Changing Sandata Whitelist IPs

Frequently Asked Questions

What is a whitelist IP?

The whitelisting of an IP address is a cybersecurity technique that gives IT administrators control over who can access business systems and resources. A whitelist IP is an IP address or range of addresses that is granted access to a system or network while others are denied. It is commonly used to enhance security by allowing only trusted entities to connect.

ADDING IP ADDRESSES

How do I add an IP address or IP Range to the whitelist?

The process varies depending on the system or service the client uses. Generally, the IT/Network Administrator from the client will need to do the following:

1. **Access the Admin Console:** Log in to the administrative interface of the system or service.
2. **Locate Whitelist Settings:** Find the section for managing IP addresses or security settings.
3. **Save Changes:** Confirm and apply the changes.

How do I verify that the new whitelist is working?

After updating, verify functionality:

- **Testing Access:** The client can try accessing the Sandata system any time after the maintenance on September 28, 2024, at 8:00 p.m. ET to confirm.

What if I encounter issues after changing whitelist IPs?

If an issue occurs, the user calling into Sandata should work with their IT/Network team and have the IT/Network team confirm they are whitelisting by IPs and have registered the range properly:

- **Double-Check Configuration:** Ensure IP range was correct added with the proper format:
    - 208.64.40.0/23

Can a client add the IP Range now to the Whitelist?

Yes, if the client has implemented whitelists by IP/IP range as their protocol, the IP range (208.64.40.0/23) can be added now. Sandata recommends adding the IP range before September 28, 2024, at 8:00 p.m. ET.

When I add the new IP Range, do I need to remove an IP address?

Please see REMOVING IP ADDRESSES below.

IMPACT OF WHITELIST IP CHANGES

Which Sandata environments will this impact?

The new IP Ranges being added are used for External Customer-facing sites, so in addition to Production applications, if your company uses a Sandata User Acceptance Testing (UAT) environment and also whitelists IP addresses for both Production and UAT environments, please add the IP Range.

Will Managed Care Organizations (MCOs) or Providers using Sandata technology hosted by the State be impacted?

It is possible there will be an impact if the MCO or Provider also chooses to whitelist IP address a security protocol or uses an IP address when accessing Sandata FTP servers or APIs instead of the DNS name.

Will this impact my nightly SFTP file exchange processing with Sandata?

It depends on the SFTP process and who is the hosting provider of the files. So, if your company hosts the SFTP site and Sandata drops and picks up files from your SFTP Server then this maintenance should have no impact.

If, by chance, you either pick up or drop off files from a Sandata SFTP server and you use the DNS name (e.g., transfers.sandata.com), you should have no impact.

Sandata recommends the use of DNS names, but if your company uses the Sandata IP address to connect, please work with your CSM or helpdesk to get the right DNS name to use for your SFTP process.

Will this impact the Sandata web APIs (HTTPS transactions) I use in my architecture?

Similar to SFTP, Sandata recommends the use of DNS names, but if the API uses an IP address, please work with your CSM or helpdesk to get the right DNS name to use for your SFTP process.

REMOVING IP ADDRESSES

What Sandata IP Addresses should be removed?

At this time, Sandata will phase in the new IP address range provided and will begin removing unused IP addressed over the course of several months to minimize disruptions. Sandata will provide updates on what IP addresses will be retired from the Sandata network.