

CHAPTER 1 SteelHead Integration (SteelFlow WTA)

AppResponse includes a powerful Web Transaction Analysis (WTA) engine that provides extensive real-time monitoring and analysis of web applications. WTA collects detailed data on all page views observed by the appliance: response times for individual pages and objects (broken down by server vs. network delays), slow pages, user counts, view rates, page views by geographic region, HTTP response codes, and so on.

The AppResponse Web Console also includes an extensive set of Quick Views, Navigators, and Custom Views that enable you to identify, analyze, and troubleshoot problematic web applications.

AppResponse and SteelHead extend the visibility of WTA from the Data Center to branch offices. You can now directly evaluate the effects of SteelHead optimization of web pages between your data center and branch offices, and between branch offices and cloud servers. With these two releases, you can

- Quantify end-user experience of your web applications at branch offices
- Compare branch office response times to each other
- Compare optimized offices to each other
- Compare non-optimized offices to optimized ones
- Measure optimization performance for business-critical applications
- Monitor and evaluate the performance of SaaS applications such as Salesforce.com
- Quickly identify web apps, pages, objects, sites, and users with high response times
- Break down HTTP response times into network vs. application delays for specific pages, objects, and applications

This section discusses the following topics:

- [“System Requirements”](#)
- [“Prerequisites”](#)
- [“What Is New”](#)
- [“Important Notes: SteelFlow WTA” on page 4](#)
- [“Key Concepts: SteelFlow WTA” on page 5](#)
- [“Data Center Deployments” on page 7](#)
- [“Cloud/SaaS Deployments” on page 16](#)
- [“SteelFlow WTA Configuration” on page 23](#)
- [“Viewing SteelFlow Data in the AppResponse Web Console” on page 28](#)

- [“Grouping Page Families into Web Applications” on page 42](#)
- [“Troubleshooting SteelFlow WTA” on page 45](#)
- [“Data Types and Sources: SteelFlow WTA \(Optimized\), WTA \(Non-Optimized\), and ASA \(Non-Optimized\)” on page 49](#)

System Requirements

This functionality requires the following:

- At least one AppResponse appliance with release 9.5 or higher installed
- At least one pair of SteelHead peers. Both SteelHeads must have RIOS release 9.0 or higher installed.
- The AppResponse appliance must have network connectivity with the SteelHead appliance that is local to the clients whose end user experience you want to monitor. The SteelHead is generally in a branch office and is paired with either a Data Center SteelHead or a Cloud SteelHead.

Prerequisites

To use SteelFlow WTA effectively, you should be familiar with the following concepts.

AppResponse configuration:

- **Business Group**—A set of IPs that represent a physical site or logical group in your organization, such as Accounting, Data Center, or Cambridge Office.
- **Web Application**—A user-defined grouping of page views that corresponds to an HTTP application with a specific set of TCP ports, server IPs, and URLs. Examples include My Sales App and IT Requests.

Web Transaction Analysis:

- **Originating Group**—If any IPs in a Business Group request web pages, the appliance creates an Originating Group (with the same name) that includes the subset of all IPs that request pages in the current time selection.
- **Page View**—One instance of a web request/download and the associated metrics: response time, number of objects, % of objects optimized, etc.
- **Page Family**—A set of pages with the same URL pattern (up to but not including parameters) and the associated metrics for those pages: page traffic, page times, number of views, etc. AppResponse groups Page Views into Page Families automatically.

For more information, see AppResponse User Guide > Web Transaction Analysis > Key Concepts: Web Transaction Analysis

SteelHeads and WAN Optimization:

- **SteelHead**—SteelFlow requires a client-side SteelHead in each branch office where you want to monitor web traffic, as well as one of the following:
 - *For Data Center deployments*—A server-side SteelHead (usually located in the Data Center)
 - *For SaaS/cloud deployments*—A SteelHead near the server in the Cloud (e.g., SteelHead SaaS)

- HTTP optimization—Must be enabled on all SteelHeads optimizing HTTP/S traffic.
- REST API—Must be enabled on the client-side SteelHead. This is required so that the AppResponse appliance can retrieve web performance data from the SteelHead.
- SSL optimization—Must be enabled on the SteelHead if any of the monitored web applications are encrypted with SSL.

For more information, see the latest version of the SteelHead Appliance *Deployment Guide*.

Important Notes: SteelFlow WTA

Note the following:

- **WARNING:** Do not enable SteelFlow WTA polling for the same SteelHead on multiple AppResponse appliances at the same time. A SteelHead can serve data to one appliance only during any given time window.
- SteelHeads do not collect WTA data for
 - Pass-through pages and objects.
 - Pages and objects that traversed a pair of SteelHeads if either was not set up for SteelFlow WTA (both SteelHeads must have HTTP Optimization and SteelFlow WTA enabled).
 - Encrypted pages and objects that the SteelHead was unable to decrypt (due to a missing certificate, for example).
- If an object/page was observed by both the SteelHeads and the AppResponse monitoring ports, AppResponse calculates metrics for that object/page using SteelFlow WTA data from the SteelHeads (not packet data from the monitoring ports).
- In some networks, the SteelHeads and the server-side AppResponse might see different IPs for the same client. This can occur in network scenarios such as proxies, firewalls, or other intermediate hosts that can hide or change IPs in transit. If AppResponse and a SteelHead see different “Client IP”s or “Originating IP”s for the same host, AppResponse cannot combine those objects into a Partially-Optimized Page View.
- If a web object or page came from a cache on a client-side Steelhead, not a server on the other side of the WAN, the "Server Busy Time" metric measures processing time at the local SteelHead and not the remote server.
- SteelFlow WTA is not supported on AppResponse v2000, AppResponse VMON, or on AL-3170 hardware models.

Key Concepts: SteelFlow WTA

This section discusses the following key concepts. See also [“Key Concepts: Web Transaction Analysis”](#) (search the *User Guide* or the online help).

- [“ASA \(Application Stream Analysis\)”](#)
- [“Fully-Optimized Page”](#)
- [“Non-Optimized”](#)
- [“Optimized”](#)
- [“Page View”](#)
- [“Partially-Optimized Page”](#)
- [“SteelFlow WTA”](#)
- [“WTA \(Web Transaction Analysis\)”](#)

ASA (Application Stream Analysis)

Application, network, utilization, and informational metrics for non-optimized traffic. These metrics are derived from spanned packets on the AppResponse monitoring interfaces.

For information about the different types of data used by to calculate metrics, see [“Data Types and Sources: SteelFlow WTA \(Optimized\), WTA \(Non-Optimized\), and ASA \(Non-Optimized\)”](#) on page 49.

Fully-Optimized Page

A page view in which all objects in the page were optimized by a pair of SteelHeads and reported to AppResponse as [“SteelFlow WTA”](#) data.

Non-Optimized

A *non-optimized web object* is one that was observed on the AppResponse monitoring interfaces and was not reported in any SteelFlow WTA data.

A *non-optimized page* is one in which all objects in the page were non-optimized.

Optimized

An *optimized web object* is one that was optimized by a pair of SteelHeads and reported to AppResponse as [“SteelFlow WTA”](#) data.

An *optimized page* is one in which at least some objects in the page were optimized. The number of optimized pages is the number of fully- and partially-optimized pages.

Page View

One complete instance of a web request/download. AppResponse reports on four types of page views:

- *Fully-Optimized page views*, in which all web objects were optimized by a pair of SteelHeads and reported to AppResponse as [“SteelFlow WTA”](#) data.

- *Non-optimized page views*, in which all web objects were
 - 1) Observed on the AppResponse monitoring interfaces, AND
 - 2) Were not reported in any SteelFlow WTA data
- *Partially-optimized page views*, which include optimized objects reported by SteelHeads and non-optimized objects observed on the AppResponse monitoring interfaces
- *Optimized page views*, in which at least some web objects were optimized by Steelheads. The number of optimized pages is the number of fully- and partially-optimized pages.

Partially-Optimized Page

A page view in which some web objects were optimized (reported by SteelHeads as SteelFlow WTA data) and some objects were non-optimized (observed on the AppResponse monitoring interfaces).

SteelFlow WTA

A process on a SteelHead that collects timestamp and HTTP payload data for web traffic that it optimizes. This data is used by AppResponse to calculate [“Web Page Metrics”](#) and [“SteelFlow WTA Metrics”](#) for optimized pages and objects.

The following steps outline the general process:

- 1) An administrator enables SteelFlow WTA data collection on two peered SteelHeads (client-side and server-side).
- 2) The client-side SteelHead collects SteelFlow WTA data on the pages and objects optimized by that SteelHead and its peer.
- 3) AppResponse sends periodic data requests to the client-side SteelHead, which serves SteelFlow WTA data back to the AppResponse appliance.
- 4) AppResponse uses the data to calculate WTA metrics on pages and objects optimized by the peered SteelHeads.

For information about the different types of data used by to calculate metrics, see [“Data Types and Sources: SteelFlow WTA \(Optimized\), WTA \(Non-Optimized\), and ASA \(Non-Optimized\)”](#) on page 49.

WTA (Web Transaction Analysis)

A process on the AppResponse appliance that collects Timestamp and HTTP payload data and uses this data to calculates metrics for web pages and objects. WTA can generate metrics from two different data sources:

- [“Page View”](#) data from SteelHeads—Used to calculate [“Web Page Metrics”](#) and [“SteelFlow WTA Metrics”](#) for optimized page views and objects
- Packet data from the AppResponse monitoring interfaces—Used to calculate [“Web Page Metrics”](#) for unoptimized page views and objects

For information about the different types of data used by to calculate metrics, see [“Data Types and Sources: SteelFlow WTA \(Optimized\), WTA \(Non-Optimized\), and ASA \(Non-Optimized\)”](#) on page 49.

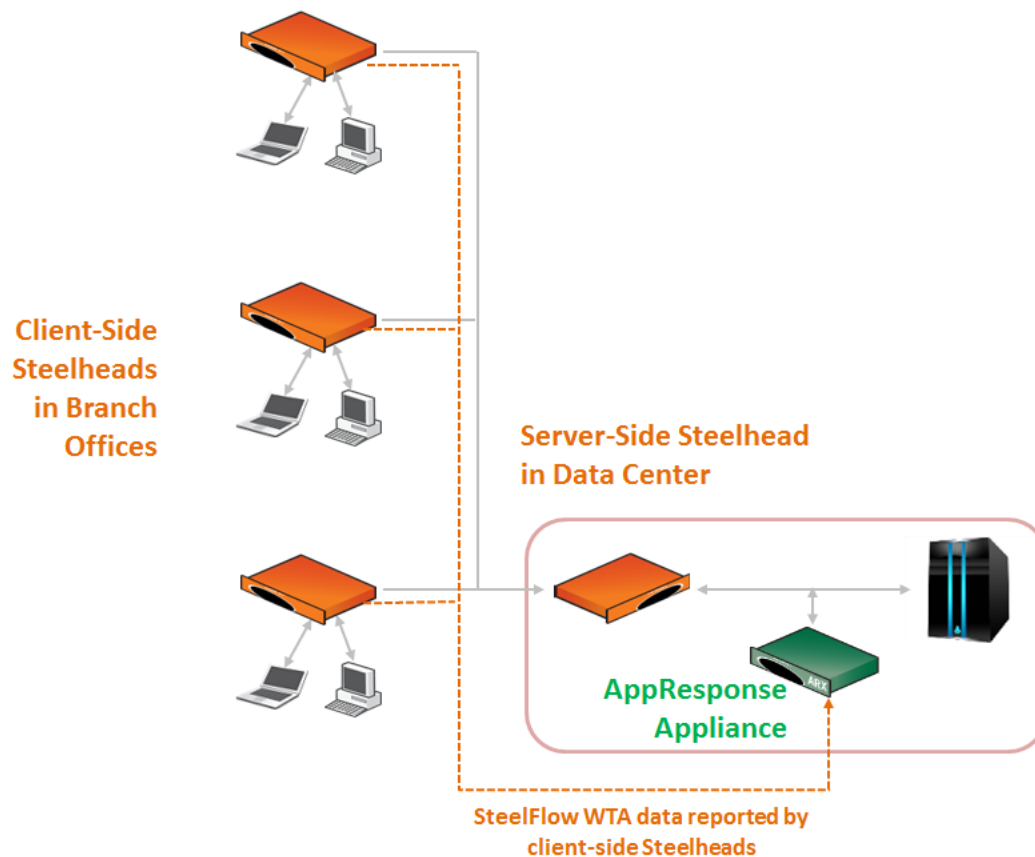
For information about WTA, see [“Web Transaction Analysis”](#) (search the *User Guide* or the online help).

Data Center Deployments

This section describes how to set up SteelFlow monitoring in a network with a Data Center SteelHead and one or more client-side SteelHeads in remote offices:

- [“Prerequisites” on page 8](#)
- [“Setup Requirements” on page 8](#)
- [“Checklist: Data Center Deployment Setup” on page 14](#)

Figure 1 SteelFlow Deployment: AppResponse and SteelHeads



Prerequisites

Before you begin setting up Steelflow data collection, it is good practice to verify that:

- All SteelHeads (client-side and server-side) are installed and set up.
- All SteelHeads (client-side and server-side) have RiOS 9.0 or higher installed.
- Every client-side SteelHead is successfully peered with the Data Center SteelHead and local clients are able to download optimized pages from the server(s).
- The AppResponse appliance is installed, set up, and monitoring traffic.
- The AppResponse appliance has release 9.5 or higher installed.

For information about installing and setting up SteelHead appliances, see the following:

- SteelHead Appliance Deployment Guide
- SteelHead Appliance Installation and Configuration Guide

For information about installing and setting up AppResponse appliances, see the following:

- AppResponse Hardware Install Guide
- AppResponse Software Install Guide

Setup Requirements

This section discusses the following:

- [“Set Up WTA on AppResponse Appliance” on page 8](#)
- [“Set Up Data Center SteelHead” on page 9](#)
- [“Set Up Client-Side SteelHeads” on page 9](#)
- [“Add SteelHeads in AppResponse Web Console” on page 10](#)
- [“Define Business Groups in AppResponse Desktop Console” on page 11](#)
- [“Verify NTP Servers” on page 12](#)
- [“Define Web Applications” on page 13](#)

Set Up WTA on AppResponse Appliance

You need to set up the following:

1) Masking of Private Data (optional)

You can configure the appliance to prevent private data in observed traffic, such as usernames or account numbers, from getting saved to disk or appearing in the user interface. If this is a priority, you need to set this up before you enable WTA. For more information, search for “setup configuration web transaction analysis” in the online help and go to the “Masking Private Data in Observed Web Traffic” section.

For more information, see [“Masking Private Data in Observed Web Traffic”](#) (search the *User Guide* or the online help).

2) Page Analysis Configuration:

- Enable Page Analysis = selected
- on Port(s)...and Server IP addresses: Specify the ports and the server IPs for the web applications for which you want to collect page metrics.

Note—To minimize load on the appliance, It is good practice to limit web page tracking to ports and hosts of interest only when possible.

For more information, see [“Page Analysis: Enabling and Configuring”](#) (search the *User Guide* or the online help).

3) Configure decryption for web apps that use SSL:

- a) Under Page Analysis Configuration Parameters, select Enable SSL decoding.
- b) Under Private Key Configuration, add the private key for each SSL-encrypted web application:
Click Add under the Private Keys list.
Paste the private key into the Private Key Details field.
- c) Click OK.

Note—It can be useful to add the private key if the SteelHeads do not optimize all objects. For HTTPS, the server-side SteelHead handles SSL decryption for optimized traffic. But if some objects are not optimized, then it makes sense to add the private key to the appliance to report on non optimized traffic for HTTPS.

For more information, see [“SSL Decoding: Enabling and Configuring”](#) (search the *User Guide* or the online help).

Set Up Data Center SteelHead

Enable SteelFlow WTA on the Data Center SteelHead:

- 1) Log in to the web UI of the Data Center SteelHead.
- 2) Enable SteelFlow WTA:
 - a) Choose Optimization > Protocols: HTTP.
 - b) In the HTTP page, select Enable HTTP Optimization. Then select Enable SteelFlow WTA.
 - c) Click Apply (immediately below Settings box) and then Save (top-right corner of Settings box) to apply your changes.

Set Up Client-Side SteelHeads

Do the following on each client-side SteelHead you want to monitor:

- 1) Log in to the SteelHead web UI.
- 2) Enable SteelFlow WTA:
 - a) Choose Optimization > Protocols: HTTP.
 - b) In the HTTP page, select Enable HTTP Optimization. Then select Enable SteelFlow WTA.

- c) Click Apply (immediately below Settings box) and then Save (top-right corner of Settings box) to apply your changes.

3) Enable REST API access:

- a) Choose Administration > Security: REST API Access.
- b) Select “Enable REST API Access” and click Apply.
- c) Add an Access Code that the AppResponse appliance can use to access data from the SteelHead:
Click Add Access Code.

Enter a user-friendly description in the Description of Use field

Select Generate a New Access Code and click Add.

Select the new access code and choose Edit > Copy (or the equivalent) in the browser window.

Figure 2 Generate REST API Access Code in SteelHead Web Interface

Configure > Security > REST API Access ?

REST API Access Settings

☒ Enable REST API Access

Apply

Access Codes:

+ Add Access Code — Remove Selected

<input type="checkbox"/>	Access Code Description	Creator
<input type="checkbox"/>	ARX	admin
<input checked="" type="checkbox"/>	AppResponse SteelFlow Export	admin

Access Code:

```
eyJhdWQ1O1A1aHR0cHM6Ly9tYWluLXZzaDEyMS5sYWJubmJ0dGVjaC5jb20vYXBPb2NvbW1vbi8xLjAvdG9rZW4iLCAiakNzIjogImh0dHBzOi8vbWVpbi12c2gxMjEubGF1Lm51dHR1Y2guY29tIiwgInByb2I6IeICJhZG1pb2I6IeICJqdGkiOiAiOTk2MDQ5OUNUeMzZhNi00NGRiLWEwMDEtcNWUwODQwYWE0MzgyIiwgImV4cCI6IeICiwiIiwgIm1hdCI6IeICiNDA4MDQ2NzUyIn0=
```

Description of Use: AppResponse SteelFlow Export

Apply

Add SteelHeads in AppResponse Web Console

Do the following:

- 1) Log in to the AppResponse web console.
- 2) In the treeview menu (left pane), choose Administration > Integration. Then select SteelHead in the right-pane table.
- 3) In the SteelHead configuration page, click Add at the bottom of the table.

