

[Tech Tips and Best Practices](#) / Orchestrator and EdgeConnect TCP/IP Ports

# Orchestrator and EdgeConnect TCP/IP Ports

This page provides information about the default ports used by Orchestrator and EdgeConnect appliances.

[View PDF](#)

## Orchestrator as a Server – Outbound

Application	Protocol & Port
FTP <sup>1</sup>	TCP 21
SCP <sup>1</sup>	TCP
SSH	TCP 22
SMTP	TCP 25
TACACS+	TCP 49
HTTP	TCP 80
HTTPS <sup>2</sup>	TCP 443
SMTPS	TCP 465, 587
DNS	TCP/UDP 53
NTP	UDP 123
Audit Log <sup>3</sup>	UDP 514
Syslog <sup>3</sup>	UDP 514
RADIUS <sup>4</sup>	UDP 1812, 1813

- <sup>1</sup> FTP and SCP are optional and used as backups to customer-owned servers in the on-prem version of Orchestrator. You can always use the HTTPS port, as it is already allowed. This is not applicable to Orchestrator-as-a-service.
- <sup>2</sup> Orchestrator communicates with Cloud Portal over both HTTPS and WebSockets over TLS 1.2.
- <sup>3</sup> Audit log and Syslog ports are configurable.

- 4 These ports may differ. Verify the ports are the same as the server during configuration.

## Orchestrator as a Server – Inbound

Application	Protocol & Port
SSH	TCP 22
HTTP <sup>1</sup> (optional)	TCP 80
HTTPS <sup>1</sup>	TCP 443

- 1 Inbound HTTP/HTTPS connections can be restricted to authorized subnets only. EdgeConnect talks on these ports.

## Orchestrator as a Client

Application	Protocol & Port
HTTPS — Google Maps (optional) <sup>1</sup>	TCP 443
HTTPS — AWS (optional) <sup>2</sup>	TCP 443

- 1 Google Maps is used to populate topology view charts — additional firewall access may be required.
- 2 Access to AWS S3 is required for case creation and uploading files to Support. If you need to configure firewall access, you can allow outbound connections to \*.s3.amazonaws.com. Refer to [this page](#) for more information — the destination S3 bucket is in the us-east-1 region. If outbound access is prohibited, users can download files from Orchestrator and manually attach to new or existing cases.

## Appliance as a Server

Application	Protocol & Port
HTTPS	TCP 443

## Appliance as a Client

Application	Protocol & Port
TACACS+	TCP 49
HTTPS	TCP 443
HTTPS — AWS (optional) <sup>1</sup>	TCP 443

Application	Protocol & Port
DNS	TCP/UDP 53
NTP	UDP 123
SNMP	UDP 161
Syslog	UDP 514
RADIUS <sup>2</sup>	UDP 1812, 1813
IPFIX <sup>3</sup>	UDP 2055

- 1 Access to AWS S3 is required for case creation and uploading files to Support. If you need to configure firewall access, you can allow outbound connections to \*.s3.amazonaws.com. Refer to [this page](#) for more information — the destination S3 bucket is in the us-east-1 region. If outbound access is prohibited, users can download files to Orchestrator and upload/manage from there.
- 2 These ports may differ. Verify the ports are the same as the server during configuration.
- 3 The IPFIX port is configurable.

## Data Plane

Application <sup>1</sup>	Protocol & Port
GRE	IP PROTO 47
IPSEC	IP PROTO 50, UDP 500, UDP 4500
UDP	UDP 4163
IPSEC_UDP <sup>2</sup>	UDP 12000, UDP 12010

- 1 By default, IPSEC\_UDP will be used for all tunnels, other protocols only need to be allowed if they are configured.
- 2 These ports may differ. The port will be the same as what you set the default UDP port in the Orchestrator settings during configuration.

© Copyright 2023 Hewlett Packard Enterprise Development LP. The information contained herein is subject to change without notice. The only warranties for Hewlett Packard Enterprise products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. Hewlett Packard Enterprise shall not be liable for technical or editorial errors or omissions contained herein. Aruba Networks and the Aruba logo are registered trademarks of Aruba Networks, Inc. Third-party trademarks mentioned are the property of their respective owners. To view the end-user software agreement, go to [Aruba EULA](#).

Do Not Sell My Personal Information