ManageEngine
Log360

Configuring ports

www.manageengine.com/log-management/

The document below outlines the Log360 prerequisites and how to configure them through Group Policy (GPO) settings

Prerequisites

Before starting Log360 in your environment, ensure that the ports are configured accordingly.

Log360

Ports	Protocol	Usage	Description
8095	HTTP	Web server	Default HTTP web server port used by Log360
8458	HTTPS	Web server	Default HTTPS web server port used by Log360
80	HTTP	Context-based reverse proxy	Default HTTP port used when context-based reverse proxy is enabled
443	HTTPS	Context-based reverse proxy	Default HTTPS port used when context-based reverse proxy is enabled
9001 - 9008	HTTP	Port-based reverse proxy	Default port series used when port-based reverse proxy is enabled
33395	TCP	PostgreSQL database	Used for connecting to the PostgreSQL database in Log360
9322, 9200	HTTP	Elasticsearch	Used by Elasticsearch, which is used as log storage by Eventlog Analyzer
389 (UDP), 636 (TCP)	UDP and TCP	AD sync/LDAP SSL-enabled	If the specified ports are occupied, any port from the 9300-9400 series will be taken
25, 587	SMTP	Mail server configuration	Used in AD sync to connect to Active Directory

Ports to be configured in your firewall

Allow outbound connections to ports on the source server and inbound connections to ports on the destination server.

Ports	Protocol	Direction	Source	Destination	Purpose
8400, 8445, 80, 443	HTTP and HTTPS	Inbound	Source where the web client is accessed	Log360 server	Used to connect to Log360 web client
389(UDP), 636(TCP)	TCP and UDP	Inbound	Log360 server	Domain controller	Used in AD sync to connect to Active Directory
25, 587	SMTP	Inbound	Log360 server	Mail server	Used to connect to the mail server

Ports required if the Microsoft SQL Database has to be configured as a backend database

Allow outbound connections to ports on the source server and inbound connections to ports on the destination servers

Ports	Protocol	Direction	Source	Destination	Purpose
1434	UDP	Inbound	Log360 server	Microsoft SQL-hosted server	Used to connect to the SQL browser service for browsing SQL server instances
1433	TCP	Inbound	Log360 server	Microsoft SQL-hosted server	Used to connect to the Microsoft SQL database Can change the port while configuring if needed

EventLog Analyzer.

Basic requirements

Ports	Description
8400	Default HTTP web server port used by EventLog Analyzer Used for communication between the remote agent and EventLog Analyzer server
8445	Default HTTPS web server port used by EventLog Analyzer
9300-9400	Used by Elasticsearch server for log data storage
33335	Used for connecting to the default PostgreSQL database
135, 139, 445	Ports required for WMI log collection
513, 514 (UDP), 514 (TCP), 513 (TLS)	Used for syslog log collection
5000, 5001, 5002	UDP ports used internally for agent-to-server communication

Windows Domain Discovery				
Port	**Inbound**	**Outbound**	**Service**	**Additional rights and permissions**
TCP/389	Domain controller	EventLog Analyzer server	LDAP	**User permissions:** • User should have read permission to Active Directory Domain Objects • Permission to run LDAP query in ADS_ SECURE_ AUTHENTICATION mode should be present

Windows agent installation from EventLog Analyzer				
Port	**Inbound**	**Outbound**	**Service**	**Additional rights and permissions**
TCP/135	EventLog Analyzer agent machine	EventLog Analyzer server	RPC	**User permissions:** • Read, write, and modify permissions to files in **\\<ipaddress>\Admin$\TEMP\ EventLogAgent should be enabled** • Access to the Remote Registry service
TCP/139	EventLog Analyzer agent machine	EventLog Analyzer server	RPC	
TCP/445	EventLog Analyzer agent machine	EventLog Analyzer server	SMB RPC/ NP	
Dynamic ranges of RPC ports: TCP/1024 to 65535	EventLog Analyzer agent machine	EventLog Analyzer server	RPC randomly allocated high TCP ports	

Windows agent management and communication				
Port	**Inbound**	**Outbound**	**Service**	**Additional rights and permissions**
TCP/135	EventLog Analyzer agent machine	EventLog Analyzer server	RPC	**User permissions:** • At least read control should be granted for winreg registry key. (Computer \HKEY_LOCAL _MACHINE\ SYSTEM\ CurrentContro lSet\Control\ SecurePipe Servers\ winreg). • Access/Read /Write registry keys - SOFTWARE\\ Wow6432Node \\ ZOHO Corp\\EventLog Analyzer\\ (or) SOFTWARE \\ZOHO Corp \\ EventLog Analyzer\\. There should be access to remote services.msc **User permissions:** • Port 8400 should be open in both the agent machine and the server machine
TCP/1024 - 65535	EventLog Analyzer agent machine	EventLog Analyzer server	RPC randomly allocated high TCP ports	
HTTP/8400 (configurable)	EventLog Analyzer server	EventLog Analyzer agent machine	HTTP/ HTTPS	

Linux agent installation				
Port	**Inbound**	**Outbound**	**Service**	**Additional rights and permissions**
TCP/22	EventLog Analyzer agent machine	EventLog Analyzer server	SSH	**Sudo user permissions:** • rwx permission should be enabled for /opt/ManageEngine/ for transferring files Permissions for SSH communication

Linux agent management and communication			
Port	**Inbound**	**Outbound**	**Additional rights and permissions**
TCP/22	EventLog Analyzer agent machine	EventLog Analyzer server	**User permissions:** • SFTP permissions should be enabled to transfer files to /opt/Manage Engine/ EventL ogAnalyzer_ Agent and /etc / audisp/plugins.d • Service start /stop/restart permission for audit should be enabled • Permissions for SSH communication
HTTP/8400 (configurable)	EventLog Analyzer server	EventLog Analyzer agent machine	

Notifications					
Block	**Port**	**Inbound**	**Outbound**	**Service**	**Additional rights and permissions**
Windows pop-ups	TCP/135	Audited Windows device	EventLog Analyzer server	RPC	**UserGroups:** Distributed COM users **User permissions:** For root\cim v2 In WMI Properties: • Execute methods • Enable account • Remote enable • Read recurity **Environment permission:** "AllowRemoteRPC" should be 1 for HKEY_ LOCAL_MACHINE\ SYSTEM\Current ControlSet\ Control\ Terminal Server
	RPC ports - TCP/1024 to 65535	Audited Windows device	EventLog Analyzer server	RPC randomly allocated high TCP ports	

Linux pop-up	TCP/ specified port	Audited Linux device	EventLog Analyzer server	-	**Environment permission:** *Sudo permission for user
Send email Windows and LinuxINUX	TCP/port mentioned while configuring using SMTP server	Audited Windows/ Linux device	EventLog Analyzer server	-	**Environment permission:** SMTP server should be configured in the EventLog Analyzer server
Send SMS Windows and Linux	-	-	-	-	**Environment permission:** SMS server should be configured in the product
Send SNMP trap Windows and Linux	UDP/port specified in workflow block	Audited Windows/ Linux device	EventLog Analyzer server	-	**Environment permission:** The port mentioned in the workflow configuration should be open

ADAudit Plus

Server ports

Ports	Purpose	Ports
8081	HTTP	Product web server
8444	HTTPS	Product web server
33307	TCP	Database port
29118	TCP	DataEngine port

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.

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

138	UDP	Inbound	ADAudit Plus server	Monitored computers	NetBIOS datagram	For Windows log collection
139	TCP	Inbound	ADAudit Plus server	Monitored computers	NetBIOS session RPC/NP	For Windows log collection
445	TCP and UDP	Inbound	ADAudit Plus server	Monitored computers	SMB RPC/ NP	For Windows log collection
389	TCP and UDP	Inbound	ADAudit Plus server	Domain controllers	LDAP	For syncing AD objects with the product Ssurce: ADAudit Plus server destination: Domain controllers
636	TCP	Inbound	ADAudit Plus server	Domain controllers	LDAP over SSL	For syncing AD objects with the product
3268	TCP	Inbound	ADAudit Plus server	Domain controllers	Global catalog	For syncing AD objects with the product
3269	TCP	Inbound	ADAudit Plus server	Domain controllers	Global catalog over SSL	For syncing AD objects with the product
88	TCP	Inbound	ADAudit Plus server	Domain controllers	Kerberos	For authentication when accessing a domain resource
25	TCP	Inbound	ADAudit Plus server	SMTP servers	SMTP	To send emails
465	TCP	Inbound	ADAudit Plus server	SMTP servers	SSL	To send emails
587	TCP	Inbound	ADAudit Plus server	SMTP servers	TLS	To send emails
49152-65535 *	TCP	Inbound	ADAudit Plus server	Monitored computers	RPC randomly allocated high TCP ports	For Windows log collection

Agent Ports:

Agent-to-server communication					
Port	**Protocol**	**Direction**	**Source**	**Destination**	**Purpose**
8555	HTTPS	Outbound	ADAudit Plus server	Monitored computers	1. Sending audit data from agent to server 2. Syncing agent running status with server 3. Pulling all configurations periodically (every 60 minutes) from the server

Server-to-agent communication					
Port	**Protocol**	**Direction**	**Source**	**Destination**	**Purpose**
Dynamic ports (49152-65535) and 135	RPC	Inbound	ADAudit Plus server	Monitored computers	1. Automatically installing, uninstalling, and upgrading the agent via the product. 2. Syncing server configuration with the agent when the agent has not communicated with the server for more than two hours. Communication between the agent and server is checked once every 30 minutes. 3. Immediately notifying the agent of the following actions: global exclude configuration changes, event collection schedule time and run-now changes, product port and protocol changes, enable/disable of servers, and more. **Note:** Agent synchronizes server configurations by HTTPS communication; if HTTPS fails then the server attempts to sync all configurations with agent via RPC.

Log360 UEBA

Ports	Purpose	Description
8096	HTTP	Default HTTP web server port used by Log360 UEBA
8446	HTTPS	Default HTTPS web server port used by Log360 UEBA
33337	HTTP	Used for connecting to the default PostgreSQL database
9230-9290	HTTP	HTTP port used by Elasticsearch
9330-9400	HTTP	TCP ports used by Elasticsearch
8179-8189	TCP	Ports used for Redis server

ADManager Plus:

Server ports

Port number	Protocol	Purpose
8080/8443	HTTP/HTTPS	Necessary to connect to the Tomcat web server
33306	TCP	To connect to the product database
9280	HTTP	To connect to the Elasticsearch database
9380	TCP	For communication between nodes in a cluster

System ports

Allow outbound connections to ports on the source server (the ADManager Plus server) and inbound connections to ports on the target servers (i.e. domain controllers).

