QRG – COMMUNICATION SETUP (ALL SYSTEMS)

This Quick Reference Guide summarizes the implementation process of the domains and communication rules required to administer Certiport certification exams through all our systems and modalities : Compass Local (Compass for Windows and Compass for Mac), Compass Cloud, and Exams from Home.

Most institutions have protection in place to prevent harmful items such as scripts, viruses, malware, and other attacks from entering their private network via the internet. To achieve this level of protection, both hardware and software can be employe d in the form of Firewalls, Proxy Servers, IP Filters, and Security Software.

In addition to these types of protection, many institutions will also restrict internet access down to an approved list, an unapproved list, or both – which are called whitel ists and blacklists, respectively. These types of lists are primarily used for websites alone, but can also be utilized in many different platforms and capacities.

- Whitelist: A list of pre -approved websites, servers, ports and/or other network rules that can always be reached/allowed if access is requested.
- Blacklist: A list of restricted websites, servers, ports and/or other network rules that can never be reached/allowed if access is requested.

Certiport has a list of domain names

QRG – COMMUNICATION SETUP (ALL SYSTEMS)

Important: As a consequence of Certiport's data center transition that occurred on January 21st, 2024, it became impossible to provide a list of specific IP addresses that must be accessible for an uninterrupted exam experience. Therefore, we are now requiring *.certiport.com and the other domain names listed below to be whitelisted.

Required:

Certiport now employs the use of DNS whitelisting (domain names). The following whi u (e)-2.9 (l)0.r (s)2.9 1 Tw 10.886 0 Td [(