Oracle® SD-WAN Edge

Enhanced Application Identification and Application Signatures Guide

Release 9.1M1
F49221-02
October 2021

Oracle SD-WAN Edge Enhanced Application Identification and Application Signatures Guide, Release 9.1M1

F49221-02

Contents

About This Guide

Oracle SD-WAN Edge Enhanced Application Identification and Applications Signatures Guide informs customers of the Application Identification feature set..

Audience

This document is meant for network administrators and architects who are familiar with Oracle SD-WAN terminology and the Edge solution.

Documentation Set

This table lists related documentation.

Document Name	Document Description
Oracle SD-WAN Edge Release Notes	Contains information about added features, resolved issues, requirements for use, and known issues in the latest Oracle SD-WAN Edge release.
Oracle SD-WAN OS Release Notes and Upgrade Guide	Contains information about inserting an OS Partition Image or OS Patch on an appliance in order to migrate to a new OS version or apply fixes to an existing version.
Oracle SD-WAN Security Guide	Contains information about security methods within the Oracle SD-WAN solution.
Oracle SD-WAN Edge Features Guide	Contains feature descriptions and procedures for all incremental releases of Oracle SD-WAN Edge. This guide is organized by release version.
Oracle SD-WAN Edge High Availability Guide	Contains information about implementing High Availability, as well as deployments and configuration.
Oracle SD-WAN Edge Virtual Appliance Installation Guide	Contains information about how to install a Virtual Appliance on a supported hypervisor.
Oracle SD-WAN Edge Service Chaining Guide	Contains information about installing a Guest Virtual Machine using the Service Chaining UI.
Oracle SD-WAN Edge Enhanced Application ID and Signatures Guide	Oracle SD-WAN Edge Enhanced Application Identification and Applications Signatures Guide informs customers of the Application Identification feature set.

My Oracle Support

My Oracle Support (https://support.oracle.com) is your initial point of contact for all product support and training needs. A representative at Customer Access Support (CAS) can assist you with My Oracle Support registration.

Call the CAS main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/

index.html. When calling, make the selections in the sequence shown below on the Support telephone menu:

1. Select 2 for New Service Request.
2. Select 3 for Hardware, Networking, and Solaris Operating System Support.
3. Select one of the following options:
   - For technical issues such as creating a new Service Request (SR), select 1.
   - For non-technical issues such as registration or assistance with My Oracle Support, select 2.

You are connected to a live agent who can assist you with My Oracle Support registration and opening a support ticket.

My Oracle Support is available 24 hours a day, 7 days a week, 365 days a year.

Emergency Response

In the event of a critical service situation, emergency response is offered by the Customer Access Support (CAS) main number at 1-800-223-1711 (toll-free in the US), or call the Oracle Support hotline for your local country from the list at http://www.oracle.com/us/support/contact/index.html. The emergency response provides immediate coverage, automatic escalation, and other features to ensure that the critical situation is resolved as rapidly as possible.

A critical situation is defined as a problem with the installed equipment that severely affects service, traffic, or maintenance capabilities, and requires immediate corrective action. Critical situations affect service and/or system operation resulting in one or several of these situations:

- A total system failure that results in loss of all transaction processing capability
- Significant reduction in system capacity or traffic handling capability
- Loss of the system's ability to perform automatic system reconfiguration
- Inability to restart a processor or the system
- Corruption of system databases that requires service affecting corrective actions
- Loss of access for maintenance or recovery operations
- Loss of the system ability to provide any required critical or major trouble notification

Any other problem severely affecting service, capacity/traffic, billing, and maintenance capabilities may be defined as critical by prior discussion and agreement with Oracle.

Locate Product Documentation on the Oracle Help Center Site

Oracle Communications customer documentation is available on the web at the Oracle Help Center (OHC) site, http://docs.oracle.com. You do not have to register to access these documents. Viewing these files requires Adobe Acrobat Reader, which can be downloaded at http://www.adobe.com.

1. Access the Oracle Help Center site at http://docs.oracle.com.
2. Click **Industries**.
3. Click the **Oracle Communications** link.
   Under the **SD-WAN** header, select a product.

4. Select the Release Number.
   A list of the entire documentation set for the selected product and release appears.
5. To download a file to your location, right-click the **PDF** link, select **Save target as** (or similar command based on your browser), and save to a local folder.

Revision History

This section provides a revision history for this document.

Date	Description
October 2021	• Initial release associated with SD-WAN Edge 9.1M1.

1

Introduction to Enhanced Application Identification & Oracle SD-WAN Edge Application Signature Library

Enhanced Application Identification allows the service to recognize an application based on domain name or sub-domain name, and allows users to steer application traffic to a defined service. Enhanced Application Identification leverages the Oracle SD-WAN Edge Application Signature Library of pre-defined categories and applications to simplify configuration while also supporting custom user-defined categories and applications. The Oracle SD-WAN Edge Application Signature Library contains more than 100 pre-defined applications. Oracle will provide updates to the Oracle SD-WAN Edge Application Signature Library based on customer feedback. New signature libraries can be upgraded independently of software packages via the Oracle SD-WAN Edge configuration editor process.

Enhanced Application Identification is configured globally for ease of use. The user may define application policies to steer applications to the local Internet service or to hair-pin them back to the data center or NCN site. Application policies may be applied to Oracle SD-WAN Edge, to a single site, or to a subset of sites within Edge. When applications are steered to a Conduit service (as when hair-pinning to the data center or Edge), traditional QOS services are applied and users may map the application to a predefined classification or select their own classification from a pre-defined list.

Additionally, the appliance now provides an application dashboard view which allows the user to view top live and cumulative applications, bandwidth usage by service, application health information. These features are described in more detail in this document.

Capabilities

Oracle SD-WAN Edge's Enhanced Application Identification provides the capability to identify an application and match multiple configuration components to a policy. Some of these configurable components are pre-defined and some are user definable. These are included below with a brief definition, and described in more detail below:

Table 1-1 Idenfication Methods

Component	Description	Used For	User Defined / Customizable	Pre-Defined	Optional Usage
Application Category	Group of Applications	Application Dashboard: Top Applications	YES	YES	YES

Table 1-1 (Cont.) Idenfication Methods

Component	Description	Used For	User Defined / Customizable	Pre-Defined	Optional Usage
Application (Defined by User)	User-defined specific application (comprised by domain name, 5 tuple). Can be enabled or disabled at any time.	Application Dashboard	YES	NO	YES
Application (Defined by Oracle)	Applications part of the Application Signature Library (comprised of subdomains, 5 tuple. By default, this is disabled.)	Application Dashboard	YES	YES	YES
DNS Snooping	Enabling any application enables DNS snooping throughout SD-WAN Edge. (Default is disabled.)	Display of Applications with Domain Name Match	YES	YES	YES
Probing Intervals	Application probing frequency for an application can be enabled or disabled, and configured. Probing is only performed when an application includes one or more domain names as match criteria.	Application Health	YES	YES	YES
Response Times	Normal and Warning level application response times can be configured. (Default to 100 for Normal and 200 for Warning.)	Application Health	YES	YES	YES

Table 1-1 (Cont.) Idenfication Methods

Component	Description	Used For	User Defined / Customizable	Pre-Defined	Optional Usage
Site Response Time Bias	Adjust the Normal and Warning level application response times on a per-site basis. (Default is 0.)	Application Health	YES	NO	YES

Application Categories

Application Categories are used to group applications for the purpose of more easily defining policies that apply to multiple applications. Application Categories can be created by users, or users can leverage the Application Categories contained in the Oracle SD-WAN Edge Application Signature Library, or a combination of both. The Oracle SD-WAN Edge Application Signature Library provides multiple pre-defined Application Categories, including Business, Music, News, Voice, and more. Users may add or remove Application Categories as desired. Application Categories may be used as one of the match criteria for Application Policies. Usage reporting is available for Application Categories via the Application Dashboard. (For more details, see the Application Dashboard Section.)

User Defined Applications

In addition to the applications included in the Oracle SD-WAN Edge Application Signature Library, users may define applications to match on protocol, port, network IP address or domain name, and DSCP tag or a combination of these items. Traffic will be evaluated against userdefined applications before being evaluated against the Oracle SD-WAN Edge Defined Applications that originate from the Oracle SD-WAN Edge Application Signature Library. Applications may be used as one of the match criteria for Application Policies. Usage reporting is available for applications via the Application Dashboard. (For more details see the Application Dashboard Section)

Oracle Defined Applications

Oracle Defined Application will originate from the Oracle SD-WAN Edge Application Signature Library that the user may elect to import and use alone or along with their User Defined Applications. The Oracle SD-WAN Edge Application Signature library includes more than 100 predefined commonly requested applications in multiple categories to save users time defining them individually. Users may customize or remove these pre-defined applications after importing the Oracle SD-WAN Edge Application Signature Library. Just as with User Defined Applications, Oracle SD-WAN Edge Defined Applications may be used as one of the match criteria for Application Policies. Usage reporting is available for applications via the Application Dashboard.

> **Note:**
>
> Oracle Defined Applications imported from the Oracle SD-WAN Edge Application Signature library are disabled by default and must be explicitly enabled in the Configuration Editor. DNS snooping will only occur after an application has been enabled.