Ports	Proto-col	Direc-tion	Source	Destina-tion	Port type	Service	Purpose
389/636	TCP and UDP	In-bound	ADMan-ager Plus server	Domain controllers	Static	LDAP	To connect to Active Directory

135	TCP	In-bound	ADMan-ager Plus server	Domain controllers	Static	RPC	For data exchange
445	TCP and UDP	In-bound	ADMan-ager Plus server	Domain controllers	Static	SMB	To get access to hared file systems
88	TCP	In-bound	ADMan-ager Plus server	Domain controllers	Static	Kerberos	For authentication when accessing a domain resource
139	TCP	In-bound	ADMan-ager Plus server	Domain controllers	Static	NetBIOS session	Required for communicat-ing within the network
3268/ 3269	TCP	In-bound	ADMan-ager Plus server	Domain controllers	Static	Global catalog	Necessary for performing search operations in the global catalog
25	SMTP	In-bound	ADMan-ager Plus server	SMTP server	Static	SMTP	To send emails
80	HTTP	In-bound	ADMan-ager Plus server	Domain controllers	Static	Ex-change	For connecting to Exchange servers
80, 443	HTTP/ HTTPS	In-bound	ADMan-ager Plus server	Microsoft 365 or Google Workspace servers	Static	Mic-rosoft 365 and Google Work-space	Required for communicat-ing with Micro-soft 365 and Google Work-space plat-forms
49152-65535	TCP	In-bound	ADMan-ager Plus server	RPC randomly allocated high TCP ports	Dynam-ic	RPC	Used to establish data exchange
8080/ 80443	HTTP/ HTTPS	In-bound	ADMan-ager Plus server	Azure end-points	Static	Azure end-points	The Backup and Recovery add-on requires hese ports

DataSecurity Plus

Server ports

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

Port	Protocol	Purpose
8800	HTTP	Product web server/agent communication
9163	HTTPS	Product web server/agent communication

System ports

The table below lists the ports on the destination computers that DataSecurity Plus uses. These ports can be opened on Windows or third-party firewalls.

Ports	Proto-col	Direction	Source	Destination	Service	Purpose
135	TCP	Outbound	DSP server	Monitored computers	RPC	Agent communication
137	TCP and UDP	Outbound	DSP server	Monitored computers	RPC	Agent communication
138	UDP	Outbound	DSP server	Monitored computers	RPC	Agent communication
139	TCP	Outbound	DSP server	Monitored computers	RPC	Agent communication
445	TCP and UDP	Outbound	DSP server	Monitored computers	RPC	For listing file shares
389	TCP and UDP	Outbound	DSP server	Domain controllers	LDAP	For syncing AD objects with DataSecurity Plus
636	TCP	Outbound	DSP server	Domain controllers	LDAP over SSL	For syncing AD objects with DataSecurity Plus
3268	TCP	Outbound	DSP server	Domain controllers	Global catalog	For syncing AD objects with DataSecurity Plus
3269	TCP	Outbound	DSP server	Domain controllers	Global catalog over SSL	For syncing AD objects with DataSecurity Plus
88	TCP	Outbound	DSP server	Domain controllers	Kerberos	For syncing AD objects with DataSecurity Plus

25	TCP	Outbound	DSP server	SMTP servers	SMTP	To send emails
465	TCP	Outbound	SMTP servers	SMTP servers	SSL	To send emails
587	TCP	Outbound	SMTP servers	SMTP servers	TLS	To send emails
49152 - 65535	TCP	Outbound	Monitored computers	Monitored computers	RPC randomly allocated high TCP ports	For agent communication and cluster configuration

Note:

1. Remote registry services must be running on all machines that have the DataSecurity Plus agent installed to monitor the agent status.
2. If you're using Windows Firewall, you can open dynamic ports 49152 to 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 the respective **rules**, and select **Enable Rule**.

Cloud Security Plus:

Server ports

Port	Protocol	Description
8055	HTTP	Default port used for Cloud Security Plus access using HTTP
8056	HTTPS	Default port used for Cloud Security Plus access using HTTP
33355	HTTP	Used for connecting to the default PostgreSQL database

Ports to be configured

Ports	Proto-col	Direction	Source	Destination	Description
25	TCP	Inbound	Cloud Security Plus server	SMTP server	Port used for SMTP mail configuration
587	TCP	Inbound	Cloud Security Plus server	SMTP server	TLS port used for SMTP mail configuration
465	TCP	Inbound	Cloud Security Plus server	SMTP server	SSL port used for SMTP mail configuration
1470	TCP	Inbound	Cloud Security Plus server	Target machine	TCP (syslog) used for log forwarder feature
513,514	UDP	Inbound	Cloud Security Plus server	Target machine	UDP (syslog) used for log forwarder feature

Exchange Reporter Plus

Server ports

Port	Protocol	Description
8181	HTTP	Default HTTP port used for Exchange Reports Plus access
8887	HTTPS	Default HTTPS port used for Exchange Reports Plus access
33309	HTTP	Used for connecting to the default PostgreSQL database

