



Monitoring Windows Systems with WMI

ScienceLogic version 8.10.1

Table of Contents

Introduction	4
Monitoring Windows Devices in the ScienceLogic Platform	5
What is SNMP?	5
What is WMI?	5
PowerPacks	5
Configuring Windows Systems for Monitoring with SNMP	7
Configuring SNMP for Windows Server 2016 and Windows Server 2012	8
Configuring Ping Responses	8
Installing the SNMP Service	9
Configuring the SNMP Service	14
Configuring the Firewall to Allow SNMP Requests	19
Configuring Device Classes for Windows Server 2016 and Windows 10	19
Manually Align the Device Class	20
Edit the Registry Key	20
Configuring SNMP for Windows Server 2008	21
Configuring Ping Responses	21
Installing the SNMP Service	22
Configuring the SNMP Service	25
Configuring the Firewall to Allow SNMP Requests	30
Configuring SNMP for Windows Desktop Systems	30
Enabling SNMP on Windows Desktop Systems	31
Additional Steps for Configuring SNMP for Windows 10	38
Configuring Windows Systems for Monitoring with WMI	39
Configuring WMI on Windows 2008 Servers	40
Step 1: Configuring Services	40
Step 2: Configuring the Windows Firewall	42
Step 3: Configuring a User Account and Permissions	42
Configuring Namespace and DCOM Security Permissions	42
Configuring User Account Control to Allow Elevated Permissions	50
Configuring WMI for Windows Desktop Systems	52
Step 1: Configuring Services	52
Step 2: Configuring Windows Firewall	56
Step 3: Setting the Default Namespace Security	56
Step 4: Setting the DCOM Security Level	62
Step 5: Disabling User Account Control	69
SNMP and WMI Dynamic Applications for Windows Devices	71
SNMP Dynamic Applications	71
WMI Dynamic Applications	72
Microsoft Base Pack	72
Creating SNMP and WMI Credentials for Windows Devices	73
Creating an SNMP Credential	73
Creating a WMI Credential	76
Testing Windows Credentials	78
SNMP Credential Test	78
Basic/Snippet Credential Test	78
Running a Windows Credential Test	78
Monitoring a Windows Cluster	80
Monitoring Windows Clusters in the ScienceLogic Platform	80
Discovering Cluster Nodes	81
Aligning a Dynamic Application with a Cluster Node	81

Disabling Collection of a Dynamic Application on a Device	82
Discovering the Cluster IP Address	83
Aligning Dynamic Applications with the Cluster Device	85
Using a Device Template to Configure Dynamic Applications	86
Automatically Restarting Windows Services	88
What is the Windows Restart Automatic Services PowerPack?	88
Configuring the Windows Restart Automatic Services PowerPack	89
Excluding Automatic Services	90
Viewing the List of Excluded Services	90
Adding an Excluded Service for All Devices	90
Adding an Excluded Service for a Single Device	91
Removing an Excluded Service	91

Introduction

Overview

This manual describes how to monitor Windows systems in the ScienceLogic platform using SNMP and Windows Management Instrumentation (WMI) credentials and Dynamic Applications.

The following sections provide an overview of SNMP and WMI, as well as the PowerPacks you can use to monitor Windows systems the ScienceLogic platform:

<i>Monitoring Windows Devices in the ScienceLogic Platform</i>	5
<i>What is SNMP?</i>	5
<i>What is WMI?</i>	5
<i>PowerPacks</i>	5

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software, which is subject to change without notice to ScienceLogic. ScienceLogic makes every attempt to maintain accurate technical information and cannot be held responsible for defects or changes in third-party vendor software. There is no written or implied guarantee that information contained herein will work for all third-party variants. See the End User License Agreement (EULA) for more information.

Monitoring Windows Devices in the ScienceLogic Platform

The ScienceLogic platform can monitor a Windows device using the following methods:

- Requesting information from the Windows SNMP agent
- Requesting information by executing a remote PowerShell command
- Requesting information from the WMI agent
- Requesting information using the ScienceLogic agent

NOTE: This manual describes how to monitor Windows with SNMP and WMI. For more information about using PowerShell to monitor Windows devices, see the *Monitoring Windows with PowerShell* manual.

For more information about using the ScienceLogic agent to monitor Windows devices, see the *Monitoring Using the ScienceLogic Agent* manual.

What is SNMP?

SNMP (*Simple Network Management Protocol*) is a set of standard protocols for managing diverse computer hardware and software within a TCP/IP network. SNMP is the most common network protocol used by network monitoring and management applications to exchange management information between devices. The ScienceLogic platform uses this protocol and other protocols to collect availability and performance information.

SNMP uses a server-client structure. Clients are called **agents**. Devices and software that run SNMP are agents. The server is called the **management system**. The ScienceLogic platform is the management system.

Most network hardware is configured for SNMP and can be SNMP-enabled. Many enterprise software applications are also SNMP-compliant. When SNMP is running on a device, it uses a standard format to collect and store data about the device and/or software. For example, SNMP might collect information on each network interface and the traffic for each interface. The ScienceLogic platform can then query the device to retrieve the stored data.

What is WMI?

Windows Management Instrumentation, or WMI, is a Windows Service developed to access management information. WMI is a middle-layer technology that enables standardized management of Windows-based computers. It collects computer management data from a wide variety of sources and makes it accessible by using standard interfaces. WMI's specific query language is similar to SQL. For a comparison of WQL and SQL, see <http://technet.microsoft.com/en-us/library/cc180454.aspx>

PowerPacks

This manual describes content from the following PowerPacks:

- *Microsoft Base Pack PowerPack*, version 105.
- *Windows Restart Automatic Services PowerPack*, version 100.

Configuring Windows Systems for Monitoring with SNMP

Overview

The following sections describe how to configure Windows Server 2016, Windows Server 2012, Windows Server 2008, and Windows desktop systems for monitoring by the ScienceLogic platform using SNMP:

Configuring SNMP for Windows Server 2016 and Windows Server 2012	8
Configuring Ping Responses	8
Installing the SNMP Service	9
Configuring the SNMP Service	14
Configuring the Firewall to Allow SNMP Requests	19
Configuring Device Classes for Windows Server 2016 and Windows 10	19
Manually Align the Device Class	20
Edit the Registry Key	20
Configuring SNMP for Windows Server 2008	21
Configuring Ping Responses	21
Installing the SNMP Service	22
Configuring the SNMP Service	25
Configuring the Firewall to Allow SNMP Requests	30
Configuring SNMP for Windows Desktop Systems	30
Enabling SNMP on Windows Desktop Systems	31
Additional Steps for Configuring SNMP for Windows 10	38

Configuring SNMP for Windows Server 2016 and Windows Server 2012

To configure SNMP on a Windows 2016 Server or a Windows 2012 Server, you must:

1. [Configure "ping" responses.](#)
2. [Install the SNMP service.](#)
3. [Configure the SNMP service.](#)
4. [Configure the firewall to allow SNMP requests.](#)
5. [Configure Device Classes.](#) (Windows Server 2016 only)

Configuring Ping Responses

For the ScienceLogic platform to discover a device, including SNMP-enabled devices, the device must meet one of the following requirements:

- The device must respond to an ICMP "Ping" request.
- One of the ports selected in the **Detection Method & Port** field for the discovery session must be open on the device. If the *Default Method* option for the **Detection Method & Port** field is selected, the ScienceLogic platform scans TCP ports 21, 22, 23, 25, and 80.

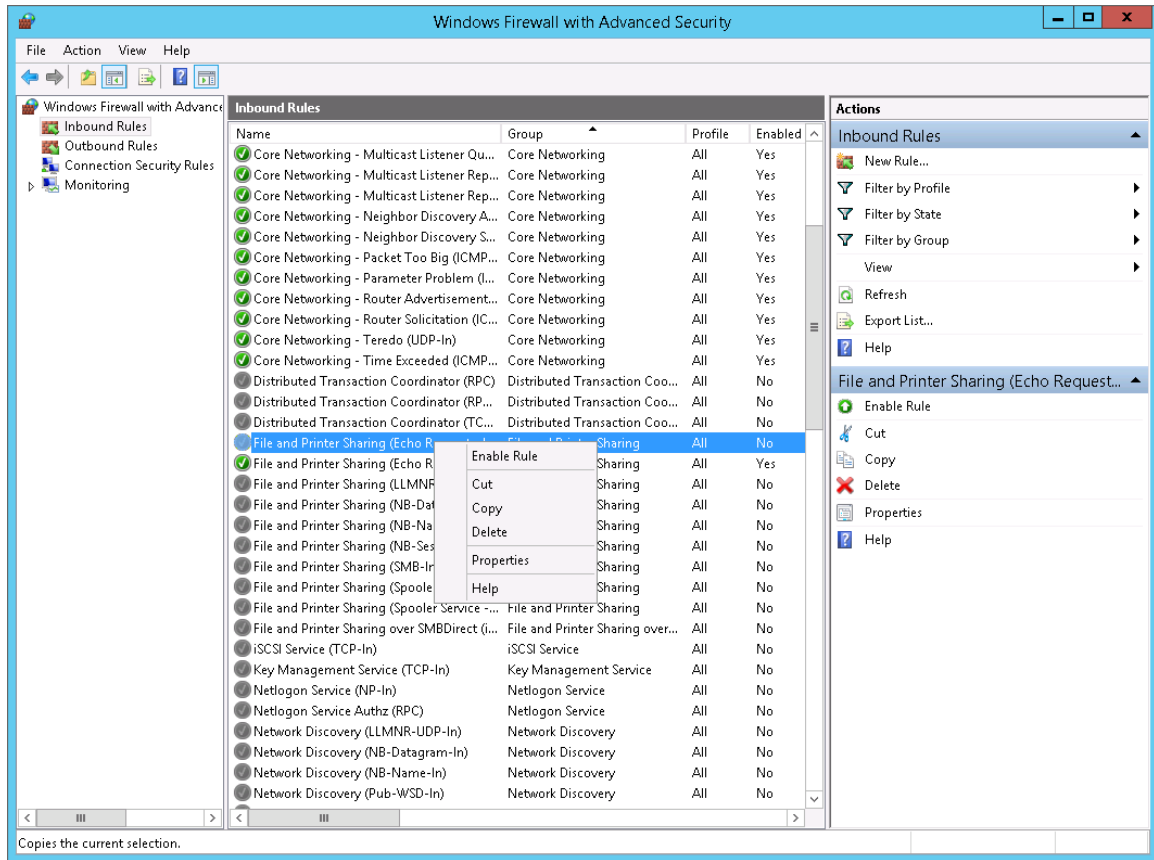
The default configuration for a Windows Server does not allow ICMP "Ping" requests and does not allow connections to TCP ports 21, 22, 23, 25, or 80. Therefore, to discover a Windows Server in the ScienceLogic platform, you must perform one of the following tasks:

- Reconfigure the firewall on the Windows Server to allow ICMP "Ping" requests. This section describes how to perform this task.
- Reconfigure the firewall on the Windows Server to allow connections to port 21, 22, 23, 25, or 80. If you have already configured your Windows Server to accept SSH, FTP, Telnet, SMTP, or HTTP connections, this task might have been completed already. You should perform this task only if you were already planning to allow SSH, FTP, Telnet, SMTP, or HTTP connections to your Windows Server.
- When you create the discovery session that will discover the Windows Server, select at least one port in the **Detection Method & Port** field that is open on the Windows Server. For example, if your Windows Server is configured as an MSSQL Server, you could select port 1433 (the default port for MSSQL Server) in the **Detection Method & Port** field.

To reconfigure the firewall on a Windows Server to allow ICMP "Ping" requests, perform the following steps:

1. In the Start menu search bar, enter "firewall" to open a **Windows Firewall with Advanced Security** window.
2. In the left pane, select *Inbound Rules*.
3. If you want the ScienceLogic platform to discover your Windows Server using an IPv4 address, locate the *File and Printer Sharing (Echo Request - ICMPv4-In)* rule.