Application Policies

Application Policies are user-defined and provide a mechanism to specify that a specific application or Application Category once identified by the system should be steered to a particular service. For example, internet-based applications such as SalesForce and Office365 may be steered to a local internet service, or they may be hair-pinned to the NCN for internet access by creating an Application Policy.

> **Note:**
>
> Once the user defines an application policy or makes any changes to an application policy, the configuration must be saved and then applied to Oracle SD-WAN Edge to implement the policy. The user would use the Change Management process to activate the updated configuration file containing the new/edited application policies.

Site Groups

Site Groups allow users to group multiple sites together for use with one or more Application Policies. There are three default site groups available for user convenience including: All Sites, ControllerSites, and NonControllerSites. Users may define additional site groups as desired for use in any Application Policies.

Network Objects

Network objects allow users to specify an IP address and subnet mask list for an application policy. Network Objects are user-defined.

Application Match Functionality

Oracle has supported application identification in the past by leveraging a 5-tuple match where the user would configure IP address or ports based on the application flow. In addition, Oracle has also supported the concept of DNS proxy which allowed the system to learn DNS resolution information from DNS replies.

The Application Identification suite also includes a DNS snooping capability which matches flows to domain names within an application flow. Prior to a host initiating a new session the host initiates a DNS request to learn the IP address of the application. This DNS request and DNS response must pass through the system, and the appliance caches DNS resolution information (A Records) for use in application matching. Once the host receives the DNS reply it initiates the session to the destination IP address. Oracle then matches the request initiated by the host to a learned IP address defined for the specific application. When DNS snooping is enabled, DNS proxy is no longer required for domain-based application identification.

> **Note:**
>
> Since the appliance must be able to read DNS information in order to identify applications, Application Identification is not supported in conjunction with Encrypted DNS.

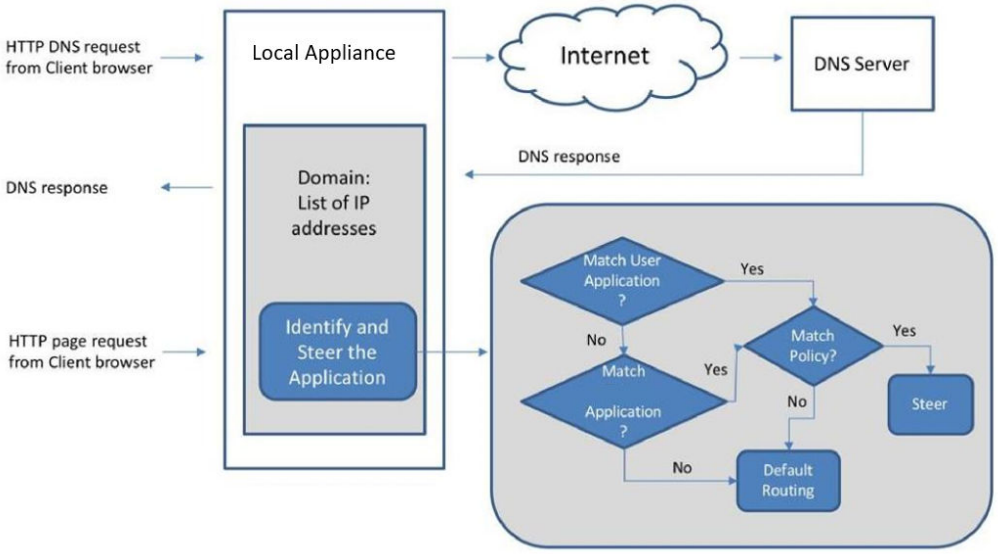
> **Note:**
>
> Application Identification only matches the first connection when multiple DNS A records resolve to the same IP address. Subsequent connections using the same IP address will be attributed to the original application match, and will block the addition of that IP address as a match for other applications. For example, if Application A uses the domain name “domain1.com” as one of its match criteria and Application B uses the domain name “domain2.com” as one of its match criteria, if the DNS resolution for both domains is “1.2.3.4” then all connections using that address will be assigned to the first application the record is matched against.

Application Policy Processing

The priority for matching on a defined policy is as follows:

- User-defined application policies
- Oracle SD-WAN Edge-defined applications

All policies are listed in priority order, with lower-numbered policies processed first. Once a session matches an application policy, additional policies will not be evaluated for that session. The user defined applications take priority over the Oracle defined applications when matching an application policy. If the session does not match an application policy, the session will default to the routing table. If the application policy is steered to a service that is down, the routing table is used to forward the flow to the appropriate destination service. Currently, users cannot configure a failover policy as the routing table is used if the service associated with an application policy is down. If the user steers an application to a service, the service must exist at the destination site. For example, if the application policy is steering to the local Internet service of a site, the Internet service must exist at that site when defining the application policy. If the service does not exist at a site, the decision to forward the packets/flow is based on the appliance routing table.



Application Health

Application Identification provides application health information on a per-application basis. Health information will be collected for all enabled applications which include domain name as a match criteria and displayed on the Application Dashboard. Health indicators are determined by RTT probing. Probing is used to determine the real-time health of an application. Probing is disabled by default and must be enabled on a perapplication basis.

> **Note:**
>
> Health information for applications is only available when probing is enabled. Probing is only performed on applications which include a domain name in the match criteria.

When probing is enabled and the application domain name is resolved by DNS snooping, a TCP request will be sent to the IP(s) associated with the application and the RTT time will be calculated based on the response (details below). For applications with more than one associated IP address, the top 5 addresses used will be probed and an average RTT calculated from the results. The TCP SYN contains the timestamp in the Options field and the expectation is that the Server will respond with a Timestamp. If the server does not respond with a timestamp the RTT is not calculated at this time. These probes will also show up in the flow table – source IP address will be an Oracle VIP address with the destination IP being that of the application domain. These will be TCP based using a source port of 2156 and a destination port of 443. The RTT is compared to the timer thresholds specified in the configuration (default or user-defined) to determine application health. Applications which are at or below the normal response time will be classified as Normal. Applications which are at or below warning response time but above the normal response time will be classified as Warning. Applications which are above the warning threshold will be classified as Critical. The user has the ability to change these values per application.

Since different sites may have different acceptable thresholds, an additional timer delay (the site bias normal / warning timer) is configurable on a per-site basis. This value is added to the value defined within each application.

2 Configuration

Configuration Overview

Application Identification is configured through the Configuration Editor tool. In order for Application Identification to provide data on application health and usage, one or more applications must be defined and enabled. In order to take advantage of Application Identification's steering capabilities, one or more application policies must be defined as well.

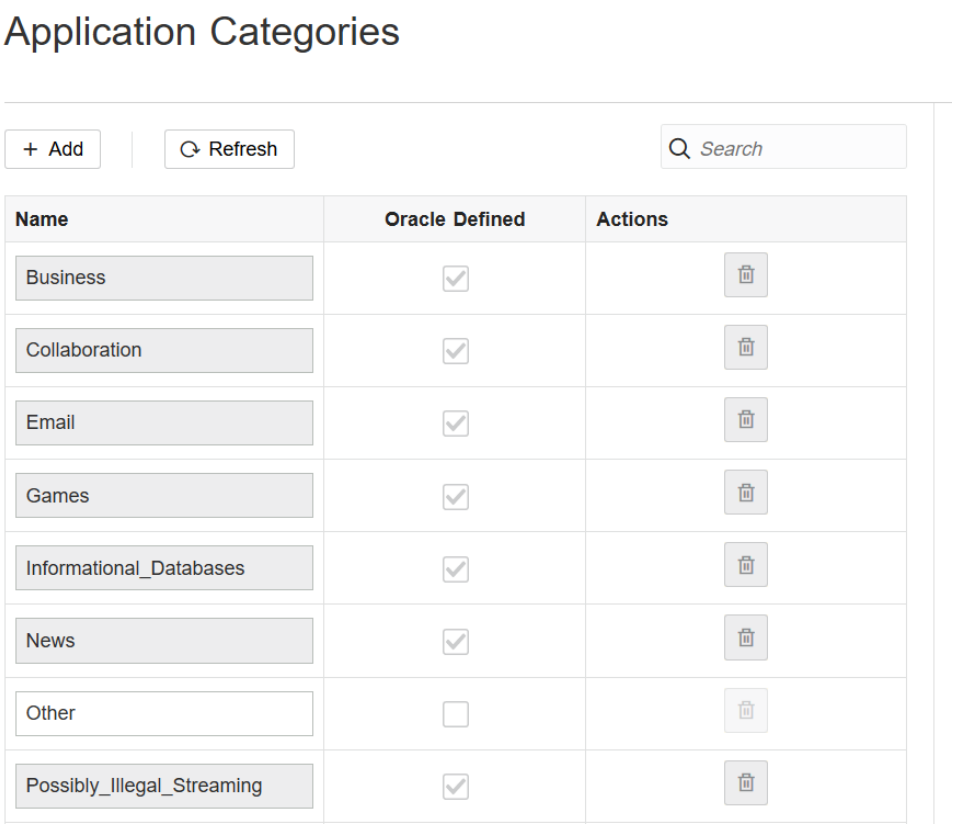
Below are more details about the configurable components that may be leveraged by the user for enhanced application identification.

Configure Application Categories (Optional)

> **Note:**
>
> Configuring or removing Application Categories is not required for Application Identification to function.