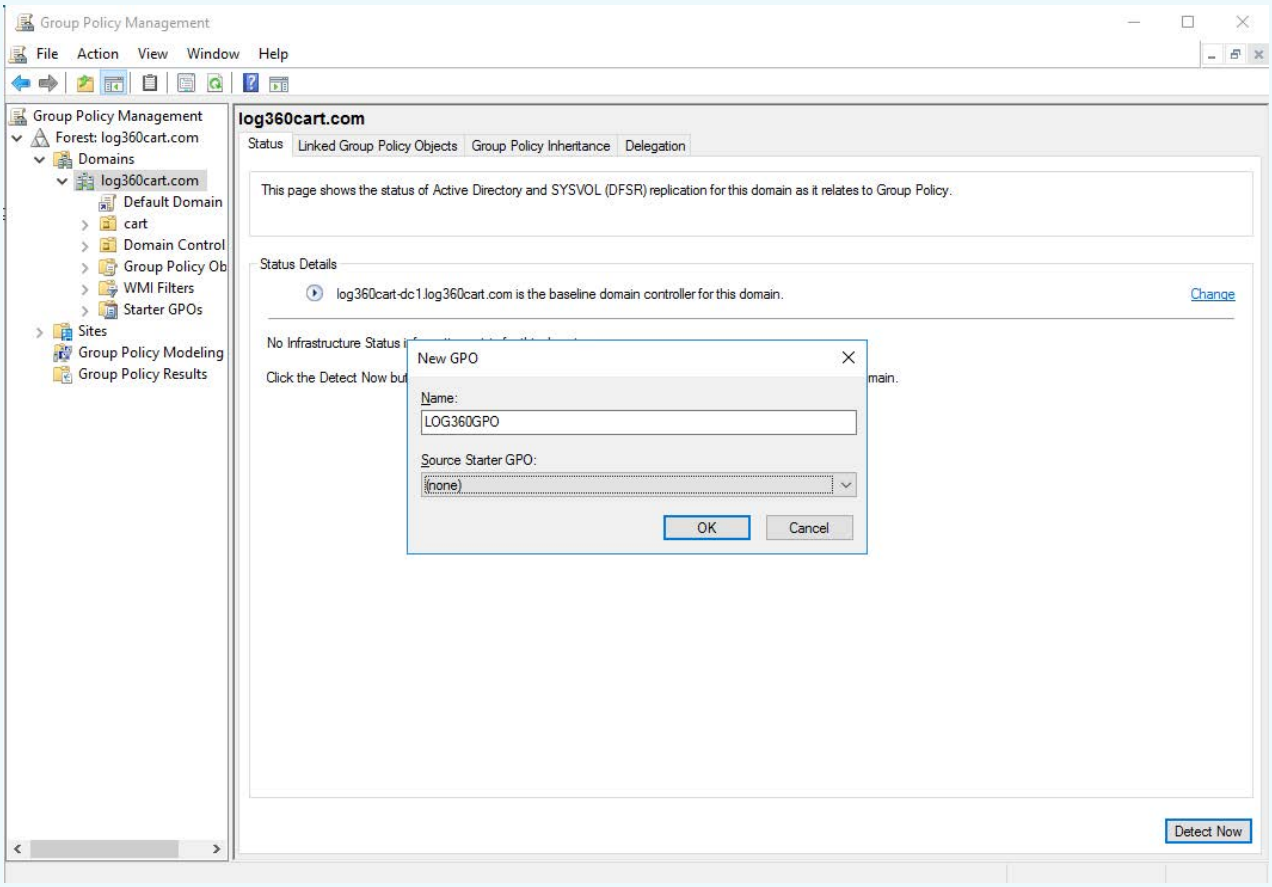
M365 Manager Plus

Server ports

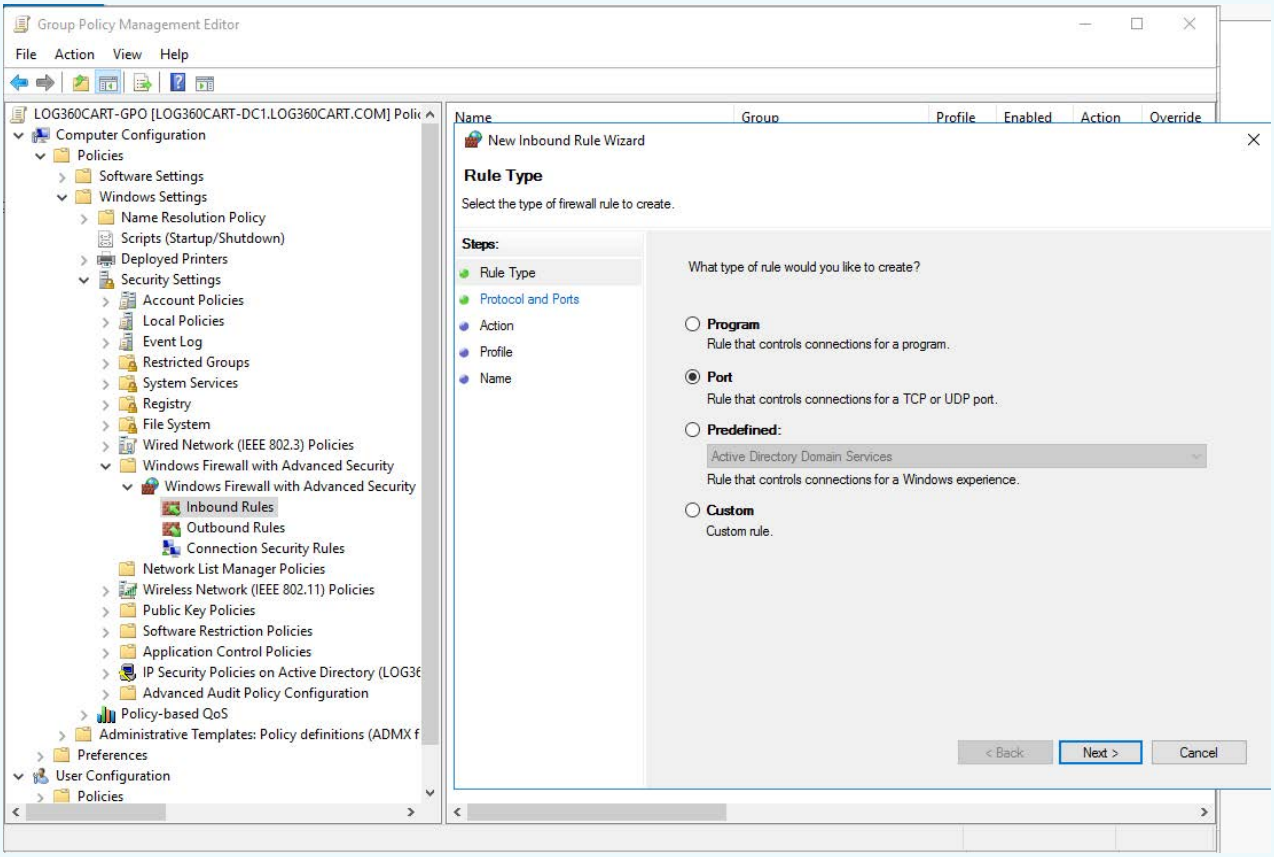
Port	Protocol	Description
8365	HTTP	Default HTTP port used for M365 Manager Plus access

9365	HTTPS	Default HTTPS port used for M365 Manager Plus access
33365	HTTP	Used for connecting to the default PostgreSQL database

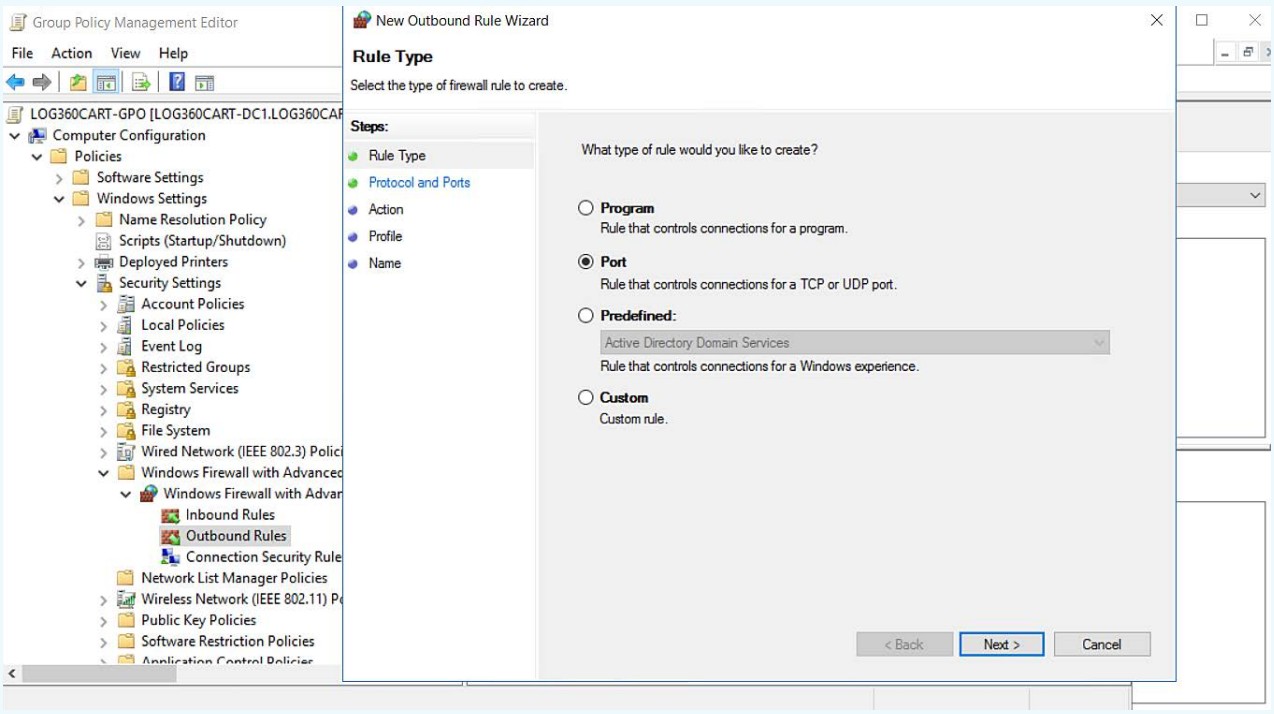
Steps to push port configuration in bulk through a GPO



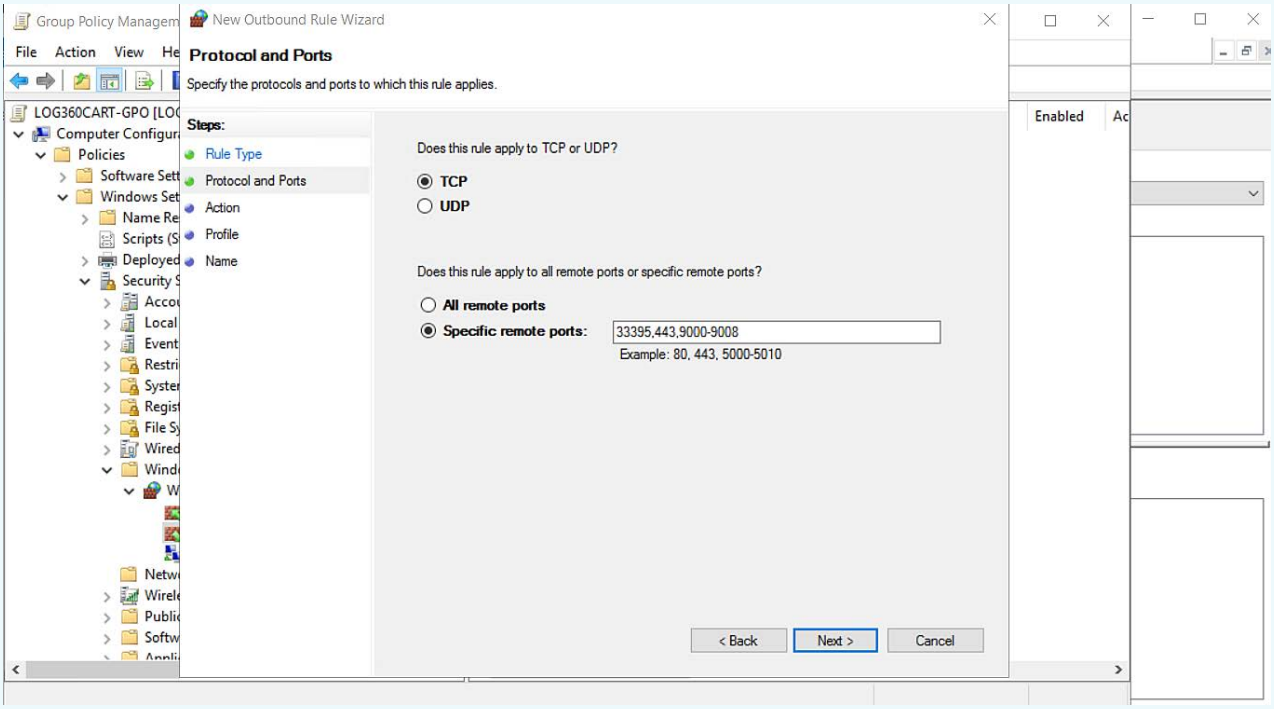
1. Open the **Run** command in the domain controller and type **gpmc.msc** to open the Group Policy Management Console.
2. Right-click the **domain > Create a GPO in this domain and link it here.**
3. Enter a **name** and click **OK.**



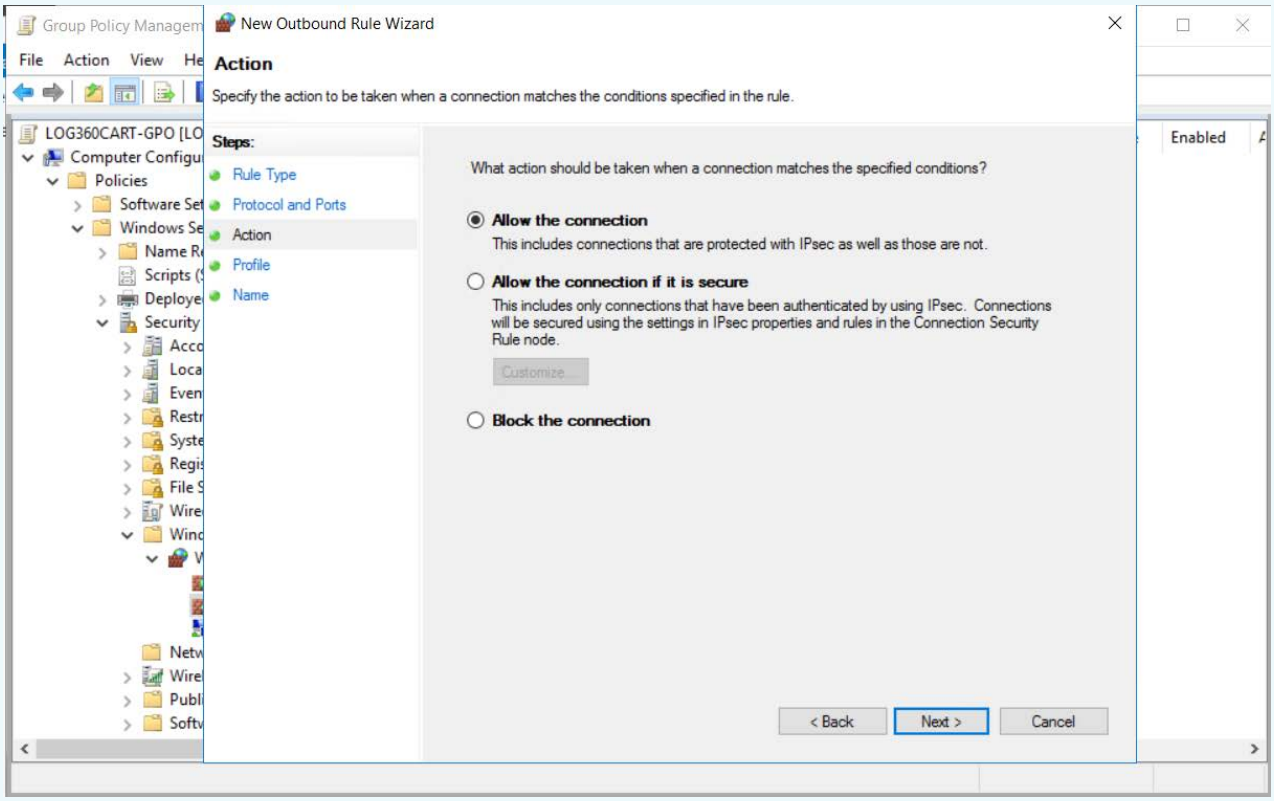
4. Right-click the created **GPO > Edit.**



