



WHITE PAPER



# EXCLUSION BY IP ADDRESS

Controlling SiteCatalyst Data Collection via IP Address

October 28, 2008

Version 8.0



# 1 Restricting Traffic by IP Address

There are two ways SiteCatalyst data can be blocked (not displayed) in the SiteCatalyst reports.

- **Blocked via Firewall:** SiteCatalyst uses specific IP addresses to collect and process SiteCatalyst data. It's important that these IP addresses are accessible from the user's machine via an organization's firewall.
- **Blocked in SiteCatalyst:** Once the image request reaches the SiteCatalyst collection servers, SiteCatalyst users can choose whether or not to display specific IP address data in the reports via the Exclude by IP Address feature.



**NOTE:** The Exclude by IP Address feature allows up to five individual or wildcard addresses. If you wish to block more IP addresses, or have more complex IP address blocking requirements, please work with Omniture Live Support to implement a VISTA rule to block these addresses.

No part of this document provides an explicit or implicit service-level guarantee. Please refer to your SiteCatalyst Service Agreement (SLA) for further information regarding SLAs.

## 1.1 Blocked via Firewall: Omniture's IP Address Space

Omniture's SiteCatalyst data collection network employs multiple providers and products resulting in multiple IP ranges. Omniture does not guarantee that the list of IP ranges contained at the end of this document will remain the same over time. Omniture's IP address space continues to grow in step with the growth and expansion of its business. Also, ARIN (the organization that manages IP address allocation) and some Internet service providers may require changes to Omniture's IP address space at any time.

Allowing access to single IP addresses through a firewall is not a sustainable long-term solution. Many of Omniture's services rely on a pool of IP addresses, which means that requests from Omniture could originate from one IP address today and another IP address in the future.

Restricting traffic to a limited set of IP addresses has some risk associated with it. While Omniture does its best to keep this document current, Omniture could be required to make sudden changes to its IP space (for example a provider goes down, or ARIN requires an immediate change, etc.), which could result in communication from our servers being blocked by the client. Although we cannot eliminate this risk entirely, the safest method of restricting traffic by IP addresses requires opening the entire applicable range of IP addresses.

When deploying SiteCatalyst, keep in mind the IP addresses mentioned in this section. These IP addresses must be open from the respect of the user's machine in order to ensure the correct collection of SiteCatalyst data.



**NOTE:** Please do not confuse this list of IP addresses with the section discussing the Exclude by IP Address feature. This IP address list is intended for a network administrator or other technical support representative so that SiteCatalyst data from user machines is not blocked at an organization's firewall. If you wish to block specific user machines (IP addresses), refer to the next section entitled *Blocked in SiteCatalyst – Restricting Traffic via IP Address*.

## 1.2 Omniture's IP Address Blocks

The following table displays the range of Omniture's SiteCatalyst IP addresses.

	<b>CIDR Notation</b>	<b>Starting IP</b>	<b>Ending IP</b>
San Jose Block 1	66.235.128.0/21	66.235.128.0	66.235.135.255
San Jose Block 2	66.235.136.0/22	66.235.136.0	66.235.139.255
Dallas Block 1	66.235.140.0/22	66.235.140.0	66.235.143.255

The following table displays the range of IP addresses for Omniture corporate headquarters.

	<b>CIDR Notation</b>	<b>Starting IP</b>	<b>Ending IP</b>
Orem Block 1	64.0.192.0/22	64.0.192.0	64.0.195.255
Orem Block 2	207.108.181.0/24	207.108.181.0	207.108.181.255



**NOTE:** The following IP blocks were migrated from in Q3 and Q4 of 2008 and are no longer in use. These blocks are provided for historical reasons only and do not need to be included in current firewall rules.