- In the Configuration Editor, open **Applications** > **Application Categories**.

Pre-defined application categories may not be edited. However, they may be deleted by clicking the **Delete** icon in the right-hand column.

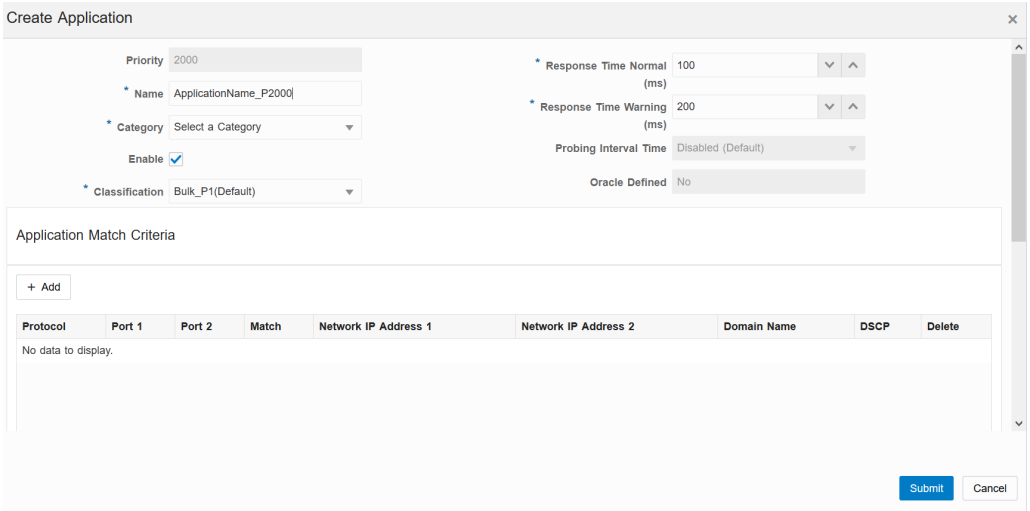


- To add a new application category, click **+ Add**, assign a name to the new category, and click **Submit**.

Configure User Defined Applications

Add a New Application

To add a user-defined application, open **Application Policies**, **Create and Manage Applications** in the Configuration Editor and click the **+ Add** button.



Applications defined are evaluated by a user-customizable priority order (see above). Once the system finds a match for the traffic, additional applications defined will not be evaluated for that traffic. More specific application definitions should be given a higher priority (closer to 100) so that theses matches will be achieved before more general criteria (e.g. an application matching based on the domain name analytics.google.com should be ordered before an application matching based on the domain name “google.com”). User defined application priorities will supersede the Defined Application priorities.The application definition priority is different from the Application Policy priority (see Application Policy Configuration Section further below) Applications will be assigned an automatically generated name. Best practice is to replace this with a descriptive name. Applications should be assigned a category to aid in grouping the application on the Application Dashboard. If no category is selected, the application will be assigned to a category named “Other.”

Classification

All applications have been defined a default classification for application identification. These default classifications map to the Default Rulesets. Details on how each default classification for application identification maps to the Default Rule sets can be found in Application ID Classification Mapping.

Response Time and Probing Interval(s)

When probing is enabled and the application domain name is resolved by DNS snooping, a TCP request will be sent to the IP(s) associated with the application and the RTT time will be calculated based on the response. The RTT is compared to the Response Time thresholds (Normal and Warning) specified in the application configuration to determine application health.

Applications which are at or below the normal response time will be classified as Normal on the Application Health section of the Application Dashboard. Applications which are at or below warning response time but above the normal response time will be classified as Warning. Applications which are above the warning threshold will be classified as Critical.

To configure Application Health related settings for an application the user should:

1. Make sure the Enable box is checked to enable DNS snooping and Application Identification.
2. Review/modify normal and warning response times for the application (see above).
3. Select a probing interval from the dropdown.

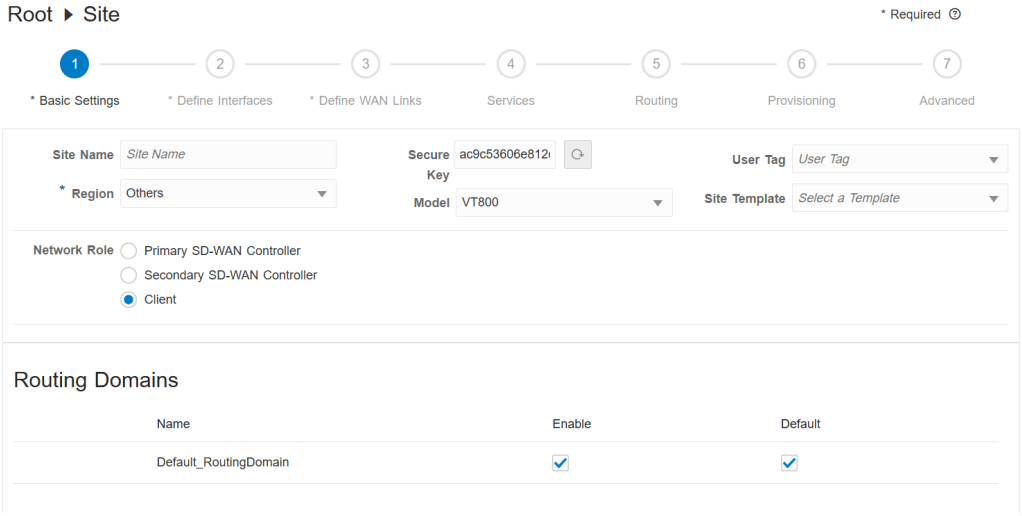
> **Note:**
>
> By default, the probing interval is disabled. When the probing interval is disabled, health checking will not be available for the application.

Site Bias

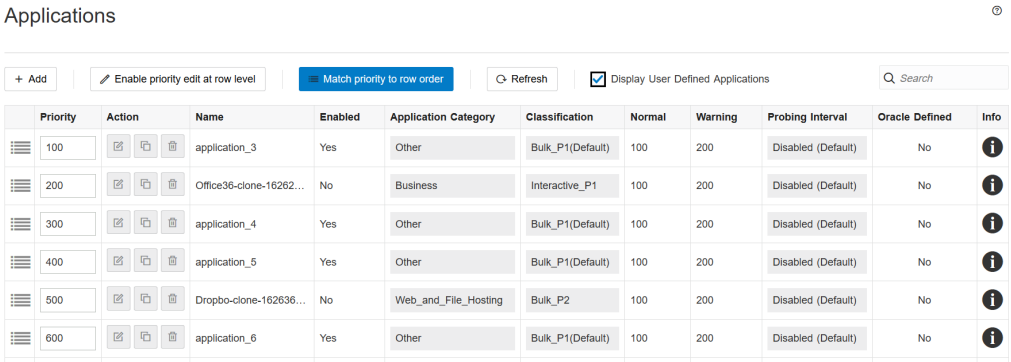
In addition to the per application response time settings, an overall Site Bias can be configured under Basic Settings for each site. The site bias allows the adjustment of the normal and warning times the system will expect to see for an individual site. This is useful when there are sites that are known to experience slower rates of speed than others.

When normal and warning response times are set up for an application with probing enabled, the site bias can be used to increase the RTT checks if a certain site is known to have slower WAN response times/higher latency across the WAN to access applications. Using the site

bias will prevent the known slower performance site from constantly showing up under the Application Dashboard Health with a warning or critical status for what is considered expected behavior at a that site.



For example: An application is defined with a Normal RTT of 30ms. However, for a specific site know to have slower performance, a site bias can be set (within the Basic Settings for the Site) to 20ms. The outcome would be that the Application Dashboard would not display a warning for this specific site and application unless the RTT is >50ms. All other sites without the site bias specified would appear with a warning on the Application Health section of the Application Dashboard if the RTT is >30ms.



Match Criteria

The final step in defining an application is the Application Match Criteria, which consists of the following attributes when the Match criteria is “Network IP”:

- Protocol: TCP, UDP, ICMP the user has an extensive selection to choose from
- Port1/Port2: The user can define ports for a specific application if required
- Network IP Address 1/Network IP Address 2: The user can define IP addresses if required
- DSCP: The user can select from a list of default DSCP values
  When the Match Criteria is “Domain Name,” all other options are greyed out and cannot be defined except for the following:
  - Domain Name: Where the user would specify a domain name like yahoo.com

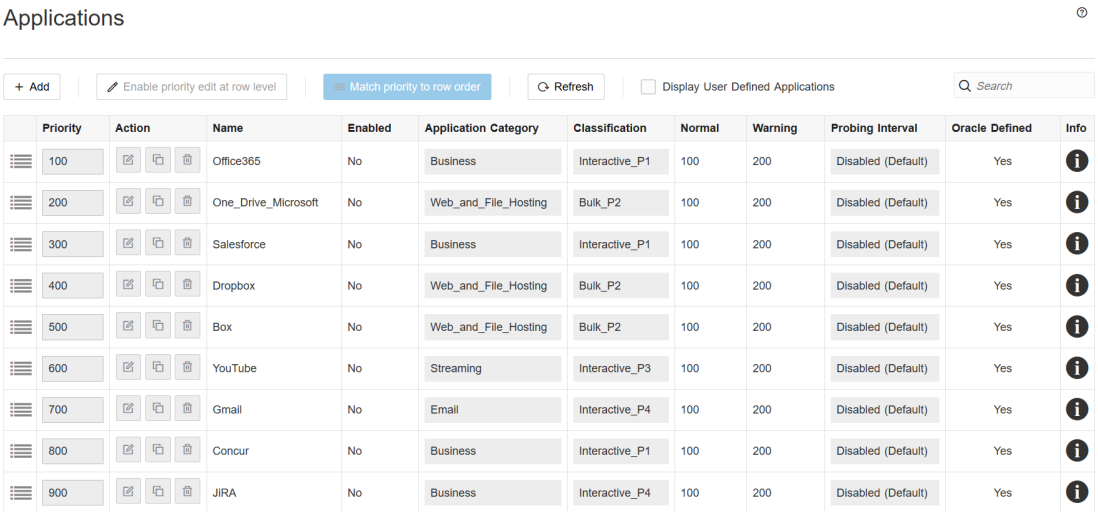
> **Note:**
>
> Any domain name defined as a match criterion will be treated for matching purposes as if it has a wildcard in front of it. Therefore, if the domain name is defined as talari.com

After all configuration details have been specified, click **Add** to add the new application.

