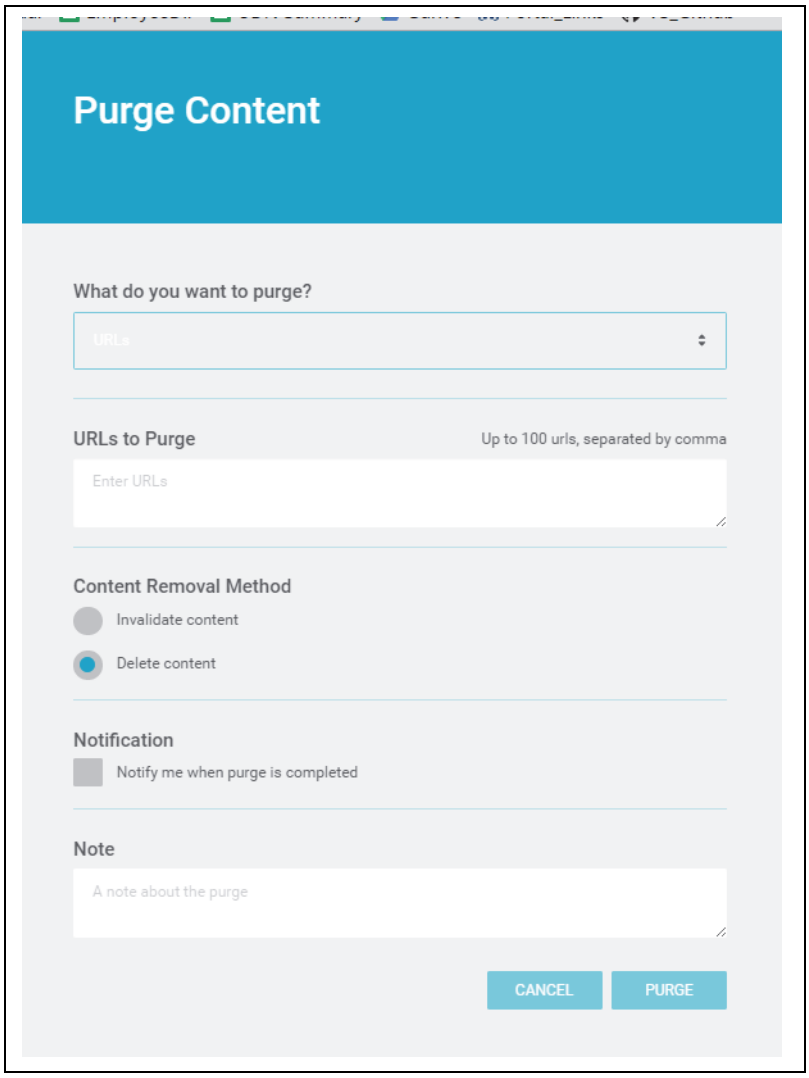
1. Navigate to the summary page for the desired Account.
2. Select the Group associated with the Property whose cache you want to purge. The Properties associated with that Group display.
3. Click the desired Property to display a Property Summary.

Figure 7-15: Property Summary Page



4. Click Purge at the top of the page. The Purge Content modal window displays.

Figure 7-16: Purge Content



5. Specify the content you want to purge. Choose one of the following:
   - URLs
   - Directories

   NOTE

   Purging based on specified Hostnames or Entire Group will be supported in a future version.

6. If you choose to purge URLs, do the following:
   a. Enter one or more URLs to purge, separated by commas.
   b. Select the Content Removal Method. Choosing Invalidate makes the content unavailable, but does not remove it from the cache. Choosing Delete both makes the content unavailable and removes it from the cache.
   c. If desired, you can choose to be notified when the purge is complete.
   d. You may add a note about this purge for future reference.

e. When finished, click Purge.