4. If you want the ScienceLogic platform to discover your Windows Server using an IPv6 address, locate the *File and Printer Sharing (Echo Request - ICMPv6-In)* rule.
5. Right click on the rule that you located, then select *Enable Rule*:

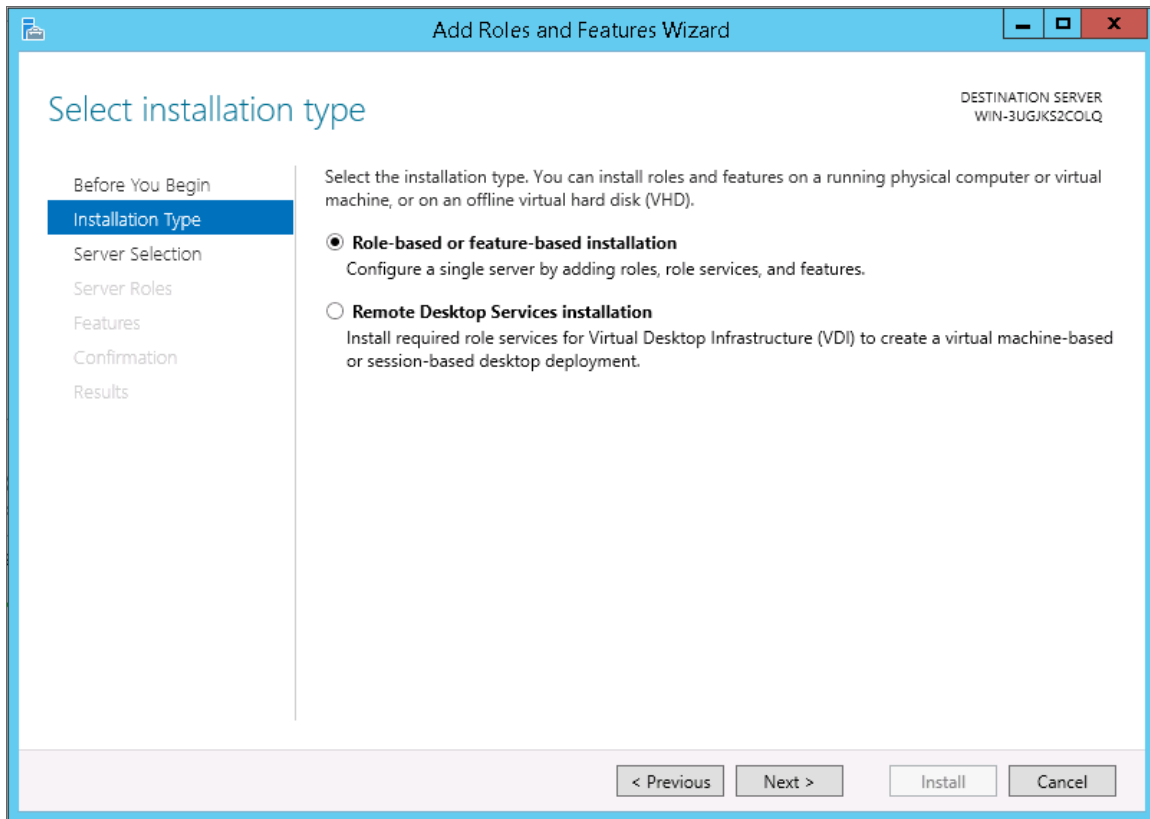


Installing the SNMP Service

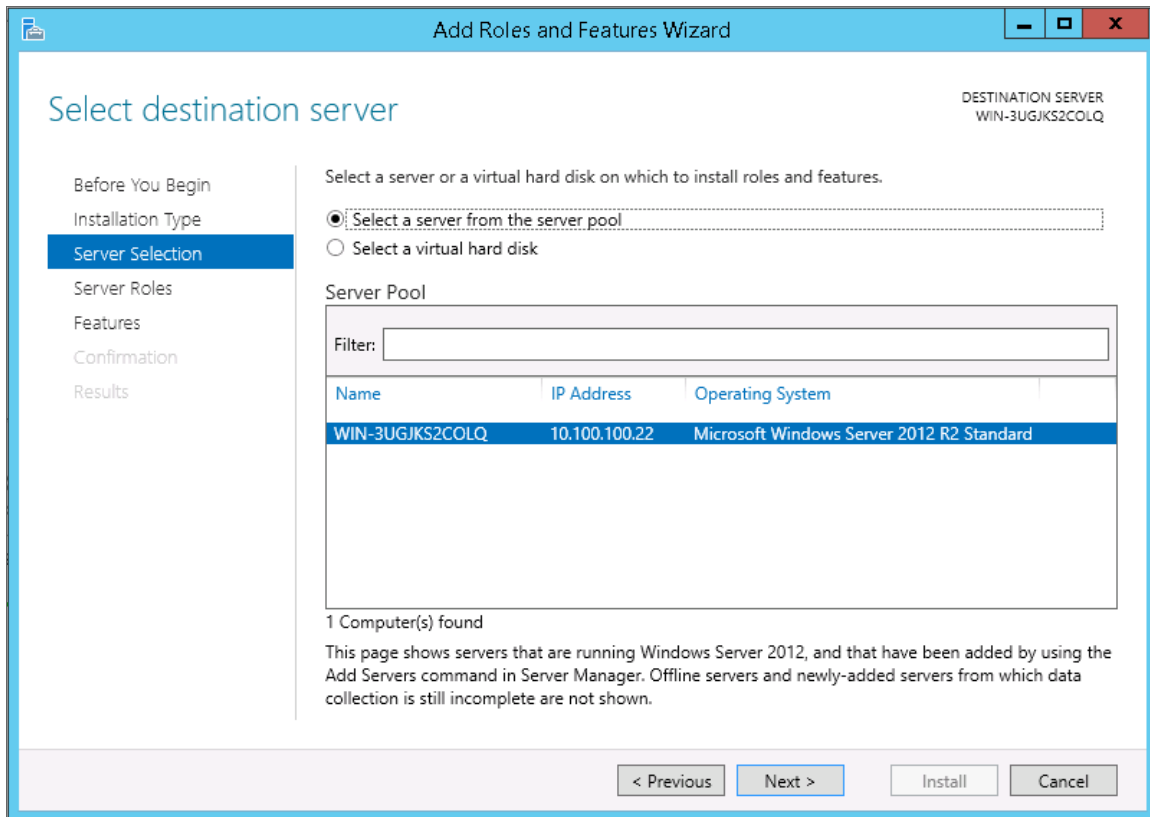
To install the SNMP service on a Windows 2012 Server or Windows 2016 Server, perform the following steps:

1. Open the **Server Manager** utility.
2. In the upper-right of the window, select **[Manage] > Add Roles and Features**. The **Add Roles and Features** window is displayed.

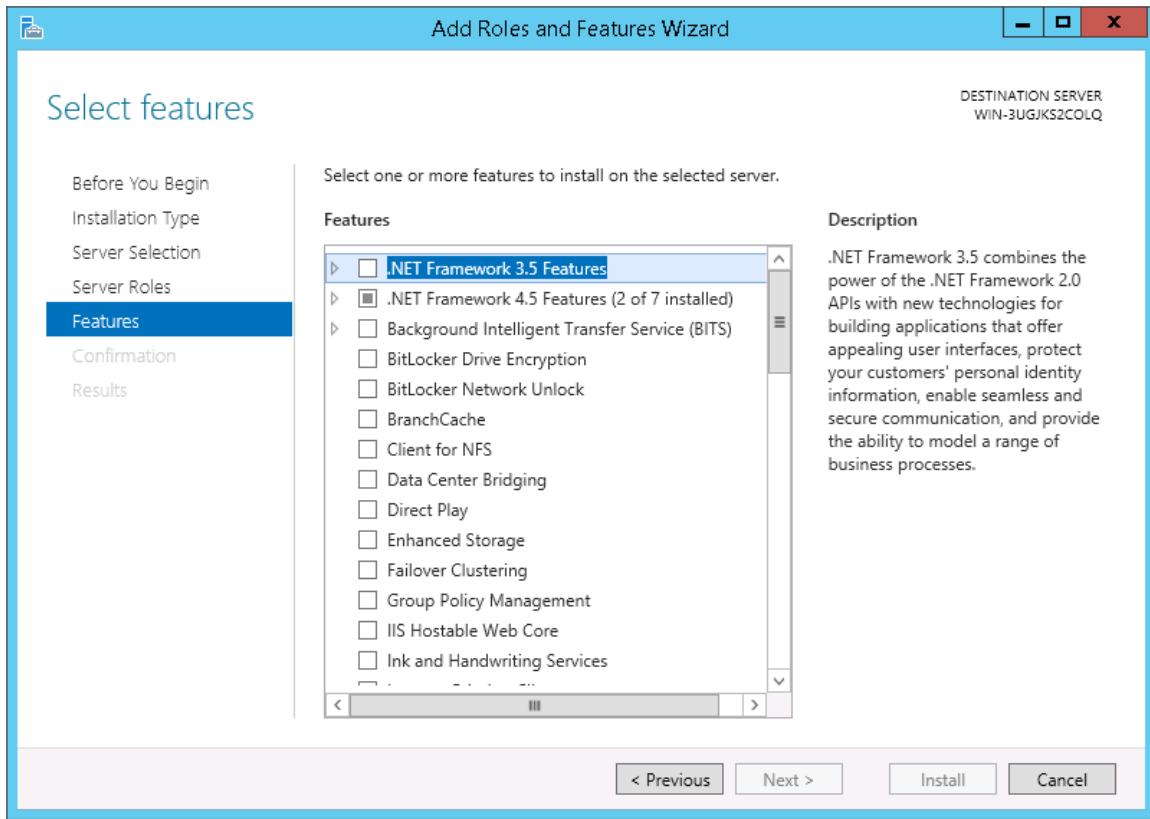
3. If the server does not skip the **Before you begin** page, click the **[Next >]** button to manually skip it. The **Select installation type** page is displayed:



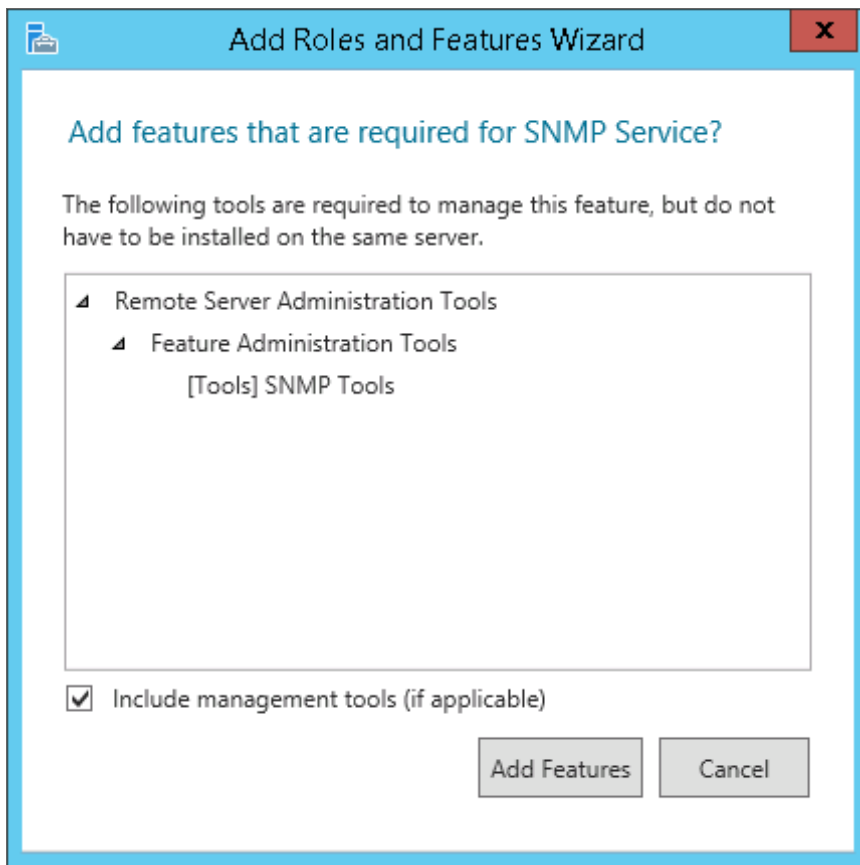
4. Click the **[Next >]** button to continue with *Role-based or feature-based installation*. The **Select destination server** page is displayed:



5. Ensure the Windows 2012 server or Windows 2016 Server is selected and then click the **[Next >]** button. The **Select server roles page** is displayed.
6. Click the **[Next >]** button without selecting any additional roles. The **Select features** page is displayed:

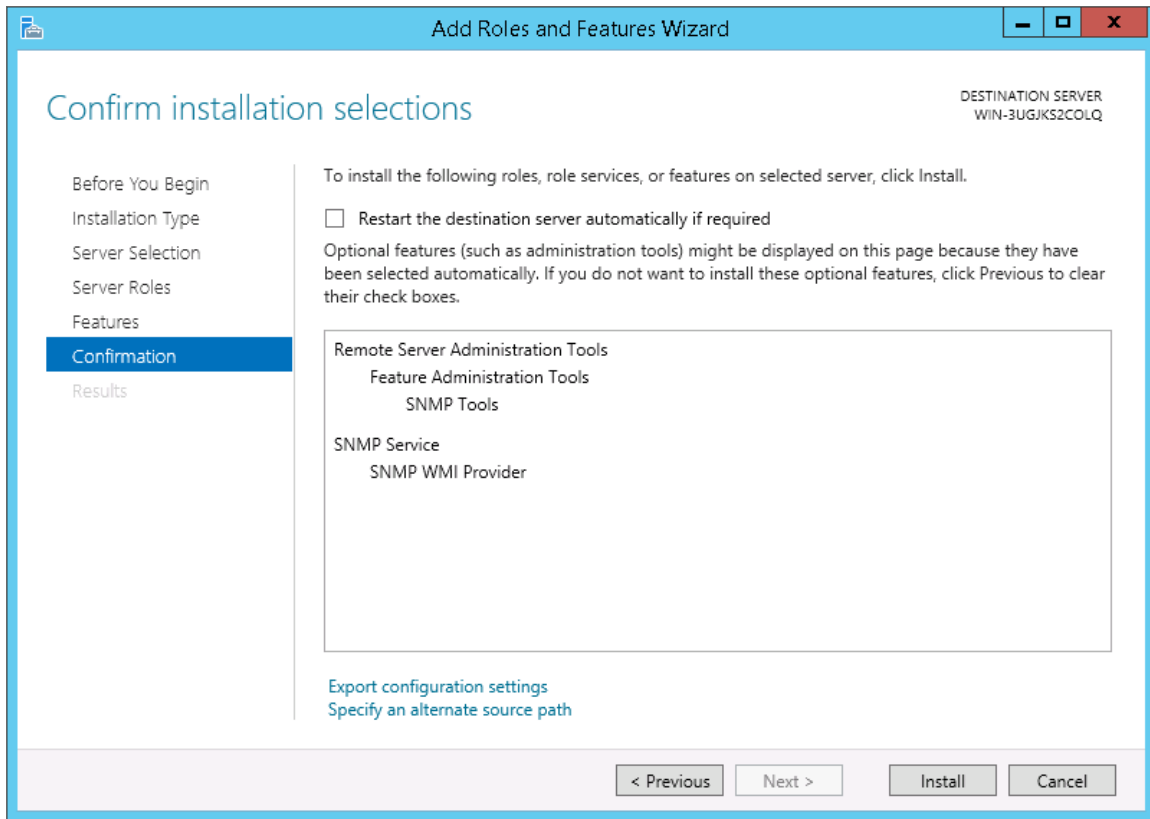


7. Select the *SNMP Service* checkbox. The following confirmation window is displayed:



8. Click the **Add Features** button.
9. In the Select features page, expand *SNMP Service* and select the *SNMP WMI Provider* checkbox.

