2nd.MD
Communication and Whitelisting Information

GABI – Our member portal, client dashboard and case management tool

For member access to portal and dashboard, users will need access to:

Description	Whitelist	Direction	Ports
Allow employees to access 2nd.md member portal[1]	*.2nd.md	Outbound	80, 443
Client corporate needs to allow Corporate Dashboard access[1]	*.2nd.md	Outbound	80, 443
API Integration (ie., SSO, RTE)	Both: 35.162.28.254 52.35.133.87	Inbound	Varies on Integration

[1] For disaster recovery and business continuity redundancy we use AWS Elastic Load Balancers with multiple IP addresses in multiple subnets to ensure redundancy. These IP addresses can change at any time.

Note: All HTTP (port 80) requests will be redirected to HTTPS (443) to ensure encryption. The redirection is performed as a convenience to our members. All modern browsers are supported. Browsers must support at least TLS 1.2 Encryption for data security.

Mobile App Access – Our member portal via app

Client corporate should allow employees to download our mobile app.

Description	IP Address	Direction
Google Play and / or Apple App Store access Allows users to download and install mobile application	17.154.0.0/16 Apple's Class B Subnet 23.63.98.0/23 Akamai Technologies CDN For Google Play Store, the IPs on this page will need to be whitelisted: https://bgp.he.net/AS15169#_prefixes	Outbound

2nd.MD
Communication and Whitelisting Information

Email Communication

Clients working with 2nd.MD for the distribution of marketing materials via email systems should whitelist as follows:

Strongly Recommended Method

2nd.MD has configured our domain to be compliant with DKIM, SPF, and DMARC standards. The easiest way is to use these standards and/or whitelist our domain, 2nd.md. This will ensure that you always have the updated IP address.

2nd.MD uses Amazon SES services and Google G-Suite and have configured and permitted the services to send emails on behalf of 2nd.MD.

This method is supported by both Marketing and Business communications.

We recommend whitelisting 2nd.md and trusting 2nd.md in your email systems and related security components.

Manual Method

Note: If you use the above recommended method, this will be automatically managed for you.

If you choose to manually whitelist IPs as of 2/20/2020, see **References** at the end of this document.

Marketing Emails

Description	IP Address	IP Address	Direction
Emails will originate from info@2nd.md	76.223.176.0/24 76.223.177.0/24 76.223.180.0/23 76.223.188.0/24 76.223.189.0/24 76.223.190.0/24	23.249.208.0/20 199.255.192.0/22 199.127.232.0/22 54.240.0.0/18 69.169.224.0/20	Receiving Email / Whitelisting

2nd.MD
Communication and Whitelisting Information

Business Communication

Description	IPv4		IPv6 **If used by client.*	Direction
2nd.MD uses G-Suite a HITRUST Certified suite of products including email services. Includes emails from 2nd.MD technical and operation teams such as account managers, IT communication, Nurses, and records teams	35.190.247.0/24 64.233.160.0/19 66.102.0.0/20 66.249.80.0/20 72.14.192.0/18 74.125.0.0/16 108.177.8.0/21 173.194.0.0/16 209.85.128.0/17 216.58.192.0/19 216.239.32.0/19	172.217.0.0/19 172.217.32.0/20 172.217.128.0/19 172.217.160.0/20 172.217.192.0/19 172.253.56.0/21 172.253.112.0/20 108.177.96.0/19 35.191.0.0/16 130.211.0.0/22	2001:4860:4000::/36 2404:6800:4000::/36 2607:f8b0:4000::/36 2800:3f0:4000::/36 2a00:1450:4000::/36 2c0f:fb50:4000::/36	Receiving Email / Whitelisting

Secure FTP Communication

Requirements: Must support TLS 1.2

Description	IP Address	Port	Direction
SFTP Services to transmit files securely. *2nd.MD Whitelisted Port	34.214.206.225	22	Outbound
SFTP Services to transmit files securely, where 2nd.MD is connecting to client's SFTP site	216.201.246.14 34.213.52.197	22	Inbound

***Please note that if you would like to send SFTP files to 2nd.MD you will need to provide an IP or CIDR for us to Whitelist. Please work with your client management resources at 2nd.MD.**

API Integration with RTE and SSO

Description	Note	IP Address	Port	Direction
API Integration with RTE	Per client, would be disclosed on implementation project	54.191.31.219 50.112.75.204 35.162.28.254		Inbound
API Integration for SSO	Per client, would be disclosed on implementation project	52.35.133.87 35.162.28.254	443	Inbound

References

Verifying IP Address for manual: Amazonses.com

```
dig TXT amazonses.com +short| grep 'v=spf1'

results:
"v=spf1 ip4:23.249.208.0/20 ip4:199.255.192.0/22 ip4:199.127.232.0/22 ip4:54.240.0.0/18
ip4:69.169.224.0/20 ip4:76.223.176.0/24 ip4:76.223.177.0/24 ip4:76.223.180.0/23
ip4:76.223.188.0/24 ip4:76.223.189.0/24 ip4:76.223.190.0/24 -all"
```

Windows Configuration

```
C:>nslookup -type=TXT amazonses.com | find "v=spf1"

results:
"v=spf1 ip4:23.249.208.0/20 ip4:199.255.192.0/22 ip4:199.127.232.0/22 ip4:54.240.0.0/18
ip4:69.169.224.0/20 ip4:76.223.176.0/24 ip4:76.223.177.0/24 ip4:76.223.180.0/23
ip4:76.223.188.0/24 ip4:76.223.189.0/24 ip4:76.223.190.0/24 -all"
```

Verifying IP Address for manual: Google.com (G-Suite Email)

```
dig TXT _spf.google.com +short| grep 'v=spf1'

results:
"v=spf1 include:_netblocks.google.com include:_netblocks2.google.com
include:_netblocks3.google.com ~all"

dig TXT _netblocks.google.com +short | grep 'v=spf1'

results:
"v=spf1 ip4:35.190.247.0/24 ip4:64.233.160.0/19 ip4:66.102.0.0/20 ip4:66.249.80.0/20
ip4:72.14.192.0/18 ip4:74.125.0.0/16 ip4:108.177.8.0/21 ip4:173.194.0.0/16 ip4:209.85.128.0/17
ip4:216.58.192.0/19 ip4:216.239.32.0/19 ~all"

dig TXT _netblocks2.google.com +short | grep 'v=spf1'

results:
"v=spf1 ip6:2001:4860:4000::/36 ip6:2404:6800:4000::/36 ip6:2607:f8b0:4000::/36
ip6:2800:3f0:4000::/36 ip6:2a00:1450:4000::/36 ip6:2c0f:fb50:4000::/36 ~all"

dig TXT _netblocks3.google.com +short | grep 'v=spf1'

results:
"v=spf1 ip4:172.217.0.0/19 ip4:172.217.32.0/20 ip4:172.217.128.0/19 ip4:172.217.160.0/20
ip4:172.217.192.0/19 ip4:172.253.56.0/21 ip4:172.253.112.0/20 ip4:108.177.96.0/19
ip4:35.191.0.0/16 ip4:130.211.0.0/22 ~all"
```

Windows Configuration

```
C:>nslookup -type=TXT _spf.google.com | find "v=spf1"
Then for each of the responses, same as above.
```