Manage Oracle Defined Applications

Pre-defined applications are disabled by default and must be explicitly enabled by the user. Users may make limited edits to applications included in the Application Signature Library. Pre-configured applications may also be deleted, if desired.

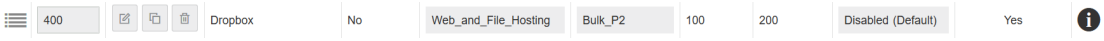
1. To edit or remove a pre-defined application, open **Application Policies**, **Create and Manage Applications** in the Configuration Editor.
2. To enable an application, click the **Edit** icon under Actions.
3. Click the **Enable** checkbox then click **Submit**.



Priority	Action	Name	Enabled	Application Category	Classification	Normal	Warning	Probing Interval	Oracle Defined	Info
100		Office365	No	Business	Interactive_P1	100	200	Disabled (Default)	Yes	
200		One_Drive_Microsoft	No	Web_and_File_Hosting	Bulk_P2	100	200	Disabled (Default)	Yes	
300		Salesforce	No	Business	Interactive_P1	100	200	Disabled (Default)	Yes	
400		Dropbox	No	Web_and_File_Hosting	Bulk_P2	100	200	Disabled (Default)	Yes	
500		Box	No	Web_and_File_Hosting	Bulk_P2	100	200	Disabled (Default)	Yes	
600		YouTube	No	Streaming	Interactive_P3	100	200	Disabled (Default)	Yes	
700		Gmail	No	Email	Interactive_P4	100	200	Disabled (Default)	Yes	
800		Concur	No	Business	Interactive_P1	100	200	Disabled (Default)	Yes	
900		JIRA	No	Business	Interactive_P4	100	200	Disabled (Default)	Yes	

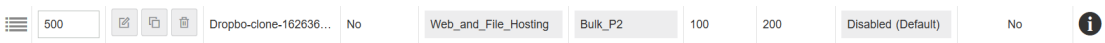
Users may not edit the application priority or name of a Defined Application. However, users may change the category, classification, response time thresholds, and probing intervals of a Defined Application, and add or delete match criteria for a pre-defined application.

Additionally, users may clone a Defined Application and further customize all values. To clone a Defined Application, click the **Clone** icon under Actions.



400		Dropbox	No	Web_and_File_Hosting	Bulk_P2	100	200	Disabled (Default)	Yes	

Once a Defined Application is cloned, it will appear as a User Defined Application to be edited as desired.



500		Dropbo-clone-162636…	No	Web_and_File_Hosting	Bulk_P2	100	200	Disabled (Default)	No	

Configure Site Groups (Optional)

Three site groups are defined by default for users to leverage. Additionally, users may create their own site groups.

The default site groups are:

- AllSites: This site group contains all of the sites in SD-WAN Edge.
- ControllerSites: This site group contains the NCN and Geo-Diverse NCN sites.
- NonControllerSites: The site group contains all client sites in SD-WAN Edge.

Default site groups may not be edited or deleted.

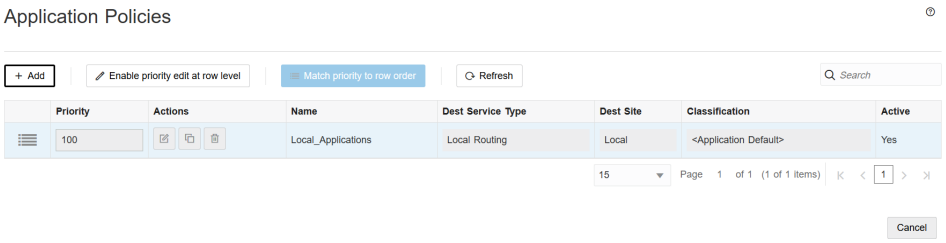
User created site groups may be added, edited, or deleted by opening **All Sites**, **Site Groups** in the Advanced view of the Configuration Editor.

A site may be in more than one site group. For example, if the Edge system consists of sites AG, and only sites A, E, and F use a particular application, a new site group containing those sites can be defined for use in a policy for that application.

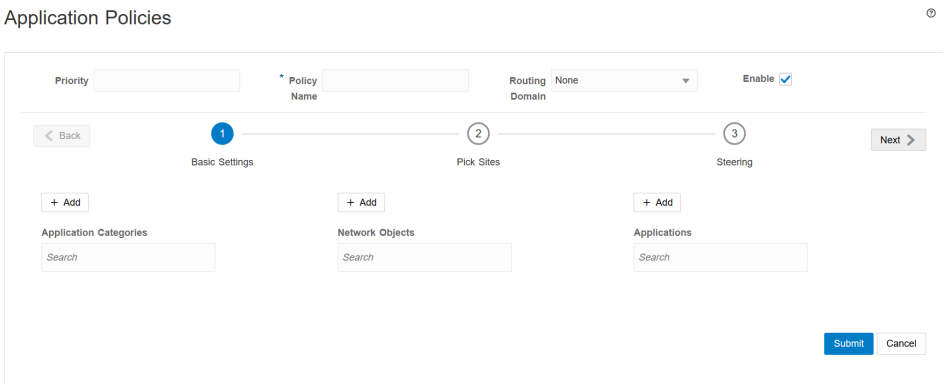
Configure Application Policies

Follow these steps to configure application policies in the Configuration Editor:

1. In the Advanced view of the Configuration Editor open **Application Policies**, **Create and Manage Policies**.



2. Click the **+** icon to add a new application policy. The new application policy will not be assigned with an automatically generated name - the Policy Name field will remain blank. Enter a descriptive name here.



3. Select a destination site (where traffic matching the policy will be sent), service type, and service name (if applicable). By default, the QoS classification for the policy will match the application the policy is applied to, but the user may select a different classification from the dropdown to override the default.

> **Note:**
>
> QoS classification is only applied when the application is steered to a Conduit service.

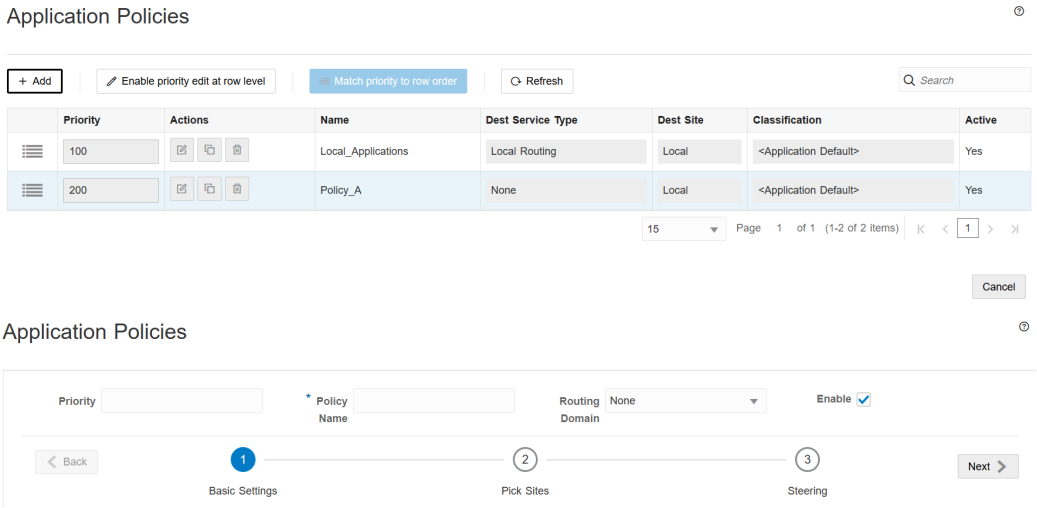
A policy may have multiple match criteria defined:

- Application Category Match: The user may select a category (group of applications) and steer the category to a service.
- Application Match: The user may select a specific application and steer it to a service.
- Network Object Match: The user may define source group address prefixes under **Global**, **Network Objects** and use them as a source match for the application policy.
- Site Group Match: The user may define a site group as a source match for a policy.
- Site Match: The user may define a single source site match for a policy. If the user has a single site with unique services this option can be selected for the specific site. The application policy is then only applied to that site.

