GENOS WHITELISTING INFORMATION

In order to ensure that your (or your client's) firewalls and other network security appliances do not inadvertently block emails from Genos and web access to Genos Surveys, we encourage you to add (or request your client to add) the following items to their "whitelists".

GENOS SURVEYS EMAILS

PRIMARY SERVER

- Originating IP addresses: 45.33.53.109, 2600:3c01:e000:251::1
- Sender domain: @genossurveys.com
- From domain: @genossurveys.com

SECONDARY SERVER

- Originating IP address: 209.61.151.237
- Sender domain: @mg.genossurveys.com
- From domain: @genossurveys.com

In the event that the primary server gets incorrectly blacklisted, Genos will switch over to the secondary server. This provides time for the primary server to be de-listed whilst ensuring that delivery of emails continues uninterrupted.

Please note that the username part of the email address is not fixed. The username is specially encoded so that we can link failed emails back to the appropriate record on Genos Surveys.

By way of example, if Genos Surveys sends a Welcome email to 'sally.sample@yourcompany.com', the email would have the following 'from' address:

genossurveys+sally.sample=yourcompany.com@genossurveys.com

This is a valid email address that has been encoded according to the VERP standard. We rely on encoding the 'from' address this way because the 'from' address is the only information that is guaranteed to be passed back from an email server in the case of failure and this allows us to determine the original 'to' address so that we can link the bounce notification to the corresponding user in our database and then notify the appropriate survey administrator(s).

GENOS INTERNATIONAL EMAILS

Certification, events and subscription-related emails from Genos International will have the following attributes:

- Originating IP addresses: 205.201.134.1
- From domain: mail1.atl31.mcdlv.net

GENOS SURVEYS WEB

Genos Surveys is only available via a secure connection: https://genossurveys.com

- The IPv4 address of genossurveys.com is: 45.33.53.109
- The IPv6 address of genossurveys.com is: 2600:3c01:e000:251::1

We own the entire /64 pool, so if the entire subnet needs to be whitelisted, the address to use is:

- 2600:3c01:e000:0251::

Like most web applications, Genos Surveys requires cookies to be enabled for the site in order to allow people to log in (including when using the unique login links that are provided in the Welcome emails). If cookies are not enabled, a "Connection Blocked" message may be displayed, or the user may simply be redirected back to the login screen.

In home environments and some business environments, individuals can configure their browsers to accept or reject cookies on a per-site basis. In this case, please refer to the following page for more information on enabling cookies in various browsers:

http://www.whatarecookies.com/enable.asp

In environments with a managed IT service, cookies and other privacy/security settings may not be configurable by the user and, as such, may require intervention by an IT administrator or outsourced service provider. In either case, "session cookies" must, at a minimum, be enabled for https://genossurveys.com in order for the site to function properly.

CALENDLY EMAILS AND WEB (FOR GENOS AUSTRALIA CLIENTS)

Genos uses Calendly.com to allow clients (participants of our Certification Program or existing practitioners) to efficiently book an appointment with a Genos master trainer by choosing an available time slot that suits them. This is especially helpful if they are in different time zones.

- Please whitelist their sending IP address: 167.89.22.99 and add notifications@calendly.com to your safe senders list.
- Please also whitelist the application "calendly.exe" if your firewalls look at the application name.

Additional security information can be found at https://help.calendly.com/hc/articles/360009867334?locale=en-us

WHITELISTING FOR A SUPERIOR EXPERIENCE

With the advent of sophisticated hacking and phishing techniques, mail servers have become much more 'suspicious' than they have ever been, with spam filters increasingly designed to err on the side of caution – rejecting even legitimate mail messages that might have suspicious characteristics.

Any sort of assessment process can fall foul of such algorithms. A typical assessment process powered by a platform like Genos Surveys will generate a large volume of messages, each having a similar look and feel, to multiple people within an organisation. For example, a single 360-degree assessment for a participant who has two bosses, six direct reports, six peers, and six 'other' raters will result in 21 such messages. Imagine that you have ten participants – it's easy to understand how 210 largely similar messages, addressed to as many as 200+ people, arriving within minutes of one another could be misconstrued as spam or even an attack – especially by increasingly sensitive network security appliances.

The time to deal with this eventuality is before it arises. Telling your client that a failure to deliver email invitations is an issue with their mail server *after* they report non-receipt of invitation emails is less than ideal. That is why we strongly suggest that you make a discussion about *whitelisting* Genos URLs and mail servers – having your clients' IT people ensure their server recognises emails from Genos as 'friendly' – a standard part of your initial conversation with clients.

You are unlikely be the first supplier to take the responsible step of initiating a whitelisting discussion with your client's IT team. It shows foresight and professionalism and avoids issues later.

Make whitelisting a standard part of your assessment project setup and ensure a superior client experience. Every time you start working with a new client, simply supply your client's IT people a copy of the whitelisting sheet below.