- 4) In the Add New SteelHead dialog box, add an entry for all client-side SteelHeads that you want to monitor. The following fields are required for each SteelHead:
 - Management Address = Management interface of the SteelHead.
 - Access Code — Select Custom and then paste the Access Code you created in the previous step. (If necessary, go back to the SteelHead web interface > Administration > Security > REST API page and copy the code again.)
 - Enable Polling = selected

Note—If you have a SteelCentral Controller to manage your SteelHeads, you can export these settings to a CSV file and then import the data into this table. For more information, see [“Export SteelHead Data to CSV \(CLI Command on SteelCentral Controller\)”](#) on page 25.

Figure 3 Add New SteelHead in AppResponse Web Console

The screenshot shows the 'Add New SteelHead' dialog box. The 'Management Address' field is filled with '10.12.14.1'. The 'Access Code' section has 'Custom' selected, and a text area contains a long alphanumeric string: 'HBzO18vbWFpb112c2gxMjEubGF1Lm5idHR1Y2guY29tIiwgInBybiI6ICJyb290IiwgImp0aSI6ICI0YjI5NDg3NC1jZjg2LTR1NjgtYjFiMi03YWM2ZGNmNmQ4ZTIiLCAiZXhwIjogIjAiLCAiaWF0IjogIjE0MDkyNjAwMjM1fQ=='. The 'Enable Polling' checkbox is checked. The background shows a table with 'SteelHeads: 0' and columns for 'Management Address' and 'Access Code'.

- 5) Select [“Enable SteelFlow WTA”](#) if it is not already selected.

Note—Changing this setting causes the web server on the appliance to reboot, so you might need to log in to the appliance again.

- 6) Once SteelFlow WTA is enabled, and if the AppResponse appliance is able to poll one or more SteelHeads in the table, the [“Display SteelHead Optimization metrics and views”](#) option should be available (otherwise it is grayed out). Select this option if it is not already selected.

If this option is not selected, the AppResponse user interface does not display any SteelFlow WTA data.

Define Business Groups in AppResponse Desktop Console

You should define a Business Group for each client-side SteelHead. Each group should include all web clients in the corresponding location. Do the following:

- 1) Open the Desktop Console: Go to the AppResponse Web Console and choose Administration > Desktop Console.
- 2) For each client-side SteelHead, define a Business Group for the branch office where the SteelHead is located.

To define a new BG, do the following:

 - a) In the Desktop Console, choose Tools > Business Groups > Business Group Manager.

b) In the Business Group Manager, click New and specify the following settings:

Table 1 Required Settings for Each Branch-Office Business Group

Tab	Item	Description
Identity	Name	User-friendly name such as SF Branch Office
	Description	It is good practice to include the SteelHead name or IP in the description. This makes it easy to see the SteelHeads that a specific page traversed.
	Classification	Business Group
	Status	Active
Business Group Definition	IP / AS Members	All local IPs in the branch office (ie, IPs on the LAN side of the client-side SteelHead)

3) Create one or more Business Groups for non-optimized web pages that you can use to compare with the optimized branch office. A comparison BG must have the following characteristics:

- The comparison location is remote from the Data Center and communicates across a similar WAN.
- The WAN is not optimized by SteelHeads.
- The branch office and comparison location should use the same web apps of interest, so you can compare optimized and non-optimized page views directly.
- The comparison location should be approximately the same distance from the Data Center as the branch office, so that the WAN latencies are comparable (compare location \leftrightarrow DC latency should be approximately equal to branch-location \leftrightarrow DC latency).

Key Concept—When selecting a comparison group in your organization, you should look for locations that are good candidates for WAN optimization. Many organizations place their SteelHeads in branch offices with the smallest WAN links and the highest round trip times. If the compare location is much closer to or further away from the Data Center, the WAN latencies will differ and you will need to consider this difference when you compare results between the two locations.

Verify NTP Servers

It is good practice to verify that all appliances (AppResponse and SteelHeads) are using a reliable NTP server.

To view and change the NTP servers used in AppResponse:

- 1) Log in to the AppResponse Web Console.
- 2) Choose Administration > System.
- 3) Choose System > Setup. The NTP Servers field is under Time Settings near the bottom of the page.

To view and change the NTP servers used in SteelHead:

- 1) Log in to the SteelHead web interface.
- 2) Choose Administration > System Settings: Date/Time.

Define Web Applications

The Desktop Console includes a Defined Application Manager where you can group related page families into defined Web Applications.

- 1) Set up Steelflow data collection (that is, perform all the other required steps).
- 2) Wait for the appliance to collect page views of interest.
- 3) In the AppResponse Web Console, go to the Page Families Navigator and view the page families you want to monitor.
- 4) In the Defined Application Manager, create web applications that group related Page Families together (see [“Grouping Page Families into Web Applications”](#) on page 42).

Checklist: Data Center Deployment Setup

The following steps list the required steps for SteelFlow monitoring in a Data Center deployment.

Table 2 Data Center Setup Checklist

Appliance	Setup Requirements
SteelHead (All)	Before you begin, it is good practice to verify that <ul style="list-style-type: none">• All appliances are installed, peered, set up, and exchanging traffic.• All SteelHeads have RiOS 9.0 or higher installed.• Every client-side SteelHead is successfully peered with the Data Center SteelHead and local clients are able to download pages from the SaaS server.• The AppResponse appliance has 9.5 or higher installed.
SteelHead (Data Center)	Enable the following in the SteelHead web interface: <ul style="list-style-type: none">• Optimization > HTTP > Enable HTTP Optimization• Optimization > HTTP > SteelFlow WTA

Table 2 Data Center Setup Checklist (Continued)

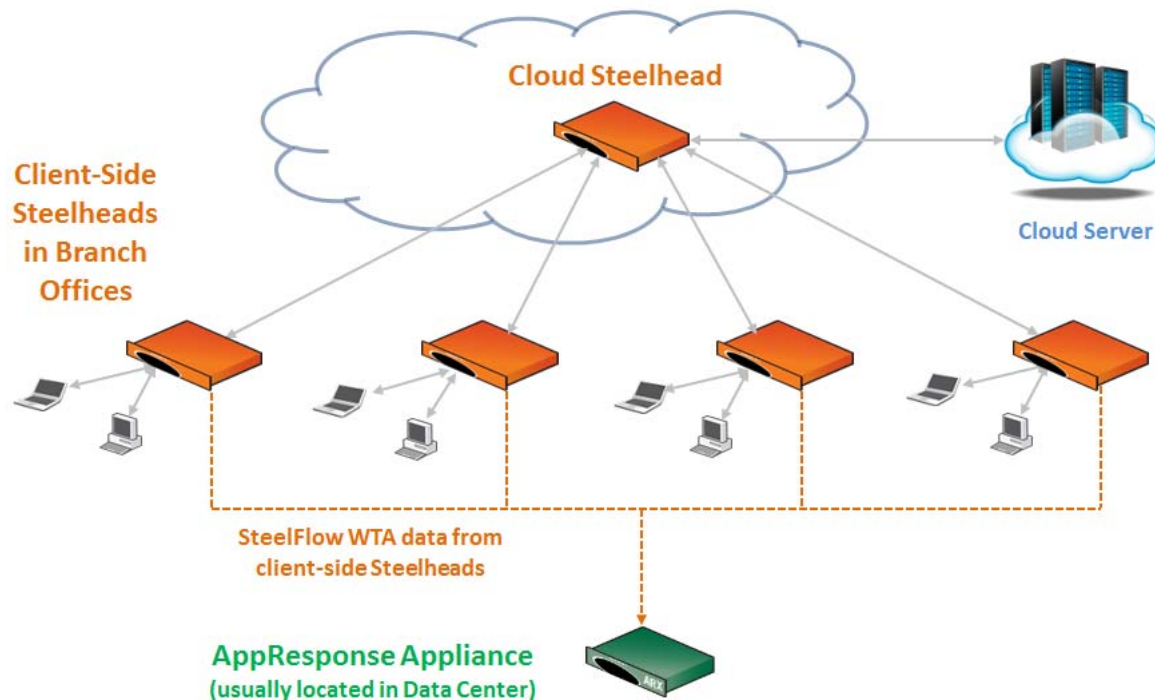
Appliance	Setup Requirements
SteelHead (client-side)	<p>For each client-side SteelHead, enable the following in the SteelHead web interface:</p> <ul style="list-style-type: none"> • Optimization > HTTP > Enable HTTP Optimization • Optimization > HTTP > SteelFlow WTA • Administration > Security > REST API Access > Enable REST API Access <p>Each client-side SteelHead needs at least one Access Code defined in the REST API Access page. You will need to copy and paste this code into the AppResponse Web Console.</p>
AppResponse	
SteelHeads Table	<p>Every client-side SteelHead must have an entry in the Web Console > Administration > System > Integration > SteelHead table. Each entry must include:</p> <ul style="list-style-type: none"> • Management Address • Access Code • Enable Polling = selected
Enable Data Collection	<p>Enable the following in the Web Console > Administration > System > Integration > SteelHead table:</p> <ul style="list-style-type: none"> • Enable SteelHead performance data collection
Web Transaction Analysis	<p>1) Set up Masking of Private Data (optional)</p> <p>2) In System > Administration web UI > System > Pages, set</p> <ul style="list-style-type: none"> • Enable Page Analysis (selected) • ...of Ports ...and Server IP addresses: specify the ports and server IPs for the web applications for which you want to collect page metrics. <p>3) Configure SSL Decryption for web apps that use SSL</p>
All appliances	<p>It is good practice to verify that all appliances (AppResponse and SteelHeads) are using a reliable NTP server.</p>
AppResponse	<p>Define Web Applications (after appliance collects page views)</p>

Cloud/SaaS Deployments

This section describes how to set up SteelFlow monitoring for SaaS applications in a network with client-side SteelHeads and an external Cloud SteelHead:

- [“Prerequisites” on page 16](#)
- [“Setup Requirements” on page 17](#)
- [“Checklist: Cloud/SaaS Deployment Setup” on page 22](#)

Figure 1 SteelFlow Deployment: AppResponse Appliance and Cloud/Client-Side SteelHeads



Prerequisites

To monitor and analyze SaaS applications such as Salesforce, you need the following:

- A client-side SteelHead (CX or EX) in each branch office of interest.
- Cloud SteelHead (CX for IaaS clouds or SteelHead SaaS) running near the SaaS application server in the cloud.
- An AppResponse appliance that has network connectivity with each client-side SteelHead.

Before you begin setting up Steelflow data collection, it is good practice to verify that:

- All SteelHeads (Edge and Cloud) are provisioned and set up.
- All SteelHeads (Edge and Cloud) have RiOS 9.0 or higher installed.

- Every client-side SteelHead is successfully peered with the Cloud SteelHead and local clients are able to download pages from the SaaS server.
- The AppResponse appliance is installed, set up, and monitoring traffic.
- The AppResponse appliance has release 9.5 or higher installed.
- The AppResponse appliance has network connectivity with each client-side SteelHead.

For information about installing and setting up SteelHead appliances, see the following:

- SteelHead Appliance Deployment Guide
- SteelHead Appliance Installation and Configuration Guide
- Riverbed Cloud Services User's Guide
- SteelHead Cloud Accelerator Software User's Guide
- Riverbed Cloud SteelHead Appliance Quick Reference

For information about installing and setting up AppResponse appliances, see the following:

- AppResponse Hardware Install Guide
- AppResponse Software Install Guide

Setup Requirements

This section discusses the following:

- ["Set Up WTA on AppResponse Appliance" on page 17](#)
- ["Set Up Cloud SteelHead" on page 18](#)
- ["Set Up Client-Side steelheads" on page 18](#)
- ["Add SteelHeads in AppResponse Web Console" on page 19](#)
- ["Verify NTP Servers" on page 20](#)
- ["Define Business Groups in AppResponse Desktop Console" on page 21](#)

Set Up WTA on AppResponse Appliance

You need to set up the following:

1) Masking of Private Data (optional)

You can configure the appliance to prevent private data in observed traffic, such as usernames or account numbers, from getting saved to disk or appearing in the user interface. If this is a priority, you need to set this up before you enable WTA. For more information, search for "setup configuration web transaction analysis" in the online help and go to the "Masking Private Data in Observed Web Traffic" section.

For more information, see ["Masking Private Data in Observed Web Traffic"](#) (search the *User Guide* or the online help).

2) Page Analysis Configuration:

- Enable Page Analysis = selected
- on Port(s)...and Server IP addresses: Specify the ports and the server IPs for the web applications for which you want to collect page metrics.

Note—To minimize load on the appliance, It is good practice to limit web page tracking to ports and hosts of interest only when possible.

For more information, see [“Page Analysis: Enabling and Configuring”](#) (search the *User Guide* or the online help).

Set Up Cloud SteelHead

Enable SteelFlow WTA on the Cloud SteelHead:

- 1) Log in to the web UI of the Cloud SteelHead.
- 2) Enable SteelFlow WTA:
 - a) Choose Optimization > Protocols: HTTP.
 - b) In the HTTP page, select Enable HTTP Optimization. Then select “Enable SteelFlow WTA.”
 - c) Click Apply (immediately below the Settings box) and then Save (top-right corner of Settings box) to apply your changes.

Set Up Client-Side steelheads

Do the following on each client-side SteelHead you want to monitor:

- 1) Log in to the SteelHead web UI.
- 2) Enable SteelFlow WTA:
 - a) Choose Optimization > Protocols: HTTP.
 - b) In the HTTP page, select Enable HTTP Optimization. Then select Enable SteelFlow WTA.
 - c) Click Apply (immediately below Settings box) and then Save (top-right corner of Settings box) to apply your changes.
- 3) Enable REST API access:
 - a) Choose Administration > Security: REST API Access.
 - b) Check “Enable REST API Access” and click Apply.
 - c) Add an Access Code that the AppResponse appliance can use to access data from the SteelHead:
Click Add Access Code.
Enter a user-friendly description in the Description of Use field
Select Generate a New Access Code and click Add.
Select the new access code and choose Edit > Copy (or the equivalent) in the browser window.

Figure 2 Generate REST API Access Code in SteelHead Web Interface

Configure > Security > REST API Access ?

REST API Access Settings

☒ Enable REST API Access

Apply

Access Codes:

+ Add Access Code
— Remove Selected

<input type="checkbox"/>	Access Code Description	Creator
<input type="checkbox"/>	ARX	admin
<input checked="" type="checkbox"/>	AppResponse SteelFlow Export	admin

Access Code:

eyJhdWQiOiAiHR0cHM6Ly9tYWluLXZzaDEyMS5eYWIubmJ0dGVjaC5jb20vYXBpL2NvbW1
vb18xLjAvdG9rZW4iLCAiaXNzIjoqImh0dHBzOi8vbWpbi12c2gMjEubGF1Lm5ldHR1Y2
guY29tIiwgInBybiI6ICJhZG1pbiIsICJqdGkiOiAiOTk2MDQ5OWU0MzZhNi00NGRiLWEwM
DQc0NWUwODQwYWE0MzgyIiwgImV4cCI6ICIwIiwgIm1hdCI6ICIxNDA4MDQ2NzUyIn0=

Description of Use: AppResponse SteelFlow Export

Apply

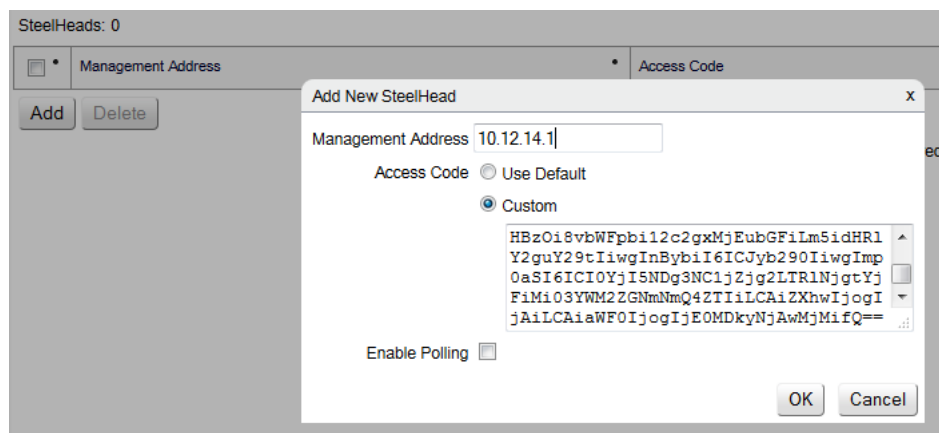
Add SteelHeads in AppResponse Web Console

Do the following:

- 1) Log in to the AppResponse web console.
- 2) In the treeview menu (left pane), choose Administration > System > Integration. Then select SteelHead in the right-pane table.
- 3) In the SteelHead configuration page, click Add at the bottom of the table.
- 4) In the Add New SteelHead dialog box, add an entry for all client-side SteelHeads that you want to monitor. The following fields are required for each SteelHead:
 - Management Address = Management interface of the Cloud / client-side SteelHead.
 - Access Code — Select Custom and then paste the Access Code you created in the previous step. (If necessary, go back to the SteelHead web interface > Configure > Security > REST API page and copy the code again.)
 - Enable Polling = selected

Note—If you have a SteelCentral Controller to manage your SteelHeads, you can export these settings to a CSV file and then import the data into this table. For more information, see [“Export SteelHead Data to CSV \(CLI Command on SteelCentral Controller\)” on page 25.](#)

Figure 3 Add New SteelHead in AppResponse Web Console



5) Select [“Enable SteelFlow WTA”](#) if it is not already selected.

Note—Changing this setting causes the web server on the appliance to reboot, so you might need to log in to the appliance again.

6) Once SteelFlow WTA is enabled, and if the AppResponse appliance is able to poll one or more SteelHeads in the table, the [“Display SteelHead Optimization metrics and views”](#) option should be available (otherwise it is grayed out). Select this option if it is not already selected.

Note—If this option is not selected, the AppResponse user interface does not display any SteelFlow WTA data.

Verify NTP Servers

It is good practice to verify that all appliances (AppResponse and SteelHeads) are using a reliable NTP server.

