Bypassing Zscaler proxies for improved performance

Zscaler is a cloud security platform that scans your data for threats. When Zscaler is installed on a presenter's computer, it will cause any Webcast audio and video data to be redirected through the Zscaler security cloud before it can reach the Webcast network. This may lead to video/audio connections being blocked completely or issues with call quality if the connection is completed.

Webcast connections are not sending any executable data, so there is not a need to scan it with Zscaler. We advise our customers to configure Zscaler to allow Webcast data to bypass to prevent potential issues.

More information about Zscaler bypasses can be found here: https://help.zscaler.com/z-app/best-practices-adding-bypasses-z-tunnel-2.0

A full list of Webcast network requirements, used to configure Zscaler, can be found at the link below. Refer to the "Webcast Presenter" columns in the Network Resources document when updating Zscaler. The Webcast Audience Member requirements do not need to be allowed in Zscaler.

Webcast Network Resources: https://webcasts.com/networkresources/

Revision #4
Created 14 October 2022 15:38:16 by Matt Engel
Updated 6 June 2024 14:38:42 by Matt Engel