7. If you choose to purge Directories, do the following:
   a. Enter one or more Directories to purge, separated by commas.
   b. Select the Content Removal Method. Choosing Invalidate makes the content unavailable, but does not remove it from the cache. Choosing Delete both makes the content unavailable and removes it from the cache.
   c. If desired, you can choose to be notified when the purge is complete.
   d. You may add a note about this purge for future reference.
   e. When finished, click Purge.

Chapter 8
Managing Security Settings

The UDN Portal enables users to manage security settings associated with SSL certificates.

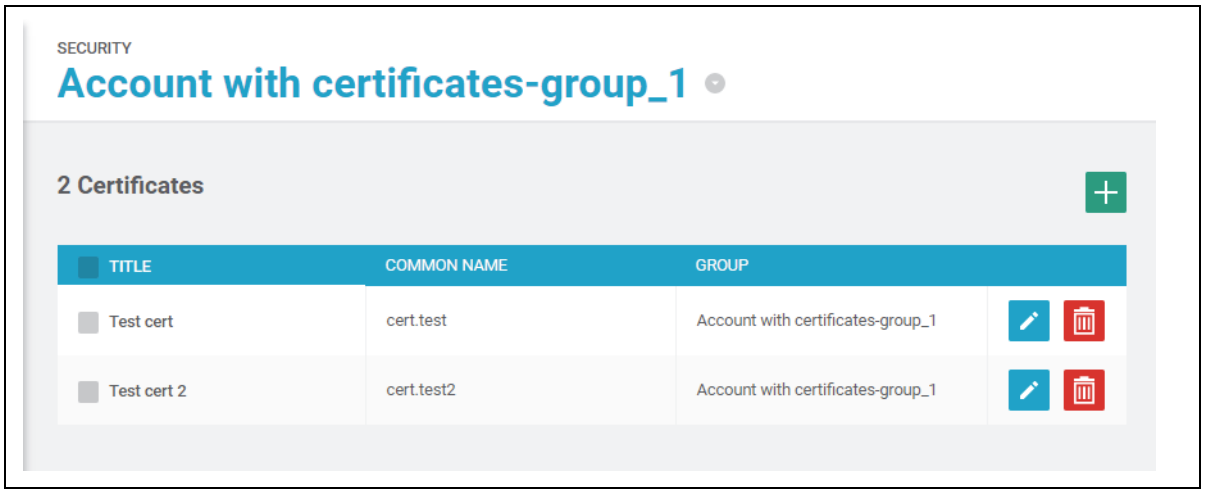
This chapter contains the following sections:

Managing SSL Certificates

To manage SSL certificates:

1. Navigate to the Summary Page for the Group to which you want to add the SSL Certificate.
2. Click the Security icon in the left navigation bar.
3. The Security page displays. Click the SSL Certificate tab (Figure 8-1).
   This page lists previously uploaded certificates.