10. Click the **[Next >]** button. The **Confirm installation selections page** is displayed:



11. Click the **[Install]** button.
12. After the installation is complete, click the **[Close]** button.

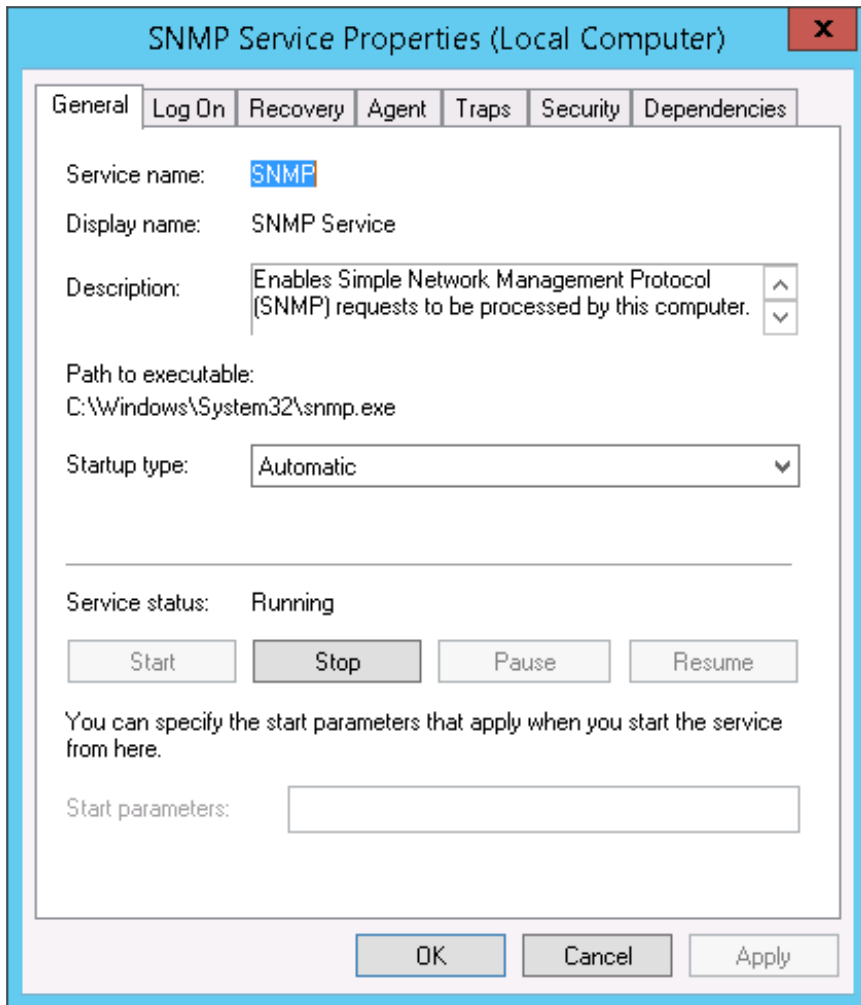
Configuring the SNMP Service

To configure the SNMP service on a Windows 2012 Server or Windows 2016 Server, perform the following steps:

NOTE: If you recently installed the SNMP service, you must wait for the **Server Manager** window to refresh to allow the SNMP service snap-in to be added. You can manually refresh the **Server Manager** window by closing the **Server Manager** and then re-opening the **Server Manager**.

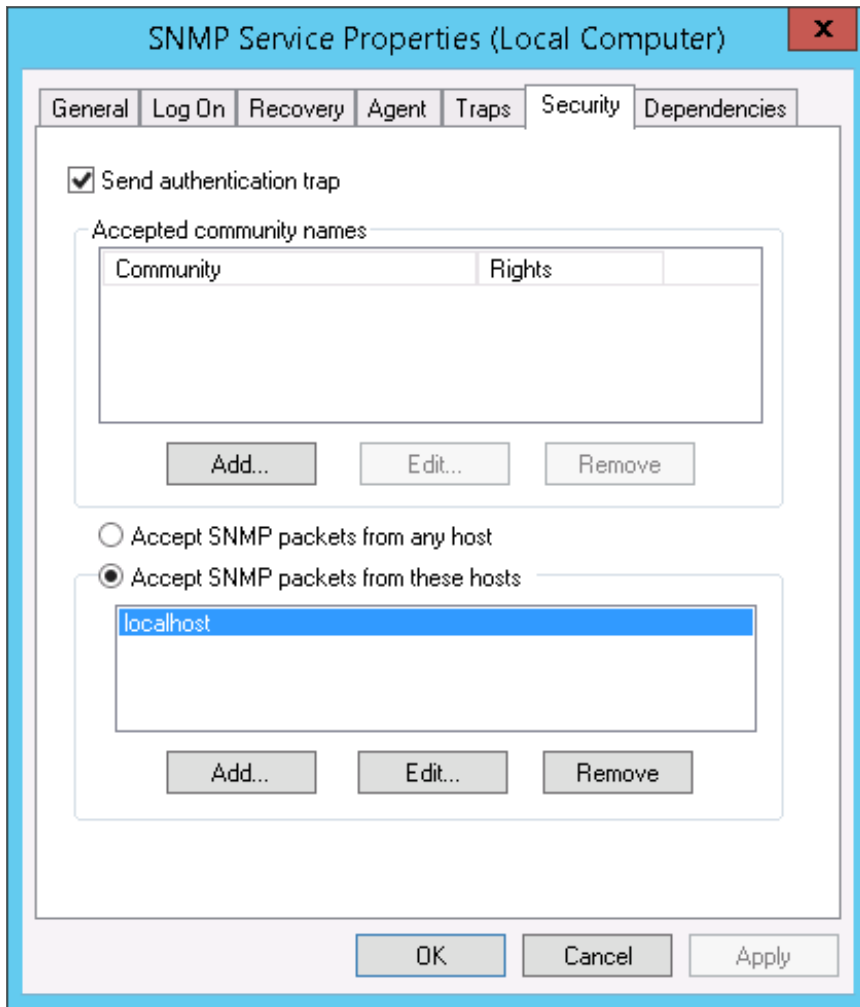
1. In the upper-right of the **Server Manager** window, select **[Tools] > Services**. The **Services** window is displayed.

2. In the **Services** window, right-click on *SNMP Service*, and then select *Properties*. The **SNMP Service Properties** window appears:

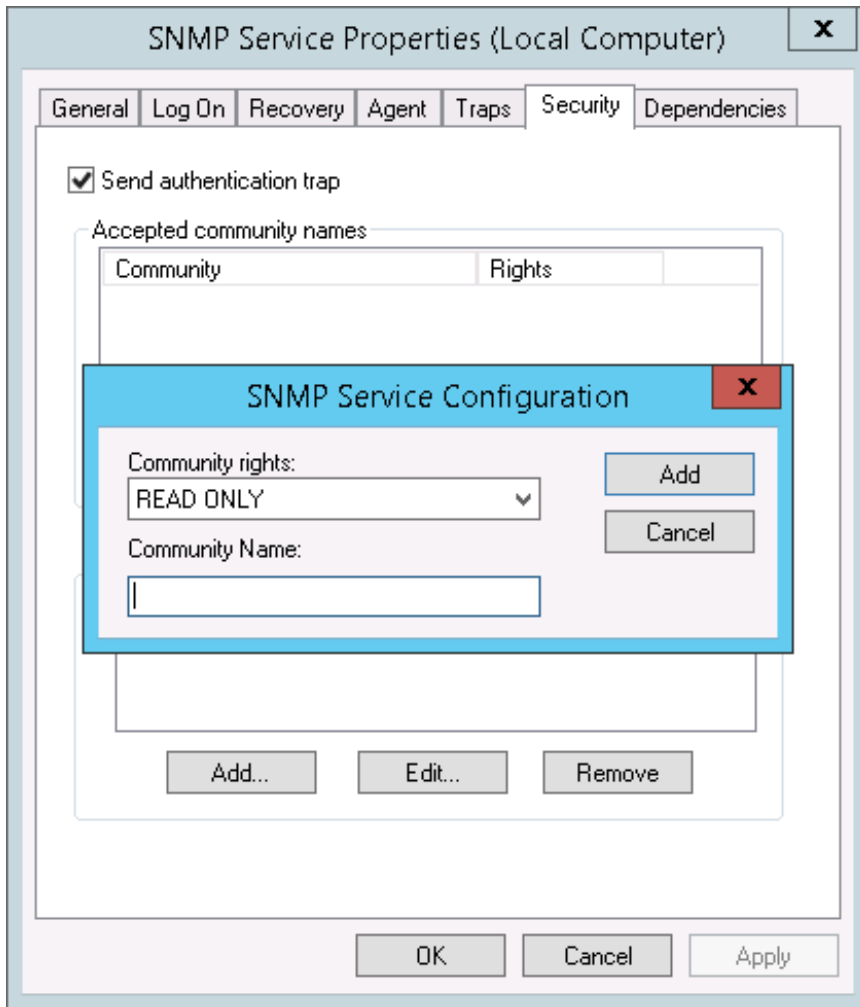


3. In the **Startup type:** field, select *Automatic*.

4. Select the **[Security]** tab. The security settings are displayed:



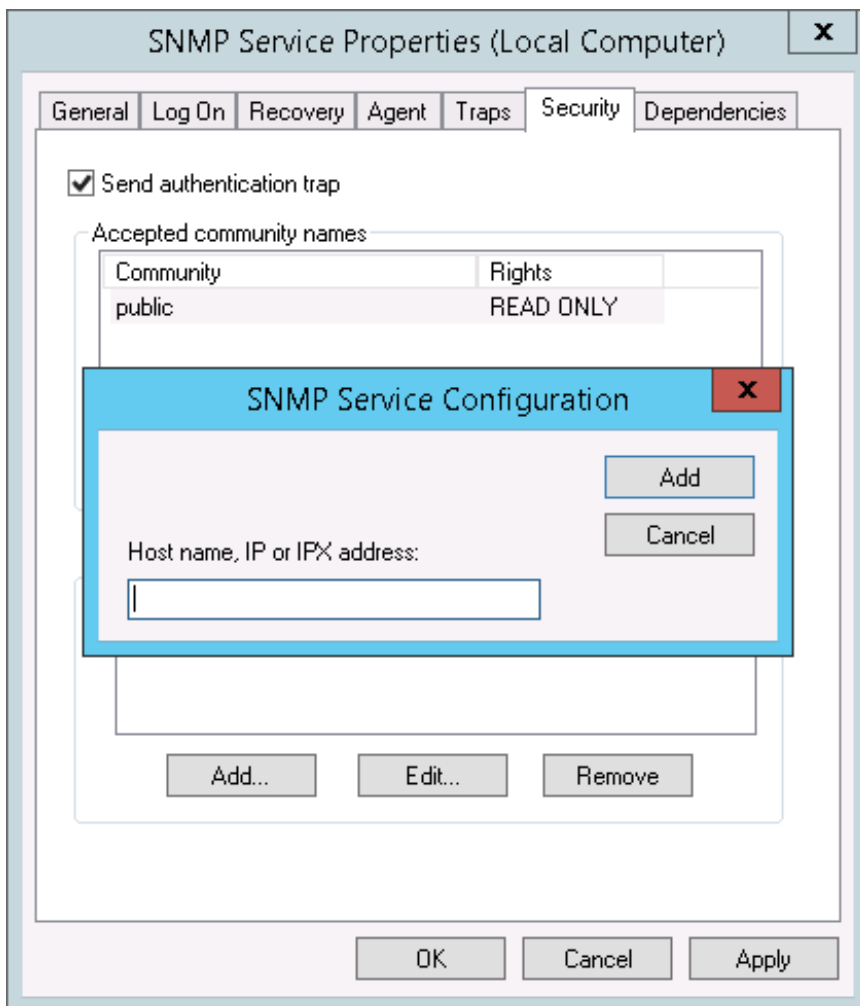
5. In the **Accepted community names** panel, click the **[Add...]** button. The **SNMP Service Configuration** pop-up window is displayed:



6. Enter a value in the following fields:

- **Community rights.** Select one of the following options from the drop-down list:
 - **READ ONLY.** Select this option to allow the ScienceLogic platform to request information from this Windows 2012 Server or Windows 2016 Server using this SNMP community string. This option does not allow the ScienceLogic platform to perform write operations on this Windows 2012 Server or Windows 2016 Server using this SNMP community string.
 - **READ WRITE.** Select this option to allow the ScienceLogic platform to request information from this Windows 2008 server and to perform write operations on this Windows 2012 Server or a Windows 2016 Server using this SNMP community string.

