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

When contacting your client's I.T. department, please include the email address that you intend to use for sending invitations to Respondents and Subjects.

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

Thank you!

Paula Schlauch
VP, Performance Support Systems
Tech Support
Monday through Friday 9:00a-5:00p ET
800-488-6463 x1
757-873-3700 x1
tech@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.

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 (Internet Explorer):

- Please add "https://www.2020insight.net" as a trusted site to the browser's **Security** and **Privacy** settings.

  From the Windows "Control Panel":

  - Please locate and select "Internet Options"
  - Click the "Privacy" tab
  - Click "Sites"
  - Under "Address of website:" type:
    https://www.2020insight.net
  - Click "Allow"
  - Type:
    https://207.21.199.174
  - Click "Allow"
  - Click "OK"
  - Click "OK" again
- 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. (These files are found in the "Insight4" folder.)
- In particular, the programs "Insight.exe" and "Project.exe" will need to access "https://www.2020insight.net/"

Please check any virus or malware software to make sure that https://www.2020insight.net/, "Insight.exe" and "Project.exe" are whitelisted there too.

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

- If the I.T. department 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 the I.T. department 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:
https://www.2020insight.net/wh41/a/login.asp

Specifically:
https://www.2020insight.net/wh41
https://207.21.199.174/wh41

Survey Subjects (Ratees) and Respondents (Raters) will need to access a site very similar to:
https://www.2020insight.net/wh41/s/login.asp?project=45551, and/or
https://www.2020insight.net/wh41/r/login.asp?project=45551

3. Respondent Email Settings *(for those RECEIVING emails)*:

Emails are sent from the mail.2020insight.net server, and use the 20/20 Insight Administrator's name and email address as the “From” address. This usually allows the Administrator to receive email address bounces, out-of-office replies, etc. In some cases the email invitations may be falsely identified as spam or spoofing.

In the case of large surveys when many invitations are sent at once, the emails may be falsely identified as "bulk" emails.

In all these cases, the clients email server may "bounce" the emails stating that it will not accept bulk or spoofed emails. In addition, the server may reject the email altogether without any warning, or the server may say that there is no such email address.

20/20 Insight and WebResponse Whitelist & Settings Information

To prevent the invitations from being falsely labeled as spam, spoofing or bulk, please have the IT department "Whitelist" our Domain and IP address:

The PSS mail domain:
mail.2020insight.net

The PSS e-mail server IP addresses:
207.21.199.174

Please also whitelist our domain & server information in any other email spam prevention systems you may have implemented, such as "Barracuda Networks Spam Firewall" or other similar products. (Specific instructions for "Barracuda Networks Spam Firewall" are included in the complete online document.)

If callout, or "sender address verification" (SAV) services, like "backscatterer.org", "Sendio" or NetWin's "Surgemail Allow Mechanism" are used, please bypass our domain within their settings as well.

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 full, up-to-date version the 20/20 Insight and WebResponse Whitelist & Settings Information document is always available here:
https://www.2020insight.net/support/whitelistsettings.asp