To view and change the NTP servers used in AppResponse:

- 1) Log in to the AppResponse Web Console.
- 2) Choose Administration > System.
- 3) Choose System > Setup. The NTP Servers field is under Time Settings near the bottom of the page.

To view and change the NTP servers used in SteelHead:

- 1) Log in to the SteelHead web interface.
- 2) Choose Administration > System Settings: Date/Time.

Define Business Groups in AppResponse Desktop Console

You should define a Business Group for each client-side SteelHead. Each group should include all web clients in the corresponding branch location. Do the following for each client-side SteelHead:

- 1) Open the Desktop Console: Go to the AppResponse Web Console and choose Administration > Desktop Console.
- 2) For each client-side SteelHead, define a Business Group for the branch office where the SteelHead is located.

To define a new BG, do the following:

- a) In the Desktop Console, choose Tools > Business Groups > Business Group Manager.
- b) In the Business Group Manager, click New and specify the following settings:

Table 1 Required Settings for Each Edge Business Group

Tab	Item	Description
Identity	Name	User-friendly name such as SF Branch Office
	Description	It is good practice to include the SteelHead name or IP in the description. This makes it easy to see the SteelHeads that a specific page traversed.
	Classification	Business Group
	Status	Active
Business Group Definition	IP/AS Members	All local IPs in the branch office (ie, IPs on the LAN side of the client-side SteelHead)

Define Web Applications

The Desktop Console includes a Defined Application Manager where you can group related page families into defined Web Applications.

- 1) Set up Steelflow data collection (that is, perform all the other required steps).
- 2) Wait for the appliance to collect page views of interest.
- 3) In the AppResponse Web Console, go to the Page Families Navigator and view the page families you want to monitor.
- 4) In the Defined Application Manager, create web applications that group related Page Families together (see [“Grouping Page Families into Web Applications” on page 42](#)).

Checklist: Cloud/SaaS Deployment Setup

The following steps list the required steps for SteelFlow monitoring in a Cloud/SaaS deployment.

Table 2 Cloud Setup Checklist

Appliance	Setup Requirements
SteelHead (All)	<p>Before you begin, it is good practice to verify that</p> <ul style="list-style-type: none"> • All SteelHeads are installed, peered, set up, and exchanging traffic. • All SteelHeads have RiOS 9.0 or higher installed. • Every client-side SteelHead is successfully peered with the Cloud SteelHead and local clients are able to download pages from the SaaS server. • The AppResponse appliance has 9.5 or higher installed.
SteelHead (Cloud)	<p>Enable the following in the SteelHead web interface:</p> <ul style="list-style-type: none"> • Optimization > Protocols> HTTP > Enable HTTP Optimization • Optimization > Protocols> HTTP > Enable SteelFlow WTA
SteelHead (client-side)	<p>For each client-side SteelHead, enable the following in the SteelHead web interface:</p> <ul style="list-style-type: none"> • Optimization > Protocols> HTTP > Enable HTTP Optimization • Optimization > Protocols> HTTP > Enable SteelFlow WTA • Configure > Security > REST API Access > Enable REST API Access <p>Each client-side SteelHead needs at least one Access Code defined in the REST API Access page. You will need to copy and paste this code into the AppResponse Web Console.</p>
AppResponse	
SteelHeads Table	<p>Every Branch SteelHead must have an entry in the Web Console > Administration > System > Integration > SteelHead table. Each entry must include:</p> <ul style="list-style-type: none"> • Management Address • Access Code • Enable Polling = selected
Enable Data Collection	<p>Enable the following in the Web Console > Administration > System > Integration > SteelHead table:</p> <ul style="list-style-type: none"> • Enable SteelHead performance data collection
Web Transaction Analysis	<p>1) Set up Masking of Private Data (optional)</p> <p>2) In System > Administration web UI > System > Pages, set</p> <ul style="list-style-type: none"> • Enable Page Analysis (selected) • ...of Ports ...and Server IP addresses: specify the ports and server IPs for the web applications for which you want to collect page metrics.
All appliances	<p>It is good practice to verify that all appliances (AppResponse and SteelHeads) are using a reliable NTP server.</p>
AppResponse	<p>Define Web Applications (after appliance collects page views)</p>

SteelFlow WTA Configuration

This section describes how to configure SteelFlow WTA data collection and describes various SteelFlow-related CLI commands. The following topics are discussed:

- [“SteelHead Configuration Page”](#)
- [“Enable SteelFlow WTA \(CLI Command on SteelHead\)”](#)
- [“Export SteelHead Data to CSV \(CLI Command on SteelCentral Controller\)”](#)

SteelHead Configuration Page

The SteelHead Configuration page is the central location for configuring the SteelHeads from which the appliance collects optimization data. In this page, you can

- Enable or disable SteelFlow WTA data collection
- Display or hide SteelFlow WTA data in the AppResponse user interface
- Specify the client-side SteelHeads that will report SteelFlow WTA data to AppResponse
- Enable and disable SteelFlow WTA data polling to specific SteelHeads

WARNING: Do not enable SteelFlow WTA polling to the same SteelHead on multiple AppResponse appliances at the same time. A SteelHead can serve data to one appliance only during any given time window.

To open this page, go to the Web Console and choose Administration > Integration

Figure 1 SteelHead Configuration Tabbed Page
(AppResponse Web Console > Administration > Integration > SteelHead)

Choose Selected Actions to configure selected Steelheads only (checkbox in left column selected)

Choose Global Actions to configure all Steelheads in the table

Enable SteelFlow WTA
Display SteelHead Optimization metrics and views

SteelHeads: 6

	Management Address	Access Code	Polling	Poll Status
<input type="checkbox"/>	10.33.131.63	Custom	Disabled	
<input type="checkbox"/>	10.3.0.2	Custom	Enabled	
<input type="checkbox"/>	10.34.227.58	Custom	Enabled	
<input checked="" type="checkbox"/>	10.33.131.203	Custom	Enabled	
<input checked="" type="checkbox"/>	10.34.227.51	Custom	Enabled	
<input type="checkbox"/>	10.34.227.60	Custom	Disabled	

Add Delete Import from CSV

Table 1 SteelHead Configuration Tabbed Page

Option	Description
Enable SteelFlow WTA	<p>Enable or disable SteelFlow WTA data collection on the AppResponse appliance.</p> <p>Note—If you change this setting, the web server on the AppResponse appliance will reboot. Data collection will be interrupted briefly and you might need to log in again.</p>
Display SteelHead Optimization metrics and views	<p>Show or hide SteelFlow WTA optimization data in the user interface.</p> <p>You might want to hide SteelFlow WTA data so that the user interfaces shows only traffic observed directly on the monitoring interfaces of the AppResponse appliance.</p>
Selected Actions... Global Actions...	<p>Configure selected SteelHeads (checkbox selected in left column), or all SteelHeads in the table</p> <ul style="list-style-type: none"> • Enable/disable the Enable SteelFlow WTA option on remote SteelHeads. • Update the Access Code required to request REST API data from remote SteelHeads. To obtain the Access Code for a SteelHead, log in to the web interface and choose Configure > Security > REST API.
SteelHeads table (left to right):	<ul style="list-style-type: none"> • Management Address • Access Code—Custom or Default • Polling—Enabled or Disabled • Polling Status: <ul style="list-style-type: none"> – green (polling enabled / OK) – yellow (polling enabled / intermittent error(s)) – red (polling enabled / persistent error(s)) – gray (polling disabled)
Add / Delete	<p>Add a new SteelHead or delete selected SteelHeads.</p> <p>In the Add New SteelHead window, you need to specify</p> <ul style="list-style-type: none"> • The management address for the SteelHead • The Access Code. You can specify a custom code for that SteelHead or the default code defined for all SteelHeads in the table.
Import from CSV	<p>If you have a lot of SteelHeads to manage, you might find it more convenient to manage your SteelHead data in a spreadsheet, save it to CSV, and import all the data at once.</p> <p>The expected CSV file has three fields per line:</p> <ul style="list-style-type: none"> • Management Address • Authorization code (empty field = use default code) • Polling status (1 = enabled, 0 = disabled) <p>If you use a SteelCentral Controller to manage your SteelHeads, you can generate a CSV file for all SteelHeads. For more information, see “Export SteelHead Data to CSV (CLI Command on SteelCentral Controller)” on page 25</p>

Enable SteelFlow WTA (CLI Command on SteelHead)

You can use the CLI command `sport steelflow-wta` command to enable or disable SteelFlow WTA data collection on an individual SteelHead. This command is equivalent to selecting or unselecting the Enable Steelflow WTA checkbox in the SteelHead web interface > Configure > Optimization > HTTP page.

To enable or disable Steelflow WTA on an individual SteelHead, do the following:

1) Log in to the SteelHead CLI as a user with admin privileges.

2) Enter the following commands in order:

- a) `cli`
- b) `enable`
- c) `configure terminal`
- d) `sport steelflow-wta enable` *or*
`sport steelflow-wta disable`
- e) `write memory`
- f) `service restart`

The following shows an example session:

```
[admin@myscc ~]# cli
myscc > enable
myscc # configure terminal
myscc (config) # sport steelflow-wta enable
You must restart the optimization service for your changes to take effect.

myscc (config) # write memory

myscc (config) # service restart
Terminating optimization service.....
Relaunching optimization service
```

Export SteelHead Data to CSV (CLI Command on SteelCentral Controller)

If you use a SteelCentral Controller to manage the SteelHeads in your network, you can generate a CSV file of the IPs, access codes, and polling status for all appliances managed by that Controller. You can then import the CSV data into AppResponse. This simplifies the management process for SteelFlow WTA, especially if the AppResponse appliance is collecting data from many SteelHeads.

To generate a SteelHead data file, do the following:

1) Log in to the SteelCentral Controller CLI as a user with admin privileges.

2) Enter the following commands in order:

- a) `cli`
- b) `enable`
- c) `configure terminal`
- d) `export steelhead access_codes to-email yourname@yourdomain.com`

The Controller then sends a CSV to the specified address. The following shows an example session:

```
[admin@myscc ~]# cli
myscc > enable
myscc # configure terminal
myscc (config) # export steelhead access_codes to-email jsmith@mycompany.com
```

To import the data, go to the AppResponse Web Console > Administration > Integration > SteelHead page.

CSV Format (Export SteelHead Data to CSV from SteelCentral Controller)

The resulting CSV file includes the following fields for each SteelHead:

- IP Address
- OAuth Code
- Polling status (*1 = enabled, 0 = disabled*)
- Serial number (*not used*)

Viewing SteelFlow Data in the AppResponse Web Console

After you finish the setup process, the AppResponse appliance should be collecting SteelFlow data from the client-side SteelHead and you should be able to view this data in the AppResponse Web Console. This section discusses the following:

- [“Important Notes”](#)
- [“Verify that the Appliance Sees Optimized Traffic”](#)
- [“SteelFlow WTA Metrics” on page 29](#)
- [“SteelFlow WTA QuickViews” on page 32](#)
- [“Viewing SteelFlow Data: Suggested Workflows” on page 37](#)
 - [“At a Glance: Quick Views for Your SteelHeads” on page 37](#)
 - [“Steelflow Navigation: Drill Down to Pages of Interest” on page 38](#)

Important Notes

Note the following when:

- The data and views you see will focus on pages requested by clients in the branch office.
- A page can be optimized, non-optimized, or partially optimized. The degree of optimization for a specific page indicates how many objects in that page were optimized:
 - Fully Optimized = All page objects were optimized by SteelHeads.
 - Non-Optimized = No page objects were optimized (because the WAN had no SteelHeads, or because the WAN had SteelHeads but they were bypassed).
 - Partially Optimized = Some page objects were optimized and other objects were bypassed.
- If all pages appear as 0% optimized, it means that
 - No branch clients requested pages that traversed the SteelHeads, or
 - The client-side SteelHead is not observing any pages, or
 - The client-side SteelHead is not sending data to the appliance, or
 - The AppResponse appliance is not receiving or processing data from the client-side SteelHead.

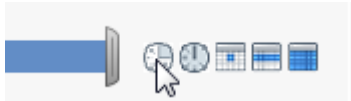
Verify that the Appliance Sees Optimized Traffic

Do the following:

- 1) Log in to the AppResponse Web Console and choose Quick Views > My SteelHeads.
- 2) The Quick Views table (right pane) shows the set of Quick Views that are specifically designed to visualize the effects of SteelHead optimization and to compare optimized, partially-optimized, and unoptimized page views.
- 3) Open the Top Optimized vs. non-Optimized Client Groups view.
- 4) Verify that you see results for both optimized and/or non-optimized groups. If either set of data is missing, do the following:

- a) Edit your existing Business Group definition(s) or create one or more new BGs based on the requirements described in Setting Up the AppResponse Appliance.
- b) After you apply your Business Group changes, return to this view and verify that you see results for both optimized and non-optimized groups. Repeat this process if necessary.

Note—New BG definitions are applied to newly-observed traffic only, not to traffic data on disk. To verify your new settings, wait a few minutes for the appliance to collect page views. Then click the “Recent 15 minutes” button in the time toolbar (to the immediate right of the slider).



- 5) In the Web Console treeview (left pane), choose Navigator > Web Transaction Analysis > Originating Groups.
- 6) Click the Columns toolbar button (above the table) and make sure that the SteelFlow WTA > % Pages Optimized metric is selected.

- 7) To verify that you defined your groups correctly, check the % Pages Optimized metric.

The optimized group should show a majority of pages (50% or more) as Optimized.

The non-optimized group should show no pages (0%) as Optimized.

If most of the pages in the optimized Group are not reported as Optimized, check the following:

- The client IPs in the Business Group are actually behind a SteelHead.
- Your SteelFlow WTA setup is correct (see [“Checklist: Data Center Deployment Setup” on page 14](#) or [“Checklist: Cloud/SaaS Deployment Setup” on page 22](#)).
- The web traffic of interest in that branch location is actually being optimized by the client-side and server-side SteelHeads.

SteelFlow WTA Metrics

The following metrics are available in relevant Quick Views (> My SteelHeads) and Navigators (> Web Transaction Analysis). All metrics are calculated as percentages of the total number of web pages or HTTP responses (web-page objects) for the selected group in the selected time window.

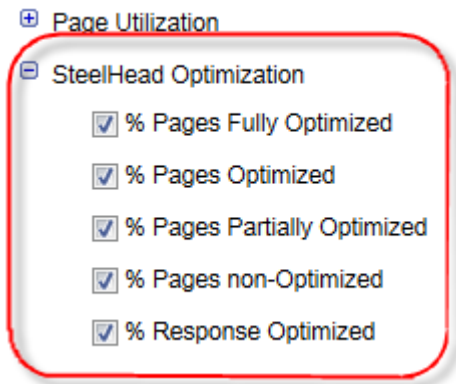
Table 1 SteelFlow WTA Metrics

Metric	Description
% Pages Fully Optimized	Percentage of page views in which <i>all objects</i> were optimized by SteelHeads
% Pages non-Optimized	Percentage of page views in which <i>no objects</i> were optimized by SteelHeads
% Pages Optimized	Percentage of page views in which <i>at least some objects</i> were optimized by SteelHeads
% Pages Partially Optimized	Percentage of pages in which <i>some, but not all, objects</i> were optimized by the SteelHeads
% Responses Optimized	Percentage of web objects that were optimized by SteelHeads

Table 1 SteelFlow WTA Metrics

Metric	Description
Average Page Time	Average page time, from first HTTP request to last HTTP response, for all page views in the group
Fully-Optimized Client Groups	Number of Originating Groups with clients that requested fully optimized pages (<i>all objects</i> in the page were optimized)
Fully-Optimized Page Time	Average page time, from first HTTP request to last HTTP response, for all fully-optimized page views (<i>all objects</i> in the page were optimized)
Non-Optimized Page Time	Average page time, from first HTTP request to last HTTP response, for all non-optimized page views (<i>no objects</i> in the page were optimized)
Non-Optimized Web Apps	Number of Defined Web Applications in which all page views were non-optimized (<i>no objects</i> in the page were optimized)
Optimized Client Groups	Number of Originating Groups with clients that requested fully- or partially-optimized page views (<i>some or all objects</i> in the page were optimized)
Optimized Page Time	Average page time, from first HTTP request to last HTTP response, for all fully- or partially-optimized page views (<i>some or all objects</i> in the page were optimized)
Optimized Web Applications	Number of Defined Web Applications with page views that were fully- or partially-optimized (<i>some or all objects</i> in the page were optimized)
Page Time	Page time, from first HTTP request to last HTTP response
Partially-Optimized Client Groups	Number of Originating Groups with clients that requested partially-optimized pages (<i>some but not all objects</i> in the page were optimized)
Partially-Optimized Page Time	Average page time, from first HTTP request to last HTTP response, for all partially-optimized page views (<i>some but not all objects</i> in the page were optimized)
x Faster When Optimized	<p>Of all page views in the group, the Fully- and Partially-optimized page views were X times faster (on average) than non-optimized page views.</p> <p>Note—This metric might underestimate the effects of optimization in your network if any of the following are true:</p> <ul style="list-style-type: none"> • The appliance observes unoptimized page views requested by clients local to the web server or in a nearby office (eg, no WAN or a very low-latency WAN between web client and server). • The appliance observes objects/pages that were optimized by SteelHeads that did not have SteelFlow WTA enabled, it counts these objects/pages as Unoptimized. <p>Note—If this metric does not appear, check the following:</p> <ul style="list-style-type: none"> • The appliance collects WTA data for all relevant servers and ports (Web Console > Administration > System > Pages). SteelFlow WTA reports on all page views optimized by a SteelHead, regardless of server/port. • The appliance is observing web traffic on its monitoring interfaces. • The appliance has Business Groups defined for both optimized and non-optimized branch offices. • You have performed all the configurations outlined in “Checklist: Data Center Deployment Setup” on page 14.

To include/exclude metrics in a Navigator, click the Columns toolbar button above the table. The relevant metrics are available under SteelHead Optimization.



