Ports used in Configuration Manager

11/19/2019 • 21 minutes to read • +9

In this article

Applies to: Configuration Manager (current branch)

This article lists the network ports that Configuration Manager uses. Some connections use ports that aren't configurable, and some support custom ports that you specify. If you use any port filtering technology, verify that the required ports are available. These port filtering technologies include firewalls, routers, proxy servers, or IPsec.

> **Note**
>
> If you support internet-based clients by using SSL bridging, in addition to port requirements, you might also have to allow some HTTP verbs and headers to traverse your firewall.

Ports you can configure

Configuration Manager enables you to configure the ports for the following types of communication:

- Application Catalog website point to Application Catalog web service point
- Enrollment proxy point to enrollment point
- Client-to-site systems that run IIS
- Client to internet (as proxy server settings)
- Software update point to internet (as proxy server settings)
- Software update point to WSUS server

- Site server to site database server
- Site server to WSUS database server
- Reporting services points

> **Note**
>
> The ports that are in use for the reporting services point site system role are configured in SQL Server Reporting Services. These ports are then used by Configuration Manager during communications to the reporting services point. Be sure to review these ports that define the IP filter information for IPsec policies or for configuring firewalls.

By default, the HTTP port that's used for client-to-site system communication is port 80, and the default HTTPS port is 443. Ports for client-to-site system communication over HTTP or HTTPS can be changed during setup or in the site properties for your Configuration Manager site.

The ports that are in use for the reporting services point site system role are configured in SQL Server Reporting Services. These ports are then used by Configuration Manager during communications to the reporting services point. Be sure to review these ports when you're defining the IP filter information for IPsec policies or for configuring firewalls.

Non-configurable ports

Configuration Manager doesn't allow you to configure ports for the following types of communication:

- Site to site
- Site server to site system
- Configuration Manager console to SMS Provider
- Configuration Manager console to the internet
- Connections to cloud services, such as Microsoft Intune and cloud distribution points

Ports used by Configuration Manager clients and site systems

The following sections detail the ports that are used for communication in Configuration Manager. The arrows in the section title show the direction of the communication:

- -- > Indicates that one computer initiates communication and the other computer always responds
- < -- > Indicates that either computer can initiate communication

Asset Intelligence synchronization point -- > Microsoft

Description	UDP	TCP
HTTPS	--	443

Asset Intelligence synchronization point -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Application Catalog web service point -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Application Catalog website point -- > Application Catalog web service point

Description	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Client -- > Application Catalog website point

Description	UDP	TCP

HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Client -- > Client

In addition to the ports that are listed in this table, wake-up proxy also uses ICMP echo request messages from one client to another client. Clients use this communication to confirm whether the other client is awake on the network. ICMP is sometimes referred to as ping commands. ICMP doesn't have a UDP or TCP protocol number, and so it isn't listed in the below table. However, any host-based firewalls on these client computers or intervening network devices within the subnet must permit ICMP traffic for wake-up proxy communication to succeed.

Description	UDP	TCP
Wake On LAN	9 Note 2 Alternate port available	--
Wake-up proxy	25536 Note 2 Alternate port available	--
Windows PE Peer cache broadcast	8004	--
Windows PE Peer cache download	--	8003

For more information, see Windows PE Peer Cache.

Client -- > Configuration Manager Network Device Enrollment Service (NDES) policy module

Description	UDP	TCP
HTTP		80
HTTPS	--	443

Client -- > Cloud distribution point

Description	UDP	TCP

HTTPS	--	443

For more information, see Ports and data flow.

Client -- > Cloud management gateway (CMG)

Description	UDP	TCP
HTTPS	--	443

For more information, see CMG Ports and data flow.

Client -- > Distribution point, both standard and pull

Description	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Client -- > Distribution point configured for multicast, both standard and pull

Description	UDP	TCP
Server Message Block (SMB)	--	445
Multicast protocol	63000-64000	--

Client -- > Distribution point configured for PXE, both standard and pull

Description	UDP	TCP

Description	UDP	TCP
DHCP	67 and 68	--

DHCP	67 and 68	
TFTP	69 Note 4	--
Boot Information Negotiation Layer (BINL)	4011	--

> **Important**
>
> If you enable a host-based firewall, make sure that the rules allow the server to send and receive on these ports. When you enable a distribution point for PXE, Configuration Manager can enable the inbound (receive) rules on the Windows Firewall. It doesn't configure the outbound (send) rules.

