

# SOLARWINDS TECHNICAL REFERENCE

## Windows Management Instrumentation Troubleshooting for Orion APM

Why do my APM WMI Monitors Show Status Unknown? .....	1
WMI Troubleshooting Flowchart for Orion APM	2
Testing Local WMI Services.....	3
Test WMI on the Target Server .....	3
Reset the WMI Counters.....	6
Testing Remote WMI Connectivity.....	6
Remotely Test WMI on the Target Server ....	6
Verify Administrator Credentials .....	9
Enable Remote Procedure Call (RPC) .....	9
Configure Distributed Component Object Model (DCOM) and User Account Control (UAC) .....	9
Add a Windows Firewall Exception for Remote WMI Connections .....	11
Verify APM Component Configuration .....	12
WMI is Still Not Working, Now What? .....	12

The following document troubleshoots environmental and connectivity issues that may be preventing Orion APM from retrieving WMI Performance Counter data for monitored nodes, applications, and services.

Copyright© 1995-2008 SolarWinds, Inc. All rights reserved worldwide. No part of this document may be reproduced by any means nor modified, decompiled, disassembled, published or distributed, in whole or in part, or translated to any electronic medium or other means without the written consent of SolarWinds. All right, title and interest in and to the software and documentation are and shall remain the exclusive property of SolarWinds and its licensors. SolarWinds Orion™, SolarWinds Cirrus™, and SolarWinds Toolset™ are trademarks of SolarWinds and SolarWinds.net® and the SolarWinds logo are registered trademarks of SolarWinds All other trademarks contained in this document and in the Software are the property of their respective owners.

SOLARWINDS DISCLAIMS ALL WARRANTIES, CONDITIONS OR OTHER TERMS, EXPRESS OR IMPLIED, STATUTORY OR OTHERWISE, ON SOFTWARE AND DOCUMENTATION FURNISHED HEREUNDER INCLUDING WITHOUT LIMITATION THE WARRANTIES OF DESIGN, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL SOLARWINDS, ITS SUPPLIERS OR ITS LICENSORS BE LIABLE FOR ANY DAMAGES, WHETHER ARISING IN TORT, CONTRACT OR ANY OTHER LEGAL THEORY EVEN IF SOLARWINDS HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Microsoft® and Windows 2000® are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Graph Layout Toolkit and Graph Editor Toolkit © 1992 - 2001 Tom Sawyer Software, Oakland, California. All Rights Reserved.

Portions Copyright © ComponentOne, LLC 1991-2002. All Rights Reserved.

Document Revised: 9/16/2008

## Why do my APM WMI Monitors Show Status Unknown?

To monitor APM applications containing WMI component monitors, the following conditions must be true:

- WMI on the remote server is enabled and functioning properly.
- The remote server is accessible through a RPC connection in order to run the WMI queries.

If these conditions cannot be met, the WMI component monitors in APM show an Unknown status. Examples of some issues that can prevent these conditions from being met include, but are not limited to:

