



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	Direction	Service	Purpose
135	TCP	Inbound	RPC	For Windows log collection Source: ADAudit Plus server Destination: Monitored computers
137	TCP and UDP	Inbound	NetBIOS name resolution RPC/named pipes (NP)	For Windows log collection Source: ADAudit Plus server Destination: Monitored computers

138	UDP	Inbound	NetBIOS datagram	For Windows log collection Source: ADAudit Plus server Destination: Monitored computers
139	TCP	Inbound	NetBIOS session RPC/NP	For Windows log collection Source: ADAudit Plus server Destination: Monitored computers
445	TCP and UDP	Inbound	SMB RPC/NP	For Windows log collection, file share audit Source: ADAudit Plus server Destination: Monitored computers
389	TCP and UDP	Inbound	LDAP	For syncing AD objects with product Source: ADAudit Plus server Destination: Domain Controllers
636	TCP	Inbound	LDAP over SSL	For syncing AD objects with product Source: ADAudit Plus server Destination: Domain Controllers
3268	TCP	Inbound	Global catalog	For syncing AD objects with product Source: ADAudit Plus server Destination: Domain Controllers
3269	TCP	Inbound	Global catalog over SSL	For syncing AD objects with product Source: ADAudit Plus server Destination: Domain Controllers
88	TCP	Inbound	Kerberos	For authentication when accessing a domain resource Source: ADAudit Plus server Destination: Domain Controllers
25	TCP	Inbound	SMTP	To send emails Source: ADAudit Plus server Destination: SMTP servers

465	TCP	Inbound	SSL	To send emails Source: ADAudit Plus server Destination: SMTP servers
587	TCP	Inbound	TLS	To send emails Source: ADAudit Plus server Destination: SMTP servers
49152-65535	TCP	Inbound	RPC randomly allocated high TCP ports	For Windows log collection Source: ADAudit Plus server Destination: Monitored computers

***Note:**

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

In case you are deploying agents, please refer to the [Agent guide](#) and open the corresponding ports.

Our Products

AD360 | Log360 | ADManager Plus | ADSelfService Plus | DataSecurity Plus | M365 Manager Plus



'ManageEngine ADAudit Plus is a real-time change auditing and user behavior analytics solution that helps keep your Active Directory, Azure AD, Windows servers, and workstations secure and compliant.

\$ Get Quote

Download