Client -- > Fallback status point

Description	UDP	TCP
HTTP	--	80 Note 2 Alternate port available

Client -- > Global catalog domain controller

A Configuration Manager client doesn't contact a global catalog server when it's a workgroup computer or when it's configured for internet-only communication.

Description	UDP	TCP
Global catalog LDAP	--	3268

Client -- > Management point

Description	UDP	TCP
Client notification (default communication before falling back to HTTP or HTTPS)	--	10123 Note 2 Alternate port available

Description	UDP	TCP
HTTP	--	80 Note 2 Alternate port

HTTP		available
HTTPS	--	443 Note 2 Alternate port available

Client -- > Software update point

Description	UDP	TCP
HTTP	--	80 or 8530 Note 3
HTTPS	--	443 or 8531 Note 3

Client -- > State migration point

Description	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available
Server Message Block (SMB)	--	445

CMG connection point -- > CMG cloud service

Configuration Manager uses these connections to build the CMG channel. For more information, see CMG Ports and data flow.

Description	UDP	TCP
TCP-TLS (preferred)	--	10140-10155
HTTPS (fallback with one VM)	--	443
HTTPS (fallback with two or more VMs)	--	10124-10139

CMG connection point -- > Management point

Version 1706 or 1710

Version 1706 or 1710

The specific port depends upon the management point configuration.

Description	UDP	TCP
HTTPS	--	443
HTTP	--	80

Version 1802

Description	UDP	TCP
HTTPS	--	443

For more information, see CMG Ports and data flow.

CMG connection point -- > Software update point

The specific port depends upon the software update point configuration.

Description	UDP	TCP
HTTPS	--	443
HTTP	--	80

For more information, see CMG Ports and data flow.

Configuration Manager console -- > Client

Description	UDP	TCP
Remote Control (control)	--	2701
Remote Assistance (RDP and RTC)	--	3389

Configuration Manager console -- > Internet

Description	UDP	TCP

HTTP	--	80
HTTPS	--	443

The Configuration Manager console uses internet access for the following actions:

- Downloading software updates from Microsoft Update for deployment packages.
- The Feedback item in the ribbon.
- Links to documentation within the console.

Configuration Manager console -- > Reporting services point

Description	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Configuration Manager console -- > Site server

Description	UDP	TCP
RPC (initial connection to WMI to locate provider system)	--	135

Configuration Manager console -- > SMS Provider

Description	UDP	TCP
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Configuration Manager Network Device Enrollment Service (NDES) policy module -- > Certificate registration point

Description	UDP	TCP
HTTPS	--	443 Note 2 Alternate port available

HTTPS 443

Data warehouse service point -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Distribution point, both standard and pull -- > Management point

A distribution point communicates to the management point in the following scenarios:

- To report the status of prestaged content
- To report usage summary data
- To report content validation
- To report the status of package downloads (pull-distribution point only)

Description	UDP	TCP
HTTP	--	80 Note 2 Alternate port available
HTTPS	--	443 Note 2 Alternate port available

Endpoint Protection point -- > Internet

Description	UDP	TCP
HTTP	--	80

Endpoint Protection point -- > SQL Server

Description	UDP	TCP

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Enrollment proxy point -- > Enrollment point

Description	UDP	TCP
HTTPS	--	443 Note 2 Alternate port available

Enrollment point -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Exchange Server Connector -- > Exchange Online

Description	UDP	TCP
Windows Remote Management over HTTPS	--	5986

Exchange Server Connector -- > On-Premises Exchange Server

Description	UDP	TCP
Windows Remote Management over HTTP	--	5985

Mac computer -- > Enrollment proxy point

Description	UDP	TCP
HTTPS	--	443

Management point -- > Domain controller

Description	UDP	TCP
Lightweight Directory Access Protocol (LDAP)	389	389

Lightweight Directory Access Protocol (LDAP)	389	389
Global catalog LDAP	--	3268
RPC Endpoint Mapper	--	135
RPC	--	DYNAMIC Note 6

Management point < -- > Site server

Note 5

Description	UDP	TCP
RPC Endpoint mapper	--	135
RPC	--	DYNAMIC Note 6
Server Message Block (SMB)	--	445

Management point -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Mobile device -- > Enrollment proxy point

Description	UDP	TCP
HTTPS	--	443

Mobile device -- > Microsoft Intune

Description	UDP	TCP

Description	UDP	TCP
HTTPS	--	443

Reporting Services point -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Service connection point -- > Microsoft Intune

Description	UDP	TCP
HTTPS	--	443

For more information, see Internet access requirements for the service connection point.

