AMSConnect System Requirements

Last updated: September 9, 2020

White Listing

AMSConnect runs on http and https protocols. Please make sure ports 80, 443, and 8443 are allowed across your fixed and wireless networks.

TCP port 5223 (Apple push notifications)
TCP port 5228 (Google push notifications)

Proxy or Firewall

Please check to make sure that the following sites are not blocked:

https://messenger.amsconnectapp.com
https://api.amsconnectapp.com
https://notify.amsconnectapp.com
https://admin.amsconnectapp.com
https://apps.amsconnectapp.com

Please check to make sure that emails from the following domain are not blocked:

amsconnectapp.com
us-west-2.amazonses.com

Wi-Fi

AMSConnect will actively send and receive messages via both Wi-Fi and a mobile data connection. If a user has enabled Wi-Fi and is running on the approved Wi-Fi networks, AMSConnect will default to Wi-Fi and only move to mobile data when that connection is not available.

Access: The Best Practice we recommend is to provide mobile users with access to a Wi-Fi network that Does Not Require Re-Authentication, such as most “guest networks”. This can create a poor user experience as users believe they are connected, however the messages are held pending authentication.

Set Up: The Best Practice is that users must turn off “Ask to Join Networks” on their mobile device. This will keep them from bouncing to unapproved or blocked Wi-Fi networks.

Users can use AMSConnect on their home Wi-Fi network.

Questions?

Please email **amsconnect@americanmessaging.net**