4. To search for a specific application match, begin typing with the dropdown selected to find an application in the list.

> **Note:**
>
> Configuring duplicate application policies with the same match criteria (source network, site, and application) that steer to different services is not supported.

Application priorities are automatically incremented by 100. When a user would like to re-order policy priorities, the application priority can be set to fall between any two other priorities.



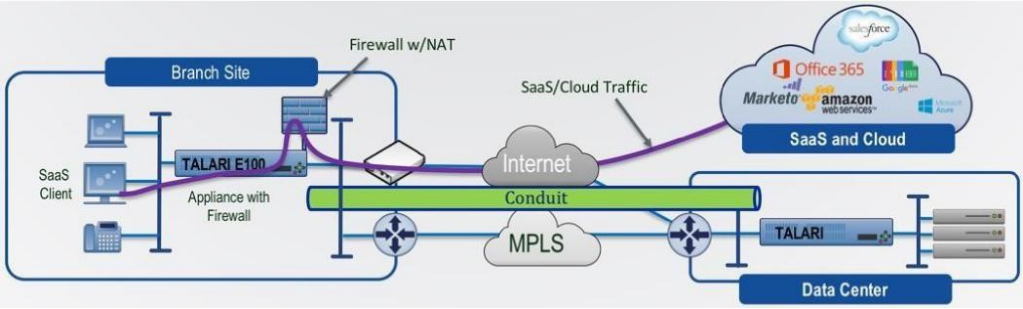
Configure Site Response Time Bias

To configure a Site Response Time Bias at a site which has higher expected latency for applications:

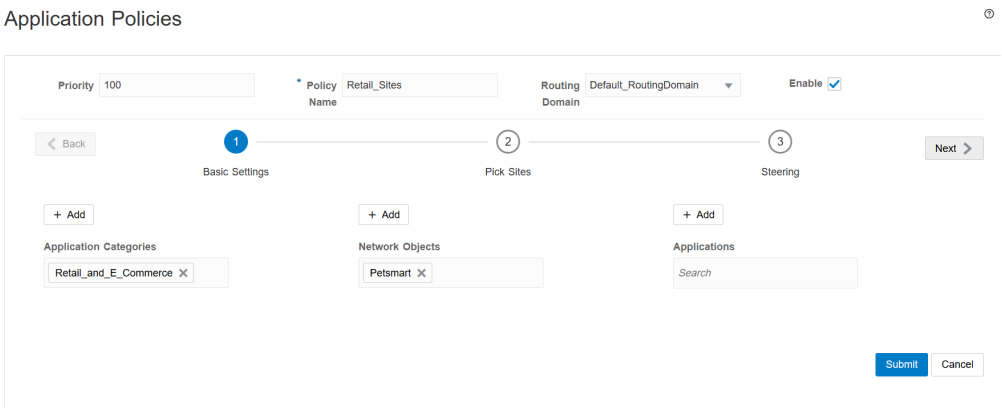
1. Navigate to **All Sites**, **[Site]**, **Basic Settings** in the Configuration Editor.
2. Click the **Edit** icon and edit the Application Normal RTT adjust time and Application Warning RTT adjust time fields. These values will be added to the application RTT for all applications at the site.

Configuration Examples

Steer to Local Internet Service

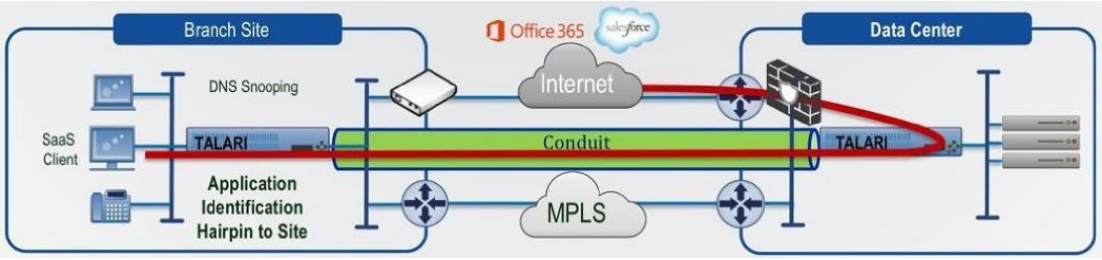


In the scenario pictured above, certain application traffic from the branch site is steered directly to the local internet service. Below is a sample application policy for this scenario:

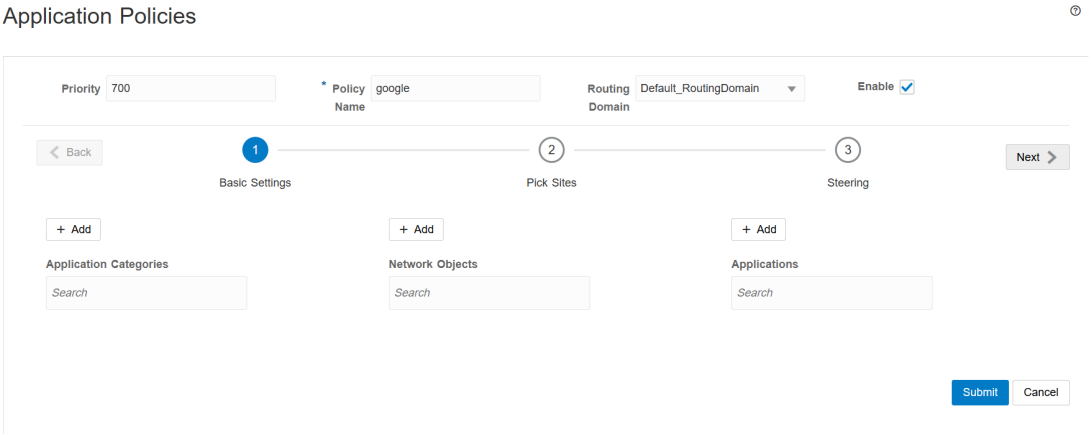


In this policy, traffic for all enabled applications in the Retail_and_E_Commerce category and the Petsmart application to/from the sites in site group Site-RS-PS will be steered to the local internet service at each site. In order for this policy to perform as intended, the sites in the chosen site group must all have a local internet service enabled which has usage allowed on at least one WAN link, and the internet service must be provisioned adequately to serve the application traffic. Further, you neet to enable "WAN-to-WAN Forwarding" or "Conduit-to-Internet Intranet Forwarding".

Hairpin to NCN or Data Center Internet Service



In the scenario pictured above, certain application traffic from a branch site is hairpinned to the NCN or data center for internet access. Below is a sample application policy for this scenario.



In this policy, traffic that matches the Google_G_Suite and Google_Drive applications to/from site RS is steered to destination site PPARK, where it uses the PPARK internet service. In order for this policy to perform as intended, the NCN must have a local internet service enabled which has usage allowed on at least one WAN link, and the internet service must be provisioned adequately to serve the application traffic. Further, "WAN-to-WAN Forwarding" or "Conduit to Internet Intranet Forwarding" must be enabled.

Verification

Once Application Policies have been configured, new routes and rules are automatically generated as needed in the configuration based on the policy criteria. These routes and rules are not editable by users.

Rules created based on application policies will display the parent Application Policy:

Routes created based on application policies will display the parent Application Policy and the application they apply to, as well as the service type and name (if applicable):

Import a Signature Library

To import the latest Application Presets Signature library you first create a new configuration.

1. Click the **Configuration Management**, **Configuration Editor** path. A new tab opens with the Configuration Management pop-up window in the foreground.

2. Ensure the baseline configuration you will add the signature library to is selected from the drop down.
3. Click **Import**.
4. The Name Conflict window appears if a selected configuration already exits. You may
   a. Change the Configuration Name value and click **Import**.
   b. Check the Overwrite option and click **Import**.
5. The screen returns to the Configuration Management window with you new or overwritten configuration selected as active.

Next, import the application presets file to this new configuration.

1. Click **Apply** button to edit the current configuration.
2. Click **Application Policies** located in the top bar on the screen.
3. Click on **Import Application Presets File** located under the previously-clicked **Application Policies**.
4. In the drop-down list "... From SD-WAN Edge", select the `latest_preset.cfg`.
5. Ensure that the "Overwrite preset changes in current package" option is selected.
6. Click **Import**. A status message will briefly display on the screen.
7. Once imported, the new Application Signature file will be applied to any new Configuration file.

> **Note:**
>
> New definitions still require configuration to become active.

Monitoring

The Application menu provides access to Application Identification monitoring data. The expected information is described by page and menu item within each of the sections below.

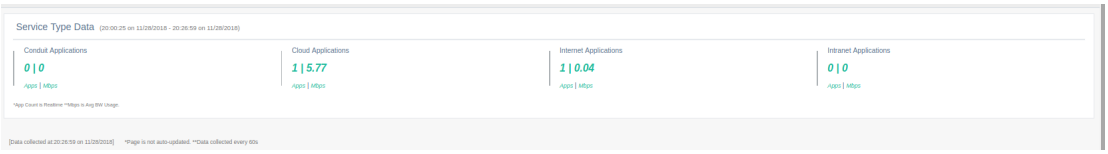
Dashboard

From the left navigation menu, the application Dashboard can be found by navigating to **Dashboard**, **Application Dashboard**. The Application Dashboard provides at-a-glance insight into application behavior and usage for all enabled applications at a site:

> **Note:**
>
> Timestamps may not be displayed on smaller screens.