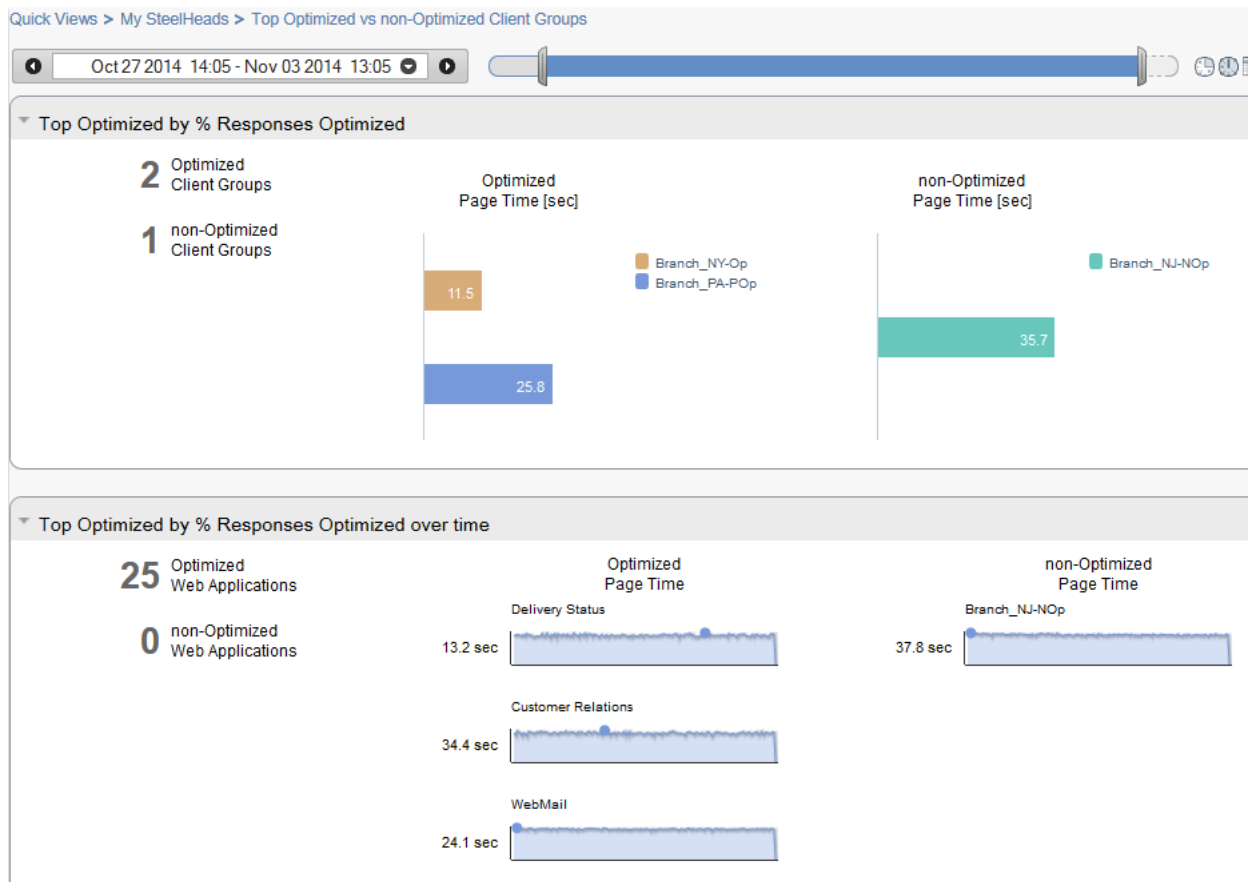
SteelFlow WTA QuickViews

The Web Console has the following QuickViews for viewing SteelFlow data:

- “Top Optimized vs non-Optimized Client Groups”
- “Top Optimized vs non-Optimized Client Groups for my Web App”
- “Top Optimized Client Groups and Web Apps”
- “Top Optimized Web Apps for my Client Group”
- “Top Optimized (Full/Partial) Client Groups”
- “Top Optimized (Full/Partial) vs non-Optimized Client Groups”

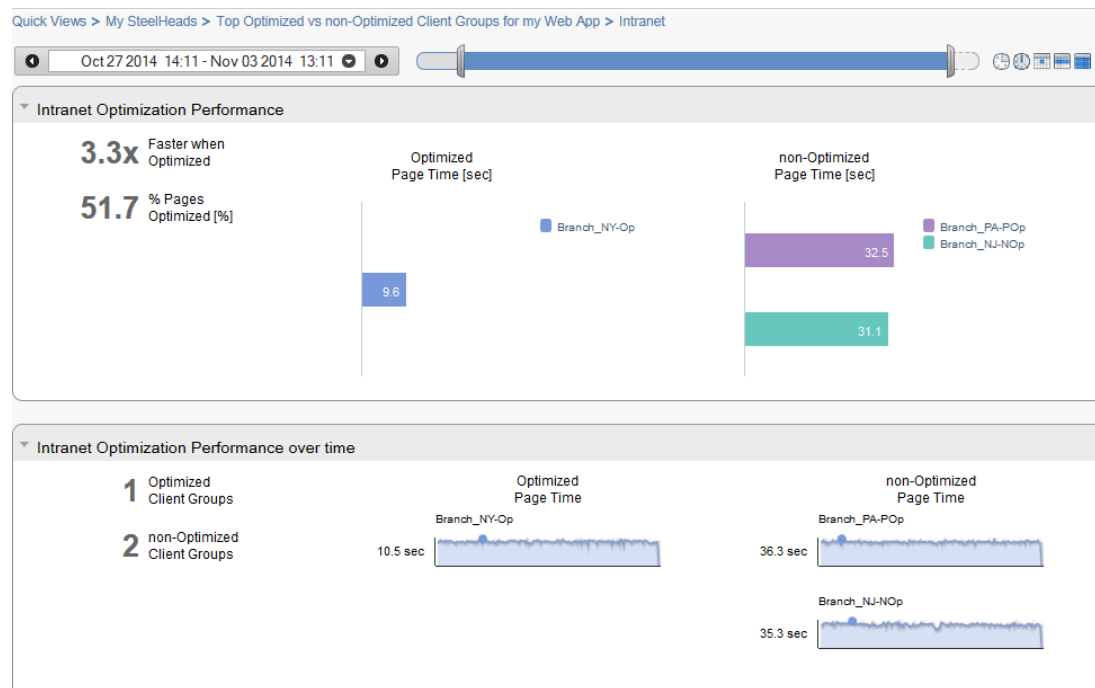
Top Optimized vs non-Optimized Client Groups

You can use this view to evaluate the effects of optimization on page times by optimized vs. non-optimized client groups with the highest page times. For metric descriptions, see [“SteelFlow WTA Metrics” on page 29](#).



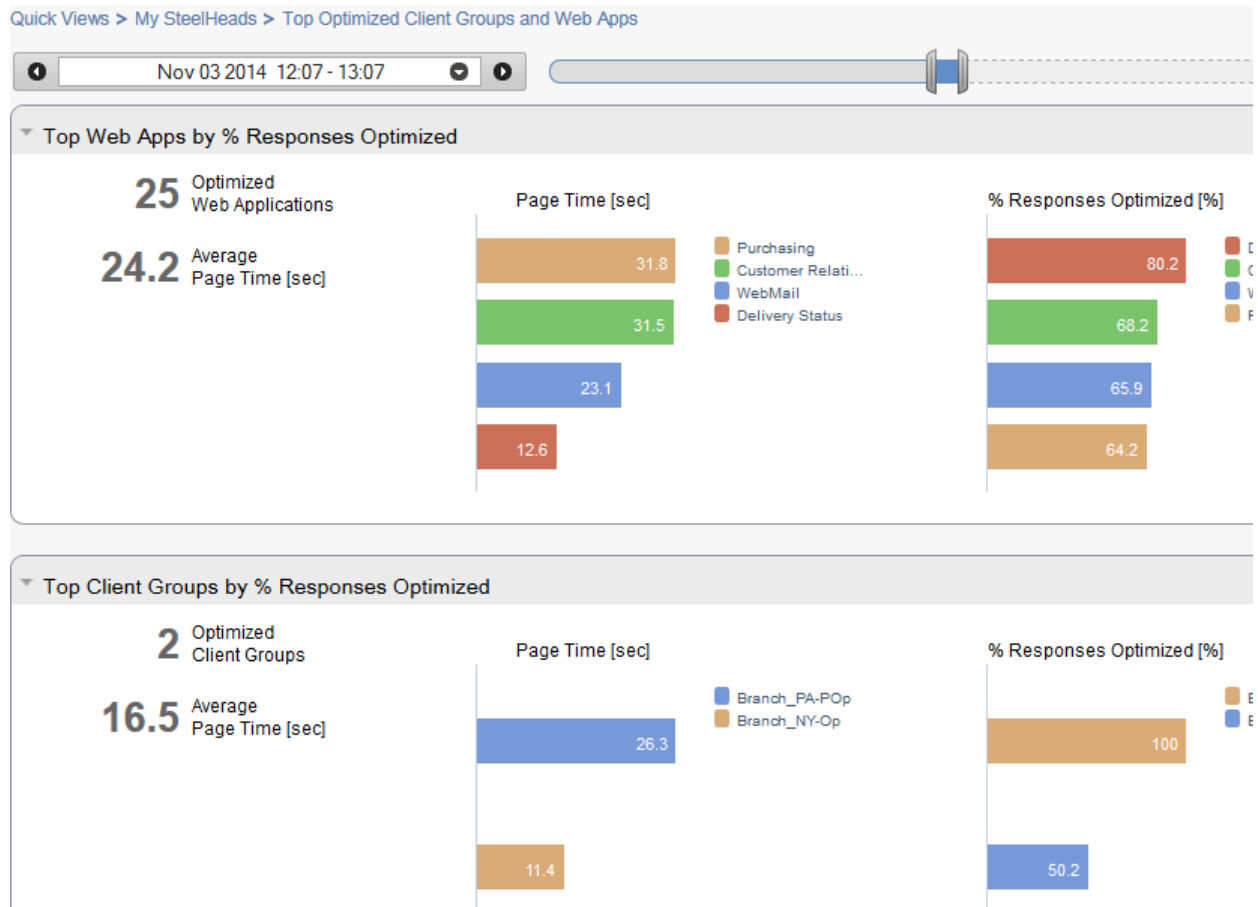
Top Optimized vs non-Optimized Client Groups for my Web App

This view enables you to compare page times for a web app when pages are requested from optimized vs. non-optimized client sites. For metric descriptions, see [“SteelFlow WTA Metrics” on page 29](#) (the [“x Faster When Optimized”](#) description also includes troubleshooting information if this field shows unexpected results).



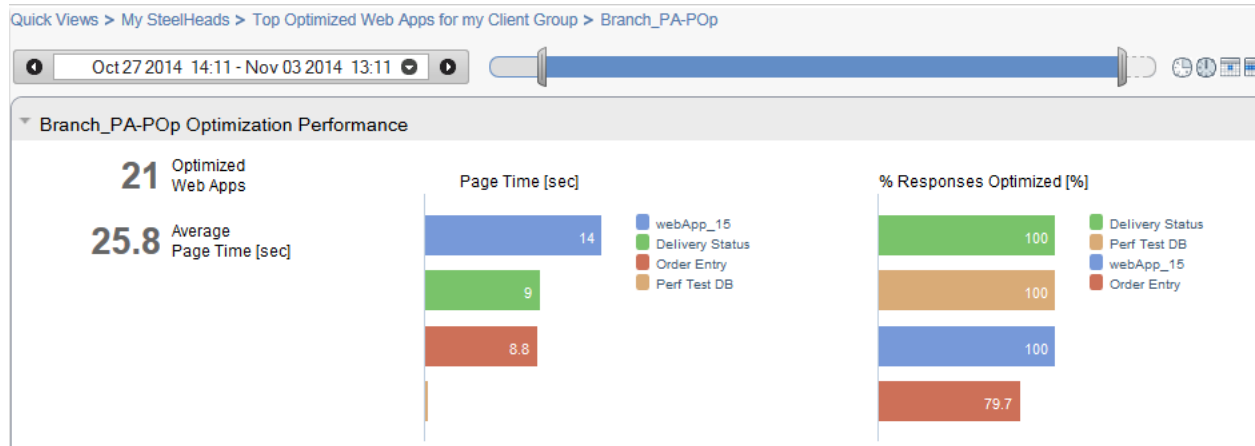
Top Optimized Client Groups and Web Apps

This view shows and compares the highest page times vs. optimization percentages for the web apps and client groups with the highest average page time. For metric descriptions, see [“SteelFlow WTA Metrics”](#) on page 29.



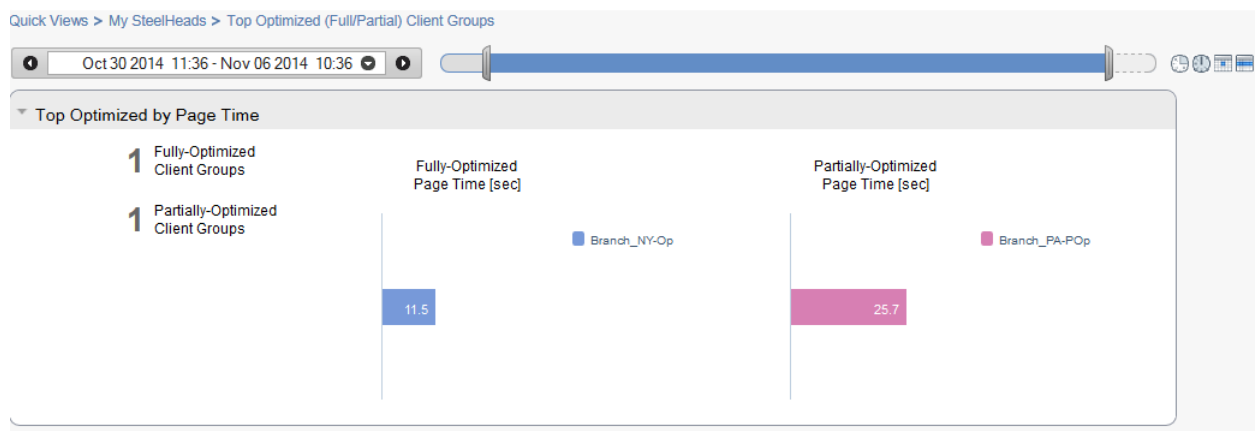
Top Optimized Web Apps for my Client Group

When you select a client group, this view shows and compares the highest page times vs. optimization percentages for the top web apps used in that group. For metric descriptions, see [“SteelFlow WTA Metrics” on page 29](#).



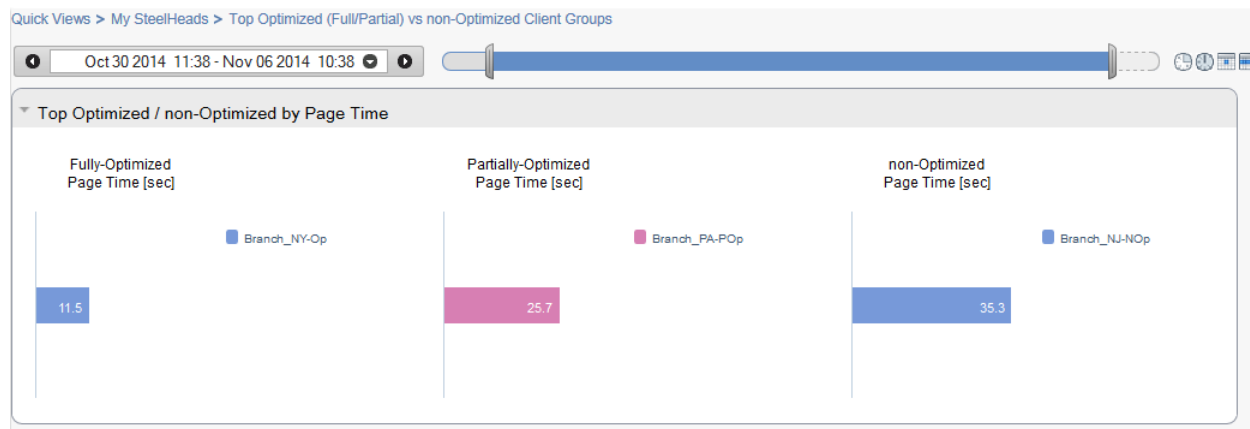
Top Optimized (Full/Partial) Client Groups

This view shows and compares the highest fully-optimized vs. partially-optimized page times in different client groups. For metric descriptions, see [“SteelFlow WTA Metrics” on page 29](#).



Top Optimized (Full/Partial) vs non-Optimized Client Groups

This view shows and compares the highest fully-optimized vs. partially-optimized vs. non-optimized page times in different client groups. For metric descriptions, see [“SteelFlow WTA Metrics” on page 29](#).



Viewing SteelFlow Data: Suggested Workflows

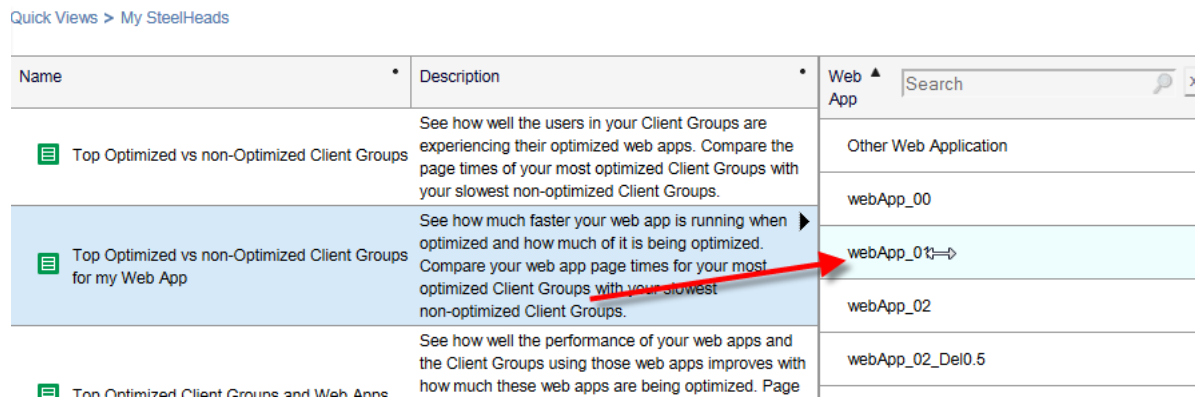
This section describes a few suggested workflows for analyzing your SteelHead performance in AppResponse:

- “At a Glance: Quick Views for Your SteelHeads” on page 37
- “SteelFlow Navigation: Drill Down to Pages of Interest” on page 38

At a Glance: Quick Views for Your SteelHeads

In this workflow, you open some Quick Views that provide at-a-glance information about optimized Business Groups and Web Applications.