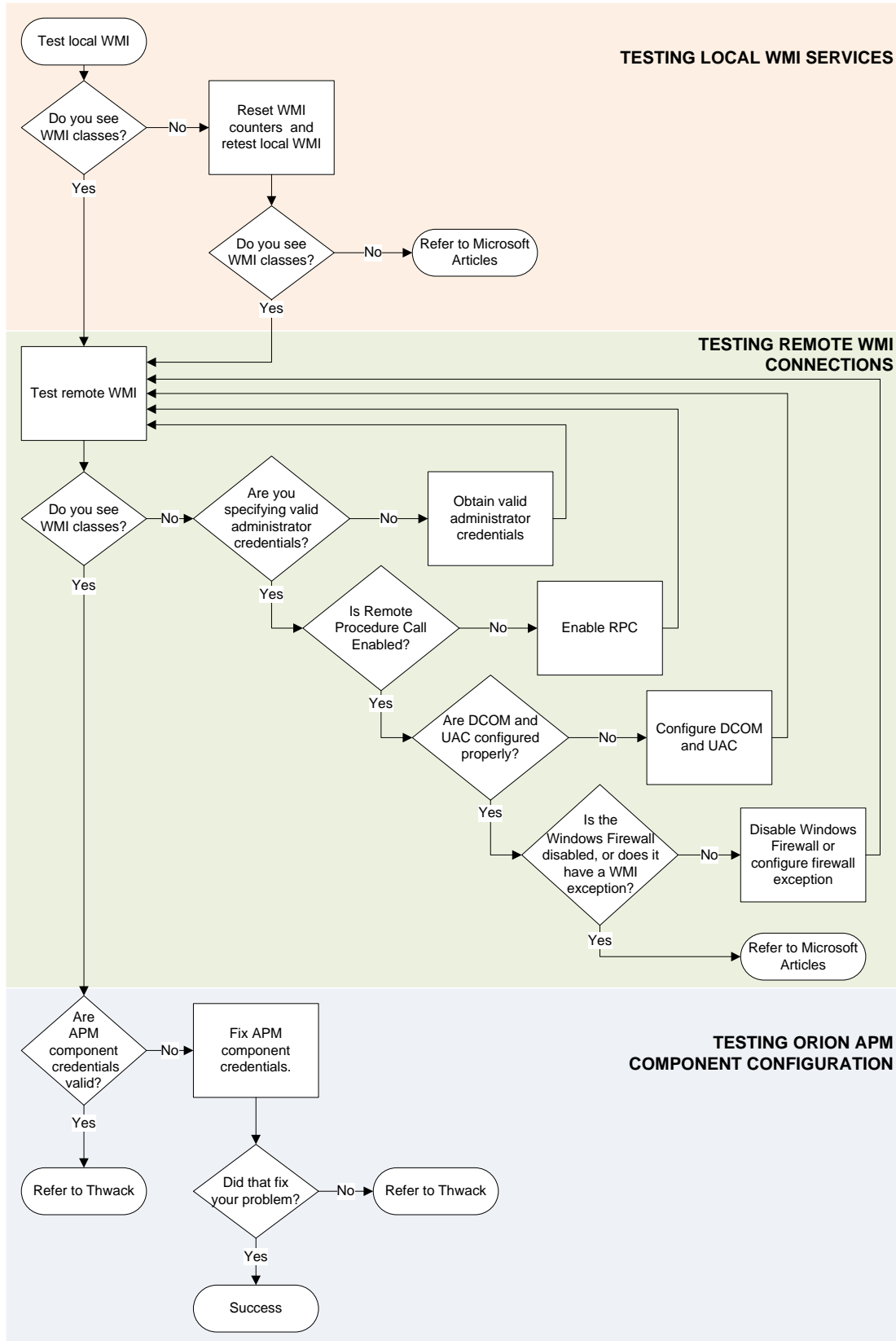
- Trying to connect to a remote computer where you do not have local Administrator rights.
- A firewall blocking the WMI traffic.
- An operating system that is not configured for WMI.
- Mistyping the credential password in the APM component monitor.

To help diagnose and fix these issues and others, we can test the WMI services, the remote WMI connections, and the Orion APM component configuration to discover and correct the issues that can prevent your WMI component monitors from functioning correctly.

The topics in this guide are as follows:

- **WMI Troubleshooting Flowchart for Orion APM.** Provides a flowchart of the troubleshooting decisions described in this guide.
- **Testing Local WMI Services.** Ensures WMI is running correctly on the target computer.
- **Testing Remote WMI Connections.** Ensures the WMI connection to the target computer is not being blocked, ignored, or rejected.
- **Testing Orion APM Component Configuration.** Ensures you are properly configuring the WMI component credentials in Orion APM.

# WMI Troubleshooting Flowchart for Orion APM



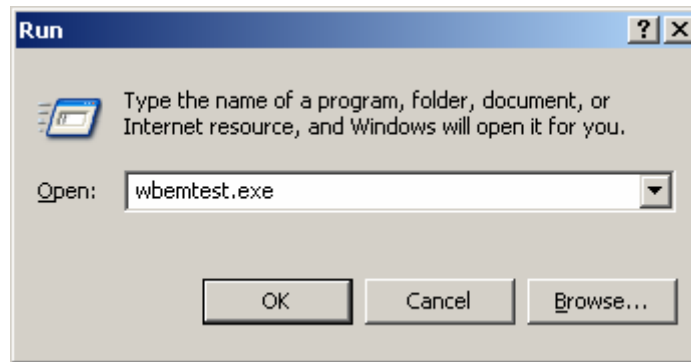
## Testing Local WMI Services

Testing the local WMI services helps us isolate any faults on the target server we are trying to monitor. The testing program is a Microsoft program named WBEMTest that comes already installed on Microsoft Windows operating systems.

