Reports

- Activity Viewers
- Report Settings
- Log Processing
- Device Detection

Activity Viewers

Live Drilldown

Dive deep into logged activity data.

Important Note:

Data in Live Drilldown will have at least a **3 minute delay** from actual occurance. If you need realtime traffic information, use the Realtime Log Viewer, accessed as follows:

- **Specific device:** Select `View Realtime Log Lines` in the hamburger menu of a Remote Device record
- **Entire system:** Select `Realtime Log Viewer` under Content Filter / Troubleshooting

Browse by Company

View all the traffic of a particular Company. (Most value in multi-tenant use-cases.)

Presents a list-view of all available Company records on the DrawBridge. After selecting a Company, the user is presented with the **Browse by Request Type**; see below for more information.

Browse by Category

View traffic statistics aggregated by Category.

Manipulate the data view with the following Select fields:

- Timerange
- Company
- Category
- Rating
- Parent Category

List view displays:

- Name of the Category

- Cumulative number of hits in the selected timerange
- Cumulative bandwidth in the selected timerange

Browse by Request Type

Note: Menu items (listed below), are basically automatic Traffic Type filters for the **Browse by Loglines** option, mentioned further below.

Request Types menu:

- **Page Views**
- **Media Views**
- **API Activity**
- **Application Files**
- **Erased Activity**
- **Shredded Activity**

Manipulate the data view with the following Select fields:

- Timerange
- Company
- Category
- Rating
- Parent Category

List views display:

Column	About
Domain	Base domain of the request
Device	Origin username or IP address of the request
Hits	Counter: displays the number of times this request was made
Bandwidth	Total bandwidth consumed by this request
Time	Timestamp of this request
Type	`Ads/Avatars/Cruft`, `API Calls`, `Audio/Video`, `General Files`, `Page Assets`, `Page Visuals`, `Programs/Applications`, `Web Page`
Category	What the request was classified as

Browse by Searches

View search queries entered by users on popular search and ecommerce sites.

Manipulate the data view with the following Select fields:

- Timerange
- Company
- Category
- Rating
- Parent Category

List view displays:

Column	About
Search term	The search query entered by a user
Device	Origin username or IP address of the request
Allow	Counter of how many time the request triggered this action
Block	Counter of how many time the request triggered this action
Domain	Site the request occured on
Category	Classification determined by the DrawBridge

Search Activity within the specified timerange by:

- Search Term
- Device
- Domain

Browse by Media Views

View Media Classification requests for media hosted on popular video hosting platforms

Manipulate the data view with the following Select fields:

- Timerange
- Company
- Category
- Rating

List view displays:

Column	About
Title	Title of the video

Column	About
Service	Platform hosting the video
Hits	Counter of how many times this request was performed

Search the data within the specified timerange by:

- Name/Title
- Service/Hosting platform

Browse by Page Titles

View title information for all visited websites. (The title is what displays in a browser tab.)

Manipulate the data view with the following Select fields:

- Timerange
- Company
- Rating
- Parent Category
- Category

List view displays:

Column	About
Title	Title of the website
Device	Device making the request
Domain	Base domain of the request
Category	Classification of the request

Search the data within the specified timerange by:

- Name/Title
- Device
- Domain

Browse by Antivirus Hits

Events logged by the optional Antivirus protection service

Manipulate the data view with the following Select fields:

- Timerange
- Company

List view displays:

Column	About
Name	Name of event
Domain	Domain of the request
File	Name of the file that was examined
Hits	Counter: number of times this file was requested
Bandwidth	Bandwidth consumed by this request

Search the data within the specified timerange by:

- Name

Browse by Applications

View traffic that originated from Applications/programs (not necessarily browsers).

Manipulate the data view with the following Select fields:

- Timerange
- Company
- Application
- App Type

List view displays:

Column	About
Name	Name of the Application
Type	Type of Application
Hits	Counter: Number of requests mapped to this Application
Bandwidth	Bandwidth consumed by this Application
Time	Estimated cumulative period of time this application generated requests

Search the data within the specified timerange by:

- Name

Browse by Domains

View all traffic sorted by domain.