- 1) In the Web Console treeview (left pane), choose Quick Views > My SteelHeads.
- 2) In the My SteelHeads table (right pane), click Top Optimized vs non-Optimized Client Groups for my Web App.
- 3) In the app-picker pane that appears, select one of the Web Applications you defined in the previous section.



- 4) In the Quick View, check the X's Faster when Optimized and % Pages Optimized results in the top-left corner. These provide an immediate snapshot of how optimization affects the application of interest.
- 5) Click the [web-app-name] link (last link in the breadcrumb path immediately above the time toolbar). A pull-down menu appears with the defined Web Applications on your appliance.
- 6) Use this link to load other Web Applications into this view. How much faster are your Web Applications when optimized?
- 7) Browse through the other Quick Views to discover more optimization results for the Business Groups and the Web Applications that correspond to your optimized locations and web apps.

Steelflow Navigation: Drill Down to Pages of Interest

In this workflow, you will navigate through the top Page Families and then drill down and analyze individual page views of interest.

Page Families

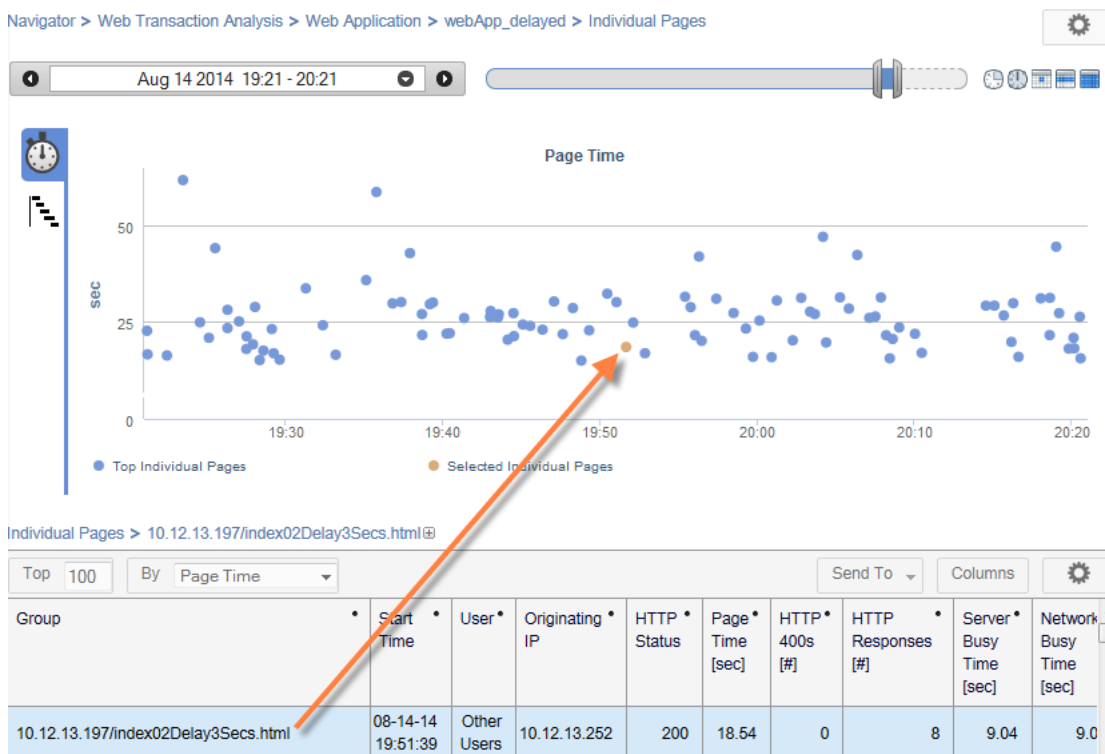
- 1) In the AppResponse Web Console treeview, choose Navigator > Web Transaction Analysis > Page Family.
- 2) In the Web Application Navigator, click the Columns button (second from right in the table toolbar). The Select Metrics dialog box appears.
- 3) In the Select Metrics dialog box, select all the SteelHead Optimization metrics and then click OK.
- 4) Examine the Page Families that appear and their related metrics.
 - Do you see any related Page Families that are part of the same application? Later you will define a Web Application so that all pages for the same application are grouped together.
 - Compare the Page Time (sec) metric for Page Families with fully optimized pages vs. non-optimized pages. Do you see a noticeable difference in page times?

Individual Page Views, the Waterfall Chart, and Page Object Delays

- 5) Examine the Page Family table and select a group with no optimized pages (that is, a family for which % Pages Optimized is 0).

6) In the table toolbar, click Send To (third from right) and choose Individual Page Views.

The Individual Page Views navigator shows results for all page views of the selected group. The time chart shows response times for all page views in the family. When you select a page view in the table, the chart highlights that page view in orange.

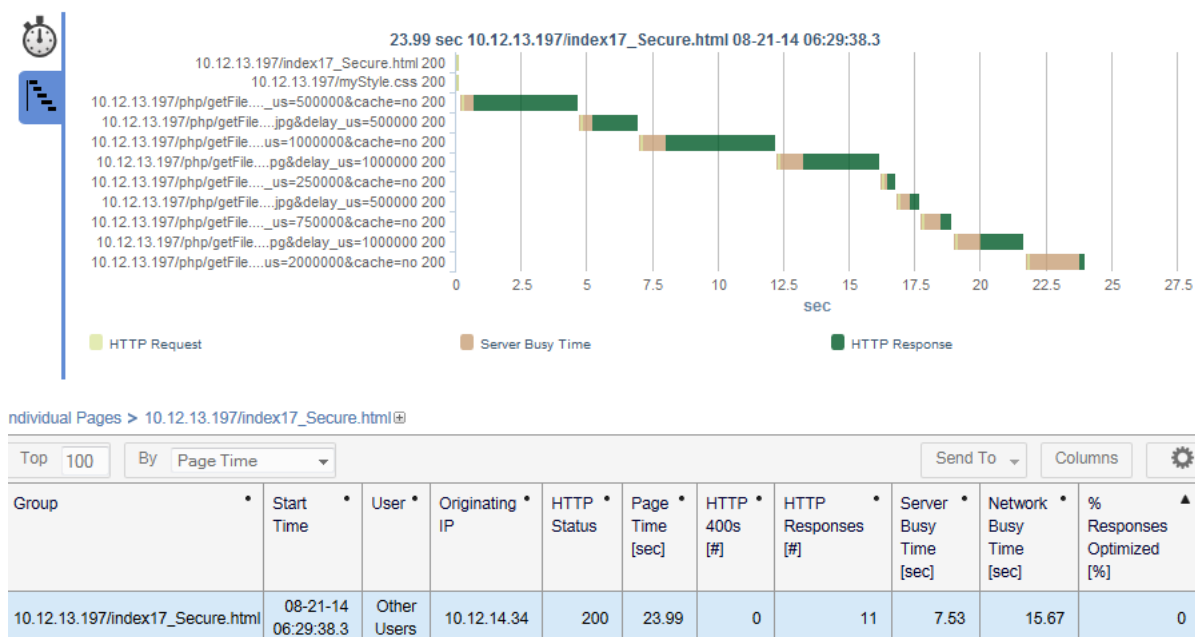


7) Sort the page based on page times, from highest to lowest: click the dot in the top-right corner of the Page Time (sec) header cell.

8)

Group	Start Time	User	Originating IP	HTTP Status	Page Time [sec]
10.12.13.197/index02.html	08-21-14 06:32:07.1	Other Users	10.12.14.34	200	23.58

9) Select the Waterfall Chart (bottom) tab to the left of the chart.



For each object in a page, the Waterfall Chart breaks down the total response time for each object into three delay categories:

- HTTP request--Network transfer time for the request from the originating IP to the server, from the first observed packet to the last.
- Server Busy Time—Time from the resource request (last observed packet) to the initial response (first observed packet).
- HTTP Response—Network transfer time for the full response payload, from the first observed packet to the last.

10) Examine the Waterfall Chart results for various non-optimized pages by scrolling up and down in the table. Examine the relative components of delay for each object in the page. Look for objects with big response times and note the relative components of delay.

- A high HTTP Request delay indicates a possible network problem or a large POST message.
- A high HTTP Response delay indicates a likely network problem, a long download, or a large object that has not been optimized.
- A high Server Busy Time delay indicates a possible problem with the server (it's overloaded) or the application (it needs to process requests more efficiently).

Optimized vs. Non-Optimized Page Views

11) Return to the Page Family Navigator view you created previously in the Page Families section.

12) In the Page Family table, select a family with a high percentage of optimized pages (% Pages Optimized is at or close to 100).

13) Click Send > Individual Page Views.

You should now have two Individual Page Views open, one for optimized pages and the other for non-optimized pages. Switch between the two views and examine various pages. Pay special attention to the total page response time (x axis in the time series chart) and the relative components of delay for the page objects. What differences do you see?

The following example show the same page transferred over a non-optimized vs. an optimized WAN. The client-side SteelHead processed requests when it could—for example, by caching and serving commonly-used objects locally—thus eliminating much of the HTTP Response delays to and from the Data Center server. As a result, the total page time was reduced from 24 seconds to 6 seconds.

Figure 1 Non-Optimized Page (Time = ~24 seconds)

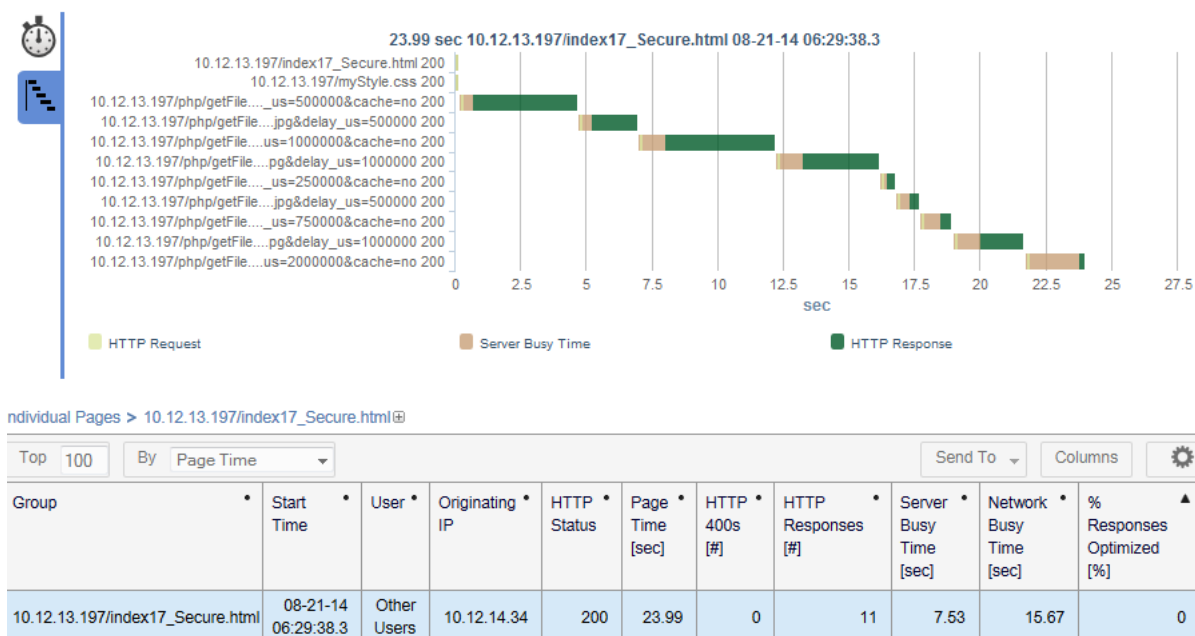
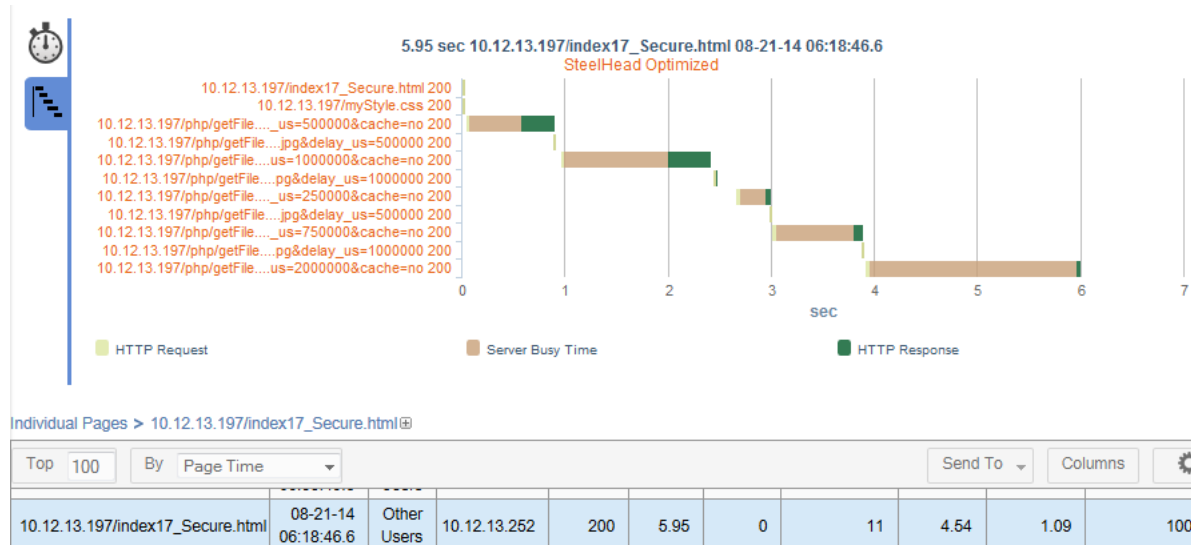


Figure 2 Optimized Page (Time = ~6 seconds)



Grouping Page Families into Web Applications

Once you see how the appliance groups your page views into Page Families, you might notice that some Page Families are actually part of the same web app. A logical next step is to define Web Applications to group these Page Families together. In the context of AppResponse, a Web Application is a grouping of Page Families based on a common set of user-specified URL patterns, servers, IPs, and ports.

Your goals in this section are the following:

- Create a Defined Application for each web app that you want to monitor.
- The Web Applications you define should include page requests from clients local to each client-side SteelHead.
- If you have one or more comparison Business Groups (unoptimized), the Web Application should include requests from the comparison BGs as well.

Note the following:

- If you make any change to the appliance that affects how traffic data is collected and organized, only traffic observed after the change is affected. This includes changes to Business Groups, Web Applications, and Named Page Families. Traffic data already stored on the appliance is not affected.
- You can define up to 100 unique Web Applications per appliance.

For more information, see [“Defined Application Manager”](#) (search the *User Guide* or the online help).

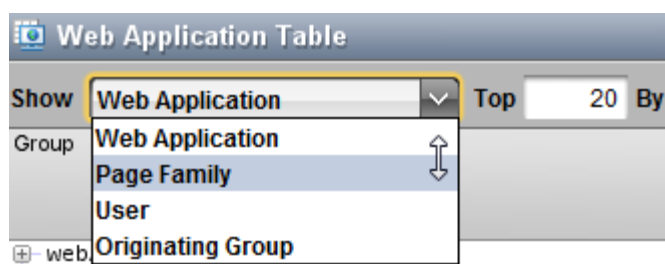
Define a Web Application

Do the following

- 1) In the Page Family Navigator, determine which Page Families are part of the same application. Focus on Page Families with the highest % Pages Optimized so you can see the effects of optimization on the corresponding applications. Ideally, you should be able to define at least three unique Web Applications.
- 2) Create a Defined Application for each logical web app you discover.

To create a Defined Application, do the following:

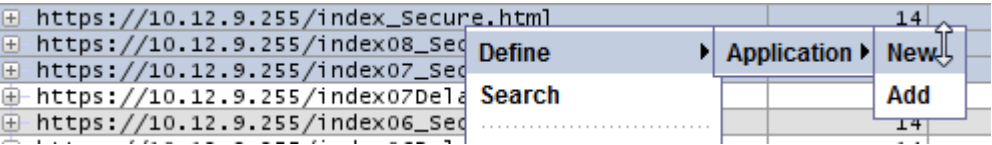
- a) Go to the Desktop Console (Administration > System > Desktop Console).
- b) Choose View > Table > Web Application.
- c) In the Web Application table, set the Show menu to Page Family.



- d) To create a Web Application from one or more Page Families, do the following:

Ctrl-click to select all the page families for the app.

Right-click on the selection and choose Define > Application > New. The Defined Application Manager opens.



e) Specify the following settings for the new Defined Application:

Table 1 Defined Web Application: Required Fields for SteelFlow WTA

Tab	Field	Description
Identity	Name	User-friendly name such as Customer Login or Account Query
Servers	IP Addresses	All web servers for the app. If you are defining a SaaS application, include the full range of IPs (0.0.0.0-255.255.255.255).

The URL patterns in the Page Families you selected are added to the URLs list automatically. For information about adding URL patterns manually, see [“Adding URLs to Web Applications”](#) (search the *User Guide* or the online help).

Troubleshooting SteelFlow WTA

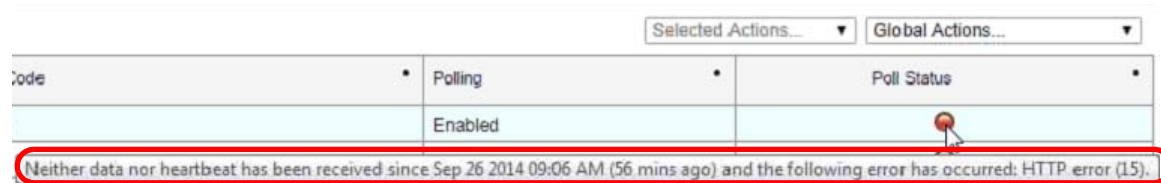
This section discusses the following topics:

- [“Status Lights and ToolTips in SteelHeads Table” on page 45](#)
- [“Red \(Error\) Status Light” on page 46](#)
- [“Yellow \(Warning\) Status Light” on page 46](#)
- [“Green \(OK\) Status Light” on page 47](#)
- [“Appliance Health Check: Performance Metrics for SteelFlow WTA” on page 48](#)

Status Lights and ToolTips in SteelHeads Table

The Web Console > Administration > Integration > SteelHeads table includes a polling status light (far-right column) for each listed SteelHead. These status lights include tooltips that indicate the last time data or a heartbeat was received and any detected errors that might have occurred.

