

Windows Firewall and Port Settings for Client Computers in Configuration Manager

Updated: May 14, 2015

Applies To: System Center 2012 Configuration Manager, System Center 2012 Configuration Manager SP1, System Center 2012 Configuration Manager SP2, System Center 2012 R2 Configuration Manager, System Center 2012 R2 Configuration Manager SP1

Client computers in System Center 2012 Configuration Manager that run Windows Firewall often require you to configure exceptions to allow communication with their site. The exceptions that you must configure depend on the management features that you use with the Configuration Manager client.

Use the following sections to identify these management features and for more information about how to configure Windows Firewall for these exceptions.

Modifying the Ports and Programs Permitted by Windows Firewall

Use the following procedure to modify the ports and programs on Windows Firewall for the Configuration Manager client.

To modify the ports and programs permitted by Windows Firewall

1. On the computer that runs Windows Firewall, open Control Panel.
2. Right-click **Windows Firewall**, and then click **Open**.
3. Configure any required exceptions and any custom programs and ports that you require.

Programs and Ports that Configuration Manager Requires

The following Configuration Manager features require exceptions on the Windows Firewall:

Queries

If you run the Configuration Manager console on a computer that runs Windows Firewall, queries fail the first time that they are run and the operating system displays a dialog box asking if you want to unblock statview.exe. If you unblock statview.exe, future queries will run without errors. You can also manually add Statview.exe to the list of programs and services on the **Exceptions** tab of the Windows Firewall before you run a query.

Client Push Installation

To use client push to install the System Center 2012 Configuration Manager client, add the following as exceptions to the Windows Firewall:

- Outbound and inbound: **File and Printer Sharing**
- Inbound: **Windows Management Instrumentation (WMI)**

Client Installation by Using Group Policy

To use Group Policy to install the Configuration Manager client, add **File and Printer Sharing** as an exception to the Windows Firewall.

Client Requests

For client computers to communicate with Configuration Manager site systems, add the following as exceptions to the Windows Firewall:

Outbound: TCP Port **80** (for HTTP communication)

Outbound: TCP Port **443** (for HTTPS communication)

Important

These are default port numbers that can be changed in Configuration Manager. For more information, see [How to Configure Client Communication Port Numbers in Configuration Manager](#). If these ports have been changed from the default values, you must also configure matching exceptions on the Windows Firewall.

Client Notification

For System Center 2012 Configuration Manager SP1 and later:

For the management point to notify client computers about an action that it must take when an administrative user selects a client action in the Configuration Manager console, such as download computer policy or initiate a malware scan, add the following as an exception to the Windows Firewall:

Outbound: TCP Port **10123**

If this communication does not succeed, Configuration Manager automatically falls back to using the existing client-to-management point communication port of HTTP, or HTTPS:

Outbound: TCP Port **80** (for HTTP communication)

Outbound: TCP Port **443** (for HTTPS communication)

Important

These are default port numbers that can be changed in Configuration Manager. For more information, see [How to Configure Client Communication Port Numbers in Configuration Manager](#). If these ports have been changed from the default values, you must also configure matching exceptions on the Windows Firewall.

Network Access Protection

For client computers to successfully communicate with the System Health Validator point, allow the following ports:

- Outbound: UDP **67** and UDP **68** for DHCP
- Outbound: TCP **80/443** for IPsec

Remote Control

To use Configuration Manager remote control, allow the following port:

- Inbound: TCP Port **2701**

Remote Assistance and Remote Desktop

To initiate Remote Assistance from the Configuration Manager console, add the custom program **Helpsvc.exe** and the inbound custom port TCP **135** to the list of permitted programs and services in Windows Firewall on the client computer. You must also permit **Remote Assistance** and **Remote Desktop**. If you initiate Remote Assistance from the client computer, Windows Firewall automatically configures and permits **Remote Assistance** and **Remote Desktop**.