Service connection point -- > Azure (CMG)

Description	UDP	TCP
HTTPS for CMG service deployment	--	443

For more information, see CMG Ports and data flow.

Site server < -- > Application Catalog web service point

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Application Catalog website point

Description	UDP	TCP
Server Message Block (SMB)	--	445

~~Server Message Block (SMB)~~		~~445~~
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Asset Intelligence synchronization point

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server -- > Client

Description	UDP	TCP
Wake On LAN	9 Note 2 Alternate port available	--

Site server -- > Cloud distribution point

Description	UDP	TCP
HTTPS	--	443

For more information, see Ports and data flow.

Site server -- > Distribution point, both standard and pull

Note 5

Description	UDP	TCP

Description	UDP	TCP
~~Server Message Block (SMB)~~	--	~~445~~

Server Message Block (SMB)		445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server -- > Domain controller

Description	UDP	TCP
Lightweight Directory Access Protocol (LDAP)	389	389
Global catalog LDAP	--	3268
RPC Endpoint Mapper	--	135
RPC	--	DYNAMIC Note 6

Site server < -- > Certificate registration point

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Endpoint Protection point

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135

Description	UDP	TCP
RPC	--	DYNAMIC Note 6

Site server < -- > Enrollment point

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Enrollment proxy point

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Fallback status point

Note 5

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server -- > Internet

Description	UDP	TCP
HTTP	--	80 Note 1

Site server < -- > Issuing certification authority (CA)

This communication is used when you deploy certificate profiles by using the certificate registration point. The communication isn't used for every site server in the hierarchy. Instead, it's used only for the site server at the top of the hierarchy.

Description	UDP	TCP
RPC Endpoint Mapper	135	135
RPC (DCOM)	--	DYNAMIC Note 6

Site server -- > Server hosting Remote Content Library Share

Starting in version 1806 you can relocate the Content Library to another storage location to free up hard drive space on your central administration or primary site servers. For more information, see Configure a remote content library for the site server.

Description	UDP	TCP
Server Message Block (SMB)	--	445

Site server < -- > Reporting services point

Note 5

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Site server

Description	UDP	TCP
Server Message Block (SMB)	--	445

Server Message Block (SMB) 445

Site server -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

During the installation of a site that uses a remote SQL Server to host the site database, open the following ports between the site server and the SQL Server:

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server -- > SQL Server for WSUS

Description	UDP	TCP
SQL over TCP	--	1433 Note 3 Alternate port available

Site server -- > SMS Provider

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135
RPC	--	DYNAMIC Note 6

Site server < -- > Software update point

Note 5

Description	UDP	TCP

Server Message Block (SMB)	--	445
HTTP	--	80 or 8530 Note 3
HTTPS	--	443 or 8531 Note 3

Site server < -- > State migration point

Note 5

Description	UDP	TCP
Server Message Block (SMB)	--	445
RPC Endpoint Mapper	135	135

SMS Provider -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Software update point -- > Internet

Description	UDP	TCP
HTTP	--	80 Note 1

Software update point -- > Upstream WSUS server

Description	UDP	TCP
HTTP	--	80 or 8530 Note 3
HTTPS	--	443 or 8531 Note 3

SQL Server --> SQL Server

Intersite database replication requires the SQL Server at one site to communicate directly

with the SQL Server at its parent or child site.

Description	UDP	TCP
SQL Server service	--	1433 Note 2 Alternate port available
SQL Server Service Broker	--	4022 Note 2 Alternate port available

> **Tip**
>
> Configuration Manager doesn't require the SQL Server Browser, which uses port UDP 1434.

State migration point -- > SQL Server

Description	UDP	TCP
SQL over TCP	--	1433 Note 2 Alternate port available

Notes for ports used by Configuration Manager clients and site systems

Note 1: Proxy server port

This port can't be configured but can be routed through a configured proxy server.