Figure 1 Rest Cursor over Poll Status Light to See ToolTip



Note—A tooltip might show the following information: ...the following errors have occurred: "http error" (# errors), "rest error" (# errors). The (# errors) field indicates the number of errors that have occurred since the time window indicated in the tool tip (for example, Neither data nor heartbeat has been received since [date] [time] (hh hours mm mins) ago). A high number of errors in a short time window indicates a possible problem. To investigate, examine the following log file for errors of the type indicated ("http error" or "rest error"):

Administration > System > Diagnostics > Log Viewer > nptranslator.stdout

The following examples show some of the tooltip messages that might appear:

■ [“Red \(Error\) Status Light”](#)

Neither data nor heartbeat has been received since [date] [time] (hh hours mm mins ago).

Neither data nor heartbeat has been received since [date] [time] (hh hours mm mins) ago, and the following errors have occurred: "http error" (# errors), "rest error" (# errors).

Polling process is not running properly for an unexpected reason and is not able to update its poll status.

■ [“Yellow \(Warning\) Status Light”](#)

Data received within the last minute. No heartbeat has been received within the last two minutes.

Data has been received within the last minute, but the following errors have occurred: "http error" (# errors), "rest error" (# errors).

No data has been collected within the last minute, but the following errors have occurred: "http error" (# errors), "rest error" (# errors).

■ [“Green \(OK\) Status Light”](#)

Data has been received within the last minute.

No data has been received within the last minute. Data last received on [date] [time] (hh hours mm mins ago).

Red (Error) Status Light

A red (error) status light indicates that AppResponse has received no data and no heartbeat messages from the SteelHead in the last two minutes. If the Poll Status light is red, try the following:

1) Verify that the SteelHead is set up correctly:

- a) Both Steelheads (the client-side SteelHead and the SteelHead with which it is paired) have RiOS 9.0 or higher installed.
- b) Both Steelheads have HTTP Optimization and SteelFlow WTA enabled.
- c) The client-side SteelHead has REST API enabled.

2) Check for configuration issues in the AppResponse Web Console:

- a) Verify that the entry in the Steelheads table has the correct IP and OAS key for the SteelHead.

To check the OAS key for the SteelHead in AppResponse, log in to the Web Console and choose Integration > Steelheads.

To check the OAS key on the SteelHead, log in to the SteelHead web interface and choose Configure > Security > REST API Access.

- b) Check for HTTP error messages in the following log:

Administration > System > Diagnostics > Log Viewer > nptranslator.stdout

Example log entry:

```
# what: HTTP code: 401 Error id: AUTH_INVALID_CODE Error text: Invalid autho code
```

- c) Check for any continuous process exits/restarts in the following log:

Administration > System > Diagnostics > Log Viewer > npsys.log

In the following example, the Translator process has stopped and restarted twice in one minute. This might indicate a possible problem:

```
Oct 09 11:10:53 npwarden[6395] exitTranslator[7345] OK => Translator
Oct 09 11:10:53 npwarden[6395] Translator[7493] restarted Oct 09
11:10:53 npwarden[6395] Translator[7493] exited Oct 09 11:10:53
npwarden[6395] call exit trigger exitTranslator Oct 09 11:10:53
npwarden[6395] exitTranslator[7494] invoked Oct 09 11:10:53
exitHandler[7494] invoked via Translator Oct 09 11:10:53
exitHandler[7494] no core from "nptranslator", assuming success Oct 09
11:10:53 exitHandler[7494] throttle 63 sec Oct 09 11:11:56
npwarden[6395] exitTranslator[7494] OK => Translator Oct 09 11:11:56
npwarden[6395] Translator[7575] restarted
```

- 3) Verify that the appliance has network connectivity with the SteelHead. To do this, log in to the AppResponse CLI and ping the SteelHead.

Yellow (Warning) Status Light

The following issues can result in an Intermittent Error (yellow) polling status:

- 1) The client-side SteelHead might have rebooted. Check the logs on the client-side SteelHead.
- 2) A Polling heartbeat was received in the past two minutes, but a transient error might have occurred.

The most likely problem is an unstable network connection between the AppResponse appliance and the SteelHead. Wait a few more minutes to see if the polling status light turns green or red. You can also check for HTTP or REST error messages in the following log:

Administration > System > Diagnostics > Log Viewer > nptranslator.stdout

Green (OK) Status Light

If the status light for a SteelHead is green but you do not see data from that SteelHead, check the following:

- 1) Rest the cursor over the Poll Status light and note the tooltip text. If the tooltip does not include a “Data received” message, do the following:
 - a) Check the pass-through policies on the SteelHead and verify that it is optimizing the web traffic of interest.
 - b) Run the Appliance Health Check insight and examine the SteelFlow WTA checks described in [“Appliance Health Check: Performance Metrics for SteelFlow WTA” on page 48](#).
 - c) Verify that the client-side SteelHead is pairing with the correct server-side SteelHead.

In some cases, the client-side SteelHead might be paired with a different SteelHead from what you expect. This can happen due to a SteelHead Interceptor appliance or other load-balancer appliance that redirects client-side SteelHead traffic to/from a different SteelHead.

Note—SteelHead deployment scenarios are outside the scope of AppResponse documentation. For more information, refer to the following manuals:

- * SteelHead Appliance Deployment Guide
- * Interceptor Appliance Deployment Guide
- * Interceptor Appliance User Guide

- 2) The data might not appear in the user interface because it does not meet the AppResponse topping criteria (for example, “Show Top 10 Web Applications by Page Views”). To verify that the appliance is collecting data from the SteelHead, do the following:
 - a) Go to the Web Console > Navigator > Web Transaction Analysis > Originating Groups page.
 - b) In the Originating Groups navigator, set the time window to include the *<receive-time>*.
 - c) Look in the table for Originating Groups that include LAN-side clients for the SteelHead you are troubleshooting. If the groups of interest do not appear in the table, increase the Top field in the table toolbar.

Gray Light (SteelHead polling disabled)

Enable SteelFlow WTA polling:

- 1) Select the SteelHead (checkbox in left column).
- 2) Under Selected Actions, click Enable Polling.

Appliance Health Check: Performance Metrics for SteelFlow WTA

It is good practice to run the Appliance Health Check periodically while the AppResponse appliance is collecting SteelFlow WTA data. To download and install this insight, do the following:

- 1) Open an instance of the Desktop Console and connect to the appliance.
- 2) Choose Insights > Update Center.
- 3) Download and install the following insight:

support.opnet.com/ace_live/insights/support/
Tools
Appliance Health Check

This insight includes the following checks for WTA and SteelFlow WTA performance:

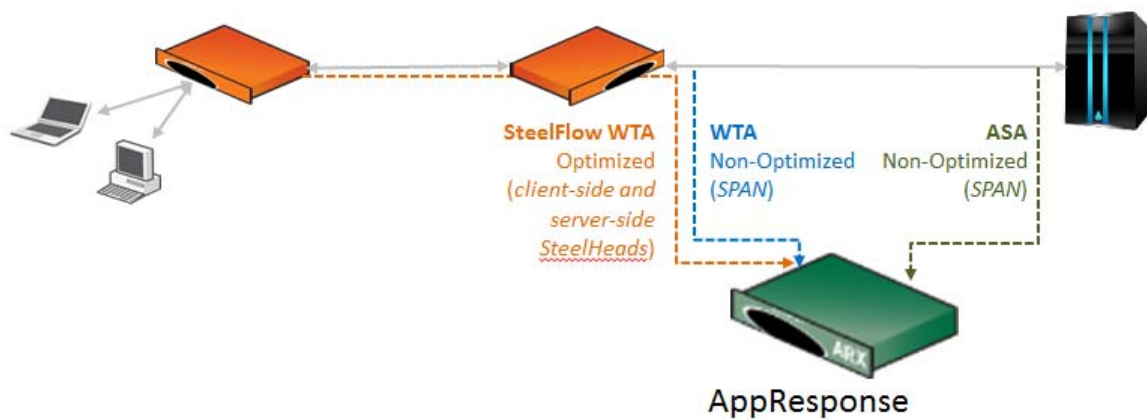
- WTA Dropped Pages [%]
Percentage of page views dropped because the filtering process (downstream from Web Transaction Analysis) cannot keep up with the load
- WTA Page Rate [# /min]
Rate of page views constructed by Web Transaction Analysis
- WTA Request Rate (span) [# /min]
Number of web requests monitored on span port and transmitted to the Web Transaction Analysis (WTA) engine, which will analyze them and combine them into web pages
- WTA Request Rate (SteelFlow WTA) [# /min]
Rate of web requests observed by SteelHeads (with SteelFlow WTA data collection enabled) and sent to Web Transaction Analysis.
- WTA Dropped Requests (SteelFlow WTA) [%]
Percentage of requests dropped when the Web Transaction Analysis (WTA) engine is unable to keep up with the load from SteelHeads. As a result, AppResponse drops SteelFlow WTA records and does not report all web traffic monitored by SteelHeads.
- Dropped SteelFlow WTA Records [%]
Percentage of SteelFlow WTA records dropped by all SteelHeads and (via drilldown) by individual SteelHeads. This can occur because
 - AppResponse and a SteelHead have some connectivity issues causing the SteelHead buffer to fill up.
 - SteelHead is generating SteelFlow WTA records faster than AppResponse can query them.
 - Multiple AppResponse appliances are polling the SteelHead (not supported). When an AppResponse appliance requests SteelFlow WTA data (via REST API) from a SteelHead, the SteelHead serves that data and then flushes the data from its buffer. As a result, that data will be unavailable to any other AppResponse appliance.

Data Types and Sources: SteelFlow WTA (Optimized), WTA (Non-Optimized), and ASA (Non-Optimized)

This section outlines the differences between the following types of data that the AppResponse appliance can process:

- “SteelFlow WTA (Optimized)”
- “WTA (Non-Optimized)”
- “ASA (Non-Optimized)”

Figure 1 AppResponse Data Types (*and Observation Points*)



SteelFlow WTA (Optimized)

Data source

- Objects and pages optimized by SteelHeads (does not include pass-through traffic).
- SteelHeads send SteelFlow WTA records to AppResponse
- AppResponse constructs Optimized page views from SteelFlow WTA records

Reported Metrics Include

- [“SteelFlow WTA Metrics”](#)—Pages Optimized, non-Optimized, Partially Optimized
- All [“Web Page Metrics”](#)
- Client/Server SteelHeads-IPs and hostnames are available for individual page views (available in Web Console > Individual Page Views navigator and Desktop Console > Individual Page Views insight)

Primary Views

- [“SteelFlow WTA QuickViews”](#)
- [“WTA \(Web Transaction Analysis\) Navigators”](#)
- [“Individual Page Views” Insight](#) in Desktop Console

Notes

- Response Time Composition Charts are available for ASA data only. RTC Charts are not available in views that display WTA data, including SteelFlow WTA data for optimized pages: Quick Views > My SteelHeads, Navigators > Web Transaction Analysis, etc.
- You can view RTC Charts for Defined Applications of type Web (such as HTTP and SSH) because metrics for these groups are calculated by the ASA analysis engine and not WTA.
- A client-side SteelHead reports only on pages that it optimized (it does not report pass-through traffic).
- You cannot download packets for optimized pages.

WTA (Non-Optimized)

Data source

Spanned packets observed on AppResponse monitoring interfaces

Reported Metrics Include

- HTTP requests—Size, throughput
- HTTP responses—Rate, size, throughput, codes (100/200/300/400/500)
- Pages—Times, rates, slow pages
- Network and Server Busy Times, per page and per object

See [“Web Page Metrics”](#) for a complete list and descriptions.

Primary Views

- [“WTA \(Web Transaction Analysis\) Navigators”](#) in Web Console
- [“Individual Page Views” Insight](#) in Desktop Console
- Insights (Desktop Console) > Page Analysis
- Tables (Web Application)

Notes

- Response Time Composition Charts are available for ASA data only. RTC Charts are not available in views that display WTA data: Individual Page Views, Navigators > Web Transaction Analysis, etc.
- You can view RTC Charts for Defined Applications of type Web (such as HTTP and SSH) because metrics for these groups are calculated by the ASA analysis engine and not WTA.
- The AppResponse appliance reports as Non-Optimized all web traffic that
 - The appliance observed on its monitoring interfaces, AND
 - Was not reported in any SteelFlow WTA data received by the appliance.

ASA (Non-Optimized)

Data source

Spanned packets observed on AppResponse monitoring interfaces

Reported Metrics Include

- [“Application Performance Metrics”](#)—Application response times, TCP connections, TCP connections, payloads
- [“Network Performance Metrics”](#)—Packet loss, retransmissions, round trip times
- [“Utilization Metrics”](#)—Throughput, packets, payloads
- [“Informational Metrics”](#)—Group information, Autonomous Systems

Primary Views

- [“Response Time Composition Chart”](#)
- Navigators > Application Stream Analysis
- Quick Views
- [“Insights”](#) (Desktop Console): Audit, Baseline, Optimize, Troubleshoot
- Tables (except Web Application, Interface, and VoIP)

Key Concepts: Web Transaction Analysis

The AppResponse user interface and documentation rely on the following concepts and terms, which have specific meanings in the context of Web Transaction Analysis:

- [“Client IP” on page 54](#)
- [“Connected Users” on page 54](#)
- [“Originating Group” on page 55](#)
- [“Originating IP” on page 55](#)
- [“Page Family” on page 56](#)
- [“Page View” on page 56](#)
- [“Server IP” on page 56](#)
- [“User” on page 56](#)
- [“User Session Tracking” on page 56](#)
- [“Web Application” on page 56](#)

Client IP

The IP of a web client or proxy that initiates the TCP connection with a web server ([“Server IP”](#)).

NOTE—In some cases, a web client might connect to a web server through a proxy such as an HTTP proxy or load balancer. When this occurs, the [“Originating IP”](#) and [“Client IP”](#) can be different for the resulting web page download. The sequence of events is:

- 1) The [“Originating IP”](#) (web client) sends the initial page request.
- 2) The [“Client IP”](#) (proxy) receives the request and forwards it to the [“Server IP”](#) (web server).
- 3) The [“Server IP”](#) processes the request and serves the requested page to the [“Client IP”](#).
- 4) The [“Client IP”](#) receives the page and forwards it back to the [“Originating IP”](#).

AppResponse parses HTTP data (such as X-Forwarded-For fields) to determine the [“Originating IP”](#) and TCP data to determine the [“Client IP”](#).

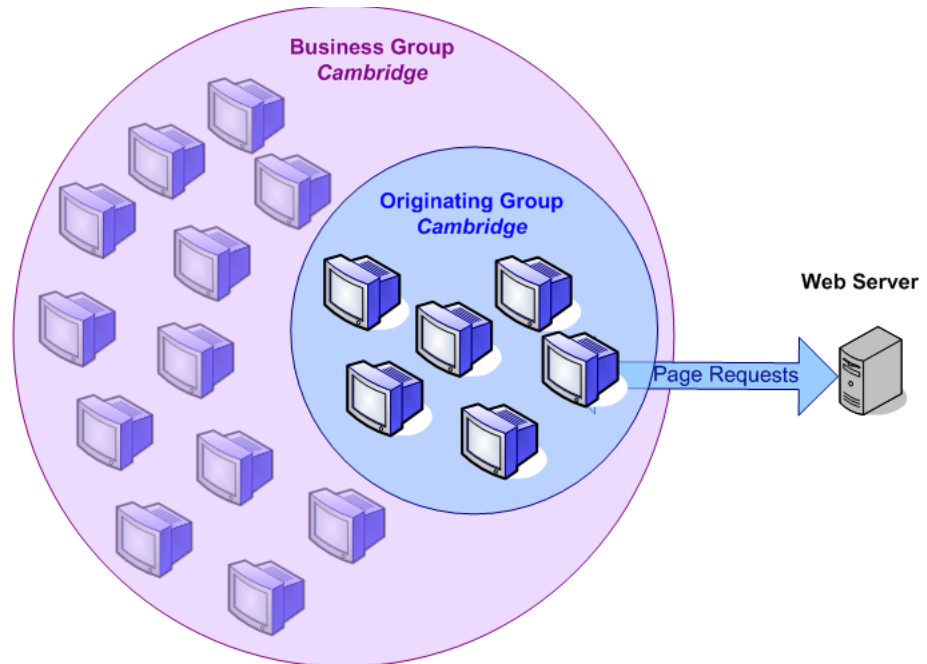
Connected Users

The set of web clients that have downloaded a specific [“User Session Tracking”](#), [“Page Family”](#), or web page. These Connected Users appear as drilldowns in the Web Applications Table.

Originating Group

The subset of IPs in a Business Group that initiate web page requests during the selected time window. If a Business Group has IPs that act as Originating IPs in the selected time window, you can see an Originating Group with the same name in the Web Application table.

Figure 1 **Originating Group = All Originating IPs within a Business Group**



You can use Originating Groups to

- Directly analyze the end user experience of web users in specific Business Groups
- View all [“Web Page Metrics”](#) for an Originating Group. These metrics are available in the following views:
 - Web Console > Navigator > Originating Groups
 - Desktop Console > View > Table > Web Application > Show Originating Group
- Create [“SLA Dashboards”](#) in the Web Console that measure page compliance (as experienced by end users) in real time. You can define web SLAs using any of the available Page metrics.

Originating IP

The IP of a web client that initiates a web page request.

If a web client connects to a web server through a proxy, the Originating IP might be different from the Client IP (see the [“Client IP”](#) description for more information).

If a proxy or load balancer changes or hides IPs, the appliance reads the X-Forwarded-for (XFF) field in HTTP headers to determine the Originating IP. If the web traffic in your network embeds the Originating IP in a different header field, you can use this option to specify this field. For more information, see [“Specify the HTTP Header Field that Contains the Originating IP”](#) on page 40.