Service Type Data

The Service Type Data section at the top of the Application Dashboard displays service data in summary with the ability for the user to view additional details. The summary data displayed is realtime information which may change each time the Dashboard is refreshed. This data is summarized for up to seven days or from the last reboot/restart of the system.



Users may click on the **Conduit Applications**, **Internet Applications**, and **Intranet Applications** text on the top of the Service Type Data on the Application Dashboard to view additional details for Conduit Applications, Internet Applications, or Intranet Applications respectively. Additionally, if the user would like to see information for all Service Types at one time, this can be achieved by clicking on the **Service Type Data** header on the top of the Application Dashboard to be directed to the Service Type data page. To navigate to this same page via the left navigation menus, this page is accessible by clicking on the **Application Menu**, **Service Type** menu item.

Top 5 Applications

Within the Application Dashboard, the Top 5 Applications (Cumulative Data) may be viewed by individual application, or by application category. The Top 5 Applications cumulative data displayed is summarized since the last reboot / restart of the system.

Additionally, for more information on all applications beyond the Top 5, the user may click on the text that reads **Top Applications** on the top of this section of the Application Dashboard, or navigate through the menus to **Application**, **Cumulative Usage**.

Application Health

The Application Health section of the Application Dashboard will provide details on the health of up to ten applications enabled for probing. Application Health data is realtime (i.e. not cumulative over any time frame) and is expected to change each time the Application

Dashboard is refreshed to show the latest information.

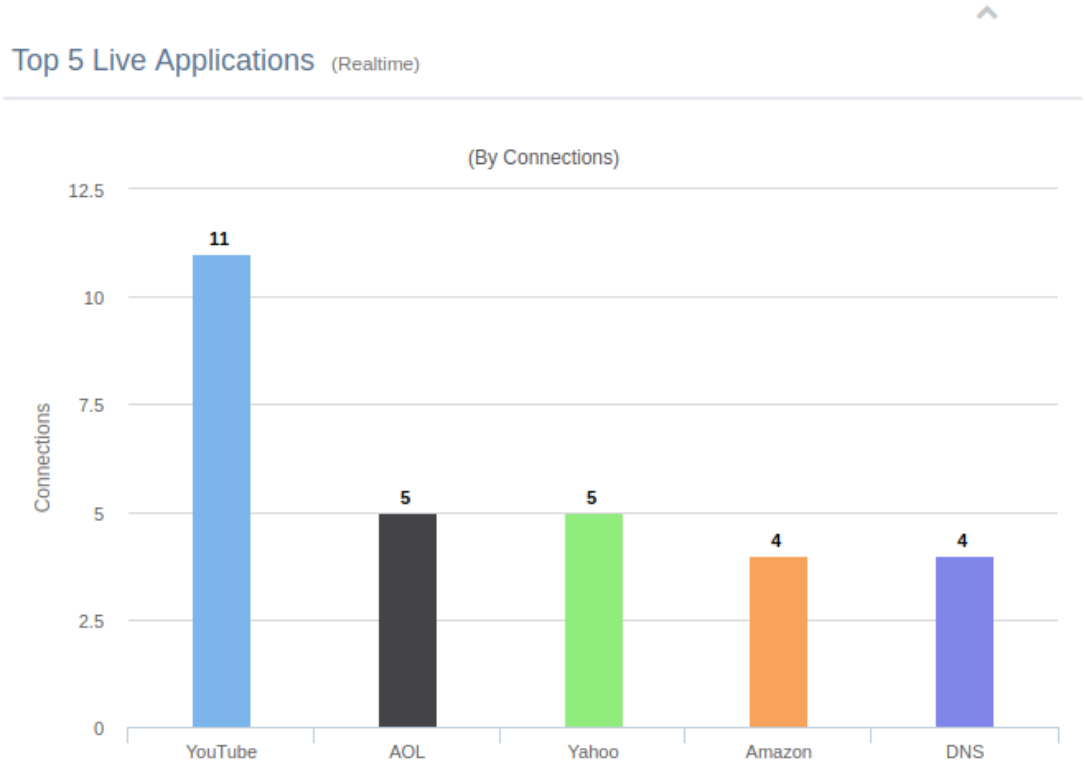
Additional applications beyond the initial ten shown on the Application Dashboard may be viewed by either clicking the **Application Health** text header on the Application Dashboard, or by navigating to the **Application**, **Health and Response** on the left navigation. For more details see the Health and Response Time Section.

Applications will be classified as Normal, Warning, or Critical based on the response time thresholds specified by the user for Normal and Warning. Any application that has a response time above the Normal threshold specified by the user will be classified as “Warning” under Application Health. Similarly, any application that has a response time above the Warning threshold specified by the user will be classified as “Critical” under Application Health.

The Probe Loss % column displayed for Application Health is calculated based upon the following calculation: (probing request sent - probing reply received)/(probing request sent). Probe loss is not used to determine application health.

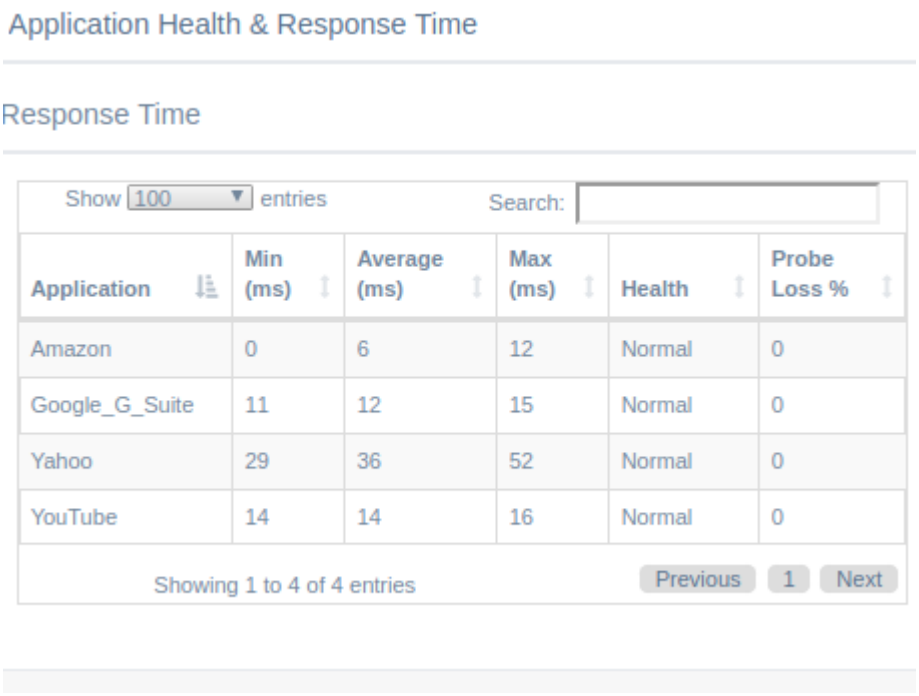
Top 5 Live Applications

The Top 5 Live Applications provides a realtime view of the top 5 live applications based upon the number of connections. The Top 5 Live Applications data is realtime (i.e. not cumulative over any time frame) and is expected to change each time the Application Dashboard is refreshed to show the latest information. To appear as a Live Application, an application must be enabled and traffic must be identified by the system.



Health and Response Time

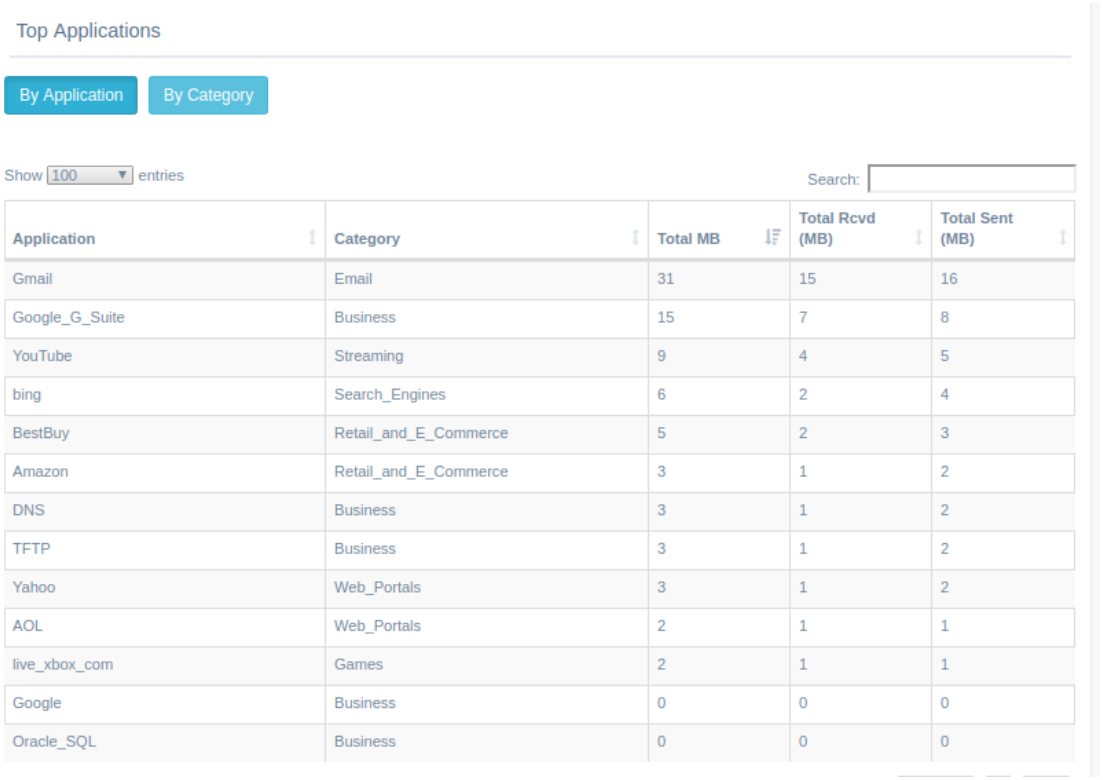
Accessible from the navigation menu from **Application**, **Health & Response**. The Health and Response Time screen shows health information for all currently enabled applications:



The minimum, maximum, and average RTT in milliseconds is shown for each application, along with a current health designation and percentage of lost probes.