- **Community name.** Enter the SNMP community string that the ScienceLogic platform will use when making SNMP requests to this Windows 2012 Server or Windows 2016 Server. When you create a credential for this Windows 2012 Server or Windows 2016 Server in the ScienceLogic platform, you will enter this community string in one the following fields in the **Credential Editor** modal page:
 - *SNMP Community (Read-Only).* Enter the SNMP community string in this field if you selected *READ ONLY* in the **Community rights** drop-down list.
 - *SNMP Community (Read/Write).* Enter the SNMP community string in this field if you selected *READ WRITE* in the **Community rights** drop-down list.
7. Click the **[Add]** button to add the community string to the list of community strings this Windows 2012 Server or Windows 2016 Server accepts.
 8. In the **Accept SNMP packets from these hosts** panel, click the **Add...** button. The **SNMP Service Configuration** pop-up window is displayed:



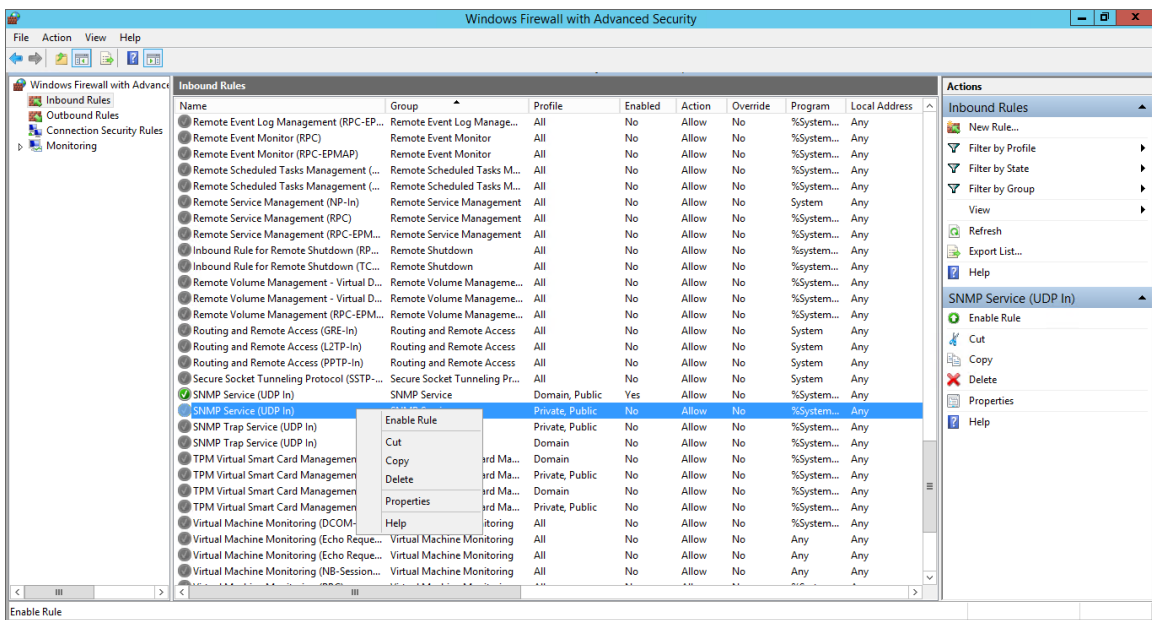
9. In the **Host name, IP or IPX address** field, enter the IP address of the All-In-One Appliance or Data Collector that will monitor this server.

10. Click the **[Add]** button to add the appliance to the list of authorized devices.
11. If you are using the ScienceLogic platform with a distributed architecture, repeat steps 8–10 for each Data Collector in the collector group that will monitor this server.
12. Click the **[Apply]** button to apply all changes.

Configuring the Firewall to Allow SNMP Requests

To configure the Windows Firewall to allow SNMP requests on a Windows 2012 server or Windows 2016 Server, perform the following steps:

1. In the Start menu search bar, enter "firewall" to open a **Windows Firewall with Advanced Security** window.
2. In the left pane, click *Inbound Rules*.
3. Locate the two *SNMP Service (UDP In)* rules.
4. If one or both of the rules is not enabled, right-click on the rule and then select *Enable Rule*:



Configuring Device Classes for Windows Server 2016 and Windows 10

There is a known problem with the Microsoft OID that contains the version number for the operation system. This problem prevents the ScienceLogic platform from using SNMP to automatically align device classes to Windows 10 devices and Microsoft Server 2016 devices.

Because Microsoft has deprecated support of SNMP on Microsoft Server 2016 and Windows 10, users who want to use SNMP to monitor Windows 10 and Microsoft Server 2016 should use one of these workarounds:

- After discovering a Microsoft Server 2016 or Windows 10 device, manually align the device class and disable nightly auto-discovery
- Edit the registry key

Both workarounds are described in the following sections.

Manually Align the Device Class

After discovering Microsoft Server 2016 devices and Windows 10 devices, you can manually align a device class with the discovered devices. To preserve your manual changes, you must disable nightly auto-discovery for those devices. You can manually align the discovered devices with one of these device classes:

- Windows Server 2016
- Windows Server 2016 Domain Controller
- Windows 10 Workstation

For details on manually assigning a device class to a device, follow the steps in the section on *Manually Changing the Device Class for a Device* in the **Device Management** manual chapter on *Managing Device Classes and Device Categories*. For details on disabling nightly auto-discovery for a device, see the section on *Maintaining the New Device Class During Auto-Discovery* in the **Device Management** manual chapter on *Managing Device Classes and Device Categories*.

Edit the Registry Key

You can log in to the device that you want to monitor and manually edit the Windows Registry Key "HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion". You can define the value CurrentVersion as either "2016" or "10.0". To do this:

1. Click the Start menu and choose Run.
2. In the Run dialog box, type regedit and then click OK.
3. Navigate to HKEY_LOCAL_MACHINE\Software\Microsoft\Windows NT\CurrentVersion
4. In the right pane, double click on the Default key.
5. Enter the appropriate value:
 - For Microsoft Server 2016, change the **Value** to 2016
 - For Windows 10, change the **Value** to 10.0

Configuring SNMP for Windows Server 2008

To configure SNMP on a Windows 2008 Server, you must:

1. [Configure "ping" responses.](#)
2. [Install the SNMP service.](#)
3. [Configure the SNMP service.](#)
4. [Configure the firewall to allow SNMP requests.](#)

Configuring Ping Responses

For the ScienceLogic platform to discover a device, including SNMP-enabled devices, the device must meet one of the following requirements:

- The device must respond to an ICMP "Ping" request.
- One of the ports selected in the **Detection Method & Port** field for the discovery session must be open on the device. If the *Default Method* option for the **Detection Method & Port** field is selected, the ScienceLogic platform scans TCP ports 21, 22, 23, 25, and 80.

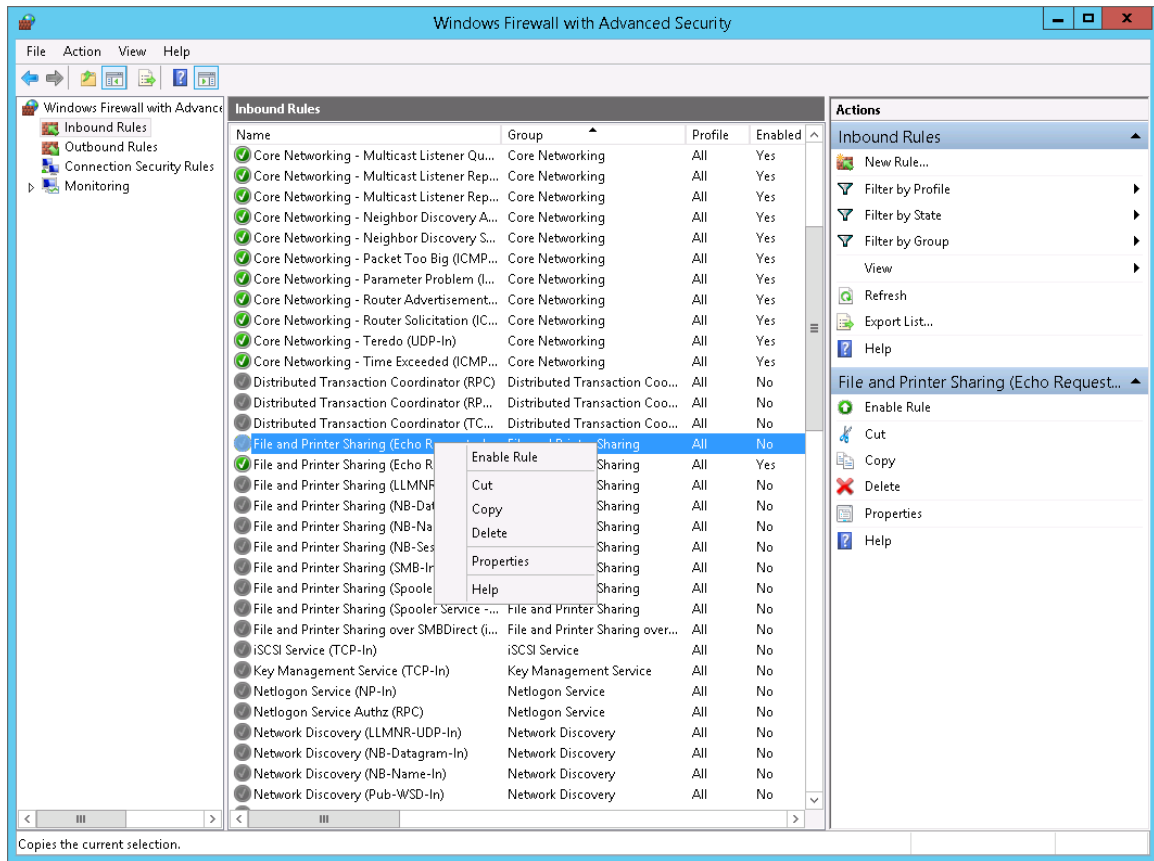
The default configuration for a Windows Server does not allow ICMP "Ping" requests and does not allow connections to TCP ports 21, 22, 23, 25, or 80. Therefore, to discover a Windows Server in the ScienceLogic platform, you must perform one of the following tasks:

- Reconfigure the firewall on the Windows Server to allow ICMP "Ping" requests. This section describes how to perform this task.
- Reconfigure the firewall on the Windows Server to allow connections to port 21, 22, 23, 25, or 80. If you have already configured your Windows Server to accept SSH, FTP, Telnet, SMTP, or HTTP connections, this task might have been completed already. You should perform this task only if you were already planning to allow SSH, FTP, Telnet, SMTP, or HTTP connections to your Windows Server.
- When you create the discovery session that will discover the Windows Server, select at least one port in the **Detection Method & Port** field that is open on the Windows Server. For example, if your Windows Server is configured as an MSSQL Server, you could select port 1433 (the default port for MSSQL Server) in the **Detection Method & Port** field.

To reconfigure the firewall on a Windows Server to allow ICMP "Ping" requests, perform the following steps:

1. In the Start menu search bar, enter "firewall" to open a **Windows Firewall with Advanced Security** window.
2. In the left pane, select *Inbound Rules*.
3. If you want the ScienceLogic platform to discover your Windows Server using an IPv4 address, locate the *File and Printer Sharing (Echo Request - ICMPv4-In)* rule.
4. If you want the ScienceLogic platform to discover your Windows Server using an IPv6 address, locate the *File and Printer Sharing (Echo Request - ICMPv6-In)* rule.