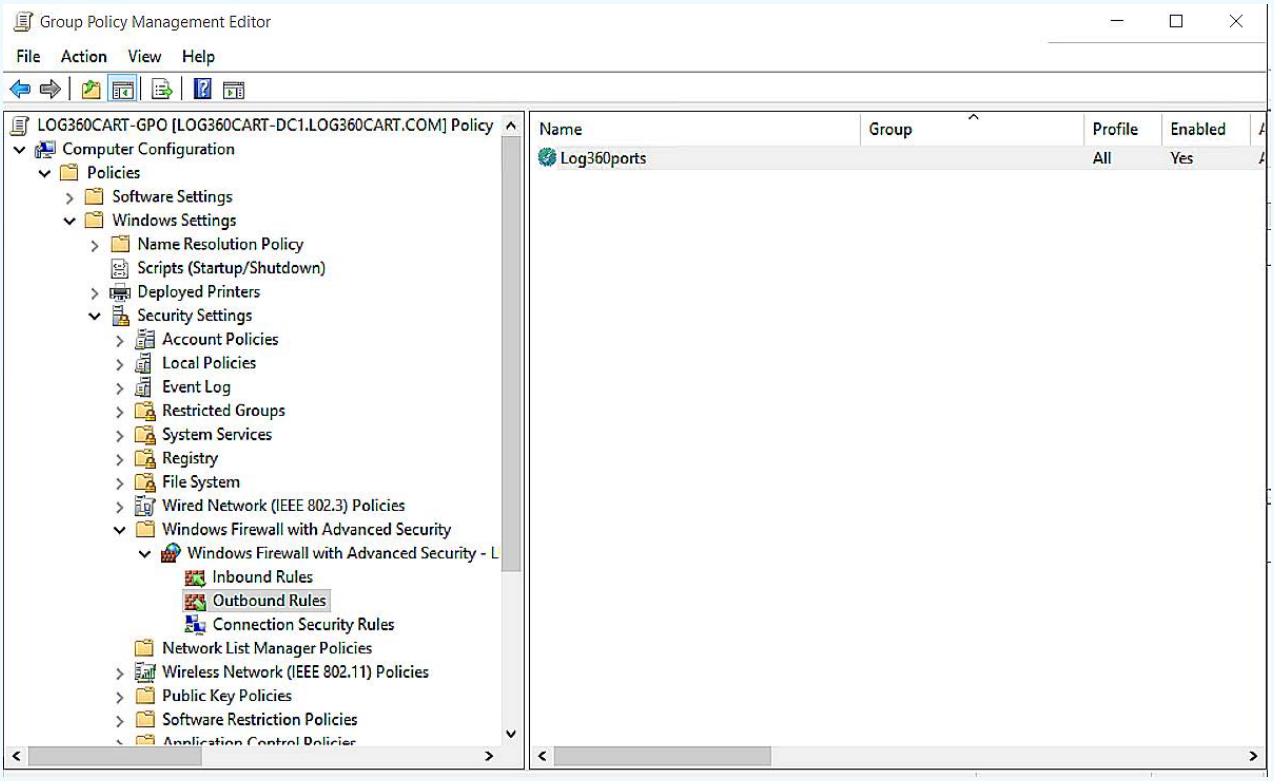
5. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Windows**



Firewall with Advanced Security > Windows Firewall with Advanced Security > Inbound Rules.