Manipulate the data view with the following Select fields:

- Timerange
- Company
- Action
- Category
- Rating

List view displays:

Column	About
Domain	Domain name of the request
Device	Origin of the request
Hits	Counter: number of times requested
Bandwidth	Bandwidth consumed by this domain
Time	Estimated cumulative period of time this domain was visited
Type	`Ads/Avatars/Cruft`, `API Calls`, `Audio/Video`, `General Files`, `Page Assets`, `Page Visuals`, `Programs/Applications`, `Web Page`
Category	Classification of the request

Search the data within the specified timerange by:

- Name/Domain
- Device

Browse by Loglines

View all traffic logged and classified.

Manipulate the data view with the following Select fields:

- Timerange
- Company
- Request Type
- Filter Action
- Category

- Rating

Match data with the following free text fields:

- Devices
- domain

Important: This view requires clicking the blue magnifying-glass Search button to apply filters to the data; it does not update "live" as the other views do.

List view displays:

Column	About
Date	Timestamp of the logline
Device	Origin of the logline
Action	Filter action taken on the logline
Method	HTTP method of the logline
Mimetype	Type of request
Length	Size/Length of the HTTP response body
Rating	Classification rating of the logline
Category	Classification rating of the logline
URL	Exact URL of this logline; click for further details

Record view

Each logline entry has a Record view with more details that is accessed by clicking the URL displayed in the logline row.

Technical data is displayed under the following headers:

- URL Details
- Application Details
- Filter Details
- Device Details
- Client Details

Classification data is shown under the following headers:

- Rating Details
- Category Details
- Rule Details

History

Report History

List of printable, regularly scheduled Usage Reports for past report periods.

Displays a list view of all report file archives.

Column	About
Report	Name of the report
Start Date	Beginning of the timeperiod covered by the report
Layout	Data visualization preset used by the report
Company	Company associated with the report

Filter the view with the following search/select fields:

- Name
- Timeframe
- Interval
- Company

Record View

Parameter	About
Sections	Data Visualization preset(s) included in this report
Schedule/Details	Link: Name of the scheduled job that ran this report
Report Type	`Alert/Notification` or `Usage Report`
Date Range	Timeperiod covered by this report
Generated on	Timestamp of report creation
Status	`Succeeded` or `Failed`
Time Taken	Amount of time it took to crunch the data to generate this report

Report Record Header buttons:

- **Delete** this report record with the red trashcan Delete Report Archive button
- **Resend** this report file with the green airplane Resend Report button
- Hamburger menu:

    - **Report Settings:** Jumps to the corresponding Report Schedule record
    - **Scheduled/Active Reports**

Informational Tabs

- **Report Files**
    - Presents a link to access the HTML report file
- **Recipients**
    - Displays **Current Recipients** and **Available Recipients** in two lists.
    - Move people from one list to the other one with the appropriate **-** or **+** buttons.
    - Add a Company Recipient with the `Add Company Recipient` button: pops up a form window to add the recipient

Note that available recipients are the contacts associated with the Company, and also any Accountability Contacts if the Company is associated with an Accountability Policy.

Autofix History

List of Autofixes and details for each incident.

List View displays:

Column	About
Date	Date of the Autofix request
User / IP	Remote Device Username, Person (Active Directory), or IP address that requested the Autofix
Domain	The web link requested to be analyzed by Autofix

Filter the view with the following search/select fields:

- Time Range
- Company
- Name

View an individual Autofix Record by clicking the URL displayed in the Domain column.

Autofix Record View

Parameter	About
Date	Timestamp of the request
Expiration	When the filter policy changes made by the AutoFix will revert to the original settings

Parameter	About
Block Details	URL that was blocked
Company	Associated company of the User or Device that requested the Autofix
Remote / Local Device	Remote Device User, Person, or IP address which requested the Autofix
Device User	Associated Person record of the Remote Device, when applicable
Comments	Information entered by the person requesting the Autofix
Blocking Category	The Classification initially determined by the DrawBridge
Score	Score of the Blocking Category for this web request
Tier	`Level1`, `Level2`, or `Level3`; see Essential Concepts: Preferences for more information
Explanation	Observations of the Autofix reclassification operation
Autofix Permitted	Autofix is permitted (True) or not (False) for this category. See Essential Concepts: Preferences for more information
Device Group	Device Group membership of the Remote / Local Device requesting the Autofix

Send for Human Review button: sends technical data of this event to Compass Foundation support staff for further analysis.