Wake-Up Proxy

For System Center 2012 Configuration Manager SP1 and later:

If you enable the wake-up proxy client setting, a new service named ConfigMgr Wake-up Proxy uses a peer-to-peer protocol to check whether other computers are awake on the subnet and to wake them up if necessary. This communication uses the following ports:

Outbound: UDP Port **25536**

Outbound: UDP Port **9**

These are the default port numbers that can be changed in Configuration Manager by using the **Power Management** clients settings of **Wake-up proxy port number (UDP)** and **Wake On LAN port number (UDP)**. If you specify the **Power Management: Windows Firewall exception for wake-up proxy** client setting, these ports are automatically configured in Windows Firewall for clients. However, if clients run a different firewall, you must manually configure the exceptions for these port numbers.

In addition to these ports, wake-up proxy also uses Internet Control Message Protocol (ICMP) echo request messages from one client computer to another client computer. This communication is used to confirm whether the other client computer is awake on the network. ICMP is sometimes referred to as TCP/IP ping commands. System Center 2012 Configuration Manager SP1 does not configure Windows Firewall for these TCP/IP ping commands and unless you are running System Center 2012 R2 Configuration Manager, you must manually permit this ICMP traffic for wake-up proxy communication to succeed.

If you have System Center 2012 Configuration Manager SP1 rather than System Center 2012 R2 Configuration Manager, use the following procedure to help you configure Windows Firewall with a custom inbound rule that allows inbound TCP/IP ping commands for wake-up proxy.

To configure Windows Firewall to allow TCP/IP ping commands

1. In the Windows Firewall with Advanced Security console, create a new inbound rule.
2. In the New Inbound Rule Wizard, on the **Rule Type** page, select **Custom**, and then click **Next**.

- 11/10/2017

Windows Firewall and Port Settings for Client Computers in Configuration Manager
3. On the **Program** page, keep the default of **All programs**, and then click **Next**.

4. On the **Protocols and Ports** page, click the drop-down for **Protocol type**, select **ICMPv4**, and then click the **Customize** button.

5. In the **Customize ICMP Settings** dialog box, click **Specific ICMP types**, select **Echo Request**, and then click **OK**.

6. In the New Inbound Rule Wizard, click **Next**.

7. On the **Scope** page, keep the default settings for any local or remote IP address, and click **Next**.

8. On the **Action** page, make sure that **Allow the connection is selected**, and then click **Next**.

9. On the **Profile** page, select the profiles that will use wake-up proxy (for example, **Domain**), and then click **Next**.

10. On the **Name** page, specify a name for this custom rule, and optionally, type a description to help identify that this rule is required for wake-up proxy communication. Then click **Finish** to close the wizard.


For more information about wake-up proxy, see the [Planning How to Wake Up Clients](#) section in the [Planning for Communications in Configuration Manager](#) topic

Windows Event Viewer, Windows Performance Monitor, and Windows Diagnostics

To access Windows Event Viewer, Windows Performance Monitor, and Windows Diagnostics from the Configuration Manager console, enable **File and Printer Sharing** as an exception on the Windows Firewall.

Ports Used During Configuration Manager Client Deployment

The following tables list the ports that are used during the client installation process.

 Important

If there is a firewall between the site system servers and the client computer, confirm whether the firewall permits traffic for the ports that are required for the client installation method that you choose. For example, firewalls often prevent client push installation from succeeding because they block Server Message Block (SMB) and Remote Procedure Calls (RPC). In this scenario, use a different client installation method, such as manual installation (running CCMSetup.exe) or Group Policy-based client installation. These alternative client installation methods do not require SMB or RPC.

For information about how to configure Windows Firewall on the client computer, see [Modifying the Ports and Programs Permitted by Windows Firewall](#).

