

---

# Ports Guide

---

# 1. Why ports need to be opened and how to check if they are?

A port is a virtual point through which programs running on different computers exchange data.

Ports need to be open to allow this data exchange.

Microsoft's PortQryUI displays the status of ports on a computer, and can be installed and run on the machine in which ADAudit Plus is installed.

PortQryUI download link: <https://www.microsoft.com/en-in/download/details.aspx?id=24009>

## 2. Product ports

The table below lists the default ports used by ADAudit Plus. These ports can be changed during or after installation.

**Note:** To change port: Open the ADAudit Plus console → Admin tab, which can be found in the top panel → Connection tab, which can be found in the left panel → Change port.

Port	Protocol	Purpose
8081	HTTP	Product web server
8443	HTTPS	Product web server
33307	TCP	Database port

## 3. System ports

The table below lists the ports that should be opened, on the destination computers. These ports can be opened on Windows/third-party firewalls.

Port	Protocol	Destination	Service	Purpose	Direction
135	TCP	Monitored computers	RPC	For Windows log collection	Outbound
137	TCP and UDP	Monitored computers	NetBIOS name resolution RPC/named pipes (NP)	For Windows log collection	Outbound

138	UDP	Monitored computers	NetBIOS datagram	For Windows log collection	Outbound
139	TCP	Monitored computers	NetBIOS session RPC/NP	For Windows log collection	Outbound
445	TCP and UDP	Monitored computers	SMB RPC/NP	For Windows log collection, file share audit	Outbound
389	TCP and UDP	Domain Controllers	LDAP	For syncing AD objects with product	Outbound
636	TCP	Domain Controllers	LDAP over SSL	For syncing AD objects with product	Outbound
3268	TCP	Domain Controllers	Global catalog	For syncing AD objects with product	Outbound
3269	TCP	Domain Controllers	Global catalog over SSL	For syncing AD objects with product	Outbound
88	TCP	Domain Controllers	Kerberos	For authentication when accessing a domain resource	Outbound
25	TCP	SMTP servers	SMTP	To send emails	Outbound
465	TCP	SMTP servers	SSL	To send emails	Outbound
587	TCP	SMTP servers	TLS	To send emails	Outbound
49152-65535*	TCP	Monitored computers	RPC randomly allocated high TCP ports	For Windows log collection	Outbound

**\*Note:**

If you are using Windows Firewall you can open dynamic ports, 49152-65535, on the monitored computers by enabling the outbound rules listed below.

- Remote Event Log Management (NP-In)
- Remote Event Log Management (RPC)
- Remote Event Log Management (RPC-EPMAP)

To enable the above rules: Open Windows Firewall → Advanced settings → Inbound Rules → Right click on respective rule → Enable Rule.

ManageEngine  
**ADAudit Plus**

ADAudit Plus' real-time alerting console instantly notifies admins of every critical event; alerts are sent straight to admins' inboxes or phones. With ADAudit Plus, admins can keep a close watch on domain users' behavior, and detect compromised credentials, lateral movement, and other malicious behavior on the spot.

\$ Get Quote

⬇ Download