Be sure to click **Send for Human Review** if the Autofix request was used to access content that was genuinely misclassified. Compass Foundation support staff will review the technical data sent over in the background and, if needed, release a permanent fix that benefits all DrawBridge users.

Human Review

List of blocked URLs submitted for Human Review.

List View displays:

Column	About
Date	Date of the Human Review request
User / IP	Remote Device Username, Person (Active Directory), or IP address that requested the Human Review
Domain	The web link requested to be analyzed

Filter the view with the following search/select fields:

- Time Range
- Company
- Name

View an individual Human Review Record by clicking the URL displayed in the Domain column.

Human Review Record View

Parameter	About
Date	Timestamp of the request
URL	URL that was blocked
Company	Associated company of the User or Device that requested the Human Review
User	The filter username, where applicable, that requested the Human Review
Device User	Associated Person record of the requesting Remote Device, when applicable
Comments	Information entered by the person requesting the Human Review
Blocking Category	The Classification determined by the DrawBridge
Permitted by Preferences	Preferences settings allow (`Yes`) Human Review requests for this Category or not (`No`)
Score	Score of the Blocking Category for this web request
Submitted	The Human Review request was sent (`Yes`) to Compass Foundation support or not (`No`)
Autofixed	`Yes` or `No` -- indicates whether the request was triggered from an Autofix request
Device Group	Device Group membership of the Remote / Local Device requesting the Autofix

Report Settings

Scheduled Reports

List view of all scheduled report jobs.

Filter the view with the following search/select fields:

- Interval
- Report (Type)
- Company

List View displays:

Column	About
Report	Type of report that is scheduled
Layout	Data Visualization Template preset selected for the scheduled report
Company	Associated Company of the scheduled report

View a Scheduled Report record by clicking the link in the Report column

Scheduled Report Record view

Parameter	About
Report	Report type
Company	Associated Company of this schedule record
Delivery	Email report files, email report links, or save to DrawBridge only (no email)
Recipients	Groups of recipients
Report Detail	`Combined - all usage in one file` or `Detailed - One File per User / IP`
Report Type	`Usage Report`, `Alert/Notification`, `DNS Firewall`, or `Access Policy Report`
Report Scope	`All Users/IPs in the Company` or `Manually Specified Users/IPs`

Scheduled Report record header menu:

- **Add** a scheduled report with the blue **+** Create Report button
- **Edit** this scheduled report with the green pencil Update Report button
- **Delete** this scheduled report with the red trashcan Delete Report button
- **Bookmark** this report with the blue ribbon Bookmark this Page button
- Hamburger menu:
  - **Report History:** Jump to the report archives for this scheduled report
  - **Add New Schedule:** Add an additional schedule line for this report
  - **Scheduled Reports:** Jump to Scheduled Reports
  - **Inactive Reports:** Jup to Inactive Reports
  - **Record Activity Stream:** View the changelog for this scheduled report record
- Sync menu (**blue chain icon**)
  - **Create on Sync Publisher:** Push this record to the Sync Server

Informational Tabs

- **Schedules:** List view of scheduled runtime(s); Delete with the red trashcan Delete Report Schedule button
- **Recipients:** List views of Current Recipients and Available Recipients; Add Company Recipients and Add (Accountability) Policy Recipients with buttons of the same name. Remove recipients with the red **-** button available on each Current Recipient line.

Report Layouts

List view of all available Report Layouts (preset data visualization templates) that can be applied to Scheduled Reports.

