

GETTING STARTED

Windows Firewall and ports

Which ports MergenHub uses, the rules the installer adds, how to open or restrict them.

Online: mergenhub.envest.com.tr/docs/firewall

ON THIS PAGE

- Ports MergenHub uses
- Rules the installer creates
- Opening or changing ports manually
- Restricting who may connect
- Third-party firewalls and antivirus
- Verifying
- Troubleshooting

MergenHub listens on two TCP ports by default and the installer opens them in Windows Firewall. This page lists every port, the rules the installer creates, and how to open, restrict or remove them by hand.

Ports MergenHub uses

PORT	DIRECTION	PURPOSE	CHANGE IN
8090 TCP	inbound	Web UI, REST API, Data Bridge REST server, MCP endpoint	Installer › <i>Server address and ports</i> ; Settings › <i>Web & REST API</i>
443 TCP	inbound	HTTPS for the same services (only when HTTPS is enabled)	Installer › <i>HTTPS</i> ; Settings › <i>Web & REST API</i>
48010 TCP	inbound	OPC UA server (<code>opc.tcp://host:48010/MergenHub</code>)	Settings › <i>OPC UA Server</i> › <i>Endpoints</i>
device ports	outbound	Modbus 502, S7 102, OMRON 9600 (FINS) / 44818 (CIP), DNP3 20000, IEC 104 2404, IEC 61850 102, MQTT 1883/8883, OPC UA client to remote servers	per channel/device
25 / 465 / 587	outbound	SMTP for e-mail notifications	Settings › <i>E-mail</i>
443	outbound	SMS provider API, license portal (activation, refresh, update check)	—

Outbound connections are normally allowed by Windows Firewall; only the inbound ports need rules.

Rules the installer creates

The installer runs `netsh advfirewall` and adds these inbound *allow* rules (all profiles, TCP):

RULE NAME	PORT
MergenHub Web	the web port you chose (8090)

RULE NAME	PORT
MergenHub OPC UA	the OPC UA port (48010)
MergenHub HTTPS	the HTTPS port (only when HTTPS was enabled)

They are removed again by the uninstaller. You can see them in *Windows Defender Firewall with Advanced Security* › *Inbound Rules*.

Opening or changing ports manually

Run in an **administrator** command prompt:

```
netsh advfirewall firewall add rule name="MergenHub Web" dir=in action=allow protocol=TCP
localport=8090
netsh advfirewall firewall add rule name="MergenHub OPC UA" dir=in action=allow protocol=TCP
localport=48010
netsh advfirewall firewall add rule name="MergenHub HTTPS" dir=in action=allow protocol=TCP
localport=443
```

PowerShell equivalent:

```
New-NetFirewallRule -DisplayName "MergenHub Web" -Direction Inbound -Protocol TCP -LocalPort 8090
-Action Allow
```

If you changed a port in *Settings*, add a rule for the new port and delete the old one:

```
netsh advfirewall firewall delete rule name="MergenHub Web"
```

Restricting who may connect

Limit a rule to specific networks instead of the whole world:

```
netsh advfirewall firewall set rule name="MergenHub OPC UA" new
remoteip=10.0.0.0/24,192.168.10.0/24
netsh advfirewall firewall set rule name="MergenHub Web" new profile=domain,private
```

For internet-facing servers prefer a reverse proxy on 443 and keep 8090 bound to `127.0.0.1` (set the host to `127.0.0.1` in *Settings* › *Web & REST API*). See [Publishing on a domain](#).

Third-party firewalls and antivirus

- Endpoint security suites (Kaspersky, ESET, Sophos ...) have their own firewall; add the same TCP ports there.
- Some products flag the unsigned installer. Right-click the file › *Properties* › *Unblock*, or add an exclusion for `C:\Program Files\MergenHub`.
- On corporate PCs with AppLocker / WDAC the installer may be blocked entirely; ask the administrator to allow the publisher or the path.

Verifying

- From another machine: `Test-NetConnection <host> -Port 8090` (PowerShell) — *TcpTestSucceeded: True* means the port is open.
- On the server: `netstat -ano | findstr :8090` shows the listening socket and the process ID of the `MergenHub` service.
- The *Event log* (... › Event Log) shows `Web API listening on ...` and `OPC UA server started` lines when the services are up.

Troubleshooting

SYMPTOM	LIKELY CAUSE
Web UI works on the server but not from other PCs	Host set to <code>localhost</code> — change it to <code>0.0.0.0</code> in <i>Settings › Web & REST API</i> and restart the service; or the firewall rule is missing
OPC UA client sees the endpoint but cannot connect	Endpoint host name differs from what the client uses; certificate not trusted; security policy mismatch
Browser says "connection reset" on HTTPS	HTTPS enabled but no valid <code>web.pfx</code> in <code>webpki\</code> ; check the event log
Port already in use	Another program (often another OPC server) uses 48010 or 8090; change the port in <i>Settings</i>