Cumulative Usage

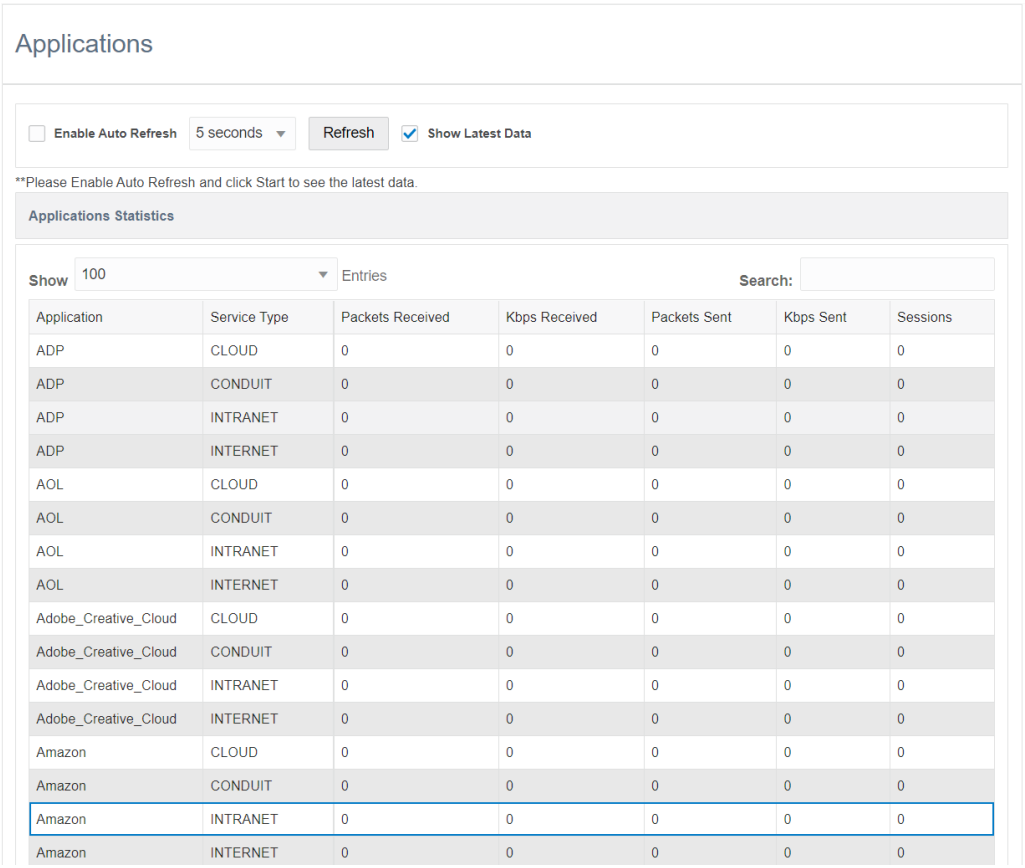
Accessible from the navigation menu from **Application**, **Cumulative Usage**. The Cumulative Usage screen shows the overall usage per application or application category:



Application	Category	Total MB	Total Rcvd (MB)	Total Sent (MB)
Gmail	Email	31	15	16
Google_G_Suite	Business	15	7	8
YouTube	Streaming	9	4	5
bing	Search_Engines	6	2	4
BestBuy	Retail_and_E_Commerce	5	2	3
Amazon	Retail_and_E_Commerce	3	1	2
DNS	Business	3	1	2
TFTP	Business	3	1	2
Yahoo	Web_Portals	3	1	2
AOL	Web_Portals	2	1	1
live_xbox_com	Games	2	1	1
Google	Business	0	0	0
Oracle_SQL	Business	0	0	0

Live Sessions

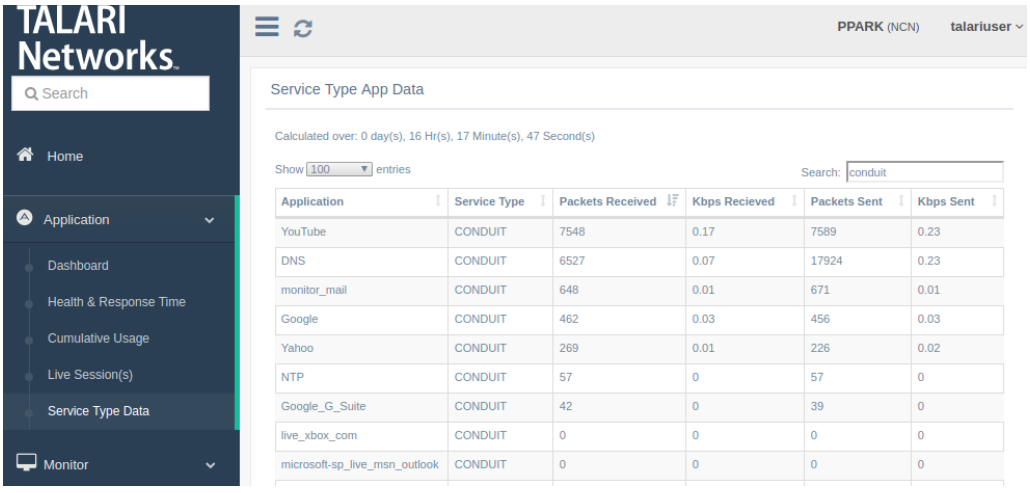
Accessible from the navigation menu from **Application**, **Live Sessions**. The Live Sessions screen shows live application statistics and can be set to auto refresh.



Application	Service Type	Packets Received	Kbps Received	Packets Sent	Kbps Sent	Sessions
ADP	CLOUD	0	0	0	0	0
ADP	CONDUIT	0	0	0	0	0
ADP	INTRANET	0	0	0	0	0
ADP	INTERNET	0	0	0	0	0
AOL	CLOUD	0	0	0	0	0
AOL	CONDUIT	0	0	0	0	0
AOL	INTRANET	0	0	0	0	0
AOL	INTERNET	0	0	0	0	0
Adobe_Creative_Cloud	CLOUD	0	0	0	0	0
Adobe_Creative_Cloud	CONDUIT	0	0	0	0	0
Adobe_Creative_Cloud	INTRANET	0	0	0	0	0
Adobe_Creative_Cloud	INTERNET	0	0	0	0	0
Amazon	CLOUD	0	0	0	0	0
Amazon	CONDUIT	0	0	0	0	0
Amazon	INTRANET	0	0	0	0	0
Amazon	INTERNET	0	0	0	0	0

Service Type Data

Accessible from the navigation menu from **Application**, **Service Type Data**. Displays a full list of all service type data with sort ability by column.

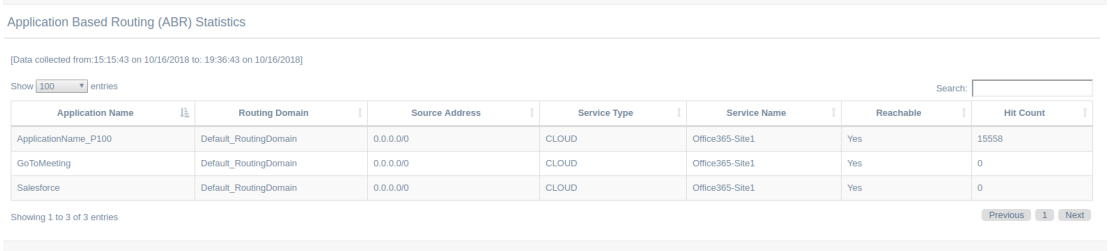


Application	Service Type	Packets Received	Kbps Recieved	Packets Sent	Kbps Sent
YouTube	CONDUIT	7548	0.17	7589	0.23
DNS	CONDUIT	6527	0.07	17924	0.23
monitor_mail	CONDUIT	648	0.01	671	0.01
Google	CONDUIT	462	0.03	456	0.03
Yahoo	CONDUIT	269	0.01	226	0.02
NTP	CONDUIT	57	0	57	0
Google_G_Suite	CONDUIT	42	0	39	0
live_xbox_com	CONDUIT	0	0	0	0
microsoft-sp_live_msn_outlook	CONDUIT	0	0	0	0

ABR Statistics

THe Application Based Routing Statistics page is accessible from the navigation menu from **Application**, **ABR Statistics**. This page lists Application Name, Routing Domain,

Source Address, Service Type, Service Name, Reachable or not and the hit count for each application.