Column	About
Name	Name of the Layout
Sections	Preset data visualization sections included in the layout
Company	Associated Company, if applicable
Policy	Associated Accountability Policy, if applicable

Report Layout record view

Parameter	About
Builtin Layout	This preset was included with the DrawBridge (`True`) or was user created (`False`)
Type	`Usage Report`, `Alert/Notification`, `DNS Firewall`, or `Access Policy Report`

Parameter	About
Report Sections	List; preset data visualizations included in this layout (see below)

Report Layout record header menu:

- **Add** a new report layout with the blue **+** Create Report Layout button
- **Clone** this report layout with the yellow Clone Report Layout button
- **View changes to this record** with the blue Record Activity Stream button
- **Bookmark** this page with the blue ribbon Bookmark this Page button
- Sync menu (**blue chainlink icon**)
  - **2 Way - Push / Pull from Server:** call a sync run for this record
  - **Push to Sync Publisher:** send this record to the sync server
  - **Pull from Sync Publisher:** fetch this record from the sync server
  - **Mark to Resync:** flag this record for inclusion in the next sync server run

Report Sections

Layouts contain one or more of the following Sections:

Section	About
`accesspolicy`	
`api`	List of domains that are likely to have been visited programatically by an operating system or other software
`autofixes`	List of Autofix requests, including the requesting user/IP address, the timestamp, URL requested, action taken, and additional information
`categories`	Overview graph of all most popular Categories visited, by percentage
`disinfected`	
`erased`	List of "background traffic" domains that were most likely linked to by websites (not visited directly by a user
`graphs`	Time-of-day Usage graph and also graphs of Page View and Search ratings and actions taken
`mediaviews`	List of videos loaded in a browser; only major hosting platform supported: YouTube, Vimeo
`pagetitles`	Full-text of the Title *every single page* loaded in a browser. The "Title" is what displays in a browser tab. Extremely detailed.
`pageviews`	List of domains that are likely to have been visited in a browser by a human
`searches`	Full-text of search queries entered on major search and ecommerce platforms

Section	About
`shredded`	List of domains that were denied on every request; origin may be system/program or human

Report Presets

List view of all Report presets, and Policy ownership, where applicable

Filter the view with the following search/select fields:

- Preset (Name)
- Template (Name)
- (Accountability) Policy

List View displays:

Column	About
Report	Name of the Report
Layout	Data Visualization Template preset selected for the scheduled report
Policy	Associated (Accountability) Policy of the Report Preset, where applicable

View a Report Preset record by clicking the link in the Report column

Report Preset record view

Parameter	About
Preset	Name of the preset
Policy	Associated Accountability Policy, if applicable
Layout	Layout used by this Preset
Schedule	Default schedule interval assigned to this Preset
Delivery	Email Report files, Email Report Links, or Save Only (no email)
Recipients	Default recipients of this Preset

Report Layout record header menu:

- **Add** a Report Preset with the blue **+** Create Report Preset button

- **Edit** this Report Preset with the green pencil Update Report Preset button
- **Clone** this Report Preset with the yellow Clone Report Preset button
- **Delete** this Report Preset with the red trashcan Delete Report Preset button
- **View the record changelog** with the blue Record Stream Activity button
- **Bookmark** this record with the blue ribbon Bookmark this Page button
- Sync menu (**blue chainlink icon**)
  - **Create on Sync Publisher:** push this record to the sync server
  - **2 Way - Push / Pull from Server:** call a sync run for this record
  - **Push to Sync Publisher:** send this record to the sync server
  - **Pull from Sync Publisher:** fetch this record from the sync server
  - **Mark to Resync:** flag this record for inclusion in the next sync server run

Note: **Built-in** (included with the DrawBridge) report presets are not editible, or deletable, and therefore won't have all the record header menu options shown above.

Log Processing

Logline Filters are employed to ensure only relevant human activity is stored in the DrawBridge web activity database.

Log Servers + **Log Sender Batches** together are an optional function used for export of DrawBridge filtering logs to an external web traffic log analysis service.

When configured: a device is filtered by the DrawBridge, which logs all the web traffic of that device. Then, on a schedule, the DrawBridge uploads those web traffic logs to a separate log analysis/Reporter server for additional operations to be performed.