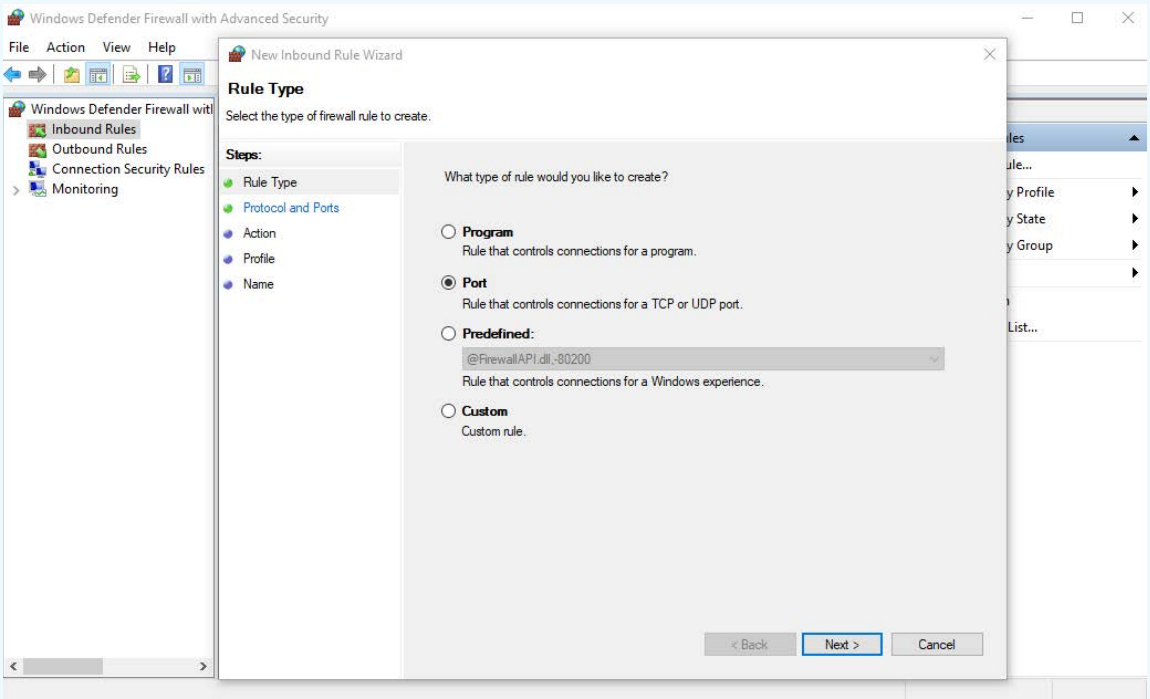


6. Right-click **Inbound Rules** and select **New Rule.**

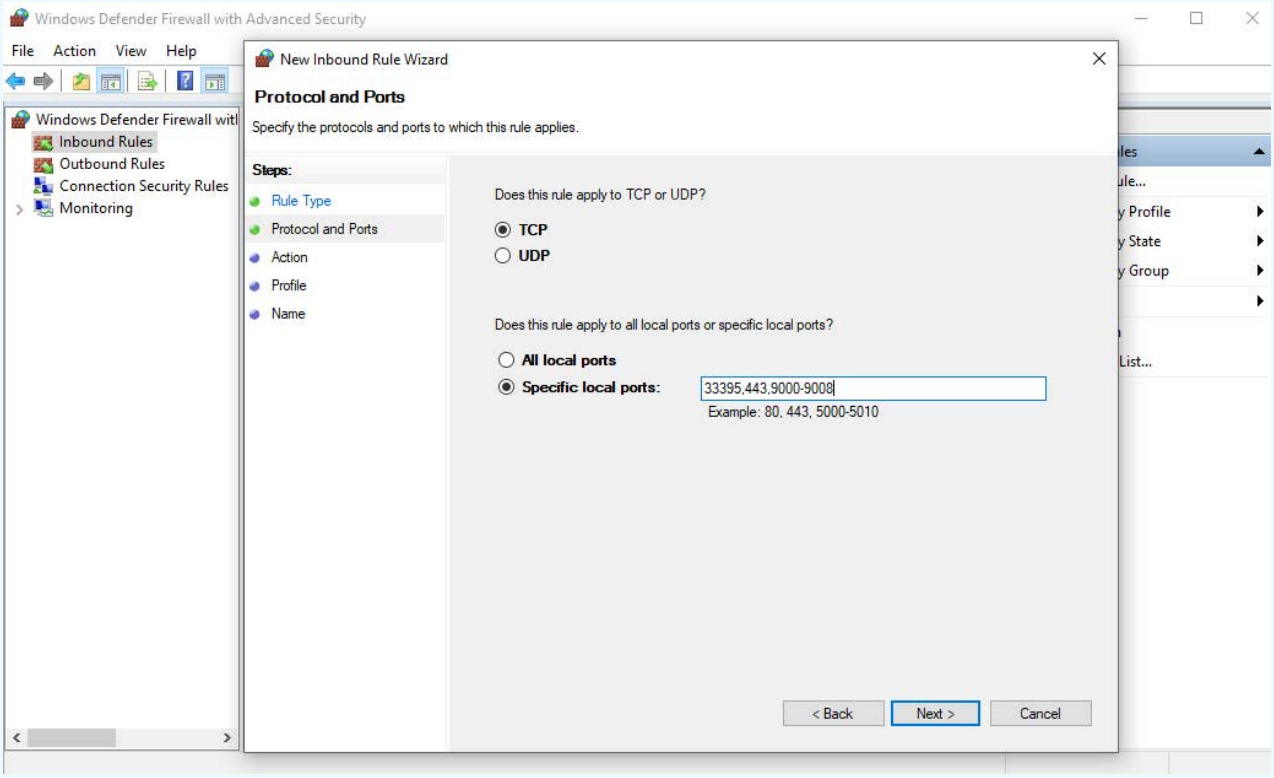


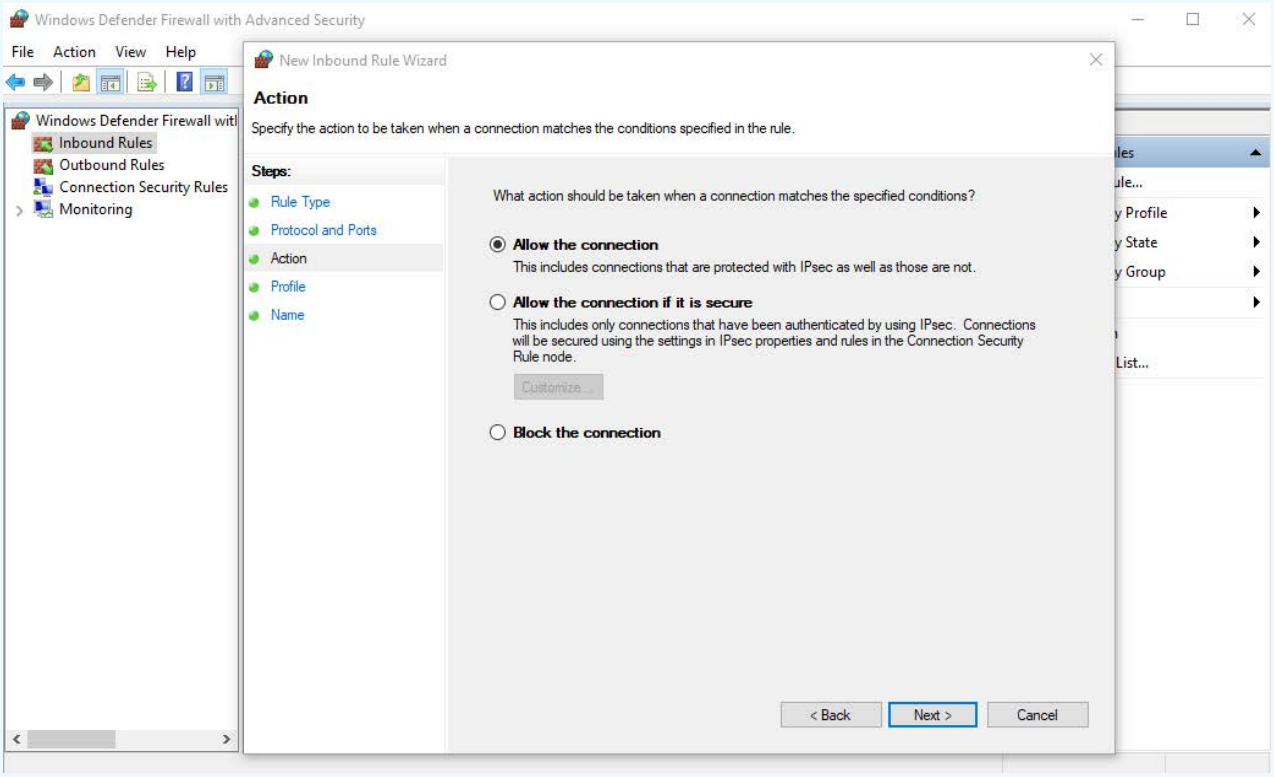
7. Select **Port** and click **Next.**

8. Enter the required ports.
9. Select **Allow the connection.**
10. Save the profile.

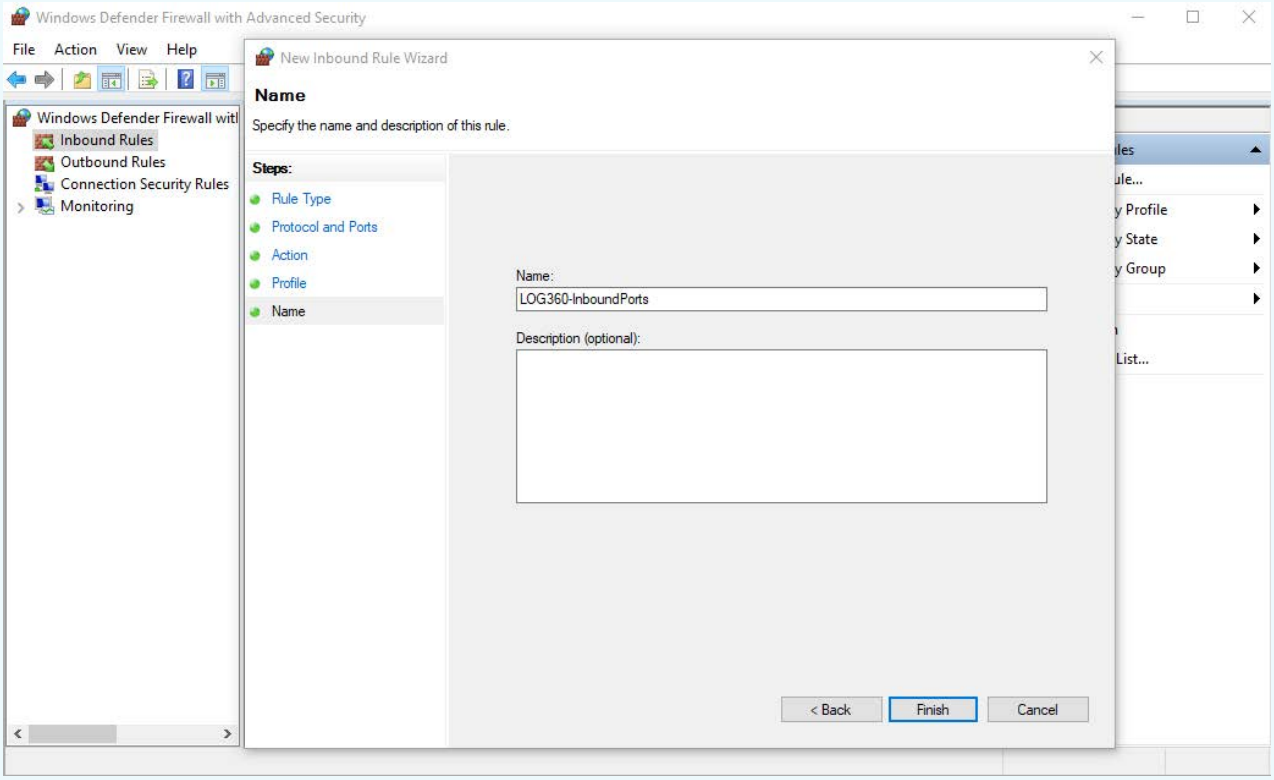


11. Execute the **gpupdate /force** command for the changes to take effect.

