Setting up a Remote WMI Connection

Article • 01/07/2021 • 6 contributors

Feedback

In this article

Connecting to a WMI namespace on a remote computer may require that you change the settings for Windows Firewall, User Account Control (UAC), DCOM, or Common Information Model Object Manager (CIMOM).

The following sections are discussed in this topic:

- Windows Firewall Settings
- User Account Control Settings
- DCOM Settings
- CIMOM Settings
- Related topics

Windows Firewall Settings

WMI settings for Windows Firewall settings enable only WMI connections, rather than other DCOM applications as well.

An exception must be set in the firewall for WMI on the remote target computer. The exception for WMI allows WMI to receive remote connections and asynchronous callbacks to Unsecapp.exe. For more information, see Setting Security on an Asynchronous Call.

If a client application creates its own sink, that sink must be explicitly added to the firewall exceptions to allow callbacks to succeed.

The exception for WMI also works if WMI has been started with a fixed port, using the **winmgmt /standalonehost** command. For more information, see Setting Up a Fixed Port for WMI.

You can enable or disable WMI traffic through the Windows Firewall UI.

To enable or disable WMI traffic using firewall UI

1. In the **Control Panel**, click **Security** and then click **Windows Firewall**.
2. Click **Change Settings** and then click the **Exceptions** tab.
3. In the Exceptions window, select the check box for **Windows Management Instrumentation (WMI)** to enable WMI traffic through the firewall. To disable WMI traffic, clear the check box.

You can enable or disable WMI traffic through the firewall at the command prompt.

To enable or disable WMI traffic at command prompt using WMI rule group

- Use the following commands at a command prompt. Type the following to enable WMI traffic through the firewall.

  netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=yes

  Type the following command to disable WMI traffic through the firewall.

  netsh advfirewall firewall set rule group="windows management instrumentation (wmi)" new enable=no

Rather than using the single WMI rule group command, you also can use individual commands for each of the DCOM, WMI service, and sink.

To enable WMI traffic using separate rules for DCOM, WMI, callback sink and outgoing connections

1. To establish a firewall exception for DCOM port 135, use the following command.

   netsh advfirewall firewall add rule dir=in name="DCOM" program=%systemroot%\system32\svchost.exe service=rpcss action=allow protocol=TCP localport=135

2. To establish a firewall exception for the WMI service, use the following command.

   netsh advfirewall firewall add rule dir=in name ="WMI" program=%systemroot%\system32\svchost.exe service=winmgmt action = allow protocol=TCP localport=any

3. To establish a firewall exception for the sink that receives callbacks from a remote computer, use the following command.

   netsh advfirewall firewall add rule dir=in name ="UnsecApp" program=%systemroot%\system32\wbem\unsecapp.exe action=allow

4. To establish a firewall exception for outgoing connections to a remote computer that the local computer is communicating with asynchronously, use the following command.

   netsh advfirewall firewall add rule dir=out name ="WMI_OUT" program=%systemroot%\system32\svchost.exe service=winmgmt action=allow protocol=TCP localport=any

To disable the firewall exceptions separately, use the following commands.

To disable WMI traffic using separate rules for DCOM, WMI, callback sink and outgoing connections

1. To disable the DCOM exception.

   netsh advfirewall firewall delete rule name="DCOM"

2. To disable the WMI service exception.

   netsh advfirewall firewall delete rule name="WMI"

3. To disable the sink exception.

   netsh advfirewall firewall delete rule name="UnsecApp"

4. To disable the outgoing exception.

   netsh advfirewall firewall delete rule name="WMI_OUT"

User Account Control Settings

User Account Control (UAC) access-token filtering can affect which operations are allowed in WMI namespaces or what data is returned. Under UAC, all accounts in the local Administrators group run with a standard user *access token*, also known as UAC access-token filtering. An administrator account can run a script with an elevated privilege—"Run as Administrator".

When you are not connecting to the built-in Administrator account, UAC affects connections to a remote computer differently depending on whether the two computers are in a domain or a workgroup. For more information about UAC and remote connections, see User Account Control and WMI.

DCOM Settings

For more information on DCOM settings, see Securing a Remote WMI Connection. However, UAC affects connections for nondomain user accounts. If you connect to a remote computer using a nondomain user account included in the local Administrators group of the remote computer, then you must explicitly grant remote DCOM access, activation, and launch rights to the account.

CIMOM Settings

The CIMOM settings need to be updated if the remote connection is between computers that do not have a trust relationship; otherwise, an asynchronous connection will fail. This setting should not be modified for computers in the same domain or in trusted domains.

The following registry entry needs to be modified to allow anonymous callbacks:

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\WBEM\CIMOM\AllowAnonymousCallback

Data type
REG_DWORD

If the **AllowAnonymousCallback** value is set to 0, the WMI service prevents anonymous callbacks to the client. If the value is set to 1, the WMI service allows anonymous callbacks to the client.

Related topics

Connecting to WMI on a Remote Computer

Feedback

Was this page helpful? Yes No

Provide product feedback | Get help at Microsoft Q&A

Additional resources

Training

Learning path

Query management information by using Common Information Model and Windows Management Instrumentation - Training

This learning path covers Windows Management Instrumentation (WMI) and Common Information Model (CIM). These technologies help to access information about a computer. Additionally, both technologies provide local and remote access to management information from the operating system, computer...

Events

Nov 20, 12 AM - Nov 22, 12 AM

Gain the competitive edge you need with powerful AI and Cloud solutions by attending Microsoft Ignite online.

Register now