Ports that are used for all installation methods

Description	UDP	TCP
Hypertext Transfer Protocol (HTTP) from the client computer to a fallback status point, when a fallback status point is assigned to the client.	--	80 (See note 1, Alternate Port Available)

Ports that are used with client push installation

In addition to the ports listed in the following table, client push installation also uses Internet Control Message Protocol (ICMP) echo request messages from the site server to the client computer to confirm whether the client computer is available on the network. ICMP is sometimes referred to as TCP/IP ping commands. ICMP does not have a UDP or TCP protocol number, and so it is not listed in the following table. However, any intervening network devices, such as firewalls, must permit ICMP traffic for client push installation to succeed.

Description	UDP	TCP
Server Message Block (SMB) between the site server and client computer.	--	445
RPC endpoint mapper between the site server and the client computer.	135	135
RPC dynamic ports between the site server and the client computer.	--	DYNAMIC
Hypertext Transfer Protocol (HTTP) from the client computer to a management point when the connection is over HTTP.	--	80 (See note 1, Alternate Port Available)
Secure Hypertext Transfer Protocol (HTTPS) from the client computer to a management point when the connection is over HTTPS.	--	443 (See note 1, Alternate Port Available)


Ports that are used with software update point-based installation

Description	UDP	TCP
Hypertext Transfer Protocol (HTTP) from the client computer to the software update point.	--	80 or 8530 (See note 2, Windows Server Update Services)
Secure Hypertext Transfer Protocol (HTTPS) from the client computer to the software update point.	--	443 or 8531 (See note 2, Windows Server Update Services)
Server Message Block (SMB) between the source server and the client computer when you specify the CCMSSetup command-line property /source: <Path> .	--	445

Ports that are used with Group Policy-based installation

Description	UDP	TCP
Hypertext Transfer Protocol (HTTP) from the client computer to a management point when the connection is over HTTP.	--	80 (See note 1, Alternate Port Available)
Secure Hypertext Transfer Protocol (HTTPS) from the client computer to a management point when the connection is over HTTPS.	--	443 (See note 1, Alternate Port Available)
Server Message Block (SMB) between the source server and the client computer when you specify the CCMSSetup command-line property /source:<Path> .	--	445

Ports that are used with manual installation and logon script-based installation

Description	UDP	TCP
<p>Server Message Block (SMB) between the client computer and a network share from which you run CCMSSetup.exe.</p> <div>  Note </div> <p>When you install System Center 2012 Configuration Manager, the client installation source files are copied and automatically shared from the <i><InstallationPath>\Client</i> folder on management points. However, you can copy these files and create a new share on any computer on the network. Alternatively, you can eliminate this network traffic by running CCMSSetup.exe locally, for example, by using removable media.</p>	--	445
Hypertext Transfer Protocol (HTTP) from the client computer to a management point when the connection is over HTTP, and you do not specify the CCMSSetup command-line property /source:<Path> .	--	80 (See note 1, Alternate Port Available)
Secure Hypertext Transfer Protocol (HTTPS) from the client computer to a management point when the connection is over HTTPS, and you do not specify the CCMSSetup command-line property /source:<Path> .	--	443 (See note 1, Alternate Port Available)
Server Message Block (SMB) between the source server and the client computer when you specify the CCMSSetup command-line property /source:<Path> .	--	445

Ports that are used with software distribution-based installation

Description	UDP	TCP
Server Message Block (SMB) between the distribution point and the client computer.	--	445
Hypertext Transfer Protocol (HTTP) from the client to a distribution point when the connection is over HTTP.	--	80 (See note 1, Alternate Port Available)
Secure Hypertext Transfer Protocol (HTTPS) from the client to a distribution point when the connection is over HTTPS.	--	443 (See note 1, Alternate Port Available)

Notes

1 Alternate Port Available In Configuration Manager, you can define an alternate port for this value. If a custom port has been defined, substitute that custom port when you define the IP filter information for IPsec policies or for configuring firewalls.

2 Windows Server Update Services You can install Windows Server Update Service (WSUS) either on the default Web site (port 80) or a custom Web site (port 8530).

After installation, you can change the port. You do not 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 higher—for example, 8530 and 8531.

See Also

[Technical Reference for Client Deployment in Configuration Manager](#)