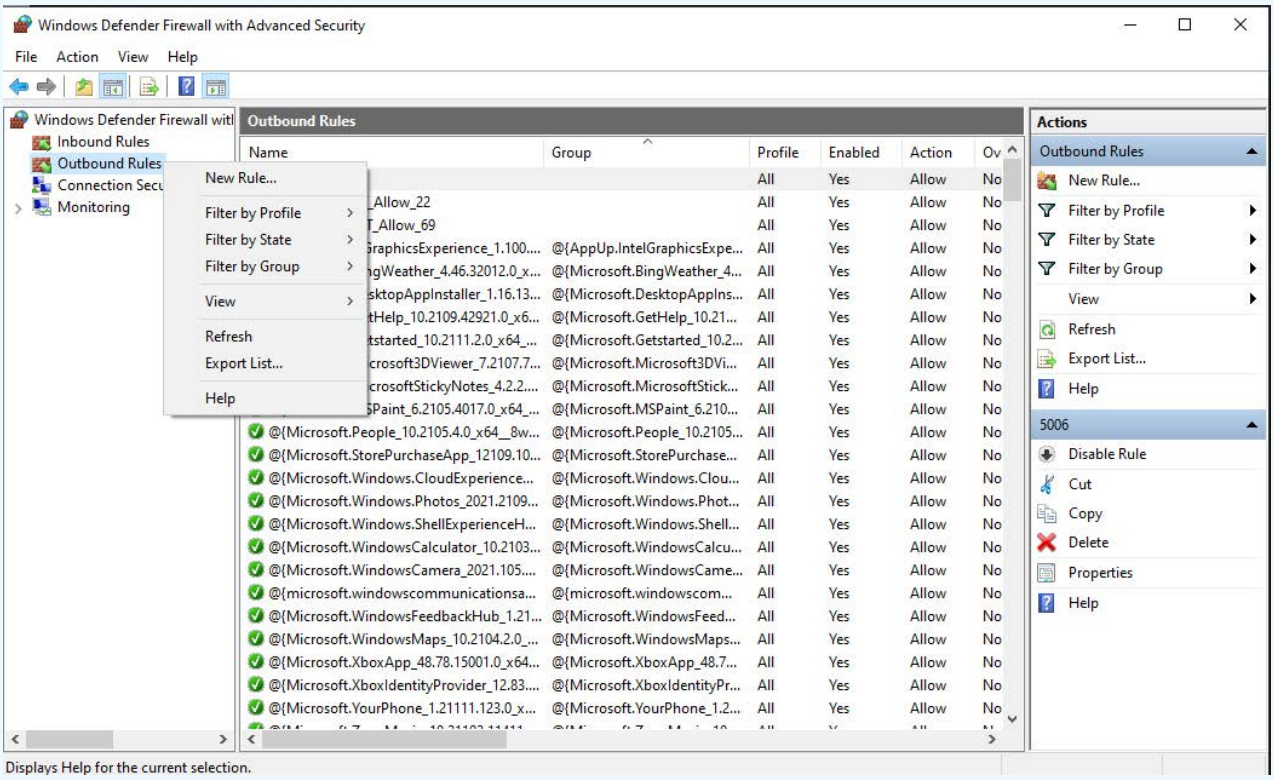


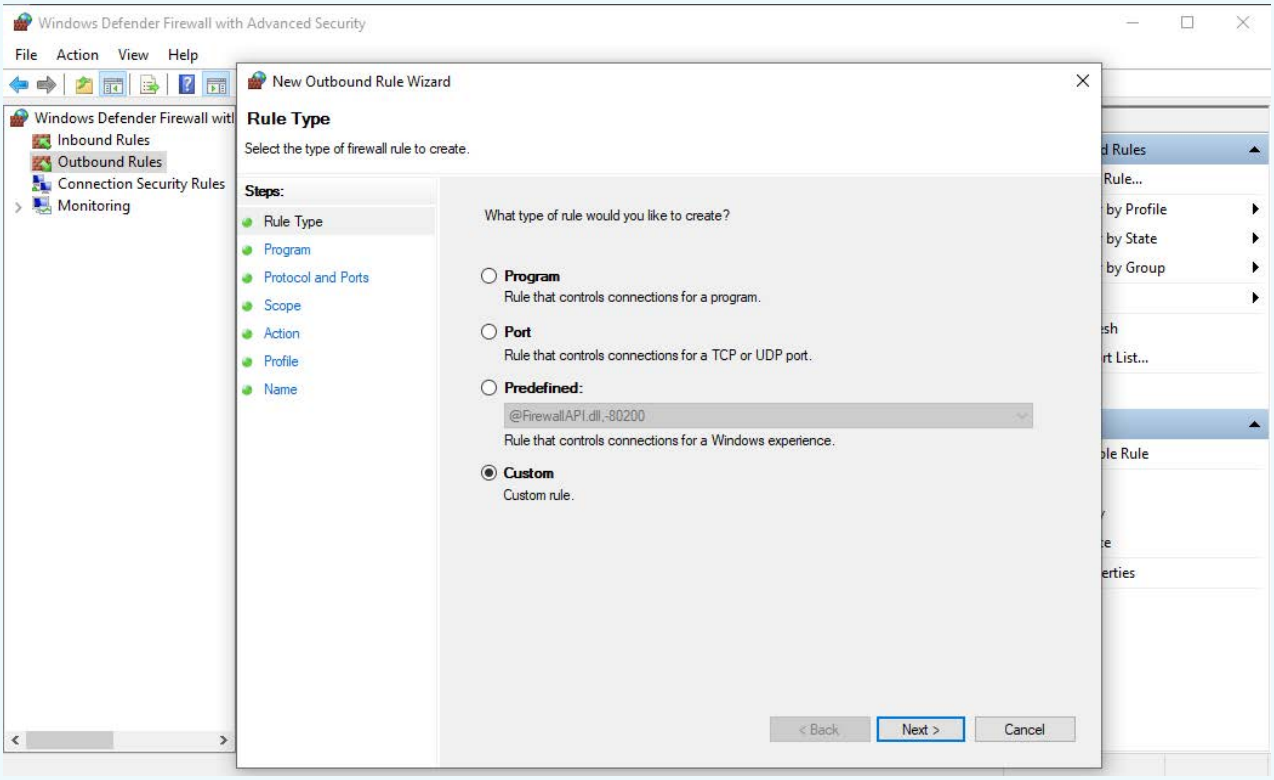


Steps to carry out in product server machine:

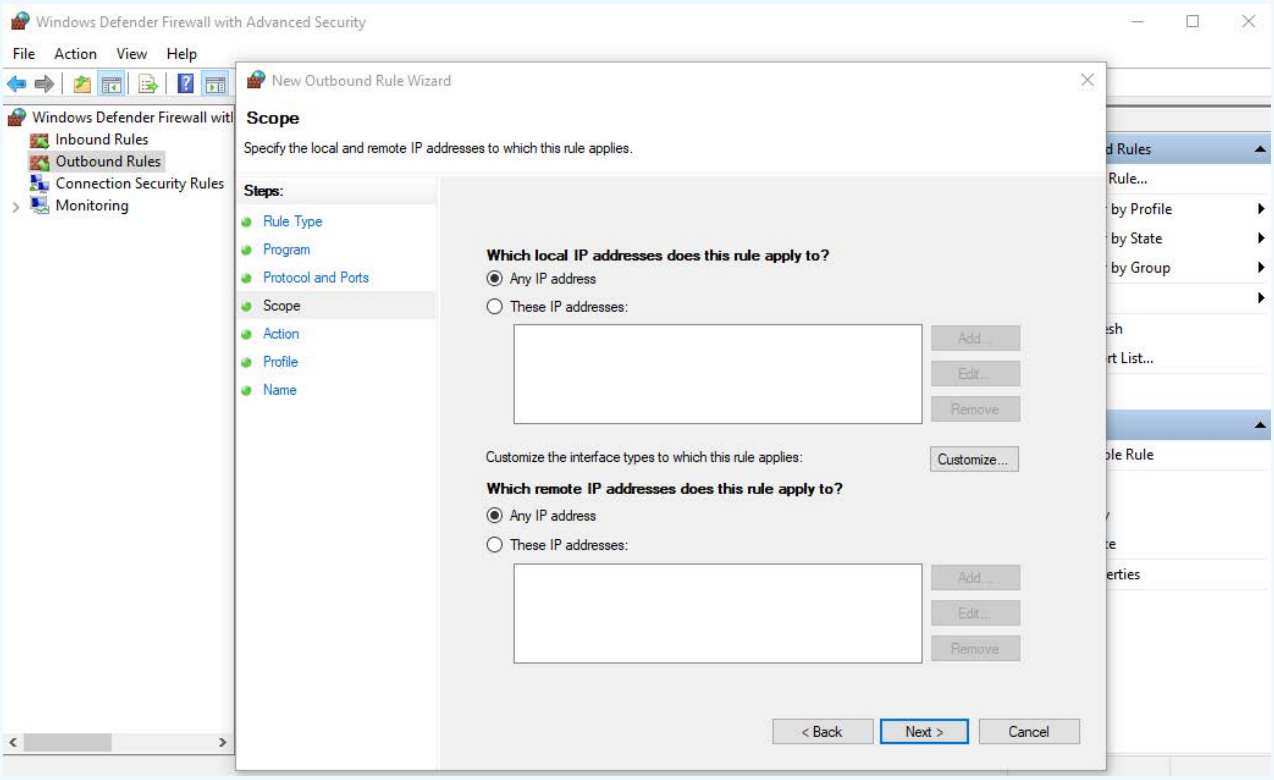


12. The required ports should be configured in the Inbound rule in the firewall.

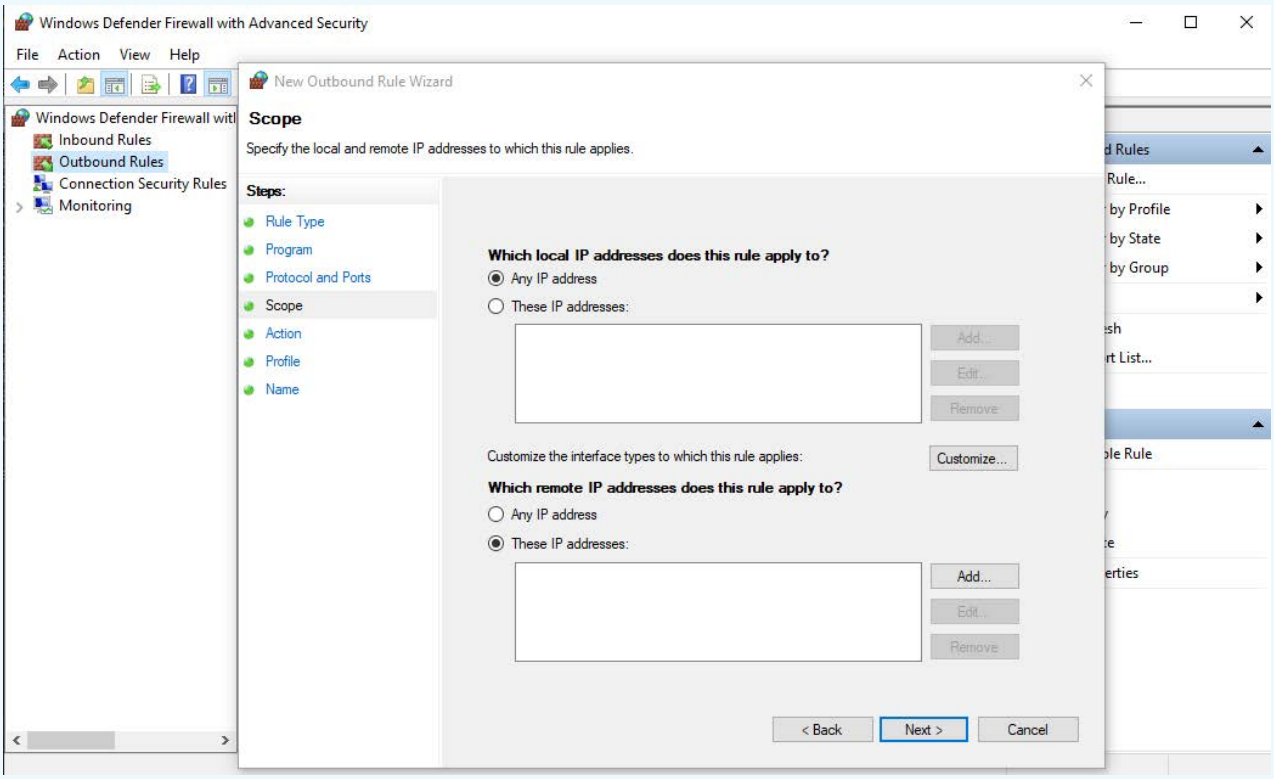




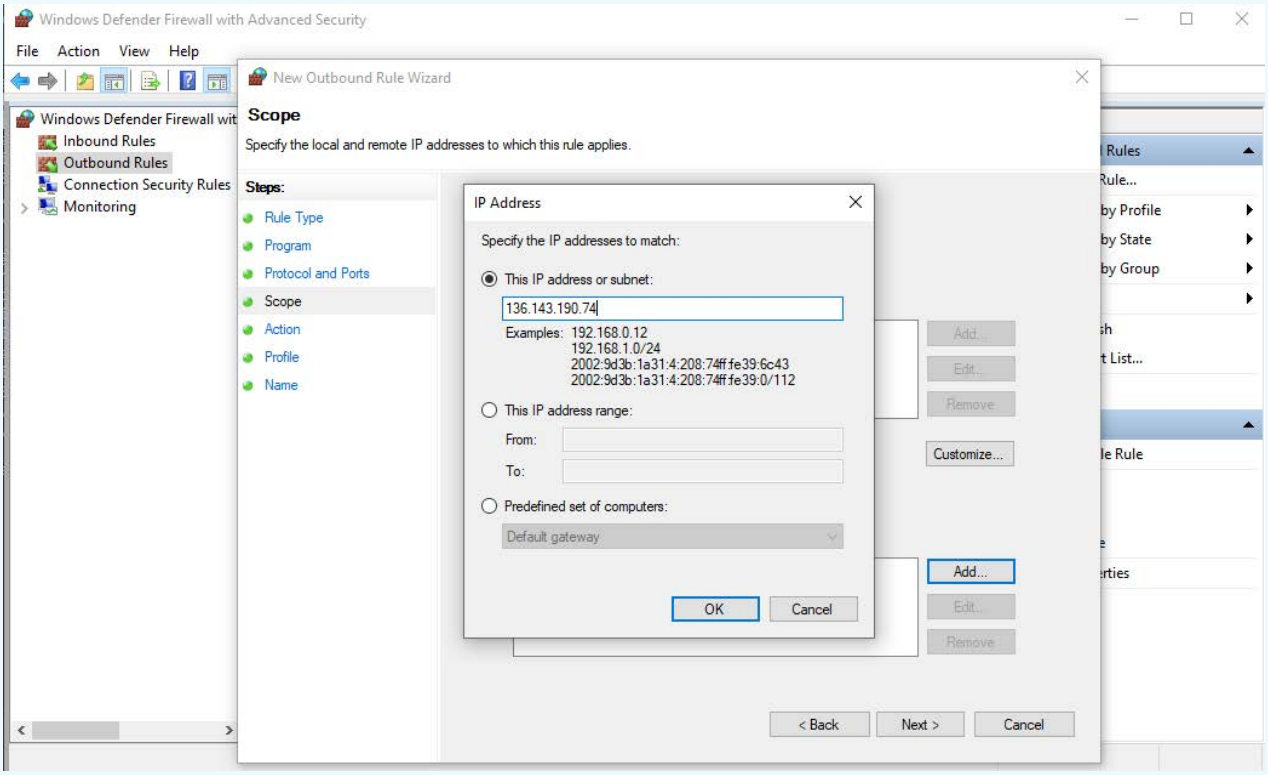
13. Open **Windows Defender Firewall**. Right-click **Inbound Rules > New Rule > Port.**