Note 2: Alternate port available

An alternate port can be defined within Configuration Manager for this value. If a custom port has been defined, substitute that custom port when defining the IP filter information for IPsec policies or for configuring firewalls.

Note 3: Windows Server Update Services (WSUS)

WSUS can be installed to use either ports 80/443 or ports 8530/8531 for client communication. When you run WSUS in Windows Server 2012 or Windows Server 2016, WSUS is configured by default to use port 8530 for HTTP and port 8531 for HTTPS. After installation, you can change the port. You don't have to use the same port number throughout the site hierarchy.

- If the HTTP port is 80, the HTTPS port must be 443.
- If the HTTP port is anything else, the HTTPS port must be 1 or higher, for example, 8530 and 8531.

  > **Note**
  >
  > When you configure the software update point to use HTTPS, the HTTP port must also be open. Unencrypted data, such as the EULA for specific updates, uses the HTTP port.

- The site server makes a connection to the SQL server hosting the SUSDB when you enable the following options for WSUS cleanup:
  - Add non-clustered indexes to the WSUS database to improve WSUS cleanup performance
  - Remove obsolete updates from the WSUS database

  If the default SQL Server port is changed to an alternate port with SQL Server Configuration Manager, ensure the site server can connect using the defined port. Configuration Manager doesn't support dynamic ports. By default, SQL Server named instances use dynamic ports for connections to the database engine. When you use a named instance, manually configure the static port.

Note 4: Trivial FTP (TFTP) Daemon

The Trivial FTP (TFTP) Daemon system service doesn't require a user name or password and is an integral part of Windows Deployment Services (WDS). The Trivial FTP Daemon service implements support for the TFTP protocol that's defined by the following RFCs:

- RFC 1350: TFTP
- RFC 2347: Option extension
- RFC 2348: Block size option
- RFC 2349: Time-out interval and transfer size options

TFTP is designed to support diskless boot environments. TFTP Daemons listen on UDP port 69 but respond from a dynamically allocated high port. Therefore, enabling this port allows the TFTP service to receive incoming TFTP requests but doesn't allow the selected server to

respond to those requests. You can't enable the selected server to respond to inbound TFTP requests unless the TFTP server is configured to respond from port 69.

The PXE-enabled distribution point and the client in Windows PE select dynamically allocated high ports for TFTP transfers. These ports are defined by Microsoft between 49152 and 65535. For more information, see Service overview and network port requirements for Windows

However, during the actual PXE boot, the network card on the device selects the dynamically allocated high port it uses during the TFTP transfer. The network card on the device isn't bound to the dynamically allocated high ports defined by Microsoft. It's only bound to the ports defined in RFC 1350. This port can be any from 0 to 65535. For information regarding what dynamically allocated high ports the network card uses, contact the device hardware manufacturer.

Note 5: Communication between the site server and site systems

By default, communication between the site server and site systems is bi-directional. The site server initiates communication to configure the site system, and then most site systems connect back to the site server to send status information. Reporting service points and distribution points don't send status information. If you select **Require the site server to initiate connections to this site system** on the site system properties after the site system has been installed, the site system won't initiate communication with the site server. Instead, the site server initiates the communication and uses the site system installation account for authentication to the site system server.

Note 6: Dynamic ports

Dynamic ports use a range of port numbers that's defined by the OS version. These ports are also known as ephemeral ports. For more information about the default port ranges, see Service overview and network port requirements for Windows.

Additional lists of ports

The following sections provide additional information about ports that are used by Configuration Manager.

Client to server shares

Clients use Server Message Block (SMB) whenever they connect to UNC shares. For

example:

- Manual client installation that specifies the CCMSetup.exe **/source:** command-line property
- Endpoint Protection clients that download definition files from a UNC path

Description	UDP	TCP
Server Message Block (SMB)	--	445

Connections to Microsoft SQL Server

For communication to the SQL Server database engine and for intersite replication, you can use the default SQL Server port or specify custom ports:

- Intersite communications use:
  - SQL Server Service Broker, which defaults to port TCP 4022.
  - SQL Server service, which defaults to port TCP 1433.
- Intrasite communication between the SQL Server database engine and various Configuration Manager site system roles defaults to port TCP 1433.
- Configuration Manager uses the same ports and protocols to communicate with each SQL Availability Group replica that hosts the site database as if the replica was a standalone SQL Server instance.