	<b>CIDR Notation</b>	<b>Starting IP</b>	<b>Ending IP</b>
Old San Jose Block 1	216.52.17.0/24	216.52.17.0	216.52.17.255
Old San Jose Block 2	128.241.21.0/24	128.241.21.0	128.241.21.255
Old San Jose Block 3	66.151.146.0/24	66.151.146.0	66.151.146.255
Old San Jose Block 4	66.151.152.0/24	66.151.152.0	66.151.152.255
Old San Jose Block 5	70.42.134.0/24	70.42.134.0	70.42.134.255
Old San Jose Block 6	128.242.125.0/24	128.242.125.0	128.242.125.255
Old San Jose Block 7	66.151.137.0/24	66.151.137.0	66.151.137.255
Old San Jose Block 8	74.201.95.0/27	74.201.95.0	74.201.95.31
Old San Jose Block 9	128.242.100.0/27	128.242.100.0	128.242.100.31
Old Dallas Block 1	66.151.244.0/24	66.151.244.0	66.151.244.255
Old Dallas Block 2	66.150.208.0/24	66.150.208.0	66.150.208.255
Old Dallas Block 3	66.150.217.0/27	66.150.217.0	66.150.217.31

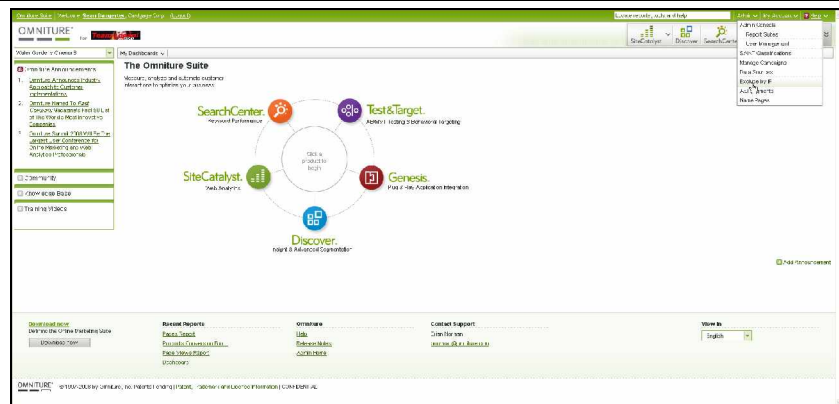
## 2 Blocked in SiteCatalyst – Restricting Traffic by IP Address

Follow the steps below to add specific IP addresses to the SiteCatalyst IP Address Exclusion List. Any IP address that is added to the IP Address Exclusion List does not take part in data collection by SiteCatalyst.

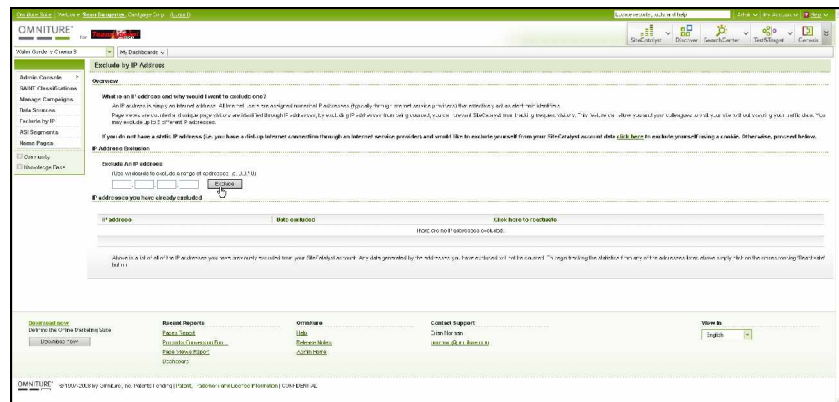
**Table 2-A: Restricting Traffic by IP Address**

**Step**

1. Log in to the Omniture Suite.
2. Click **Admin > Exclude by IP**.



3. Type the IP address or the range of IP addresses.
4. Click **Exclude**.





**CALL 1.877.722.7088**  
**1.801.722.0139**

[www.omniture.com](http://www.omniture.com)  
[info@omniture.com](mailto:info@omniture.com)

550 East Timpanogos Circle  
Orem, Utah 84097