### *Test WMI on the Target Server*

Complete the following procedure to check whether WMI on the target server is functioning correctly:

1. Log on to the target server with an administrator account.
2. Click **Start > Run**, enter `wbemtest.exe` and then click **OK**.



3. Click **Connect** on the Windows Management Instrumentation Tester window.

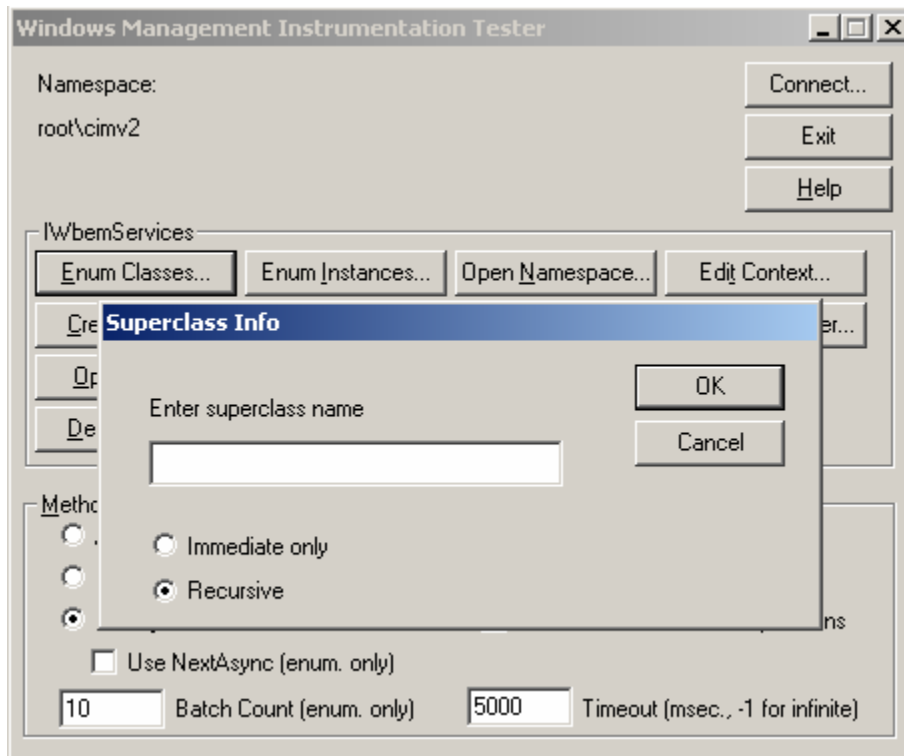
4. Enter `\root\cimv2` in the field at the top of the dialog box next to the **Connect** button.

The screenshot shows a 'Connect' dialog box with the following fields and options:

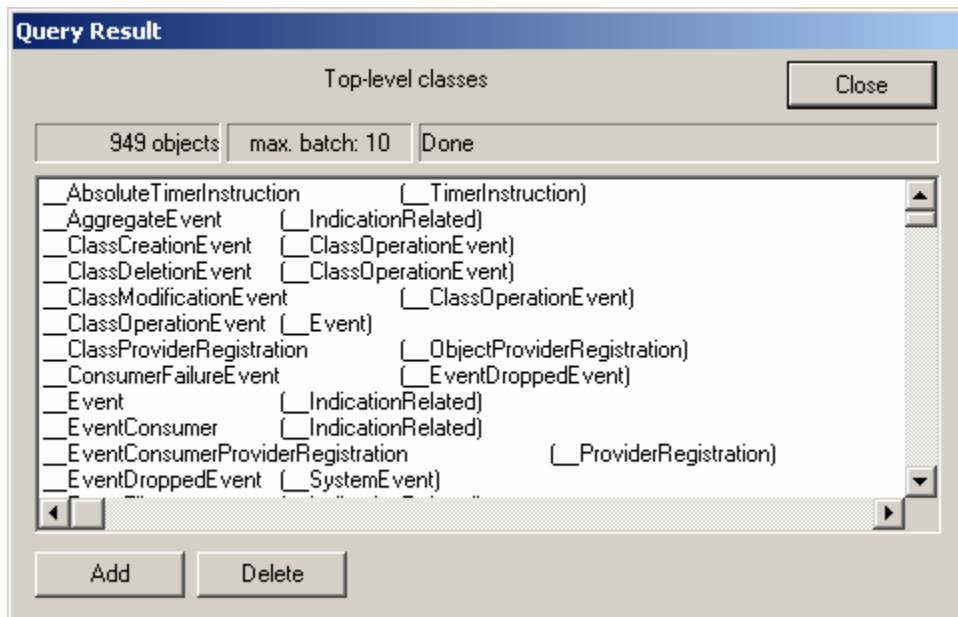
- Text field: `\root\cimv2`
- Buttons: **Connect**, **Cancel**
- Connection:
  - Using: IWBemLocator (Namespaces)
  - Returning: IWBemServices
  - Completion: Synchronous
- Credentials:
  - User: [ ]
  - Password: [ ]
  - Authority: [ ]
- Locale: [ ]
- How to interpret empty password:
  - NULL
  - Blank
- Impersonation level:
  - Identify
  - Impersonate
  - Delegate
- Authentication level:
  - None
  - Packet
  - Connection
  - Packet integrity
  - Call
  - Packet privacy

