

# Ports used by Unimus

Please note all ports documented in this article are the **default ports** for their respective services.

All **outbound ports are configurable**, and depend on the configuration of the service Unimus connects to. **Inbound ports are also fully configurable**, with links to documentation provided below.

## Inbound

You should open the following ports inbound to your Unimus server:

Purpose	Protocol + Port
Web UI and API (default value - can be configured) <a href="#">Configuring server port or bind address</a>	TCP 8085
Core connection port - used for Remote Cores (default value - can be configured) configured in "/etc/unimus/unimus.properties" or "C:\ProgramData\Unimus\unimus.properties"	TCP 5509

## Outbound

Required outbound connections:

Purpose	Destination	Protocol + Port
Database connection - MySQL / MariaDB (only used if MySQL or MariaDB used as the database for Unimus)	Configured by user	TCP 3306
Database connection - PostgreSQL (only used if PostgreSQL used as the database for Unimus)	Configured by user	TCP 5432
Database connection - MSSQL (only used if MSSQL used as the database for Unimus)	Configured by user	TCP 1433
License validation (can be proxied - <a href="#">Running Unimus behind a HTTP(S) proxy</a> )	<a href="https://licensing.unimus.net">https://licensing.unimus.net</a>	TCP 443
Device communication SSH (default value - can be configured globally or per device)	Any device added to Unimus	TCP 22
Device communication Telnet (disabled by default) (default value - can be configured globally or per device)	Any device added to Unimus	TCP 23

Optional outbound connections - these will only be performed if the relevant feature is enabled:

Purpose	Destination	Protocol + Port
<b>Zones - zone proxy / local poller</b>		
Remote Core used as a Zone proxy / local poller (only used if using Zones with "Remote Core" connection method)	Configured by user	TCP 5509
NetXMS Agent used as a Zone proxy / local poller (only used if using Zones with "NetXMS Agent" connection method)	Configured by user	TCP 4701
<b>NMS Sync (importers)</b>		
NetXMS importer	Configured by user	TCP 4701
Zabbix importer	Configured by user	TCP 80 / TCP 443
Powercode importer	Configured by user	TCP 80 / TCP 443

PRTG importer	Configured by user	TCP 80 / TCP 443
Observium importer	Configured by user	TCP 80 / TCP 443
Panopta importer	<a href="https://aggregator2.panopta.com">https://aggregator2.panopta.com</a>	TCP 443
LibreNMS importer	Configured by user	TCP 80 / TCP 443
<b>Network Scan</b>		
Network Scan - ICMP (even if ICMP does not respond, network scan will scan SSH / Telnet if enabled)	Any Network Scan destinations	ICMP
Network Scan - SSH (Network Scan uses the default SSH connector settings)	Any Network Scan destinations	TCP 22
Network Scan - Telnet (disabled by default) (Network Scan uses the default Telnet connector settings)	Any Network Scan destinations	TCP 23
<b>Notifications</b>		
Email notification sender	Configured by user	TCP 25
Pushover notification sender	<a href="https://api.pushover.net">https://api.pushover.net</a>	TCP 443
Slack notification sender	<a href="https://slack.com">https://slack.com</a>	TCP 443
<b>External AAA</b>		
Radius - authentication and authorization	Configured by user	UDP 1812
Radius - accounting	Configured by user	UDP 1813
LDAP - authentication and authorization	Configured by user	TCP 389