Page Family

A set of web pages that share a common URL pattern, for which AppResponse calculates metrics such as Page Traffic, Page Times, and number of downloads. Note the following:

- When AppResponse calculates page metrics, it includes all objects in each page (.html, .gif, .jpg, and so on).
- AppResponse auto-discovers Page Families by grouping together web pages whose common URL patterns include paths up to (but not including) parameters. Thus, the following URLs are in the same Page Family:

- `http://www.dictionary.com/dict/search?term=this`
- `http://www.dictionary.com/dict/search?term=that`

The following URLs are in different Page Families:

- `http://.www.dictionary.com/dict/search?term=this`
- `http://www.dictionary.com/thes/search?term=this`

Page View

One complete instance of a web request/download.

Server IP

The IP of a web server that receives a page request from a “Client IP” and serves a web page in response.

User

An individual web client, as identified by the username associated with a web session. Note that if the same physical user has different web sessions using different usernames (such as `jsmith` and `john_smith`), these web clients will be tracked as different “users.”

User Session Tracking

The AppResponse process of tracking individual users and the pages they download automatically, based on usernames and session IDs found in the observed web traffic.

To enable this process, you need to specify the relevant key strings for pages of interest in the User Session Tracking Manager (search for “wta setup” in the online help). Each entry in this window defines a set of web pages, all of which use the same user and session keys in key/value pairs (for example, `username=jsmith` and `sessionID=1131`).

Web Application

A grouping of Page Families based on a common set of user-specified URL patterns, servers, IPs, and ports.

A Web Application is configured by creating a Defined Application of type Web. AppResponse will populate page metrics and drilldowns automatically. For more information, see “[Defined Application Manager](#)” on page 64.

Named Page Families

Named Page Families enable you to organize your page views and to define user-friendly names for cryptic URL strings. This can make it much easier to discover and identify pages of interest.

WTA assigns every page view it observes to a Page Family. The default behavior is to assign views to families based on the page view URL, for example:

`www.dropbox.com/check_update/query?type=automatic` ----> `www.dropbox.com/check_update/query...`

Named Page Families enable you to customize this behavior. You can create an NPF definition with a user-friendly family name and a set of matching criteria—URL patterns, URL parameters, and/or HTML page titles—to assign matching views to that Page Family. For example:

`www.dropbox.com/check_update/query?type=automatic` ----> `Dropbox Update`

Figure 1 Default and Named Page Families

Default Page Families	Named Page Families																				
Appliance assigns page views to families based on raw URL patterns	Appliance assigns page views to families with friendly names based on user-defined filtering criteria:																				
<table><tr><th>Group</th><th>▲</th></tr><tr><td>http://download.windowsupdate.com/c/msdownload/update/...</td><td></td></tr><tr><td>http://download.windowsupdate.com/d/msdownload/update/...</td><td></td></tr><tr><td>http://drop.ndtv.com/liveblog/prod/593361/...</td><td></td></tr><tr><td>http://ds.download.windowsupdate.com/v11/2/microsoftupdate/...</td><td></td></tr><tr><td>http://notify1.dropbox.com/subscribe...</td><td></td></tr><tr><td>http://notify6.dropbox.com/subscribe...</td><td></td></tr></table>	Group	▲	http://download.windowsupdate.com/c/msdownload/update/...		http://download.windowsupdate.com/d/msdownload/update/...		http://drop.ndtv.com/liveblog/prod/593361/...		http://ds.download.windowsupdate.com/v11/2/microsoftupdate/...		http://notify1.dropbox.com/subscribe...		http://notify6.dropbox.com/subscribe...		<table><tr><th>Group</th><th>•</th></tr><tr><td>Dropbox Notifier Service</td><td></td></tr><tr><td>Windows Update</td><td></td></tr></table>	Group	•	Dropbox Notifier Service		Windows Update	
Group	▲																				
http://download.windowsupdate.com/c/msdownload/update/...																					
http://download.windowsupdate.com/d/msdownload/update/...																					
http://drop.ndtv.com/liveblog/prod/593361/...																					
http://ds.download.windowsupdate.com/v11/2/microsoftupdate/...																					
http://notify1.dropbox.com/subscribe...																					
http://notify6.dropbox.com/subscribe...																					
Group	•																				
Dropbox Notifier Service																					
Windows Update																					

This section discusses the following:

- [“Important Notes”](#)
- [“Creating a Named Page Family” on page 2](#)
- [“Built-In Rule for Grouping Salesforce.com Pages into Named Page Families” on page 4](#)

Important Notes

Note the following:

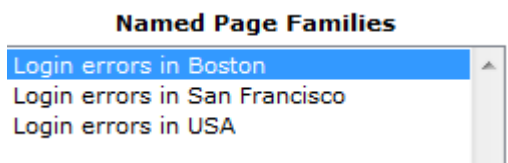
- Any change to your Named Page Family list applies only to pages observed after you apply your changes; older page views are not affected.
- You can define up to 500 Named Page Families per appliance.

- Riverbed recommends an iterative approach to defining Named Page Families:
 - Define your Web Apps to group pages into high-level groups.
 - Navigate through your page tables and drill down into individual pages.
 - Examine the URLs of important page views and see how you might want to further group them into families.
 - Define or edit your Named Page Families based on criteria that makes sense to you.
- For each page view it observes, WTA does the following:
 - Iterates through the list of Named Page Families on the appliance.
 - If it finds a matching NPF definition, assigns the view to the corresponding Page Family.
 - If no matching NPF is found, assigns to a Page Family based on the page URL (default behavior).

This means that the order in which the NPF definitions are listed can determine the Page Family to which a specific view is assigned. If a specific view matches multiple NPF definitions, it is assigned to the first (topmost) matching NPF listed in the AppResponse web UI.

In general, it is good practice to include more specific NPFs higher in the list and more general, all-inclusive NPFs lower in the list. Otherwise you might find that all views are assigned to the general NPF rather than to more targeted NPFs lower in the list.

Specific First, General Last (GOOD)



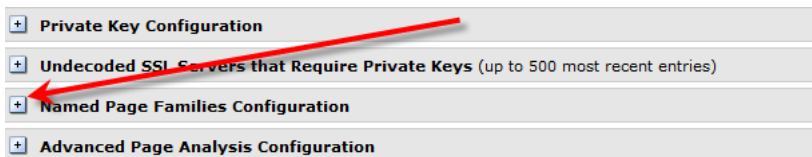
General First, Specific Last (BAD)



- The Page Families table (Desktop Console > View > Table > Web Application > Page Families) includes a right-click operation for defining a new Defined Application of type Web (Define > Application > New). **Do not use this right-click operation for a Named Page Family** if the Named Page Family name is not a valid URL pattern.

Creating a Named Page Family

- 1) In the Web Console, choose Administration > System.
- 2) In the Administration > System web UI, choose System > Pages.
- 3) If the Named Page Families Configuration options are not visible, click the '+' button to show them.



- 4) Click Add (below the table, second from left). A new, generic name appears in the Named Page Families table and the Name field.

Named Page Families Configuration

Named Page Families

Not-Blank-Test РУССКИЙ \$soap_metho
STUDIO TEST
ar.wikipedia.org/wiki TEST
www.weather.com TEST
New Named Page Family 5 (new)

Total: 5

Delete Add Up Down

Definition Details

Name: New Named Page Family 5

☒ **URL Pattern** ?

☒ **and URL Parameters** ?

Key Pattern **Value Pattern**

☒ **and Title Pattern** ?

- 5) In the Name field (top right), enter a user-friendly name for the page family. All pages in this family appear with this name in the Page Family and other navigator views.
- 6) Define the page filter: if the appliance sees a page view that matches this filter, the page is added to the family. You can include or exclude each set of criteria using the check boxes.

URL Pattern — The HTTP GET data includes one or more of these patterns.

and URL Parameters — The HTTP GET data includes one or more of these key/value pairs.

and Title Pattern — The HTML title includes one or more of these strings.

When matching, the appliance performs an OR match for elements in the same field and an AND match for elements in different fields:

```
((urlPattern1 || urlPattern2) &&
(urlKeyVal1 || urlKeyVal2) &&
(titlePattern1 || titlePattern2))
```

Note—Aside from asterisk (*) wildcards, AppResponse does not encode or decode the data in these fields. Therefore, you must specify fully-encoded URL patterns and parameters so that they match exactly the data observed on the monitoring interfaces. Because spaces are illegal in URLs, for example, you should specify %20 (in URL paths) and + (in URL parameters) instead:

Definition Details

Name:

☒ **URL Pattern** ?

customer%20logins

☒ **and URL Parameters** ?

Key Pattern	Value Pattern
location	usa+ma+cambridge

- 7) Use the Up and Down buttons (below the Named Page Families list) to order the new NPF definition in the list. The order of NPFs in this list is important because
 - A page can belong to one and only one family.
 - For each page, WTA searches the table (top to bottom) and adds the page to the first family in the list that matches the filters included in its definition.
- 8) Click Apply (at the very bottom of the page) to save your changes on the appliance.

Built-In Rule for Grouping Salesforce.com Pages into Named Page Families

This release includes the following built-in rule for grouping Salesforce.com page views into Named Page Families:

```

IF the HTTP URL includes the pattern company-name.my.salesforce.com
  IF the HTML page title includes the string "~ salesforce"
    rename the page family to:
      [salesforce:company-name] html-page-title-before-tilde-salesforce
  ELSE rename the page family to:
    [company-name:salesforce] url-path-from-domain-to-question-mark

```

Examples:

- URL = `https://mycompany.my.salesforce.com/sales/usa/east/month`
 Title = `USA Sales (East Coast)~salesforce.com Unlimited Edition`
 Named Page Family = `[salesforce:mycompany] USA Sales (East Coast)`
- URL = `https://mycompany.my.salesforce.com/ts/srch?status=open&assigned=jsmith`
 Title = `salesforce`
 Named Page Family = `[mycompany:salesforce]/ts/srch...`

Note: This rule is built in to the software and takes precedence over any user-defined Named Page Family rules for Salesforce.com that might be defined on the appliance. This rule does not appear in the interface for defining Named Page Families (web UI > System > Pages Named Page Families Configuration)

If you want to disable or override this rule, log in to the CLI and enter the following command:

```
WTA-StitcherConfig add disable-sfdc-support
```

To re-enable this rule, enter the following command:

```
WTA-StitcherConfig delete disable-sfdc-support
```

WTA (Web Transaction Analysis) Navigators

This section describes some of the advanced WTA Navigators that include additional features not available in standard Navigator views:

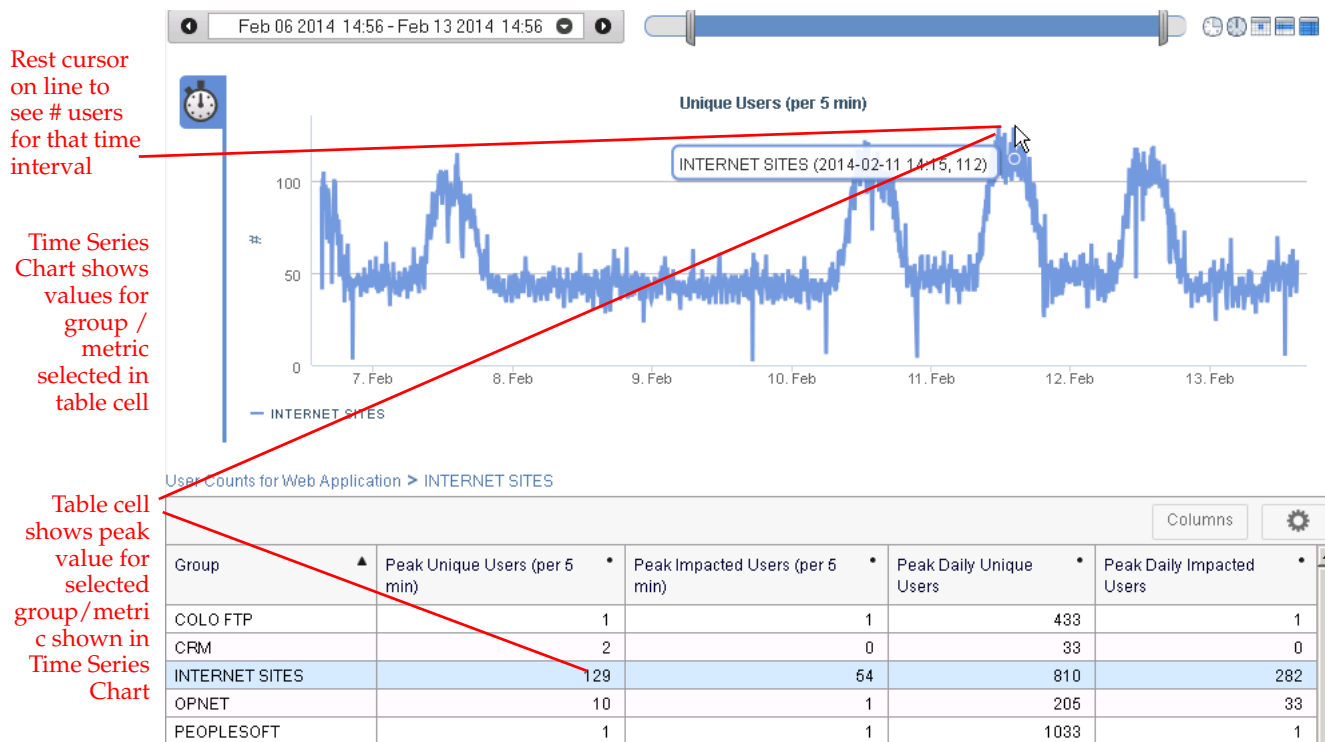
- “User Counts”
- “GeoMap View” on page 9
- “Individual Page Views Navigator” on page 11
 - “Waterfall Graph in Individual Page Views Navigator” on page 13
- “WTA Navigator Configuration Options” on page 15
 - “User Counts View Option: Reset User Counts at Midnight (Appliance Time or UTC)” on page 15
 - “GeoMap View Configuration: Map Private IPs to Geographic Regions” on page 16

User Counts

The User Counts Navigator (under Navigator > Web Transaction Analysis) shows the number of unique and impacted users for one or more Web Applications. In this context, an *impacted user* is a unique user that has experienced at least one slow page view within the time window of interest.

(The “Default Slow Page Threshold” setting defines the global default. Web Applications also have a “Slow Page Threshold” attribute that overrides the global threshold. All Slow Page thresholds are set to 5 seconds by default.)

Figure 1 User Counts Navigator



This view has the following components:

- **Time Series Chart**—Shows the number of unique and impacted page users for the time window specified in the toolbar. When you click on a cell in the table, this chart displays data for the selected group, metric, and time window.
- **Metric table**—This table shows the following metrics for each group:
 - **Peak Unique Users (per hour | per 5 minutes)**—The highest number of unique users in any 5-minute interval in the entire time window. Like all cells in the table, this number identifies the peak value shown in the Time Series Chart.

If the selected time window is 8 days or more, this metric measures users per hour. Otherwise this metric measures users per 5 minutes.
 - **Peak Impacted Users (per hour | per 5 minutes)**—The highest number of unique users who were impacted by one or more Slow Pages in any 5-minute interval in the entire time window.

If the selected time window is 8 days or more, this metric measures users per hour. Otherwise this metric measures users per 5 minutes.
 - **Peak Daily Unique Users**—The highest number of unique users in any one-day interval in the entire time window.

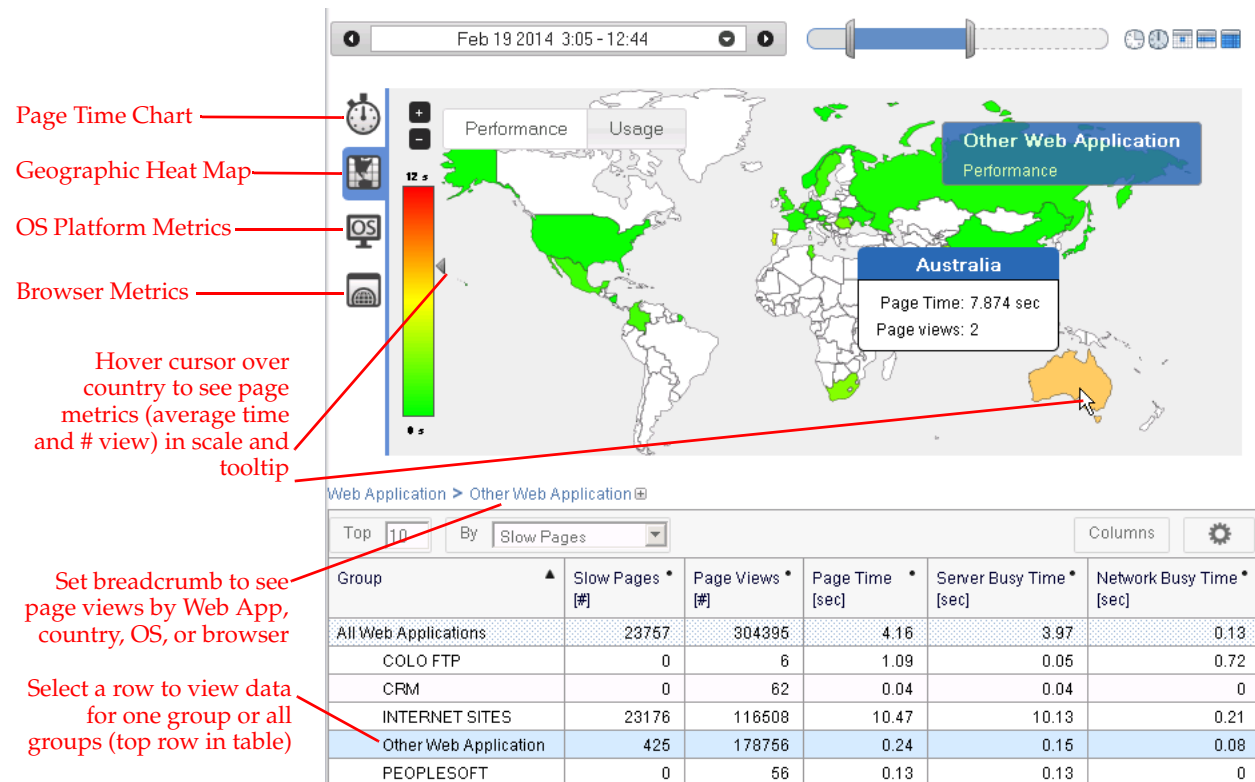
Note—The user count resets at midnight (local time of the appliance, or UTC). The Web Console shows times based on the browser-host time zone. If you are viewing user counts in a time zone three hours ahead of the appliance, you will see the user counts reset at 3am rather than at midnight.

