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 [1]	TCP 21
SCP [1]	TCP
SSH	TCP 22
SMTP	TCP 25
TACACS+	TCP 49
HTTP	TCP 80
HTTPS [2]	TCP 443
SMTPS	TCP 465, 587
DNS	TCP/UDP 53
NTP	UDP 123
Audit Log [3]	UDP 514
Syslog [3]	UDP 514
RADIUS [4]	UDP 1812, 1813

1 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.

2 Orchestrator communicates with Cloud Portal over both HTTPS and WebSockets over TLS 1.2.

3 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 [1] (optional)	TCP 80
HTTPS [1]	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) [1]	TCP 443
HTTPS — AWS (optional) [2]	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) [1]	TCP 443

Application	Protocol & Port
DNS	TCP/UDP 53
NTP	UDP 123
SNMP	UDP 161
Syslog	UDP 514
RADIUS [2]	UDP 1812, 1813
IPFIX [3]	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 [1]	Protocol & Port
GRE	IP PROTO 47
IPSEC	IP PROTO 50, UDP 500, UDP 4500
UDP	UDP 4163
IPSEC_UDP [2]	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.