- Right click on the rule that you located, then select *Enable Rule*:

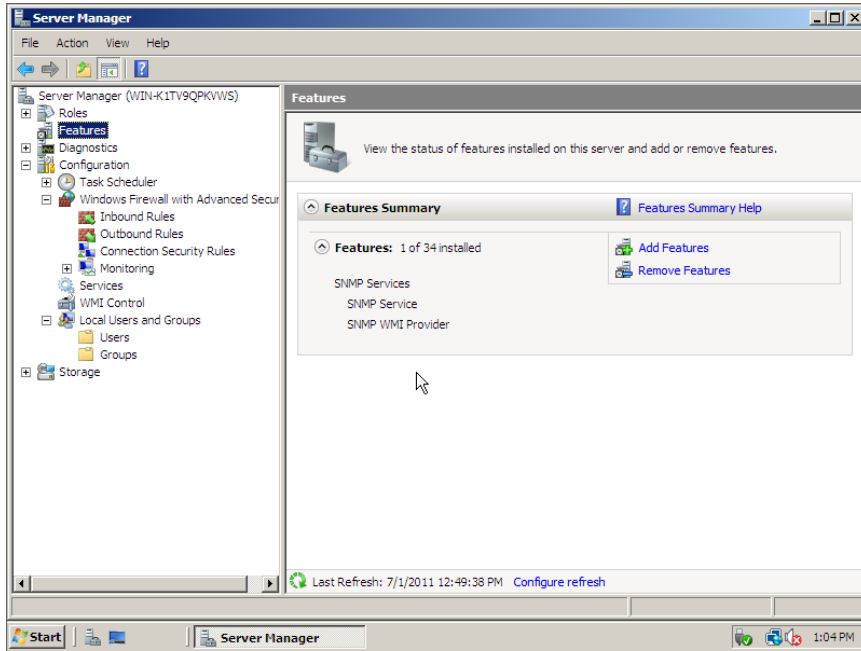


Installing the SNMP Service

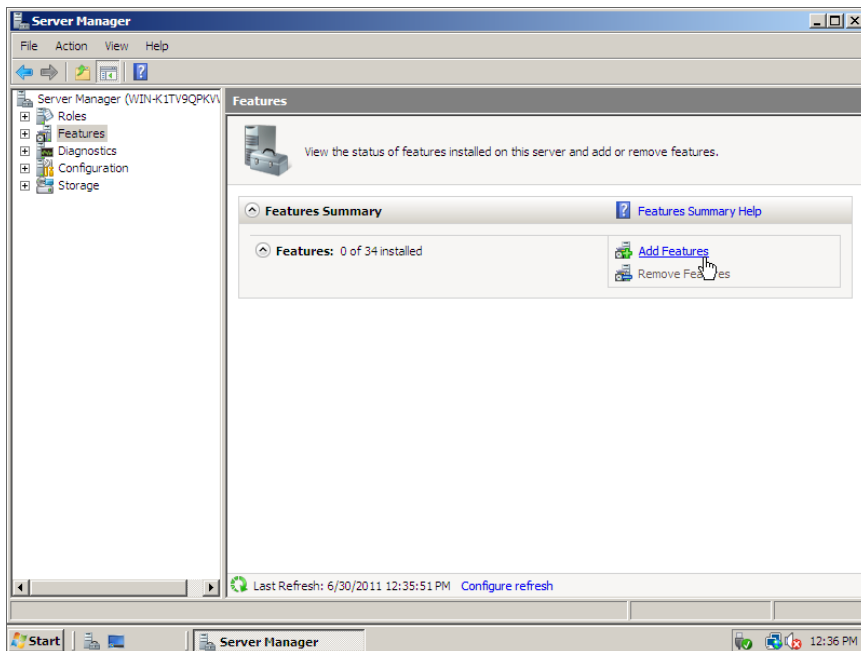
To install the SNMP service on a Windows 2008 Server, perform the following steps:

- Open the **Server Manager** utility.

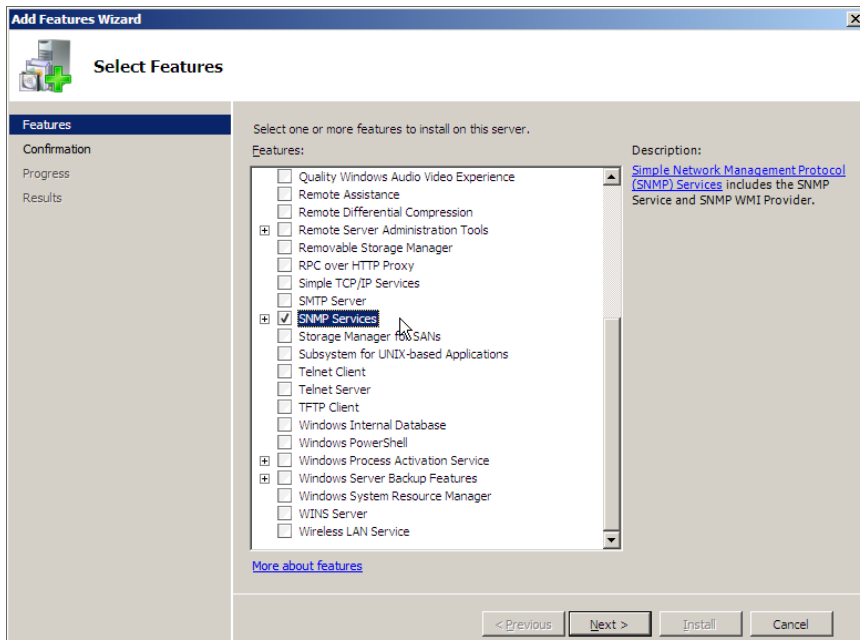
2. In the left pane of the **Server Manager** window, select *Features*. The **Features Summary** is displayed:



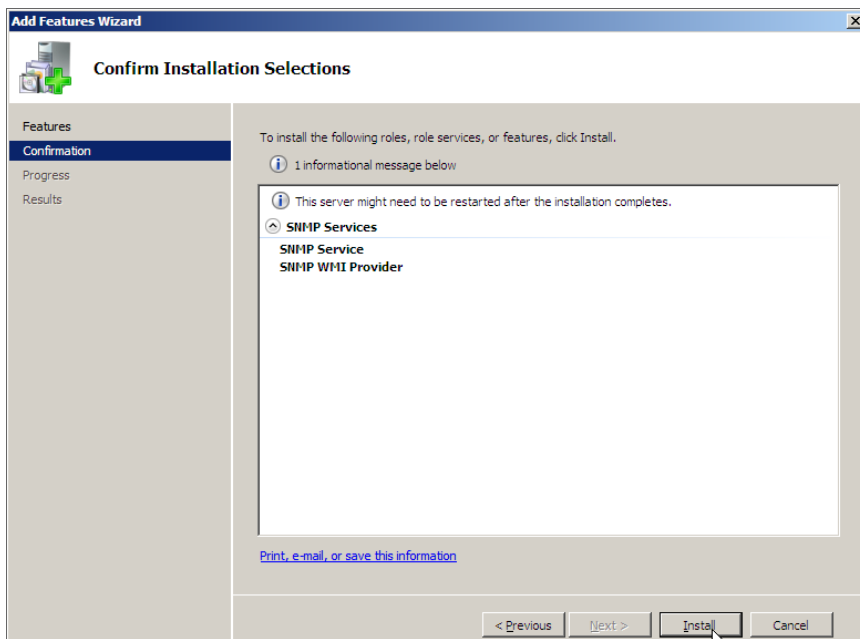
3. If the **Features Summary** displays "SNMP Service" and "SNMP WMI Provider" in the list of installed services (as shown above), you can skip to the section on configuring the SNMP service. If "SNMP Service" and "SNMP WMI Provider" are not included in the list of installed services, select **Add Features**:



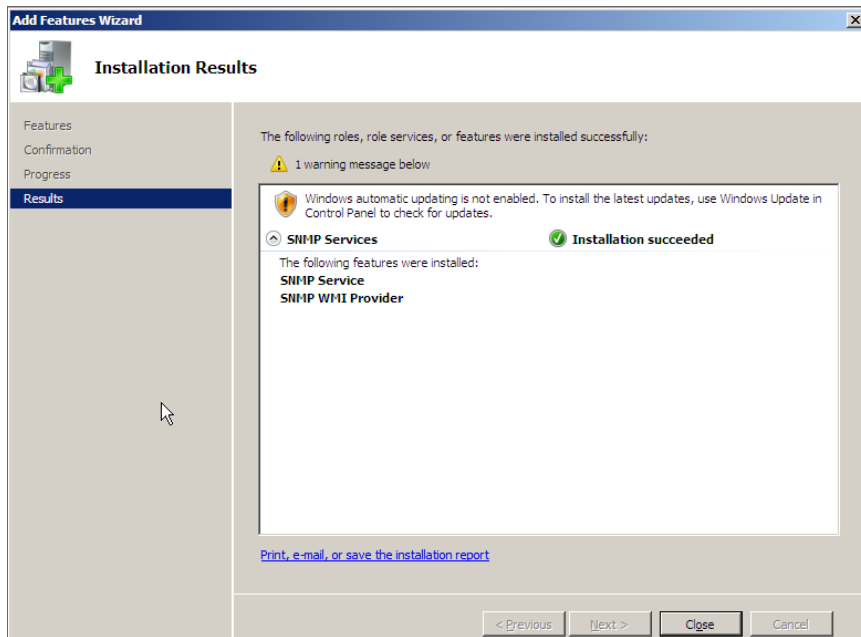
4. In the **Select Features** window, select **SNMP Services**:



5. Click the **[Next >]** button. The **Confirm Installed Selections** window is displayed with "SNMP Service" and "SNMP WMI Provider" in the list of features that will be installed:



6. Click the **[Install]** button. After the installation is completed, the **Installation Results** window will be displayed:



7. Click the **[Close]** button.

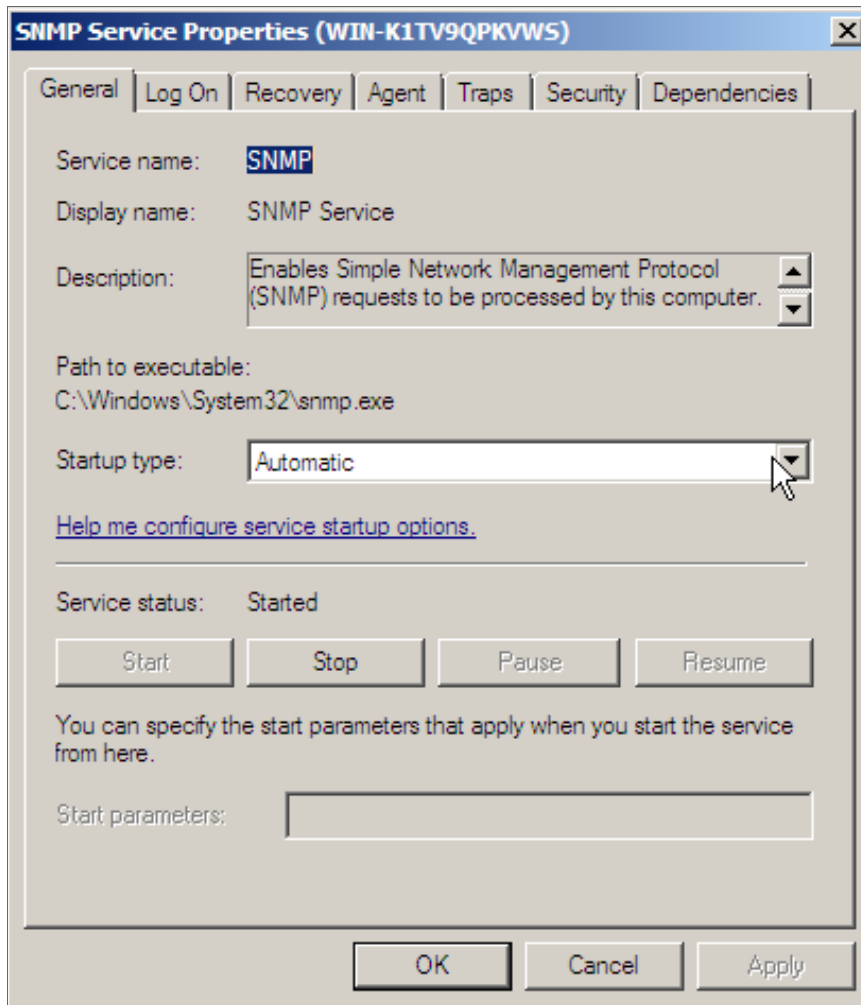
Configuring the SNMP Service

To configure the SNMP service on a Windows 2008 Server, perform the following steps:

NOTE: If you recently installed the SNMP service, you must wait for the **Server Manager** window to refresh before it will display the SNMP service snap-in. You can manually refresh the **Server Manager** window by closing the **Server Manager** and then re-opening the **Server Manager**.