14. Enter the required **ports** and click **Next.**

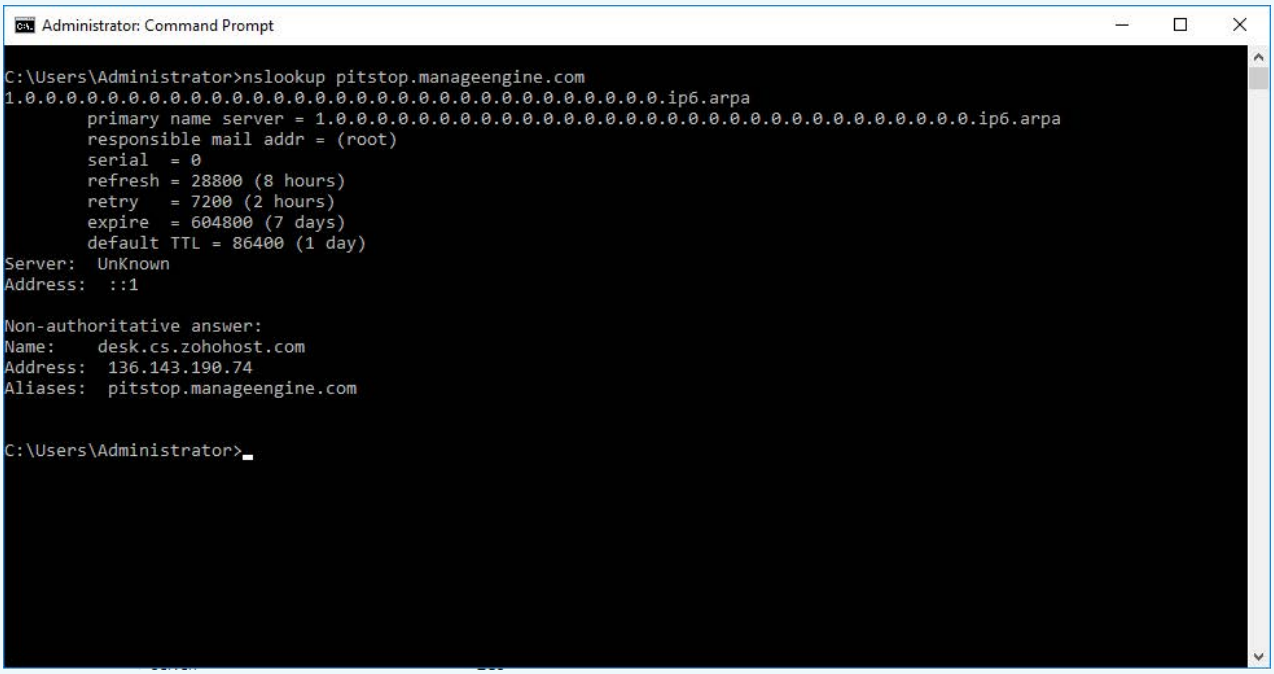


15. Select **Allow the connection.**

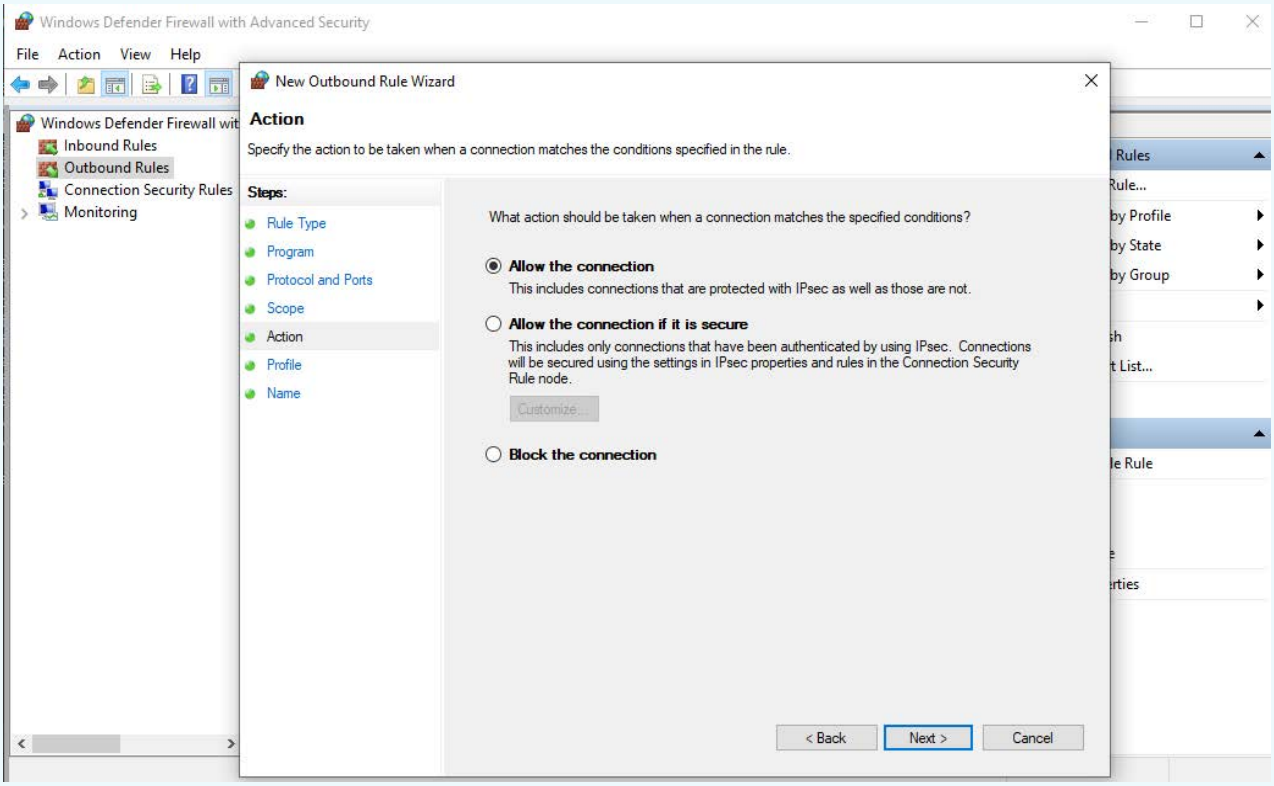


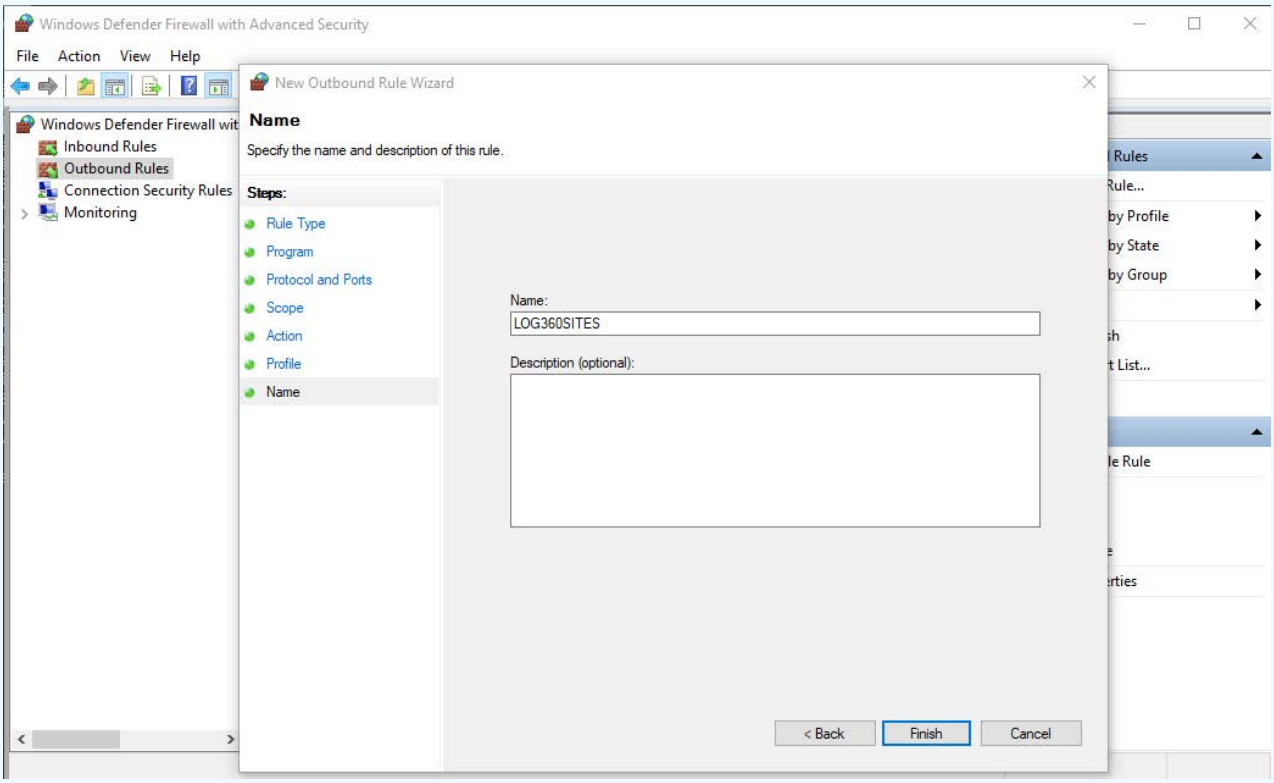
16. Save the **profile.**

17. To configure requires sites, right-click **Outbound Rules > New Rule**. Select **Custom.**
18. Click **Next** until you reach the *Scope* page.