5. Click **Connect**.
6. Click **Enum Classes**.

8. Select the **Recursive** radio button without entering a superclass name, and then click **OK**.



9. *If the WMI class you are querying appears in this list*, local WMI services are functioning correctly. Skip to the next topic and test remote WMI.



10. *If the list does not appear or does not contain the desired WMI class*, WMI is not functioning correctly. Continue reading this section for guidance on repairing WMI services on the target server.
11. Click the **Close** button, and then click **Exit**.

## Reset the WMI Counters

At times, the WMI performance counters may not get transferred to WMI because services were delayed or started out of order (<http://support.microsoft.com/kb/820847>).

To manually reset the WMI counters:

1. Stop the **Windows Management Instrumentation** service.
2. Click **Start**, click **Run**, type `cmd`, and then click **OK**.
3. At the command prompt, type `winmgmt /resyncperf`, and then press `ENTER`.
4. At the command prompt, type `wmiadap.exe /f`, and then press `ENTER`.
5. Type `exit`, and then press `ENTER` to close the command prompt.
6. Start the **Windows Management Instrumentation** service.

After resetting the WMI counters, retest WMI. If resetting the WMI counters did not solve your problem, see “WMI is Still Not Working, Now What?” on page 12.

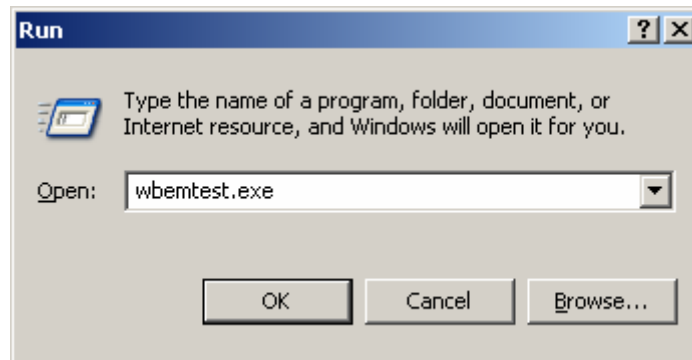
## Testing Remote WMI Connectivity

Testing the remote WMI connectivity of the target server helps us isolate faults that could prevent the target server from receiving or responding to our remote WMI requests. The testing program is a Microsoft program named `WBEMTest` that comes already installed on Microsoft Windows operating systems.

### Remotely Test WMI on the Target Server

Complete the following procedure to check whether the target server is responding appropriately to remote WMI requests that originate from the Orion APM server:

1. Log on to the Orion APM server with an administrator account.
2. Click **Start > Run**, enter `wbemtest.exe` and then click **OK**.