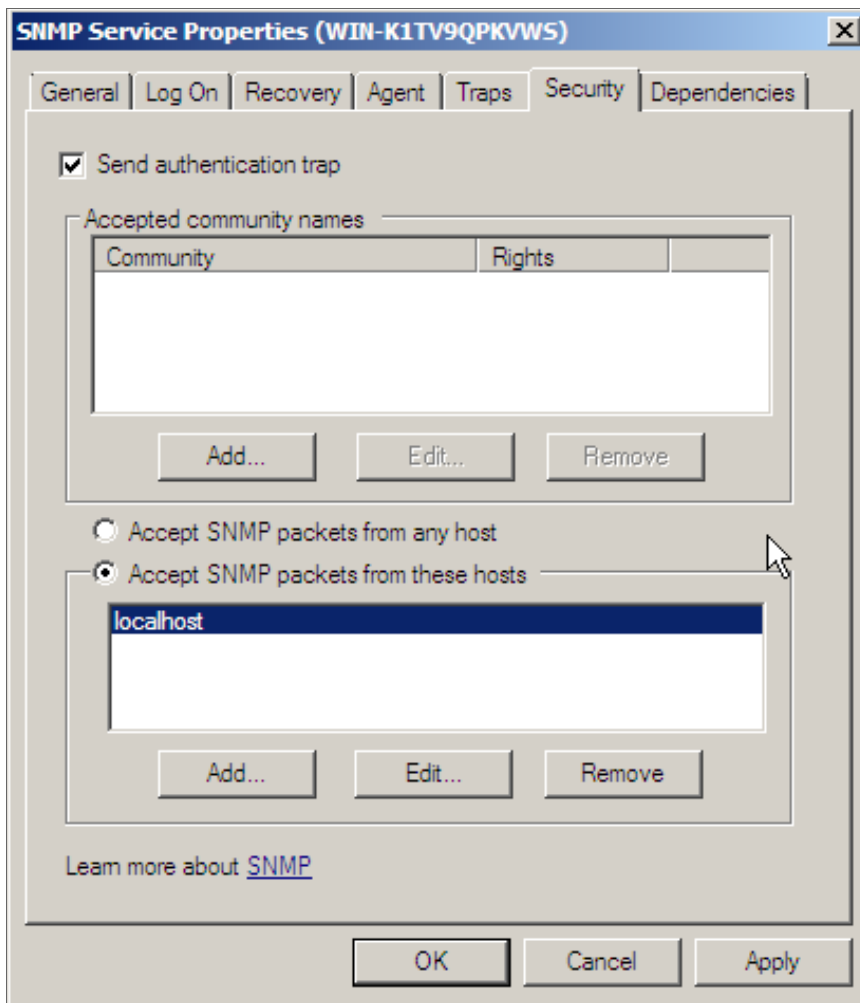
1. In the left pane of the **Server Manager** window, expand the *Configuration* section, and then select *Services*.

2. In the list of services, right-click on *SNMP Service*, and then select *Properties*. The **SNMP Service Properties** window appears:

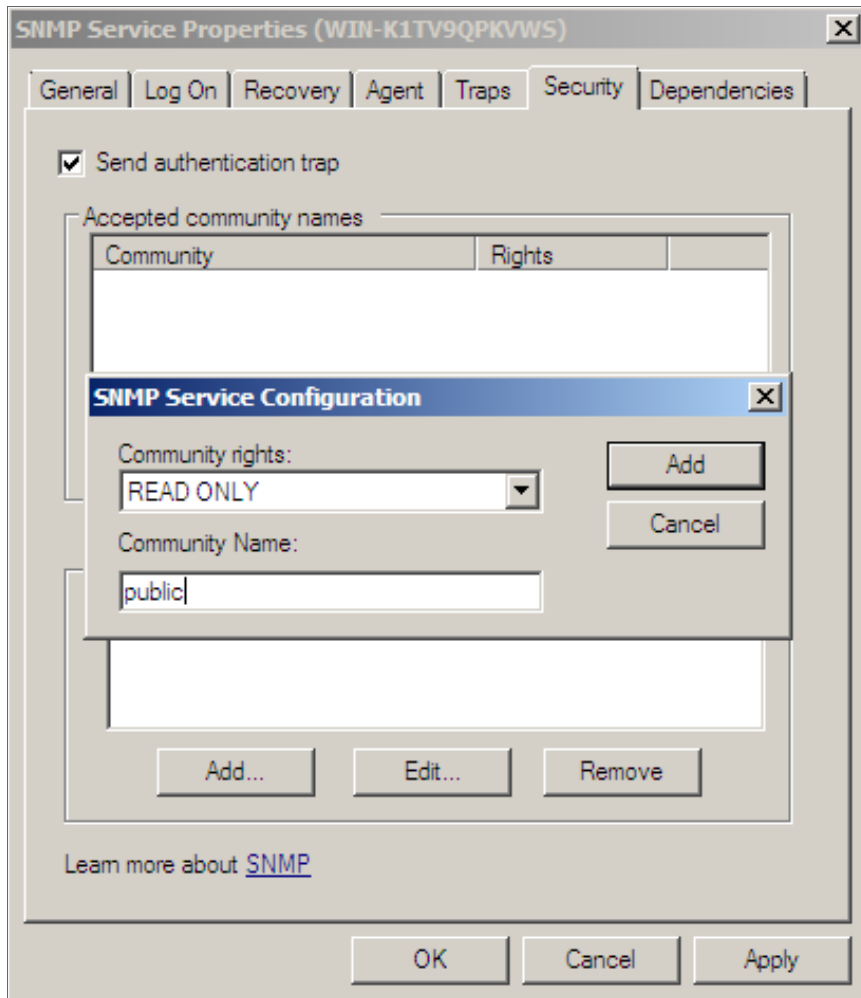


3. In the **Startup type:** field, select *Automatic*.

4. Select the **[Security]** tab. The security settings are displayed:



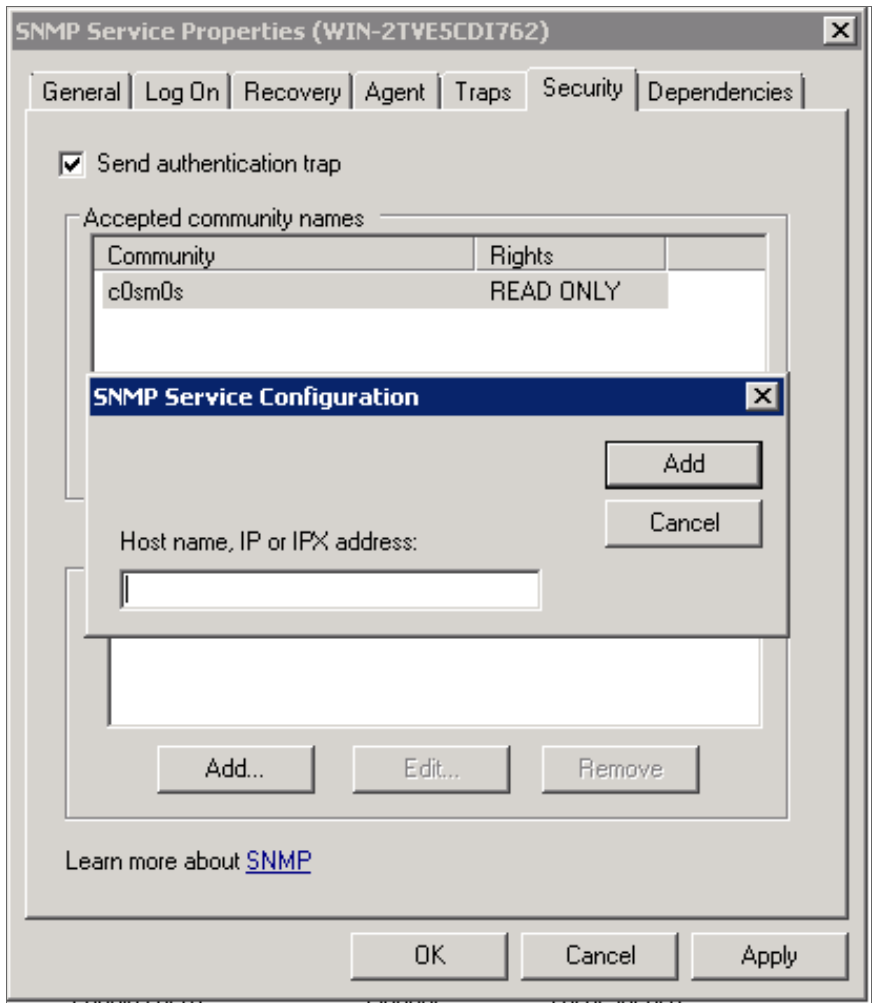
5. In the **Accepted community names** panel, click the **[Add...]** button. The **SNMP Service Configuration** pop-up window is displayed:



6. Enter a value in the following fields:

- **Community rights.** Select one of the following options from the drop-down list:
 - **READ ONLY.** Select this option to allow the ScienceLogic platform to request information from this Windows 2008 Server using this SNMP community string. This option does not allow the ScienceLogic platform to perform write operations on this Windows 2008 Server using this SNMP community string.
 - **READ WRITE.** Select this option to allow the ScienceLogic platform to request information from this Windows 2008 server and to perform write operations on this Windows 2008 Server using this SNMP community string.

- **Community name.** Enter the SNMP community string that the ScienceLogic platform will use to make SNMP requests to this Windows 2008 Server. When you create a credential for this Windows 2008 Server in the ScienceLogic platform, you will enter this community string in one the following fields in the **Credential Editor** modal page:
 - SNMP Community (Read-Only). Enter the SNMP community string in this field if you selected *READ ONLY* in the **Community rights** drop-down list.
 - SNMP Community (Read/Write). Enter the SNMP community string in this field if you selected *READ WRITE* in the **Community rights** drop-down list.
7. Click the **[Add]** button to add the community string to list of community strings this Windows 2008 Server accepts.
 8. In the **Accept SNMP packets from these hosts** panel, click the **Add...** button. The **SNMP Service Configuration** pop-up window is displayed:



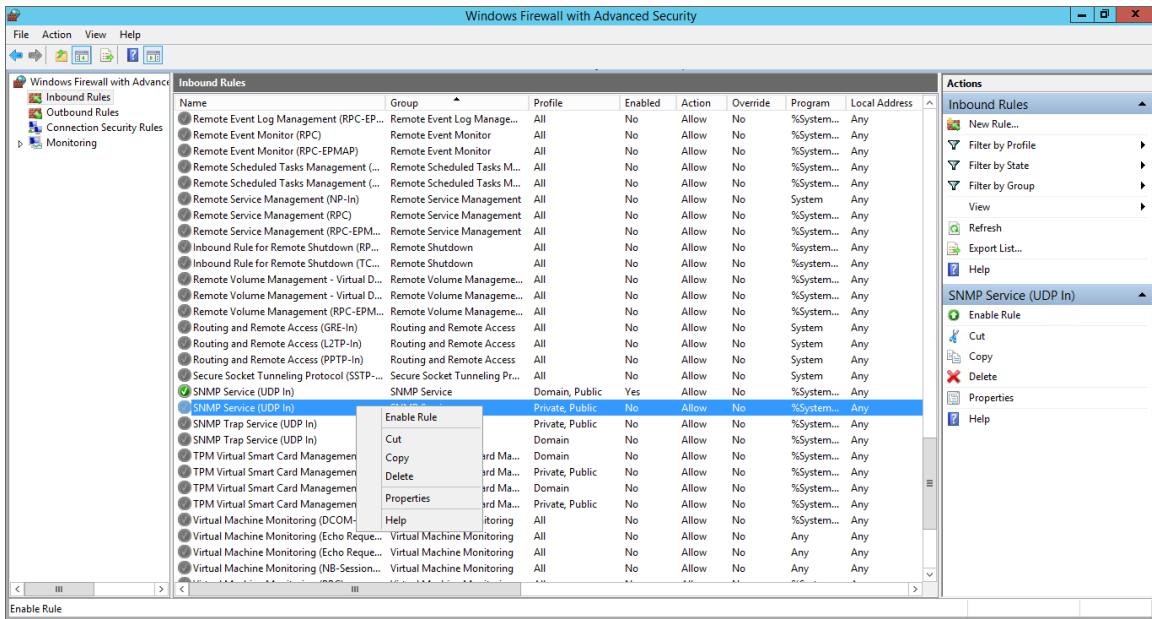
9. In the **Host name, IP or IPX address** field, enter the IP address of the All-In-One Appliance or Data Collector that will monitor this server.

10. Click the **[Add]** button to add the appliance to the list of authorized devices.
11. If you are using the ScienceLogic platform with a distributed architecture, repeat steps 8–10 for each Data Collector in the collector group that will monitor this server.
12. Click the **[Apply]** button to apply all changes.

Configuring the Firewall to Allow SNMP Requests

To configure the Windows Firewall to allow SNMP requests on a Windows 2008 server, perform the following steps:

1. In the Start menu search bar, enter "firewall" to open a **Windows Firewall with Advanced Security** window.
2. In the left pane, click *Inbound Rules*.
3. Locate the two *SNMP Service (UDP In)* rules.
4. If one or both of the rules is not enabled, right-click on the rule and then select *Enable Rule*:



Configuring SNMP for Windows Desktop Systems

This section describes how to configure devices that are running a desktop version of the Windows operating system for monitoring by the ScienceLogic platform using SNMP.

Before performing the tasks described in this section, you must know the IP address of each ScienceLogic appliance in your network. If you have not installed a ScienceLogic appliance, you must know the future IP address that will be used by each ScienceLogic appliance.