Important Note: The Log Server/Sender system is inactive unless the following two conditions are met:

- A Log Server is configured. (See below)
- A Log Server Account Number is configured on one or more Company records. See **Accounts: Companies** for more information.

Logline Filters

Remove unwanted Log Lines before saving them to Reporter database.

Displays a list view of rulesets which apply to loglines prior saving them in the DrawBridge log database.

List view displays:

Column	About
Sequence	Priority of rule when processing is performed
Filter	Name of rule
Scope	Defines operations of the rule
Field	Parameter of Logline database field to which the rule applies
Operator	Data matching parameter (`In`, `Contains`, `Starts With`, and so forth)

Logline Filter Record view

Parameter	About
Name Details	Name of the rule
Notes	Comments about the rule, where applicable
Matches If	Expressions which trigger the rule
data list	Exact text that is referenced in the expression.

Logline Filter Record header buttons:

- **Add** a Logline Filter record with the blue **+** Create Logline Filter button
- **Edit** this Logline Filter record with the green pencil Update Logline Filter button
- **Delete** this Logline Filter record with the red trashcan Delete Logline Filter button
- Sync menu (**blue chainlink icon**)
  - **2 Way - Push / Pull from Server:** call a sync run for this record
  - **Push to Sync Publisher:** send this record to the sync server
  - **Pull from Sync Publisher:** fetch this record from the sync server
  - **Mark to Resync:** flag this record for inclusion in the next sync server run

Scope options:

A rule can apply with the following scope of action:

- `Skip All Logging` -- Discard/Don't Save or Upload traffic matching this rule
- `Log Summary Details Only` -- Skip detailed logging data for traffic matching this rule
- `DNS Log Lines` -- Discard/Don't Save or Upload traffic containing these domain names

Log Servers

Uploaded Log Lines to compatible Report Server for further processing.

Displays a list view of configured Log Servers.

List View displays:

Column	About
Name	Display name of the log server
URL	Web address of the log server

Log Server Record View

Parameter	About
Name	Display name of the Log Server
Status	This record is Active or Inactive
URL	Web address of the log server

Log Server Record header buttons:

- **Add** a Log Server record with the blue **+** Create Log Server button
- **Edit** this Log Server record with the green pencil Update Log Server button
- **Delete** this Log Server record with the red trashcan Delete Log Server button
- **Bookmark** this record with the blue ribbon Bookmark This Page button
- Sync menu (**blue chain icon**)
  - **Create on Sync Publisher:** Push this record to the Sync Server

Log Sender Batches

Log Sender Batch Details

Displays a list view of all configured Log Sender batches for Company records which have a Log Server Account number specified.

Filter the data with the following Select field:

- Company

List View displays:

Column	About
Name	Display name of batch job
Company	Associated company of the batch job
Date	Timestamp of last batch job run event
Uploaded To	Timestamp of most recent data uploaded
Results	What the Log Processor job did

Log Sender Batches is informational-only and does not have a record view.

FAQ:

- **Q:** Why does the Log Sender Batch indicate 0 lines uploaded, even though devices on the Company are being used?
  A: Either the devices are not properly connecting to the DrawBridge, or, any data that was recorded was considered system activity, not human activity, and was therefore discarded. See **Logline Filters** above for more information.

Device Detection

Detect network devices by analyzing traffic.

User Agents

A User Agent (UA) text string identifies the software making a web request in HTTP. For example, a browser may identify as a particular version of Chrome.

List view displays:

Column	About
User Agent	The exact text string of the UA
Device	Device type assigned to the UA
App	Application type assigned to the UA

Click the User Agent name link to view an individual User Agent record.

User Agent Record View

Parameter	About
Device	The Device Type contained in the UA
Application	The Application contained in the UA
OS	The Operating System contained in the UA
Canonical ID	The globally-unique identifier in the DrawBridge ecosystem
Device Type	The device type assigned to the UA
Application Type	The Application type assigned to the UA

User Agent Record header buttons:

- **Add** a new User Agent record with the blue **+** Create User Agent Record button
- **Edit** this User Agent record with the green pencil Update User Agent Record button
- **Delete** this User Agent record with the red trashcan Delete User Agent Record button
- **Bookmark** this User Agent record with the blue ribbon Bookmark This Page button

Ja3 Hashes

Ja3 hashes can be used to positively identify an application based on a TLS fingerprint. Read more about the standard on the official Github page.