3. Click **Connect** on the Windows Management Instrumentation Tester window.

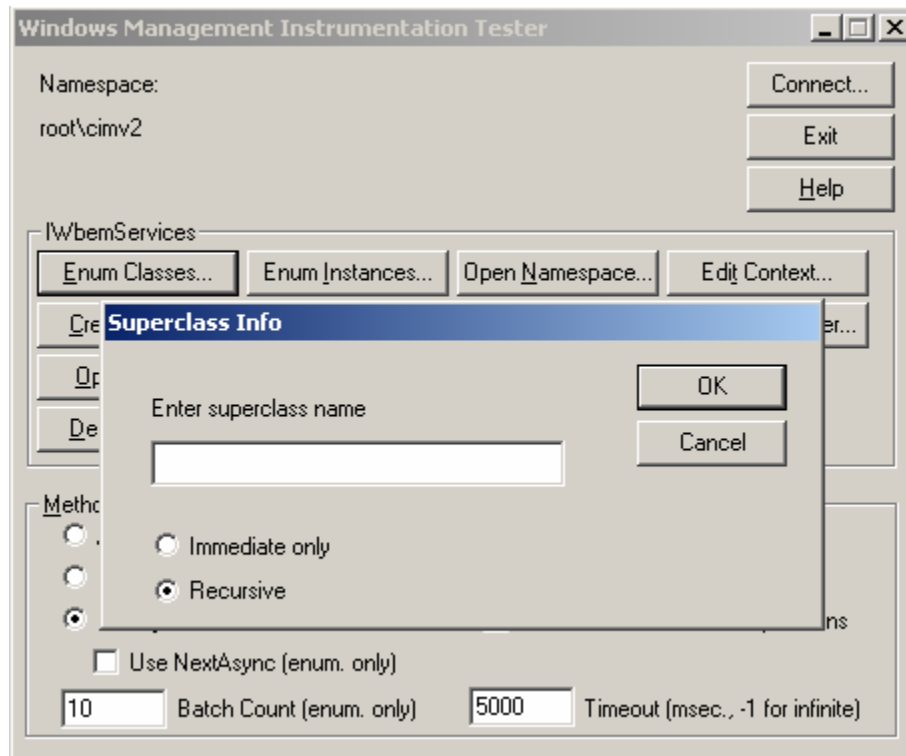
4. Enter `\\Target_Primary_IP_Address\root\cimv2` in the field at the top of the dialog box. Replace *Target\_Primary\_IP\_Address* in the above example with the actual Hostname or Primary IP Address of the target server.

The screenshot shows the 'Connect' dialog box with the following configuration:

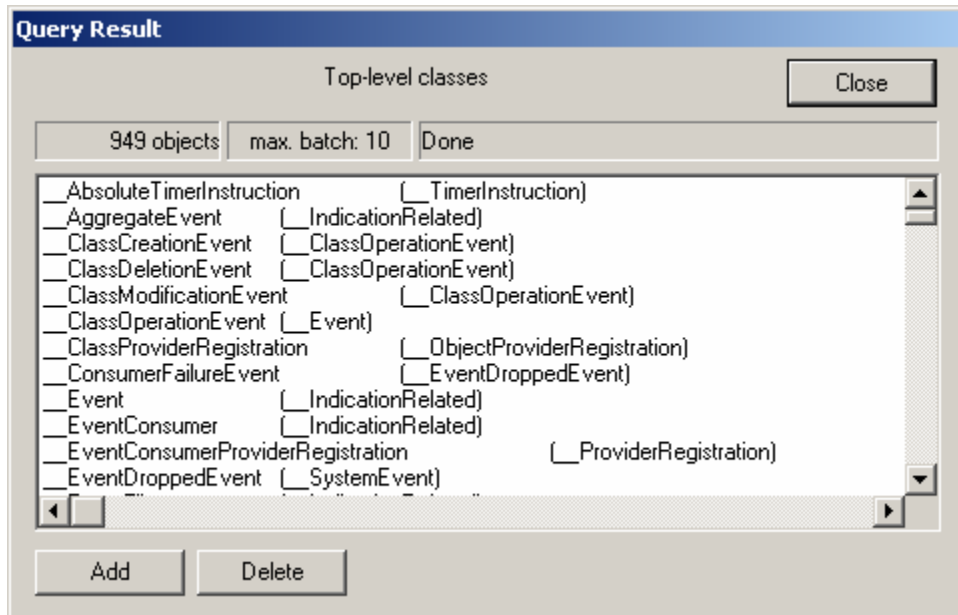
- Path:** \\Target\_Primary\_IP\_Address\root\cimv2
- Connection:**
  - Using: IWBemLocator (Namespaces)
  - Returning: IWBemServices
  - Completion: Synchronous
- Credentials:**
  - User: Administrator
  - Password: \*\*\*\*\*
  - Authority: NTLMDOMAIN:NameOfDomain
- How to interpret empty password:**
  - NULL
  - Blank
- Impersonation level:**
  - Identify
  - Impersonate
  - Delegate
- Authentication level:**
  - None
  - Packet
  - Connection
  - Packet integrity
  - Call
  - Packet privacy

5. Enter the user name in the **User** field, the password in the **Password** field, and `NTLMDOMAIN:NameOfDomain` in the **Authority** field. Replace *NameOfDomain* with the domain of the user account specified in the User field.
6. Click **Connect**.
7. Click **Enum Classes**.