NOTE: To be monitored by the ScienceLogic platform, a Windows device must be running the Windows 7 operating system or later.

NOTE: TCP/IP must be installed and configured before you can install SNMP on a Windows device.

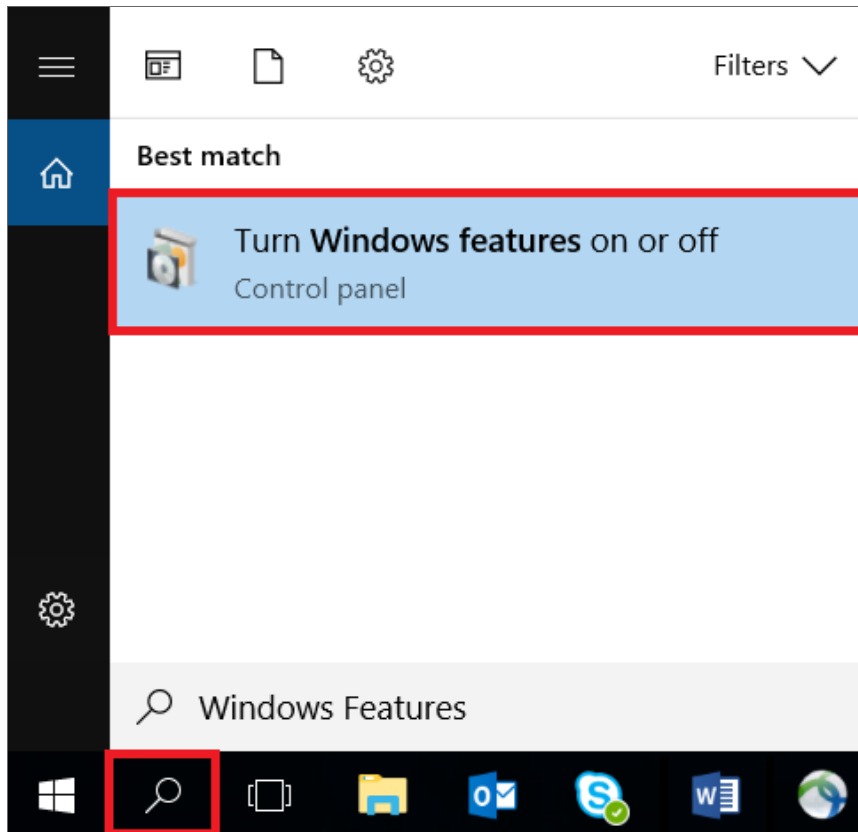
Enabling SNMP on Windows Desktop Systems

You must enable SNMP on each Windows device that you want to monitor with the ScienceLogic platform.

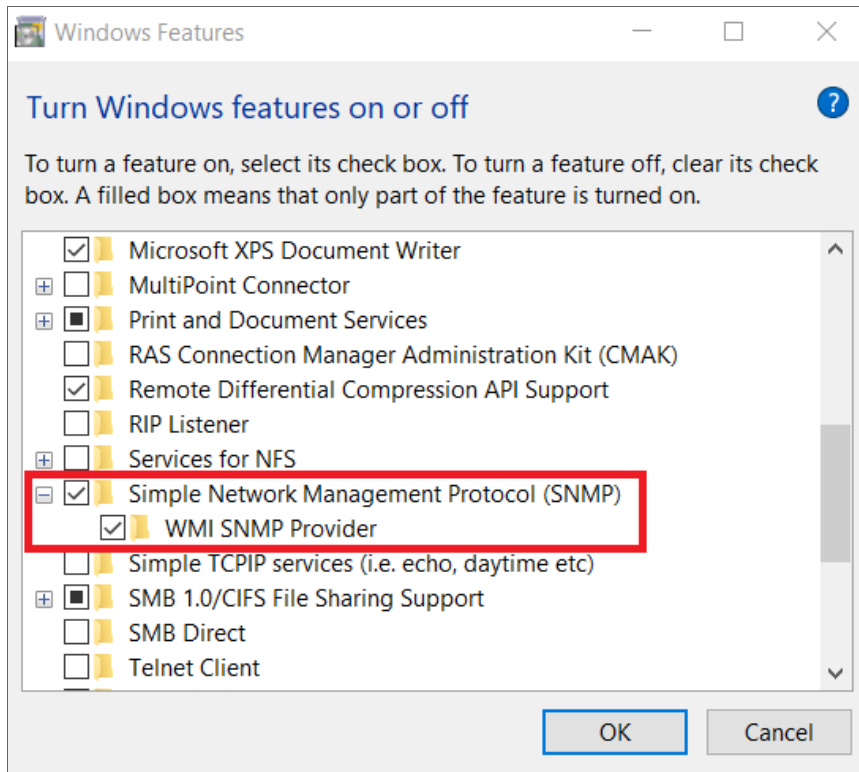
NOTE: The following instructions describe how to enable SNMP on devices running a desktop version of the Windows 10 operating system. For instructions on how to enable SNMP on earlier Windows versions, consult Microsoft's documentation.

To enable SNMP on a device running a desktop version of the Windows 10 operating system:

1. Click the magnifying glass icon in the bottom-left corner and type "Windows Features" in the **Search Windows** field.
2. Click **Turn Windows features on or off**.

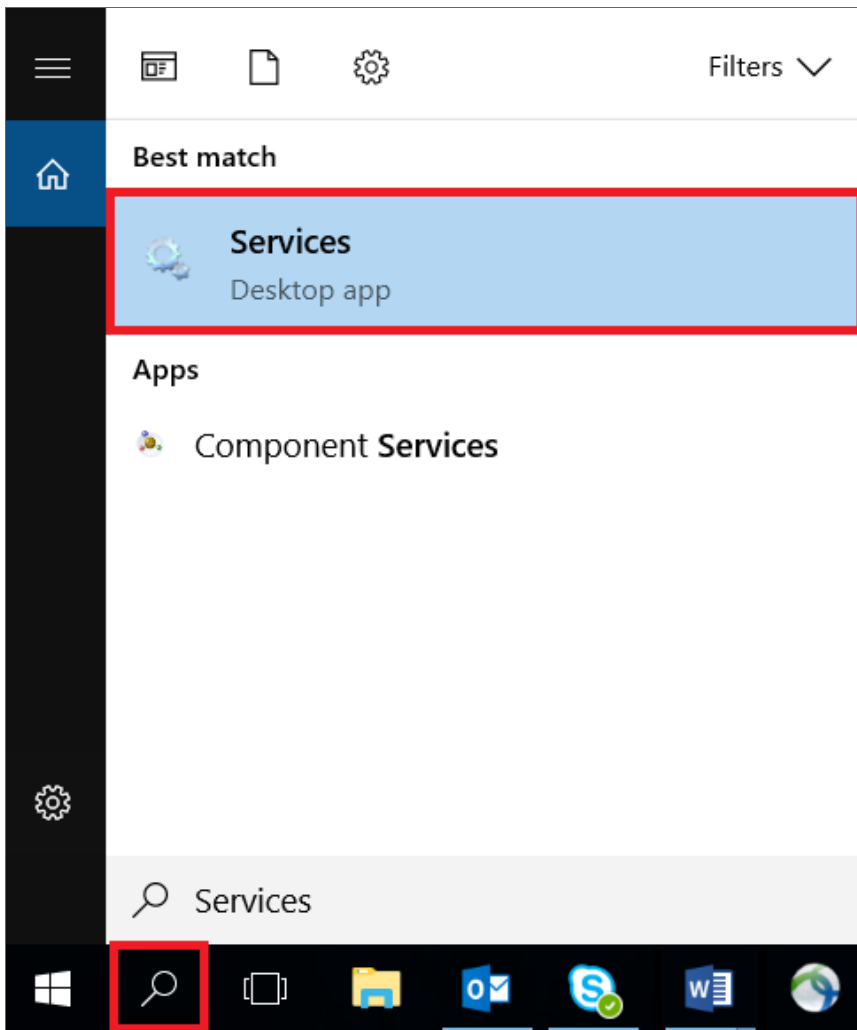


3. In the **Turn Features on or off** window, expand the **Simple Network Management Protocol (SNMP)** folder and then select the **WMI SNMP Provider** checkbox.



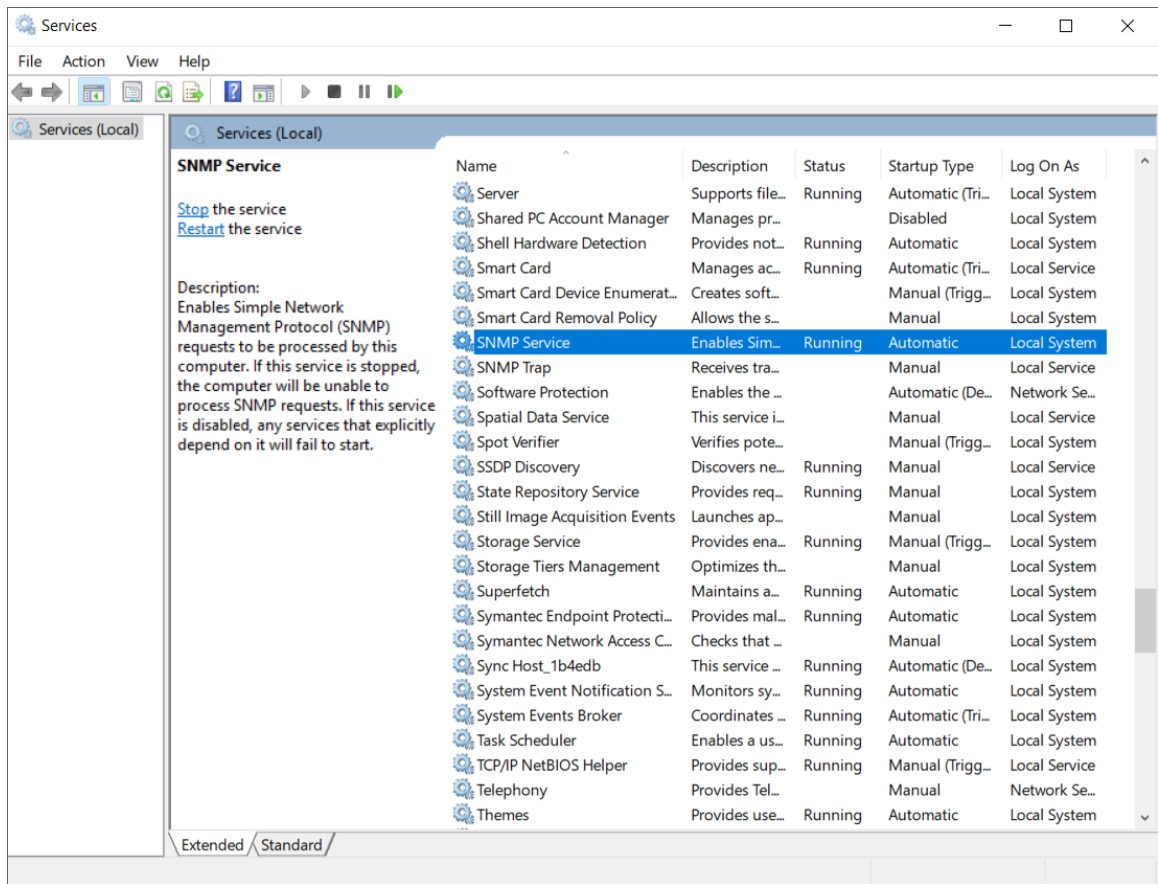
4. Click **[OK]**, and then click **[Close]** after the confirmation message appears.
5. Click the magnifying glass icon in the bottom-left corner and type "Services" in the **Search Windows** field.