When you use Azure and the site database is behind an internal or external load balancer, configure the following components:

- Firewall exceptions on each replica
- Load balancing rules

Configure the following ports:

- SQL over TCP: TCP 1433
- SQL Server Service Broker: TCP 4022
- Server Message Block (SMB): TCP 445
- RPC Endpoint Mapper: TCP 135

> ⚠ Warning

> ⚠ Warning
>
> Configuration Manager doesn't support dynamic ports. by default, SQL Server named instances use dynamic ports for connections to the database engine. When you use a named instance, manually configure the static port for intrasite communication.

The following site system roles communicate directly with the SQL Server database:

- Application Catalog web service point
- Certificate registration point role
- Enrollment point role
- Management point
- Site server
- Reporting Services point
- SMS Provider
- SQL Server --> SQL Server

When a SQL Server hosts a database from more than one site, each database must use a separate instance of SQL Server. Configure each instance with a unique set of ports.

If you enable a host-based firewall on the SQL server, configure it to allow the correct ports. Also configure network firewalls in between computers that communicate with the SQL server.

For an example of how to configure SQL Server to use a specific port, see Configure a server to listen on a specific TCP port.

Discovery and publishing

Configuration Manager uses the following ports for the discovery and publishing of site information:

- Lightweight Directory Access Protocol (LDAP): 389
- Global catalog LDAP: 3268
- RPC Endpoint Mapper: 135
- RPC: Dynamically allocated high TCP ports
- TCP: 1024: 5000

- TCP: 49152: 65535

External connections made by Configuration Manager

On-premises Configuration Manager clients or site systems can make the following external connections:

- Asset Intelligence synchronization point -- > Microsoft
- Endpoint Protection point -- > Internet
- Client -- > Global catalog domain controller
- Configuration Manager console -- > Internet
- Management point -- > Domain controller
- Site server -- > Domain controller
- Site server < -- > Issuing Certification Authority (CA)
- Software update point -- > Internet
- Software update point -- > Upstream WSUS Server
- Service connection point -- > Microsoft Intune
- Service connection point -- > Azure
- CMG connection point -- > CMG cloud service

Installation requirements for site systems that support internet-based clients

> **Note**
>
> This section only applies to internet-based client management (IBCM). It doesn't apply to the cloud management gateway. For more information, see **Manage clients on the internet**.

Internet-based management points and distribution points that support internet-based clients, the software update point, and the fallback status point use the following ports for installation and repair:

- Site server --> Site system: RPC endpoint mapper using UDP and TCP port 135.
- Site server --> Site system: RPC dynamic TCP ports
- Site server < --> Site system: Server message blocks (SMB) using TCP port 445

Application and package installations on distribution points require the following RPC ports:

- Site server --> Distribution point: RPC endpoint mapper using UDP and TCP port 135
- Site server --> Distribution point: RPC dynamic TCP ports

Use IPsec to help secure the traffic between the site server and site systems. If you must restrict the dynamic ports that are used with RPC, you can use the Microsoft RPC configuration tool (rpccfg.exe) to configure a limited range of ports for these RPC packets. For more information about the RPC configuration tool, see How to configure RPC to use certain ports and how to help secure those ports by using IPsec.

> **Important**
>
> Before you install these site systems, ensure that the remote registry service is running on the site system server and that you have specified a site system installation account if the site system is in a different Active Directory forest without a trust relationship. For example, the remote registry service is used on servers running site systems such as distribution points (both pull and standard), remote SQL servers, and the Application Catalog.

Ports used by Configuration Manager client installation

The ports that Configuration Manager uses during client installation depends on the deployment method.

- For a list of ports for each client deployment method, see Ports used during Configuration Manager client deployment
- For more information about how to configure Windows Firewall on the client for client installation and post-installation communication, see Windows Firewall and port settings for clients

Ports used by migration

The site server that runs migration uses several ports to connect to applicable sites in the source hierarchy. For more information, see Required configurations for migration.

Ports used by Windows Server

The following table lists some of the key ports used by Windows Server.

Description	UDP	TCP
DNS	53	53
DHCP	67 and 68	--
NetBIOS Name Resolution	137	--
NetBIOS Datagram Service	138	--
NetBIOS Session Service	--	139
Kerberos authentication	--	88

For more information, see the following articles:

- Service overview and network port requirements for the Windows Server system.
- How to configure a firewall for domains and trusts