8. Select the **Recursive** radio button without entering a superclass name, and then click **OK**.



9. **If the WMI class list appears**, remote WMI is functioning correctly. Skip to the next topic and test your APM credentials.



10. **If the list does not appear**, remote WMI is not functioning correctly. Continue reading this topic for guidance on restoring remote WMI connections on the target server, and retest remote WMI after completing each troubleshooting step.
11. Click the **Close** button, and then click **Exit**.

### **Verify Administrator Credentials**

Only a credential that has administrator rights on the target server has the necessary permissions to access the target server's WMI services. Make sure that the username and password you are using belongs to an administrator on the target server.

If the administrator credential is a domain member, be sure to specify both the user name and the domain in the standard Microsoft syntax. For example: `DOMAIN\Administrator`.

### **Enable Remote Procedure Call (RPC)**

Remote WMI connections use RPC as a communications interface. If the RPC service is disabled on the target server, remote WMI connections cannot be established.

#### **To enable the RPC service:**

1. Log on to the target server with an administrator account.
2. Click **Start**, click **Run**, type `services.msc`, and then press `ENTER`.
3. Scroll the list to **Remote Procedure Call (RPC)**
4. Right-click **Remote Procedure Call (RPC)**, and then click **Start** on the shortcut menu.

### **Configure Distributed Component Object Model (DCOM) and User Account Control (UAC)**

If the target computer is running Windows Vista or Windows Server 2008, you may be required to make settings changes to allow remote WMI requests ([http://msdn.microsoft.com/en-us/library/aa822854\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa822854(VS.85).aspx)).

<b>Item</b>	<b>Need</b>
DCOM	<p>Default and Limits permissions edited to allow the following actions:</p> <ul style="list-style-type: none"> <li>• Local launch (default permission)</li> <li>• Remote launch (default permission)</li> <li>• Local activation (limits permission)</li> <li>• Remote activation (limits permission)</li> </ul> <p>For more information, see "Enabling DCOM" on page 10.</p>
WMI Namespaces	<p>Modify the CIMV2 security to enable and remote enable the account used to access the server or workstation through WMI. You must ensure the security change applies to the current namespace and subnamespaces. For more information, see "Enabling Account Privileges in WMI" on page 10.</p>
User Account Control	<p>Remote UAC access token filtering must be disabled when monitoring within a workgroup environment. For more information, see "Disabling Remote User Account Control for Workgroups" on page 11.</p>

## Enabling DCOM

WMI uses DCOM to communicate with monitored target computers. Therefore, for Application Performance Monitor to use WMI, DCOM must be enabled and properly configured.

### To enable DCOM permissions for your Application Performance Monitor credentials:

1. Log on to the target server with an administrator account.
2. Navigate to **Start > Control Panel > Administrative Tools > Component Services**. You need to switch to the Classic View of the Control Panel to use this navigation path. You can also launch this console by double-clicking `comexp.msc` in the `/windows/system32` directory.
3. Expand **Component Services > Computers**.
4. Right-click **My Computer**, and then select **Properties**.
5. Select the **COM Security** tab, and then click **Edit Limits** in the Access Permissions grouping.
6. Ensure the user account you want to use to collect WMI statistics has `Local Access` and `Remote Access`, and then click **OK**.
7. Click **Edit Default**, and then ensure the user account you want to use to collect WMI statistics has `Local Access` and `Remote Access`,
8. Click **OK**.
9. Click **Edit Limits** in the Launch and Activation Permissions grouping.
10. Ensure the user account you want to use to collect WMI statistics has `Local Launch`, `Remote Launch`, `Local Activation`, and `Remote Activation`, and then click **OK**.
11. Click **Edit Default**, and then ensure the user account you want to use to collect WMI statistics `Local Launch`, `Remote Launch`, `Local Activation`, and `Remote Activation`.
12. Click **OK**.