Note—By default, each appliance resets the counter at midnight based on the local time of the appliance. You can override this default, and have the counters reset at midnight UTC instead. For more information, see [“User Counts View Option: Reset User Counts at Midnight \(Appliance Time or UTC\)”](#).
 - **Peak Daily Impacted Users**—The highest number of unique users who were impacted by one or more Slow Pages in any 5-minute interval in the entire time window. The appliance resets the impacted-users count to 0 at the start of each day.

GeoMap View

The GeoMap View Navigator (under Navigator > Web Transaction Analysis) enables you to view performance and usage metrics for Web Applications and Page Views. You can quickly see how Web Applications and Page Views are distributed by Web Application, region, platform, and browser type.

Figure 2 GeoMap View Navigator



The chart visualizes page view metrics for the selected Web Applications (table below) and time window (toolbar above). Use the table breadcrumbs to drill down to specific regions, browsers, and platforms.

Note the following:

- The appliance has an internal database for mapping public IPs to geographic regions. However, you must specify the mappings for the *private* IPs in your network. For more information, see [“GeoMap View Configuration: Map Private IPs to Geographic Regions” on page 16](#).
- You cannot view any geographic WTA data in RPM Dashboards.

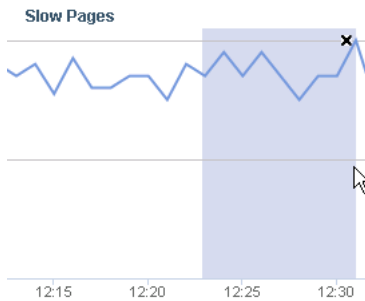
You can view the following metrics in this view:

- “Slow Pages”
- “Page Views”
- “Page Time”
- “Network Busy Time (per page)”
- “Server Busy Time (per page)”

Use the vertical tabs (left of chart) to switch between the following views:

- Page Time Chart

This chart shows the average page view speeds over time. You can use this chart to establish baseline for your page times. If you see an unexpected or unusual spike in page times, you can drag horizontally to see metrics for that region only.



- **Geographic Heat Map**

This map shows performance (average page time) or usage (total page views) metrics for all page views in individual countries and regions. The appliance determines page locations based on the [“Originating IP”](#) of each page view and the [“GeoMap Country and Region Codes”](#).

Use the table breadcrumbs to drill down into region, browser, and platform metrics; the map updates to show per-country performance or usage results when you select a new row in the table.

- **Browser Metrics**

Shows the division of page views by browser type for the selected items in the table. Rest the cursor over a pie slice to see a tooltip summary of the page views in that slice.

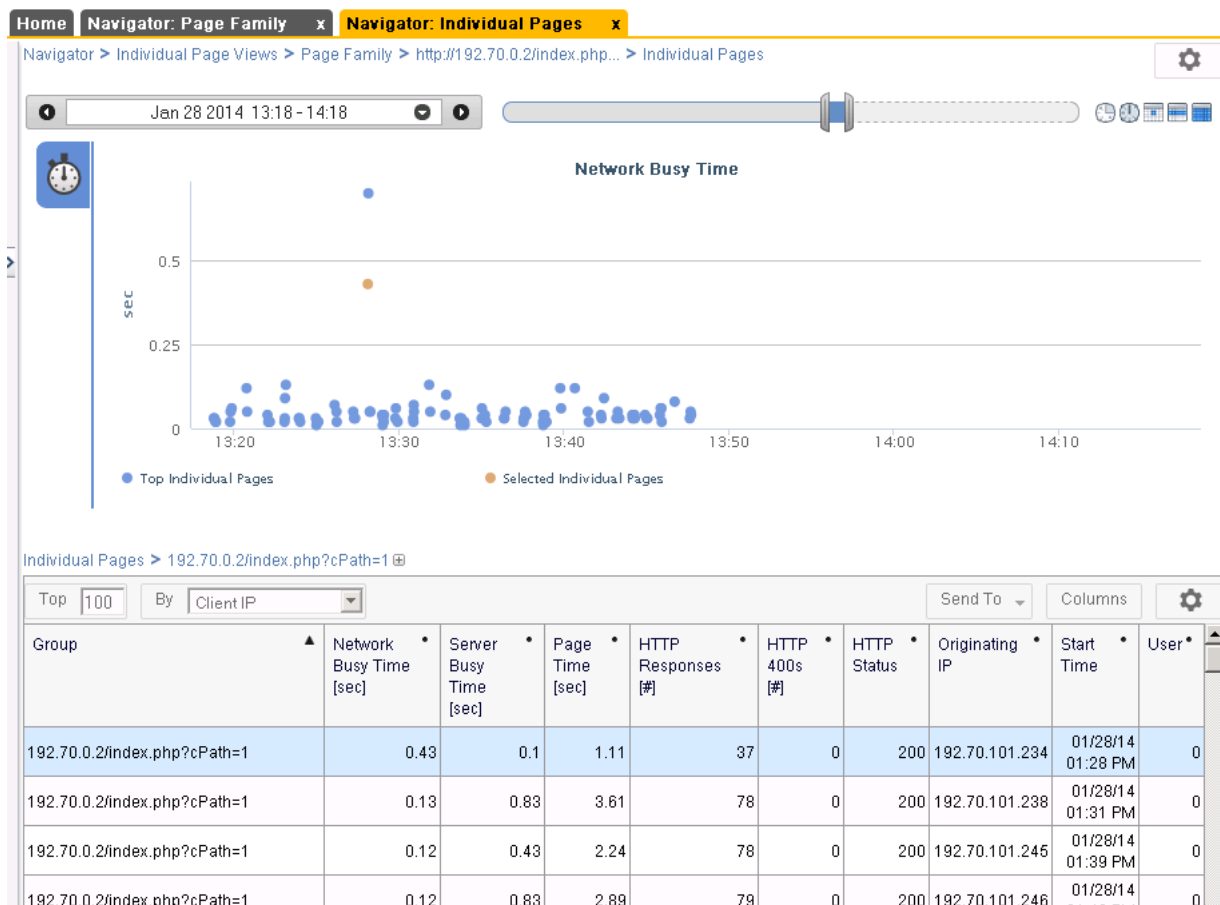
- **OS Platform Metrics**

Shows the division of page views by OS/platform for the selected items in the table. Rest the cursor over a pie slice to see a tooltip summary of the page views in that slice.

Individual Page Views Navigator

This Navigator enables you to identify and analyze page views of interest. You can find top page views based on performance or utilization metrics such as page download times; percentage of slow pages; or percentage of 3xx, 4xx, or 5xx response codes. You can also find the top page views for selected Web Applications and Page Families. If the appliance has captured packets for an individual page view, you can download these packets for in-depth analysis in Transaction Analyzer, Wireshark, or other programs.

Figure 3 “Individual Page Views” Navigator



To use this insight, do the following:

Procedure 1 Individual Page Views Navigator: Recommended Workflow

- Open one of the following views in the Web Console:
 - Navigator > Web Transaction Analysis > Web Application
 - Navigator > Web Transaction Analysis > Page Family
 - Navigator > Web Transaction Analysis > Page Family
- Select the groups whose page views you want to analyze and choose Send To > Individual Page Views.
 - The Individual Page Views Navigator appears in a new tab. Note that

- The time series graph (top right) shows a summary graph of all page views for the Page Family or Web Application you selected in the previous tab.
- The Top Individual Pages table (bottom) shows the top views for the selected item.
- The metric and topping criteria in the table are based on the **Top:** and **By:** fields in the table toolbar.

3. At this point, you can do the following:

- View individual components of delay for a page in the Waterfall Graph (see [“Waterfall Graph in Individual Page Views Navigator” on page 13](#)).

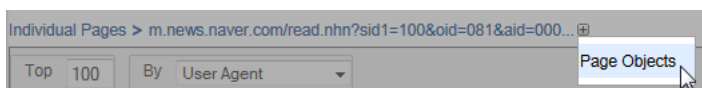
- Select another topping threshold or performance metric for the selected item:

Set the **Top:** and **By:** fields. The time series graph and table update automatically.

- Change the metrics shown in the Top Individual Pages table (see [“Page Performance Metric Definitions” on page 7](#))

- View metrics for the component resources in a page view:

Select the page view in the table. Then, in the table breadcrumbs, click the ‘+’ button to drill down to the objects contained in that page.



- Download packets for an individual page view:

cc-nashua...		0	2778.74	2778.74
m.news.na...	081&	0.62	3.08	61.8
aid=000...				
notifv1.dro...		0	56.09	56.0

Right-click on a page view in the table, then choose one of the following:

- Send to Transaction Analyzer
- Send Packets to Wireshark
- Download Packets
- Open Page [in a web browser]

Note—These operations are supported only if a packet capture was running at the time that the specific page view was observed by the AppResponse appliance.

Note—Transaction Analyzer does not retain downloaded packets on the local host unless you save the resulting file in Trace Explorer or Transaction Analyzer. If you close either window without saving, the downloaded packets will be discarded on the local host. (If you want to view these packets again, you will need to download them again before they are overwritten in the appliance buffer.)

End of Procedure 1

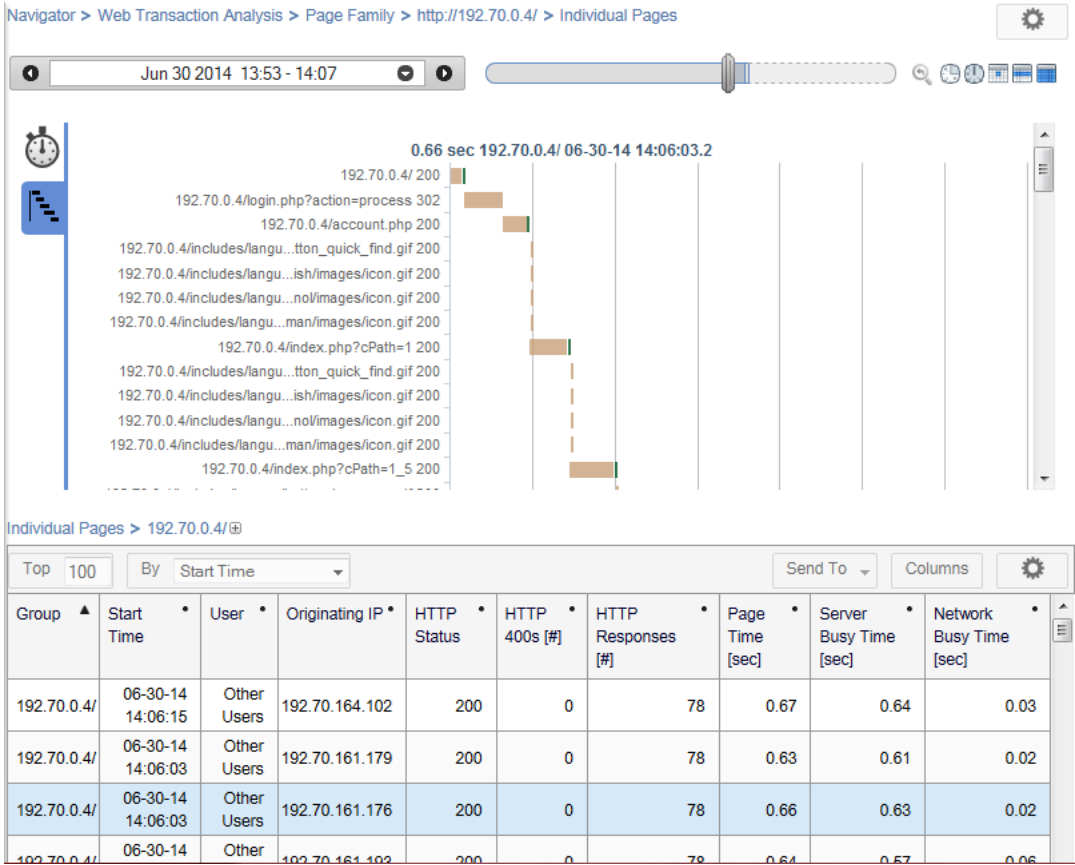
Waterfall Graph in Individual Page Views Navigator

The Individual Page Views navigator includes a Waterfall graph that shows the Server Busy Time for individual resources and for the entire page. Previously, waterfall graphs were available only in the Desktop Console > Individual Page Views insight. This view is useful when you want to identify when server processing delays contribute significantly slow page times.

To see the Waterfall graph, do the following:

- 1) In the Web Console > Navigator > Web Transaction Analysis menu, choose Web Application or Page Family.
- 2) In the Navigator, select a web app or page family in the table and choose Send To > Individual Page Views.
- 3) In the Individual Pages tab, select a page view in the table and click the Waterfall Chart tab.

As illustrated in the following figure, a Waterfall graph enables you to see clearly the server processing delays (pink) for individual resources, as well as the intervals when the server processes multiple requests in parallel. The string [partial] indicates that the appliance did not see the full request/response (due to a connection reset, packet loss, or some other cause).



This view shows the following metrics:

- Network Busy Time (per resource)--Network transfer time for the full payload of an individual request or response, from the first observed packet to the last.
- Network Busy Time (per page)--Network transfer time for all resources in a page. Because the server might have processed multiple requests in parallel, the total-page-view busy time might be less than the sum of the busy times for all resources in the view.
- Server Busy Time (per resource)--The time that the HTTP server spent processing an individual resource request. This time is measured from the resource request (last observed packet of HTTP request) to the initial response (first observed packet).
- Server Busy Time (per page)--The total time that the HTTP server spent processing all resource requests in a page. Because the server might have processed multiple requests in parallel, the total-page-view busy time might be less than the sum of the busy times for all resources in the view.

White gaps between objects in this chart indicate delays that are due to an undetermined cause (something other than network, server, or HTTP request/response delay).

WTA Navigator Configuration Options

The following configuration options are available for “WTA (Web Transaction Analysis) Navigators”:

- “User Counts View Option: Customizing Counting of Unique Users”
- “User Counts View Option: Reset User Counts at Midnight (Appliance Time or UTC)”
- “GeoMap View Configuration: Map Private IPs to Geographic Regions”

User Counts View Option: Customizing Counting of Unique Users

The User Counts Navigator tracks the number of unique and impacted page users per day. You can customize how Web Transaction Analysis (WTA) calculates the number of unique users shown in this Navigator. WTA can consider any combination of the following criteria to determine whether a user is unique:

- Originating IP
- Client IP
- User Agent
- User ID

By default, WTA considers the Client IP, Originating IP, and user agent to track users; each user has a unique combination of all three attributes.

To change the set of attributes used by WTA to count unique users, log in to the appliance CLI as Administrator and enter the following command with a space-separated list of attributes:

```
WTA-GeoConfig unique-user-tracking-user-identification [new list of attributes]
```

The following example shows the command with the list of all possible attributes:

```
WTA-GeoConfig unique-user-tracking-user-identification client-ip originating-ip user-agent user-id
```

Note the following:

- Any change to the attribute list can affect the potential number of unique users calculated. The more attributes in the list, the stricter the definition of a “unique user” and the more potential unique users for any given traffic sample.
- Any change you make to the tracking criteria will not take effect until the end of the current day. This is intentional behavior to ensure that user metrics for the current day (such as “Daily Unique Users (Today)”) are calculated using consistent criteria.

User Counts View Option: Reset User Counts at Midnight (Appliance Time or UTC)

The “User Counts” Navigator tracks the number of unique and impacted page users per day. Every day at midnight, the appliance stops counting users for the previous day and starts counting users for the next day.

By default, “midnight” is based on the local time of the appliance. This is usually the desired behavior if your appliances are centralized in one location such as a data center. If you have appliances distributed across multiple time zones, you might want to have all appliances reset their user counts at the same absolute time.

To configure the appliance to reset its user counts at midnight UTC (Coordinated Universal Time), log in to the appliance CLI as Administrator and enter the following command:

```
WTA-GeoConfig unique-user-tracking-day-boundary-utc
```

To revert to the default behavior, and reset the user counts at midnight local time, enter the following command:

```
WTA-GeoConfig unique-user-tracking-day-boundary-local
```

GeoMap View Configuration: Map Private IPs to Geographic Regions

The AppResponse Web Console includes a GeoMap View Navigator, which collects and reports the geographic locations of page views for monitored Web Applications. You can customize how the appliance maps IPs to geographic regions. This is usually necessary if you want to collect geographic information on private network IPs (since these IP locations are not public knowledge). You can also use the following method to override the default locations for public IPs.

The following steps outline the workflow:

- 1) Create a CSV file in the format described in [“IP-to-Region Custom Mapping File Format”](#).
- 2) Place the CSV file on a remote host that can connect to the appliance over an SSH connection.
- 3) To add the file to the appliance, run one of the following commands from the remote host:

Windows host (all on one line):

```
plink.exe -ssh -pw [admin-password] [admin-username]@[appliance-name]  
WTA-GeoConfig add-private-ip-geo-data < [input-file]
```

UNIX host (all on one line):

```
ssh [admin-username]@[appliance-name] WTA-GeoConfig add-private-ip-geo-data  
< [input-file]
```

- 4) The appliance CLI also supports the following commands.

To delete the current custom mapping on the appliance and revert to the default, enter the following:

```
WTA-GeoConfig delete-private-ip-geo-data
```

To view the current geographic mapping, enter the following:

```
WTA-GeoConfig view-private-ip-geo-data
```

IP-to-Region Custom Mapping File Format

To customize the mapping of IPs to geographic regions, create a CSV file in the following format:

Figure 4 IP-to-Region Custom Mapping File Format

```
# Mapping file has the following comma-separated fields per line:  
# 1) IP address, IP range, or CIDR prefix/mask  
# 2) Country code - 3 characters  
# 3) Region code - 2 characters  
# 4) Latitude - optional  
# 5) Longitude - optional  
  
# Note--version:1 (all lowercase) is required at start of file  
  
# Example:  
version:1  
127.0.0.0, DNK, 17  
172.16.6.6-172.16.6.220, USA, CA
```


Note the following:

- The CSV file must start with the following line: all lowercase, with no blank line afterwards:

`version:1`

- For a list of country and region codes, go to the Riverbed Knowledge Base (<http://supportkb.riverbed.com>) and search for solution number **S23787**.
- If your custom mappings have overlapping IP ranges, you might experience unpredictable results.

