

Firewall and Proxy Server considerations when using Netop's WebConnect /WebConnect 3.0 communication

Article Number: 182 | Last Updated: Fri, Oct 20, 2017 9:29 AM

Â When configuring Netop Remote Control (or Netop OnDemand) to use the WebConnect /WebConnect 3.0 communication instances when access must be allowed through a company's proxy server and/or firewall. **Netop Hosted WebConnect**

Data traffic protocols must be allowed outbound through a firewall to the Connection Manager and Connection Server modules. Outbound communication to the WebConnect Connection Manager is HTTP:80 and/or HTTPS:443.Â Outbound communication to the WebConnect Connection Servers is TCP:6502 and/or HTTP(TCP encapsulated):80.

Rules or exceptions may need to be created that allow communication through a proxy server to communicate with the Connection Manager and Connection Server modules.

Netop's hosted WebConnect environment offers three separate environments.Â Connection Manager URL is based on their region.Â Here is a list of I.P. addresses that you may refer to if you need to create firewall or proxy rules for WebConnect communication.

For the European (EU) WebConnect service, the following communication needs to be allowed: Outbound HTTP:80 to the Connection Manager (webconnect01eu.netop.com), having the public IP 54.246.197.203 Outbound HTTP(TCP encapsulated):80 to the first Connection Server, having the public IP 54.246.236.65 Outbound TCP:6502 and/or HTTP(TCP encapsulated):80 to the second Connection Server, having the public IP 46.51.206.56 For the North American (US) WebConnect service, the following communication needs to be allowed: Outbound HTTPS:443 and/or HTTP:80 to the Connection Manager (webconnect01us.netop.com), having the public IP 54.200.219.230 Outbound TCP:6502 and/or HTTP(TCP encapsulated):80 to the first Connection Server, having the public IP 54.200.190.121 Outbound TCP:6502 and/or HTTP(TCP encapsulated):80 to the second Connection Server, having the public IP 52.24.214.0 **Netop Hosted WebConnect 3.0 Data traffic protocols must be allowed outbound through a firewall to the Connection Manager and Connection Server.Â Outbound communication to the WebConnect 3.0 Connection Manager is HTTP:80 and/or HTTPS:443.Â Outbound communication to the WebConnect 3.0 Connection Servers is TCP:6502 and/or HTTP(TCP encapsulated):80.**

Rules or exceptions may need to be created that allow communication through a proxy server to communicate with the Connection Manager and Connection Server modules.

Netop's hosted WebConnect 3.0 environment offers three separate environments.Â Connection Manager URL is based on their region.Â Here is a list of I.P. addresses that you may refer to if you need to create firewall or proxy rules to allow WebConnect communication.

For the European (EU) WebConnect 3.0 service, the following communication needs to be allowed: Outbound HTTP:80 to the Connection Manager (webconnect3eu.netop.com), having the public IP 52.208.116.223 Outbound TCP:443 to the first Connection Server, having the public IP 52.48.144.190 Outbound TCP:443 to the second Connection Server, having the public IP 52.51.33.226 For the North American (US) WebConnect 3.0 service, the following communication needs to be allowed: Outbound HTTPS:443 to the Connection Manager (webconnect3us.netop.com), having the public IP 52.24.48.84 Outbound TCP:443 to the first Connection Server, having the public IP 52.41.220.110 Outbound TCP:443 to the second Connection Server, having the public IP 52.41.220.110

Posted - Thu, Nov 17, 2011 9:03 PM.

Online URL:

<https://kb.netop.com/article/firewall-and-proxy-server-considerations-when-using-netop-s-webconnect-webconnect-3>