19. Under *Which remote IP addresses does this rule apply to?*, select **These IP addresses.**





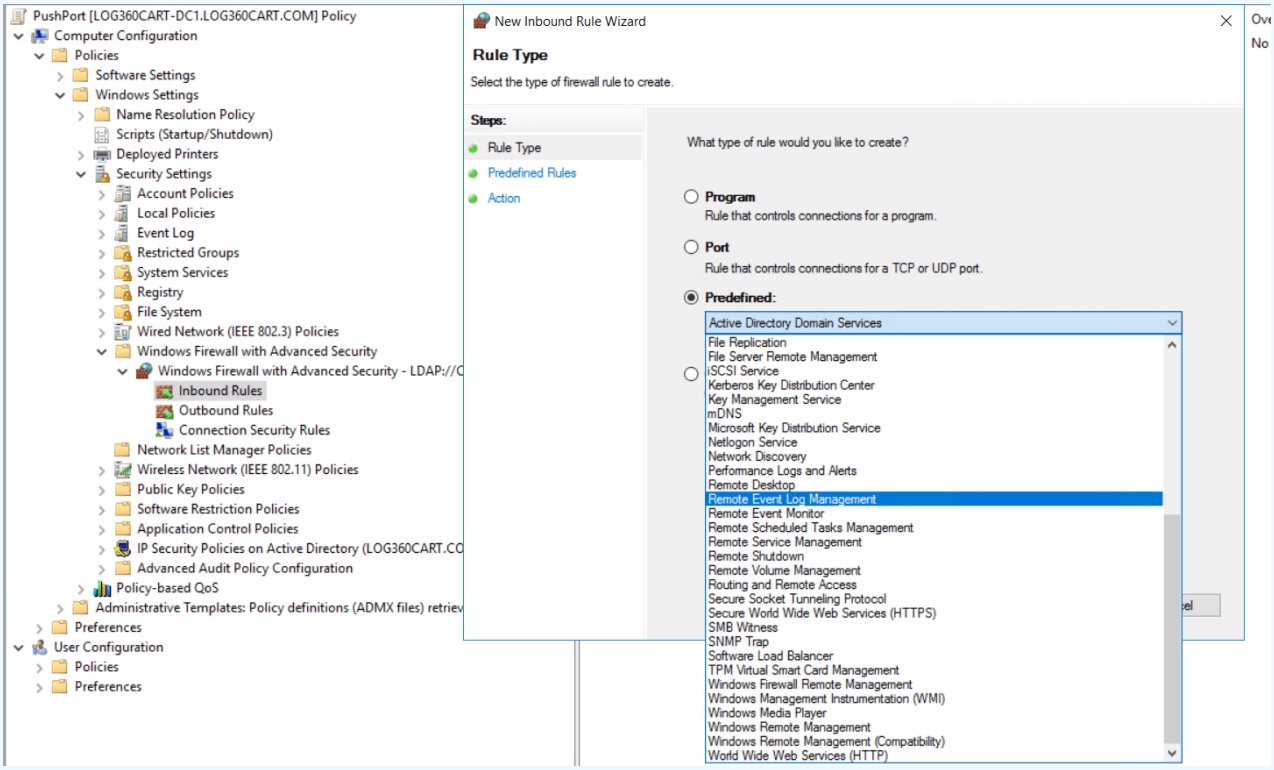
20. Click **Add.** Enter the **IP addresses** that need to be excluded and click **OK.**

Sites to be allowed:

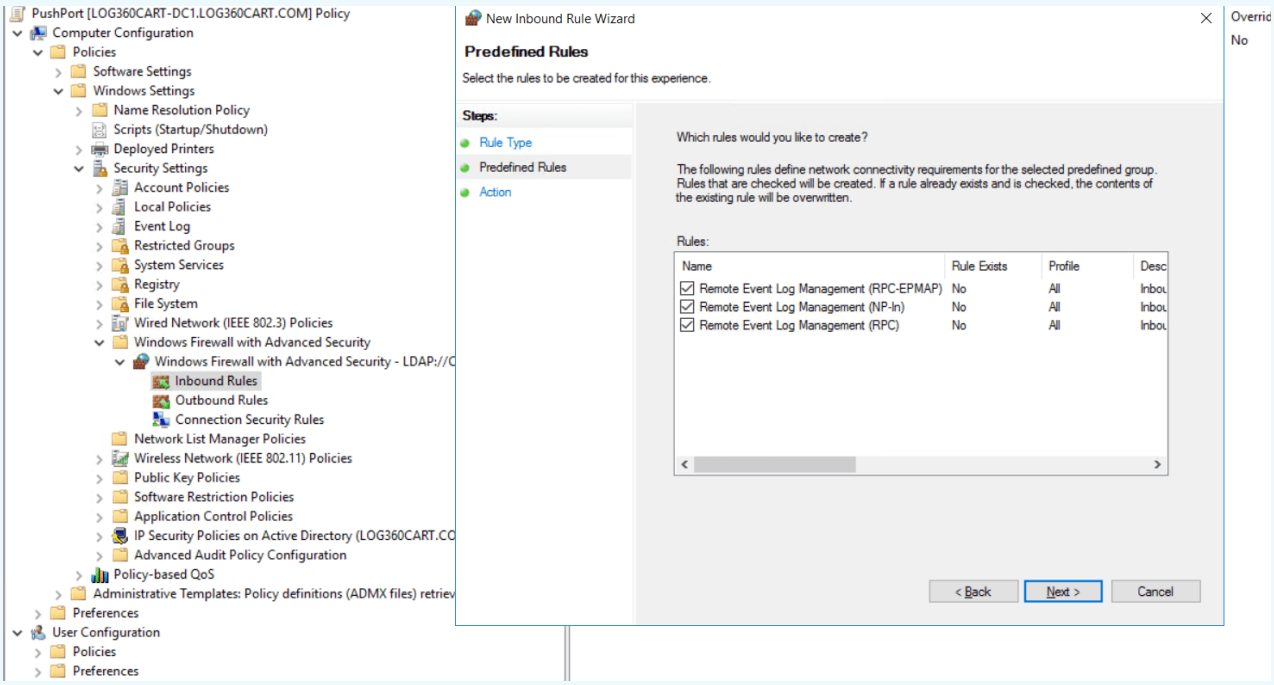
1. **www.manageengine.com** - All promotion URLs
2. **pitstop.manageengine.com** - Used in support pages
3. **store.manageengine.com** - Used in support pages
4. **updates.manageengine.com** - To download PPM certificates
5. **creator.zoho.com** - Auto-update, push notifications
6. **download.manageengine.com** - To download child components
7. **tools.manageengine.com** - To render some icons in browsers
8. **forum.manageengine.com** - Used in support pages

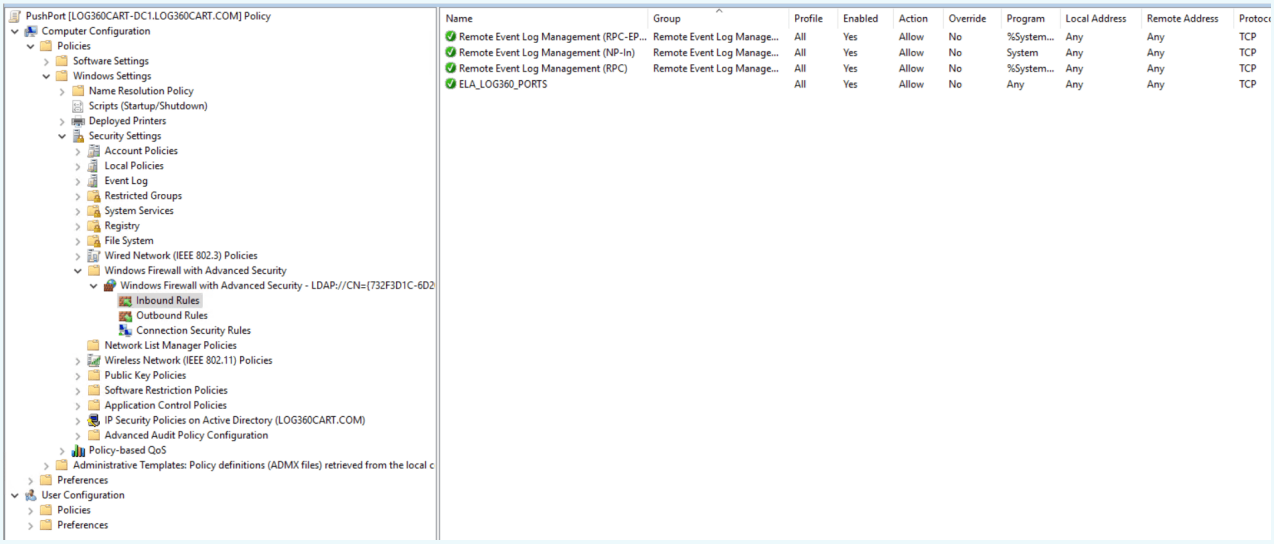
To open the RPC ports required for Windows log collection:

1. Right-click the created **GPO** and click **Edit.**
2. Expand **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security > Inbound Rules.**
3. Click **Create New Rule.**
4. Select **Predefined**. Select **Remote Event Log Management** from the drop-down, and click **Next.**



5. Make sure to check all the three boxes under Predefined Rules and click **Next**. Make sure **Allow the connection** is selected and click **Finish.**





Our Products

AD360 | ADAudit Plus | EventLog Analyzer | DataSecurity Plus
Exchange Reporter Plus | M365 Manager Plus

ManageEngine
Log360

Log360 is a unified SIEM solution with integrated DLP and CASB capabilities that detects, prioritizes, investigates and responds to security threats. Vigil IQ, the solution's TDIR module, combines threat intelligence, an analytical Incident Workbench, ML-based anomaly detection and rule-based attack detection techniques to detect sophisticated attacks, and it offers an incident management console for effectively remediating detected threats. Log360 provides holistic security visibility across on-premises, cloud and hybrid networks with its intuitive and advanced security analytics and monitoring capabilities. For more information about Log360, visit manageengine.com/log-management/ and follow the LinkedIn page for regular updates.

$ Get Quote Download