## Enabling Account Privileges in WMI

The account you specify in the Credentials Library must possess security access to the namespace and subnamespaces of the monitored target computer. To enable these privileges, complete the following procedure.

### To enable namespace and subnamespaces privileges:

1. Log on to the computer you want to monitor with an administrator account.
2. Navigate to **Start > Control Panel > Administrative Tools > Computer Management > Services and Applications**. You need to switch to the Classic View of the Control Panel to use this navigation path.
3. Click **WMI Control**, and then right-click and select **Properties**.
4. Select the **Security** tab, and then expand **Root** and click **CIMV2**.
5. Click **Security** and then select the user account used to access this computer and ensure you grant the following permissions:
  - `Enable Account`
  - `Remote Enable`
6. Click **Advanced**, and then select the user account used to access this computer.
7. Click **Edit**, select `This namespace and subnamespaces` in the **Apply to** field, and then click **OK**.

8. Click **OK** on the Advanced Security Settings for CIMV2 window.
9. Click **OK** on the Security for Root\CIMV2 window.
10. Click **Services** in the left navigation pane of Computer Management.
11. Select `Windows Management Instrumentation` in the Services result pane, and then click **Restart**.

## Disabling Remote User Account Control for Workgroups

If you are monitoring a target in a workgroup, you need to disable remote User Account Control (UAC). This is not recommended, but it is necessary when monitoring a workgroup computer. Disabling remote user account control does not disable local user account control functionality.

**Warning:** The following procedure requires the modification or creation of a registry key. Changing the registry can have adverse effects on your computer and may result in an unbootable system. Consider backing up your registry before making these changes.

### To disable remote UAC for a workgroup computer:

1. Log on to the computer you want to monitor with an administrator account.
2. Click **Start > Accessories > Command Prompt**.
3. Enter `regedit`.
4. Expand `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System`.
5. Locate or create a DWORD entry named `LocalAccountTokenFilterPolicy` and provide a DWORD value of 1.

**Note:** To re-enable remote UAC, change this value to 0.

## Add a Windows Firewall Exception for Remote WMI Connections

If the target computer has Windows Firewall enabled, it must have a Remote WMI exception to allow remote WMI traffic through ([http://msdn.microsoft.com/en-us/library/aa389286\(VS.85\).aspx](http://msdn.microsoft.com/en-us/library/aa389286(VS.85).aspx)). To add this exception:

1. Click **Start**, click **Run**, type `cmd` and then press `ENTER`.
2. At the command prompt, type `netsh firewall set service RemoteAdmin enable`, and then press `ENTER`.
3. At the command prompt, type `exit`, and then press `ENTER`.

If adding the firewall exception did not solve your problem, see “WMI is Still Not Working, Now What?” on page 12.

## Verify APM Component Configuration

Make sure that the credential you are using for remote WMI is the same credential that you are using in the APM component.

After you click **Set Component Credentials** to set the component credentials, you must also click **Submit** at the bottom of the page.

### Edit "Exchange Server 2000 and 2003 (APM 2.0)" ? Help

#### Application Monitor Template

Template Name:

#### Quick Credentials (optional)

Are most or all of your component credentials the same? Use quick credentials to pre-fill all component credential fields. You can always change component credentials individually.

Choose Credential:

Credential Name:

User Name:

Password:

Confirm Password:

Process Queue Length

RENAME DELETE

Number of Processes

RENAME DELETE

MS IMAP4 Monitor

RENAME DELETE

Add a component

## WMI is Still Not Working, Now What?

This guide depicts only the most common scenarios that can cause WMI services to fail. If you are unable to get WMI services to work by this point, it is time to consult the Microsoft articles on this topic.

"WMI Isn't Working!: Troubleshooting Problems with WMI Scripts and the WMI Service." Microsoft TechNet. <http://www.microsoft.com/technet/scriptcenter/topics/help/wmi.mspx>

"WMI Diagnosis Utility: A New Utility for Diagnosing and Repairing Problems with the WMI Service." Microsoft TechNet. <http://www.microsoft.com/technet/scriptcenter/topics/help/wmidiag.mspx>

"WMI Troubleshooting." Microsoft Developer Network. <http://msdn.microsoft.com/en-us/library/aa394603.aspx>