everbridge
500 N Brand Blvd, Suite 1000
Glendale, CA 91203 USA
tel: 888.366.4911
fax: 818.484.2299

Everbridge Whitelisting Best Practices

January 2014

At Everbridge, we continually strive to improve our broadcast capabilities to better serve our customers. As part of this ongoing effort, Everbridge regularly adds new infrastructure and re-allocates existing infrastructure to increase system performance, resiliency and better meet the needs of our growing customer base.

As a best practice, Everbridge customers who need to restrict access to Everbridge services for security reasons should follow the whitelisting guidelines below:

WHAT IS WHITELISTING?

Whitelisting ensures that communication between trusted sources will not be inadvertently blocked by security systems and policies, e.g. firewall rules, email spam filtering and proxy server settings.

WHY SHOULD I WHITELIST?

As the Everbridge service is used to send critical communications, we want to ensure that users are able to access Everbridge services to send critical communications whenever necessary. Additionally, we want to ensure intended recipients are also able to receive such notifications.

CAN I WHITELIST BY IP ADDRESS?

Everbridge strongly discourages whitelisting by specific IP addresses or IP ranges, since IP addresses used to deliver Everbridge services are continually expanding as we grow to meet the critical communication needs of our customers. If the guidelines below are not adequate for your organization and you need specific IP addresses to whitelist, please contact Everbridge Support.

HOW DO I WHITELIST?

Your organization's network and security administrator(s) will know whether whitelisting is required within your organization and how to implement it. To whitelist Everbridge solutions, please provide them with the following information:

Whitelisting Everbridge Email, including Email Notifications:
It is recommended to configure your organization's email servers to rely on "Sender Policy Framework (SPF)", an industry standard for determining which servers are authorized to send email on behalf of Everbridge. If SPF implementation is not a viable option, your network administrator(s) should ensure that e-mail notifications sent from the following domains are allowed:

- Domains: everbridge.com, everbridge.net
- Mail domains: *.everbridge.com, *.everbridge.net, *.everbridgemail.com

500 N Brand Blvd, Suite 1000
Glendale, CA 91203 USA
tel: 888.366.4911
fax: 818.484.2299

Whitelisting Everbridge web and API usage:

It is recommended to allow HTTP (port 80) and HTTPS (port 443) access to the following domain names:

- For Everbridge Aware, SmartGIS and Matrix solutions:
  - www.everbridge.net
  - matrix.everbridge.net
  - quicklaunch.everbridge.net
  - ww2.everbridge.net
  - mobile.everbridge.net
- For Everbridge Suite solution, which includes Mass Notifications, Interactive Visibility and Incident Management:
  - manager.everbridge.net
  - api.everbridge.net
  - member.everbridge.net

Whitelisting Everbridge SFTP for uploads:

If your organization uses the Everbridge SFTP service for uploading data, then SFTP (port 22) access to the following hostnames should be allowed:

- For Everbridge Aware, SmartGIS and Matrix solutions:
  - sftp.everbridge.net
- For Everbridge Suite solution, which includes Mass Notifications, Interactive Visibility and Incident Management:
  - sftp-acct.everbridge.net
  - sftp-us.everbridge.net
  - sftp-uk.everbridge.net
  - sftp-us-e01.everbridge.net
  - sftp-ca.everbridge.net
  - sftp-de.everbridge.net

Whitelisting Everbridge Client Portal and Everbridge University:

It is recommended to allow HTTP (port 80) and HTTPS (port 443) access to the following domain names:

- clientportal.everbridge.com
- na6.salesforce.com
- cys.na6.visual.force.com
- everbridge.adobeconnect.com

If your organization has additional questions please open a support case with the Everbridge Support Team via methods provided here: http://www.everbridge.com/customer-support/.