



## Performance Support Systems, Inc.

### **20/20 Insight and WebResponse Whitelist & Settings Information**

Below is the general “whitelist” and settings information for 20/20 Insight & WebResponse.

Most of the time, 20/20 Insight works “out-of-the-box”. In some cases, strict firewalls or other security settings may interfere with an Administrator’s or Participant’s access to the complete program or send invitations. These settings are provided to prevent such problems.

Reviewing and implementing these settings before the launch of a survey will allow easier access for 20/20 Insight Administrators to create and test survey and send email invitations. Implementation will also make it easier for Participants to receive emails and complete surveys.

Security settings change all the time, so it is always a good idea to provide the information in this document to your Participant’s IT Department well before launching a survey.

The most recent version of this document is always available here:

<http://www.2020insight.net/support/whitelistsettings.asp>

If I can provide additional details on anything else in this email, please feel free to contact me.

Thank you!

#### **Jake Foley**

Tech Support

Performance Support Systems

Monday through Friday 8:00a-6:00p ET

800-488-6463 x1

757-873-3700 x1

tech.support.pss (Skype)

[jake@2020insight.net](mailto:jake@2020insight.net)

<http://www.2020insight.net>

## **20/20 Insight and WebResponse Whitelist & Settings Information**

### **Overview:**

20/20 Insight is comprised of a Desktop component and a web-based component: WebResponse. Surveys are created in the desktop component and then uploaded to the web-based component. The web-based component then presents the surveys to participants, collects the responses and synchronizes the data back to the desktop component, where results are compiled.

### **1. Connectivity:**

WebResponse is a web-based application and requires a reliable internet connection. Some survey administration is also completed online and Subjects and Respondents also use WebResponse for completing rater assignments & surveys.

An unreliable or slow internet connection can affect connecting to WebResponse. Wireless connections can be unreliable.

Please recommend accessing WebResponse from a LAN-based connection.

## 20/20 Insight and WebResponse Whitelist & Settings Information

### 2. Browser, Firewall & Server Settings:

#### Web-browsers:

**Supported Browsers:** (No additional ActiveX or plug-ins or extensions required.)

- Internet Explorer 5 and higher
- Firefox
- Chrome
- Safari

#### Browser Settings:

- Please add "http://www.2020insight.net" as a trusted site to the browser's **Security** and **Privacy** settings.
- Please make sure "Session Cookies" are enabled on computers to be used by the 20/20 Insight Administrator, Subjects (Ratees) and Respondents (Raters).  
(Cookies are used by WebResponse during Project surveys and Administrative sessions to provide continuity for users over several pages of a survey.)

#### Local Firewall Settings:

If there is a local firewall installed:

- Please add "2020insight.net" to the "whitelist" of any local firewalls.
- The firewall will need to allow "Insight.exe" and "Project.exe" access to the internet.
- In particular, the programs "Insight.exe" and "Project.exe" will need to access "http://www.2020insight.net/"

#### I.T. Department's Server and Firewall Settings:

- If I.T. employs a Proxy Server, please allow users access to "2020insight.net"
- If I.T.'s firewall or ISA Server Firewall is set to cache websites, please disable caching for "2020insight.net"
- If I.T. employs a firewall that interferes with cookies or blocks sites, please have them list "2020insight.net" as a friendly site.

The 20/20 Insight Administrator will need to be able access:

<http://www.2020insight.net/wh4/a/login.asp>

Specifically:

<http://www.2020insight.net/wh4> or <http://66.132.174.223/wh4>

Survey Subjects (Ratees) and Respondents (Raters) will need to access a site very similar to:

<http://www.2020insight.net/wh4/s/login.asp?project=xxxx> , or  
<http://www.2020insight.net/wh4/r/login.asp?project=xxxx>

## **20/20 Insight and WebResponse Whitelist & Settings Information**

### **3. Email Settings:**

Emails are sent from the mail.2020insight.net server, but “spoofed” with the 20/20 Insight Administrator’s email address.

The emails originate from the mail.2020insight.net server, but have the Administrator’s name and email listed.

This usually allows the Administrator to receive email address bounces, out-of-offices replies, etc.

Some email servers "bounce" email addresses if they are falsely identified as spam instead of simply rejecting them.

The "bounce" may say that the address isn’t recognized, but it may actually have been rejected.

Please “Whitelist” all of the following:

**The PSS mail domain:**

mail.2020insight.net

**The PSS e-mail server IP addresses:**

66.132.174.42

66.132.174.223

Please also whitelist our domain & server information in any other email spam prevention systems you may have implemented.

If you use callout, or “sender address verification” (SAV) services, like “backscatterer.org”, “Sendio” or NetWin’s “Surgemail Allow Mechanism”, please bypass our domain within their settings.

Please exclude our domain & server IP from list checking services like "Spam Cannibal" or others.

After you have whitelisted our information, a test email can be generated by your 20/20 Insight Administrator using any project and the “Test Subject”.

## 20/20 Insight and WebResponse Whitelist & Settings Information

### 4. Barracuda Networks Spam Firewall Settings:

If you use a Barracuda Networks Spam Firewall, please add PSS to the “devices” Whitelist. If any assistance is needed setting the Barracuda Networks Spam Firewall please contact Barracuda Systems Tech Support directly at (408)342-5300.

1. Go to the “**PREFERENCES**” --> “**Whitelist/Blacklist**” tab.
2. A list of your existing whitelisted and blacklisted addresses appears on this page.
3. Type **2020insight.net** into the “**Allowed Email and Domains (Whitelist)**” field.
4. Click the corresponding “**Add**” button.
5. Please also add the **20/20 Insight Administrator’s** email into the “**Allowed Email and Domains (Whitelist)**” field. The 20/20 Insight Administrator should have included his/her email when they forwarded this email.
6. Click the “**Add**” button.

The most recent version of this document is always available here:

<http://www.2020insight.net/support/whitelistsettings.asp>