A

Upgrade Scenarios

Upgrade with No Applications Defined

If no application objects have previously defined in the configuration and no changes are made to the configuration in conjunction with the upgrade, the application dashboard will show “0” for all service type data, and Top Applications, Top Live Applications, and Application Health will display no data. Pre-set applications will be displayed in the Configuration Editor, but all pre-set applications are disabled by default.

> **Note:**
>
> When no Application Health data is available, the message “No real time snooping data available” will be displayed.

Upgrade with Applications Defined

If application objects have been previously defined in the Talari configuration with domain names as match criteria, DNS snooping is automatically enabled for these applications after upgrading. The application dashboard will automatically begin populating the Service Type Data, Top Applications, and Top Live Applications sections. No Application Health or Application Category data will be available.

Oracle defined applications will be displayed in the Configuration Editor, but all pre-set applications are disabled by default.

> **Note:**
>
> When no Application Health data is available, the message “No real time snooping data available” will be displayed.

Upgrade and Customize Applications

If application objects have been previously defined in the configuration with domain names as match criteria, DNS snooping is automatically enabled for these applications after upgrading. If a probing interval is enabled on applications after upgrade, all sections of the application dashboard will populate, including Application Health data. If previously-configured application objects are edited to add category information or Oracle defined applications are enabled, Application Category data will be available on the Application Dashboard.

Revert to an Earlier Release

After a configuration file has been edited in the Configuration Editor, it cannot be used when reverting back to a previous release. Configuration files are not compatible with previous software versions.

If a configuration was saved prior to upgrading, it may be loaded to Change Management on the NCN. After confirming that the appropriate configuration is selected, follow the process outlined in the Software Update Guide to upload new software packages for the desired version and proceed with the Change Management process as usual to stage and activate.

B

Application ID Classification Mapping

Summary of how application policy priority maps to existing Default Rules.

Policy Priority Name	Default Rule	Classification
Real-Time-P1	Default_EF	Real-Time
Real-Time-P2	Default_UDP	Real-Time
Interactive-P2	Default_SSH	Interactive
Interactive-P3	Default_HTTP	Interactive
Interactive-P4	Default_Telnet	Interactive
Bulk-P1	Default_CIFS	Bulk
Bulk-P2	Default_FTP	Bulk
Interactive-P1	Default_ICMP	Interactive

C

Application Signature Library v2.0

The Application Signature Library v2.0 includes the following applications:

Table C-1 Commercial Applications and Categories for Enhanced Application ID feature set

Name	Category
Office 365	Business
Microsoft OneDrive	Web and File Hosting
Salesforce	Business
Box	Web and File Hosting
YouTube	Streaming
Gmail	Email
Concur	Business
Jira	Business
Zendesk	Business
ADP	Business
Dropbox	Web and File Hosting
Adobe Creative Cloud	Business
Confluence	Business
DocuSign	Business
FedEx US	Business
GitHub	Business
Microsoft	Business
NetSuite	Business
ServiceNow	Business
Workday	Business
GoToMeeting	Collaboration
WebEx	Collaboration
Zoom (Application)	Collaboration
Zoom Phone	Collaboration
Zoom Cloud Room Connector	Collaboration
RingCentral	Voice
Vonage	Voice
The 8x8	Voice
Outlook	Email
Facebook	Social
LinkedIn	Social
Twitter	Social
Instagram	Social
Netflix	Streaming
Reddit	Social

Table C-1 (Cont.) Commercial Applications and Categories for Enhanced Application ID feature set

Name	Category
Snapchat	Social
Tumblr	Social
Pinterest	Social
Vimeo	Streaming
Pandora	Streaming
Spotify	Streaming
Yahoo Mail	Email
Voice Cisco Signal Control	Voice
Voice Signal Control	Voice
Voice H323	Voice
CAPWAP Control	Business
CAPWAP Data	Business
Cisco VPN	Business
Remote Desktop Protocol	Business
TACACS	Business
RADIUS	Business
Stateless Browsing	Business
Google	Business
Oracle SQL	Business
MS SQL	Business
SMTP	Business
NTP	Business
DNS	Business
TFTP	Business
Syslog	Business
NetFlow	Business
BBC	News
CNN	News
Fox News	News
MSNBC	News
IMDB	News
Amazon	Retail and E-Commerce
Best Buy	Retail and E-Commerce
eBay	Retail and E-Commerce
Walmart	Retail and E-Commerce
ESPN	Sports
FOX Sports	Sports
NBA	Sports
MLB	Sports
NFL	Sports
NHL	Sports
Apple iCloud	Web and File Hosting
Skype	Social

Table C-1 (Cont.) Commercial Applications and Categories for Enhanced Application ID feature set

Name	Category
Yahoo	Web Portals
Bing	Search Engines
Slack	Business
Facebook Messenger	Social
WhatsApp	Social
MSN	Web Portals
Wikipedia	Informational Databases
Ask	Social
Yelp	Informational_Databases
UPS	Retail and E-Commerce
USPS	Retail and E-Commerce
Forbes	News
The New York Times	News
The Huffington Post	News
CNET	News
Target	Retail and E-Commerce
AOL	Web Portals
Steam Community	Games
IGN	Games
GameSpot	Games
SteamPowered	Games
The Pirate Bay	Possibly Illegal Streaming
Craigslist	Retail and E- Commerce
Xfinity	Retail and E -Commerce
GoDaddy	Business
Groupon	Retail and E-Commerce
Home Depot	Retail and E-Commerce
Thesaurus	Informational Databases
Twitch	Games
VK	Social
Nextdoor	Social
PlayStation	Games
SoundCloud	Streaming
BuzzFeed	News
Trello	Collaboration
Crackle	Streaming
Daily Mail	News
Baidu	Search Engines
Zillow	Retail and E-Commerce
Kohls	Retail and E-Commerce

D

Application Signature Library v1.0

The Application Signature Library v1.0 includes the following applications:

Name	Category
Office 365	Business
Microsoft OneDrive	Web and File Hosting
Salesforce	Business
Box	Web and File Hosting
YouTube	Streaming
Gmail	Email
Concur	Business
Jira	Business
Zendesk	Business
ADP	Business
Dropbox	Web and File Hosting
Adobe Creative Cloud	Business
Confluence	Business
DocuSign	Business
FedEx US	Business
GitHub	Business
Microsoft	Business
NetSuite	Business
ServiceNow	Business
Workday	Business
GoToMeeting	Collaboration
WebEx	Collaboration
Zoom	Collaboration
RingCentral	Voice
Vonage	Voice
The 8x8	Voice
Outlook	Email
Facebook	Social
LinkedIn	Social
Twitter	Social
Instagram	Social
Netflix	Streaming
Reddit	Social
Snapchat	Social
Tumblr	Social
Pinterest	Social
Vimeo	Streaming
Pandora	Streaming

Name	Category
Spotify	Streaming
Yahoo Mail	Email
Voice Cisco Signal Control	Voice
Voice Signal Control	Voice
Voice H323	Voice
CAPWAP Control	Business
CAPWAP Data	Business
Cisco VPN	Business
Remote Desktop Protocol	Business
TACACS	Business
RADIUS	Business
Stateless Browsing	Business
Google	Business
Oracle SQL	Business
MS SQL	Business
SMTP	Business
NTP	Business
DNS	Business
TFTP	Business
Syslog	Business
NetFlow	Business
BBC	News
CNN	News
Fox News	News
MSNBC	News
IMDB	News
Amazon	Retail and E-Commerce
Best Buy	Retail and E-Commerce
eBay	Retail and E-Commerce
Walmart	Retail and E-Commerce
ESPN	Sports
FOX Sports	Sports
NBA	Sports
MLB	Sports
NFL	Sports
NHL	Sports
Apple iCloud	Web and File Hosting
Skype	Social
Yahoo	Web Portals
Bing	Search Engines
Slack	Business
Facebook Messenger	Social
WhatsApp	Social
MSN	Web Portals
Wikipedia	Informational Databases

Name	Category
Ask	Social
Yelp	Informational_Databases
UPS	Retail and E-Commerce
USPS	Retail and E-Commerce
Forbes	News
The New York Times	News
The Huffington Post	News
CNET	News
Target	Retail and E-Commerce
AOL	Web Portals
Steam Community	Games
IGN	Games
GameSpot	Games
SteamPowered	Games
The Pirate Bay	Possibly Illegal Streaming
Craigslist	Retail and E- Commerce
Xfinity	Retail and E -Commerce
GoDaddy	Business
Groupon	Retail and E-Commerce
Home Depot	Retail and E-Commerce
Thesaurus	Informational Databases
Twitch	Games
VK	Social
Nextdoor	Social
PlayStation	Games
SoundCloud	Streaming
BuzzFeed	News
Trello	Collaboration
Crackle	Streaming
Daily Mail	News
Baidu	Search Engines
Zillow	Retail and E-Commerce
Kohls	Retail and E-Commerce