List view displays:

Column	About
Hash	Ja3 Hash
Notes	Information about the hash

Ja3 Hash Record View

Parameter	About
Name	Exact Ja3 hash
Notes	Further information about this particular hash
Canonical ID	Globally-unique record identifier in the DrawBridge ecosystem

List: **Application** -- displays Applications associated with this particular Ja3 hash. Add an Application to the hash record with the `Add TLS Fingerprint` button above the Application list view in the record.

**Ja3 Hash Record header buttons:

- **Add** a new Ja3 Hash record with the blue **+** Create J A3 Hash button
- **Edit** this Ja3 Hash record with the green pencil Update J A3 Hash button
- **Delete** this Ja3 Hash record with the red trashcan Delete J A3 Hash button
- **Bookmark** this Ja3 Hash record with the blue ribbon Bookmark This Page button
- Sync menu (**blue chain icon**)
  - **Create on Sync Publisher:** Push this record to the Sync Server

Devices

Specific hardware identity records.

List view displays:

Column	About
Model	The model of the Device
Brand	The manufacturer of the Device
Type	The device type, eg. `Smartphone`, `Desktop PC`, and so forth

Locate a specific record with the following search/select fields:

- Name

Device record view

Parameter	About
Name	Name of the specific hardware
Type	Device type, eg. `Smartphone`, `Desktop PC`, and so forth
OS	Operating System of the Device
Canonial ID	Globally-unique record identifier in the DrawBridge ecosystem
Brand	Manufacturer of the Device

Device Record header buttons:

- **Add** a new Device record with the blue **+** Create Device button
- **Edit** this Device record with the green pencil Update Device button
- **Delete** this Device record with the red trashcan Delete Device button
- **Bookmark** this Device record with the blue ribbon Bookmark This Page button
- Sync menu (**blue chainlink icon**)
  - **2 Way - Push / Pull from Server:** call a sync run for this record
  - **Push to Sync Publisher:** send this record to the sync server
  - **Pull from Sync Publisher:** fetch this record from the sync server
  - **Mark to Resync:** flag this record for inclusion in the next sync server run

Applications

Comprehensive listing of Mobile Device and Desktop applications

List view displays:

Column	About
Name	Name of the Application

Column	About
Type	Type of application, if known. Eg. `Browser`, `Mobile App`, and so forth

Locate a specific record with the following search/select fields:

- Name

Application record view

Parameter	About
Name	Name of the Application
Type	Type of application, if known. Eg. `Browser`, `Mobile App`, and so forth
Canonial ID	Globally-unique record identifier in the DrawBridge ecosystem

Application Record header buttons:

- **Add** a new Application record with the blue **+** Create Application button
- **Edit** this Application record with the green pencil Update Application button
- **Delete** this Application record with the red trashcan Delete Application button
- **Bookmark** this Application record with the blue ribbon Bookmark This Page button
- Sync menu (**blue chainlink icon**)
    - **2 Way - Push / Pull from Server:** call a sync run for this record
    - **Push to Sync Publisher:** send this record to the sync server
    - **Pull from Sync Publisher:** fetch this record from the sync server
    - **Mark to Resync:** flag this record for inclusion in the next sync server run

Informational Tabs

- **App Store IDs** -- List view of unique App Store identifiers; Add an ID with the `Add App Store ID` button above the list
- **UA Patterns** -- List view of User Agent regular expressions to match this Application; Add a UA pattern with the `Add UA Pattern` button
- **JA3 Hashes** -- List view of Ja3 Hashes of this Application; add a new hash with the `Add TLS Fingerprint` button
- **User Agents** -- List view of User Agent strings associated with this Application

Applications (ACL-ready)

Accessed as a sub-menu item under Applications in the left sidebar menu.

Appstore IDs

Accessed as a sub-menu item under Applications in the left sidebar menu.

Brands

Operating Systems