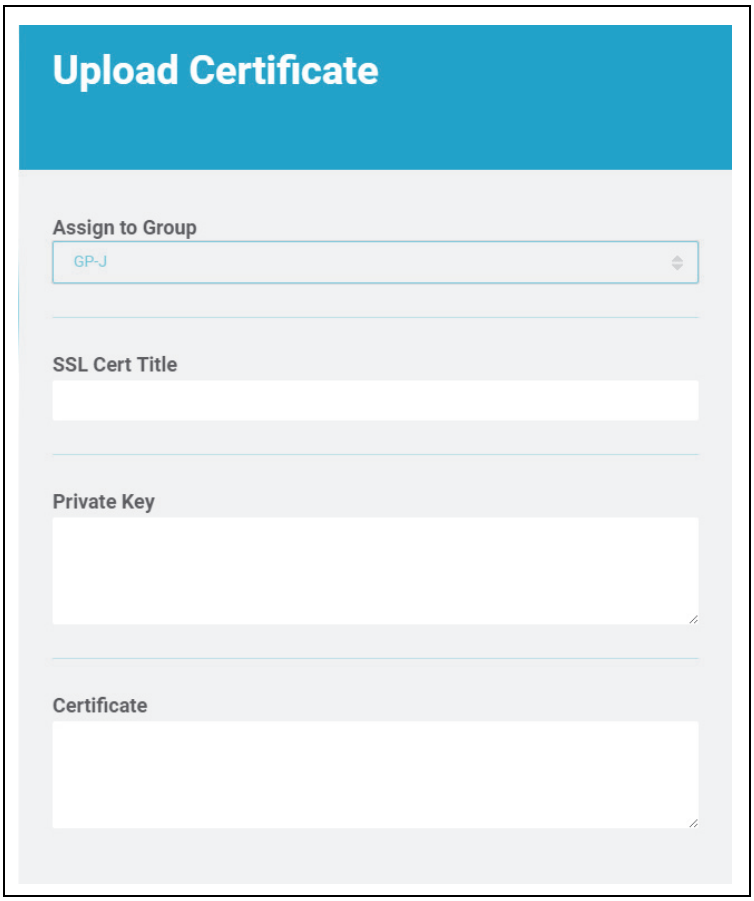
Figure 8-1: Security Page: SSL Certificate tab



4. To add or edit an SSL Certificate:
   a. Do one of the following:
      - To add a new SSL Certificate, click the Add (+) icon.
      - To edit an existing SSL Certificate, locate the certificate in the list and click the Edit (pencil) icon.

   The Upload or Edit Certificate modal window displays. Figure 8-2 shows the Upload Certificate modal window.

Figure 8-2: Upload Certificate



b. Enter the Title for the SSL Certificate.
c. Copy and paste the Private Key associated with the Certificate.
d. Enter the Certificate itself.
e. When finished, click Save.

5. To delete an SSL Certificate:
   a. Select the row associated with the SSL Certificate you want to delete.
   b. Click the Delete (trash) icon on that row.
   c. Confirm the deletion to complete the operation.

Chapter 9
Accessing Support Resources

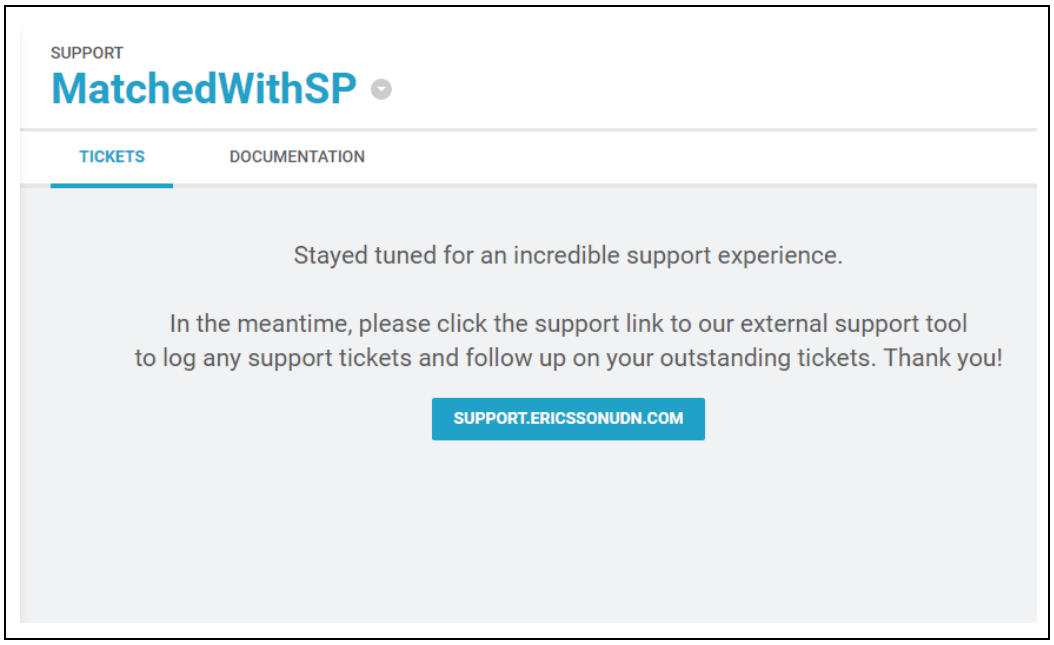
The Support page of the Portal provides access to the ZenDesk ticketing application. it also provides access to Portal documentation. This chapter contains the following sections:

Accessing Support

To access Support:

1. Click the Support icon on the left navigation bar. the Support page displays (Figure 9-1).

Figure 9-1: Support: Tickets Tab



2. To access the Ericsson UDN Support Site, click the SUPPORT.ERICSSONUDN.COM button. The link will bring you to the UDN Support site. The site provides links to helpful UDN information including Frequently Asked Questions.
3. To Submit a Request for assistance, click the Submit a Request link in the upper right corner of the page. The Submit a Request page displays.
4. To file a ticket, select UDN Support Ticket.
   a. Enter the following information for your request:
      - Subject: Enter a title for your ticket briefly describing the current issue.
      - Description: Enter a description of your current issue or need.
      - Priority: Select a priority for your issue.
      - Type: Select the issue Type (Question, Incident, Problem, Task, or Integration)
      - Service Type: Specify the Service Type associated with your request.
      - Attachments: Add any attachments that you feel would benefit the support effort.

   b. When finished, click Submit.
5. To make a change request, select UDN Change Request
   a. Enter the following information for your request:
      - Subject: Enter a title for your ticket briefly describing the current issue.
      - Description: Enter a description of your current issue or need.

- Change Type: Specify whether this is a normal, standard, or emergency change.
- Service Type: Specify the service type associated with your request.
- Change Risk: Specify the risk level of the change.
- Change Impact: Select the impact of the change on your system.
- Attachments: Add any attachments that you feel would benefit the support effort.

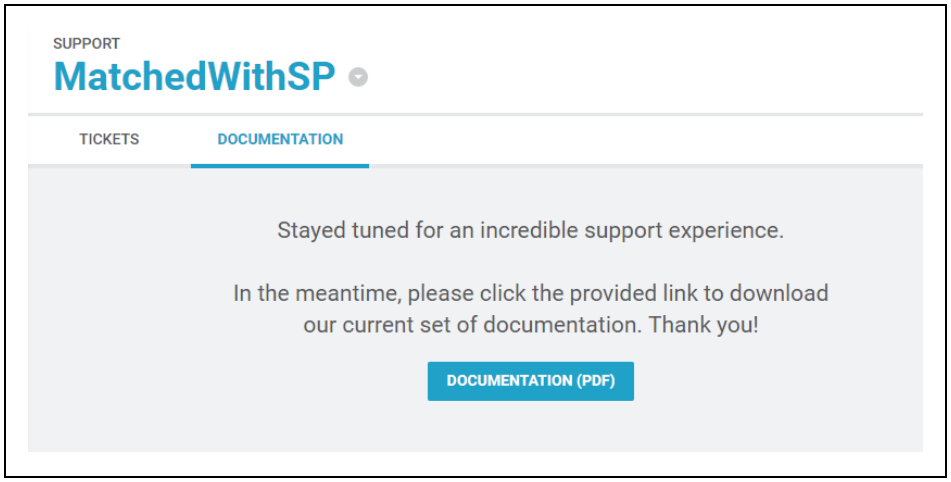
b. When finished, click Submit.

Accessing Documentation

To access the Portal User Guide associated with your User Role:

1. Click the Support icon on the left navigation bar.
2. Click the Documentation tab (Figure 9-2).

Figure 9-2: Support: Tickets Tab



3. Click the DOCUMENTATION button. The user guide associated with your current User Roles launches as a PDF file.