6. Click the **Services** Desktop app.

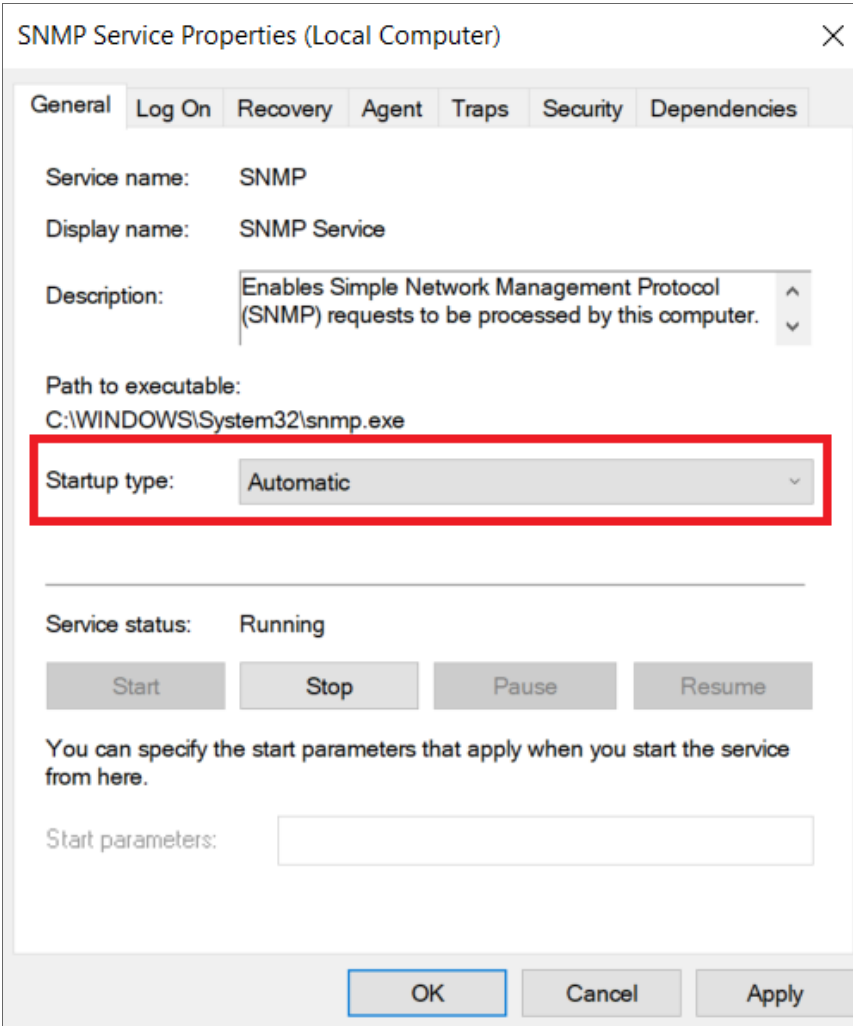


2

7. From the list of services in the right pane, double-click **SNMP Service**.



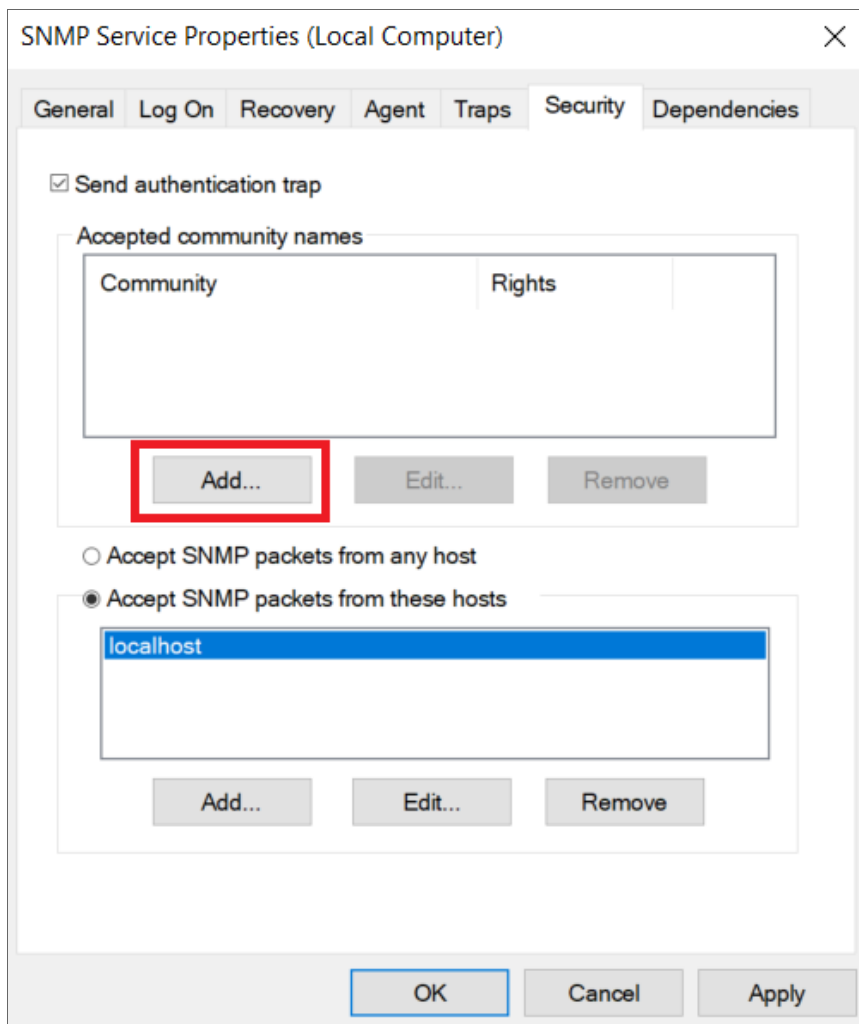
8. In the **SNMP Service Properties** dialog box, click the **[General]** tab and enter the following:



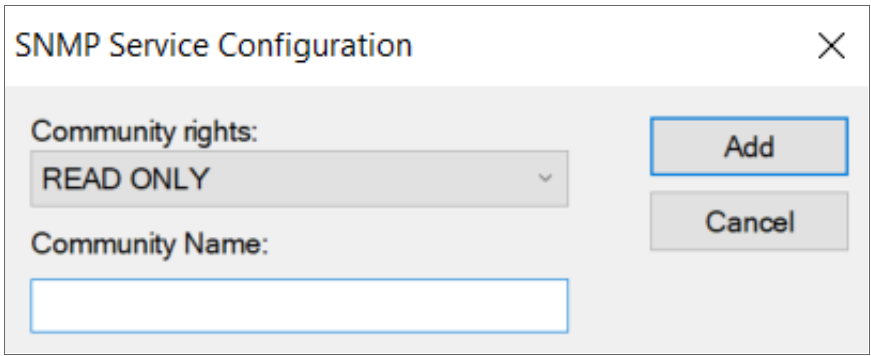
The screenshot shows the 'SNMP Service Properties (Local Computer)' dialog box with the 'General' tab selected. The 'Startup type' dropdown menu is highlighted with a red box and is set to 'Automatic'. Other visible fields include 'Service name: SNMP', 'Display name: SNMP Service', 'Description: Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.', and 'Path to executable: C:\WINDOWS\System32\snmp.exe'. The service status is 'Running' and there are buttons for 'Start', 'Stop', 'Pause', and 'Resume'. At the bottom, there are 'OK', 'Cancel', and 'Apply' buttons.

- **Startup type.** Select *Automatic*.

9. In the **SNMP Service Properties** dialog box, click the **[Security]** tab.
10. In the **Accepted community names** pane, click **[Add]**.



11. In the **SNMP Service Configuration** dialog box, complete the following fields:

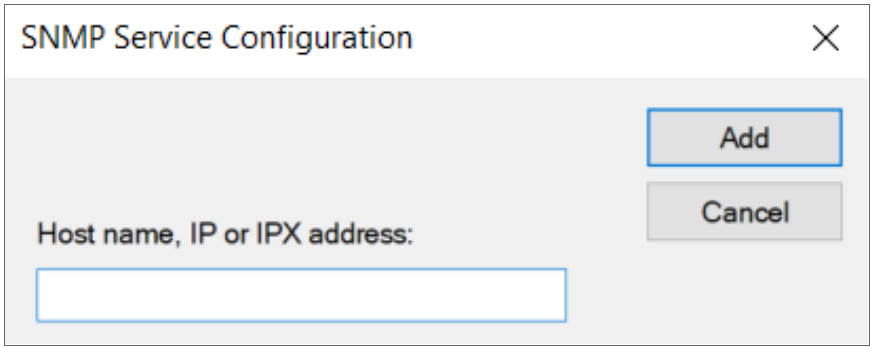


- **Community rights.** Select *READ ONLY*.
- **Community Name.** Type the SNMP Community String.

12. Click the **[Add]** button.

13. In the **SNMP Service Properties** dialog box, in the **[Security]** tab, select the *Accept SNMP packets from these hosts* checkbox and then click **[Add]**.

14. In the **SNMP Service Configuration** dialog box, complete the following field:

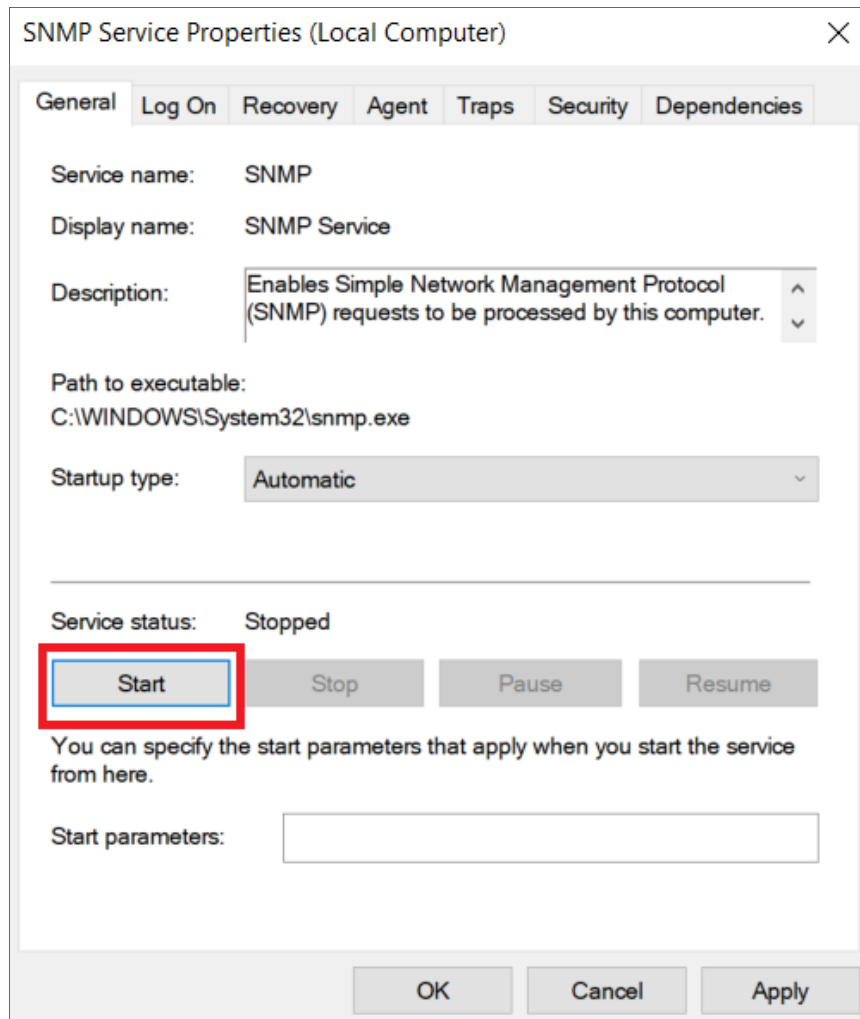


- **Host name, IP or IPX address.** Type the IP address of your ScienceLogic Data Collector or All-In-One Appliance.

15. Click **[Add]**.

16. In the **SNMP Service Properties** dialog box, click the **[General]** tab.

17. If the service is not running, click the **[Start]** button in the **Service status** pane.



18. Click **[OK]**.

Additional Steps for Configuring SNMP for Windows 10

To configure SNMP for Windows 10 operating systems, you must also [Configure Device Classes for Windows 10](#).

Configuring Windows Systems for Monitoring with WMI

Overview

The following sections describe how to configure Windows Server 2008 and Windows desktop systems for monitoring by the ScienceLogic platform using SNMP:

<i>Configuring WMI on Windows 2008 Servers</i>	40
<i>Step 1: Configuring Services</i>	40
<i>Step 2: Configuring the Windows Firewall</i>	42
<i>Step 3: Configuring a User Account and Permissions</i>	42
Configuring Namespace and DCOM Security Permissions	42
Configuring User Account Control to Allow Elevated Permissions	50
<i>Configuring WMI for Windows Desktop Systems</i>	52
<i>Step 1: Configuring Services</i>	52
<i>Step 2: Configuring Windows Firewall</i>	56
<i>Step 3: Setting the Default Namespace Security</i>	56
<i>Step 4: Setting the DCOM Security Level</i>	62
<i>Step 5: Disabling User Account Control</i>	69

Configuring WMI on Windows 2008 Servers

Windows Management Instrumentation, or WMI, is the infrastructure that provides information about operations and management on Windows-based operating systems. WMI can be configured to respond to remote requests from the ScienceLogic platform.

To configure a Windows 2008 device to respond to remote requests, you must perform the following steps:

1. [Configure Services](#)
2. [Configure the Windows Firewall](#)
3. [Configure a user account and permissions](#)

Most remote requests can be performed by a standard (non-administrator) user account that has been granted specific privileges. However, some requests can be performed only by a user with elevated permissions. For requests performed by the ScienceLogic platform to a Windows 2008 server, the following users have elevated permissions:

- The default "Administrator" user account.
- A user account in the **Administrators** group on a Windows 2008 server that has User Account Control disabled.
- A user account in the **Administrators** group on a Windows 2008 server where a registry entry has been added to disable remote User Account Control filtering.

For a list of WMI classes that require elevated permissions, see <http://msdn.microsoft.com/en-us/library/windows/desktop/aa826699%28v=vs.85%29.aspx>

For a list of default WMI Dynamic Applications that require elevated permissions, see the chapter on [Dynamic Applications for Windows Devices](#).

Step 1: Configuring Services

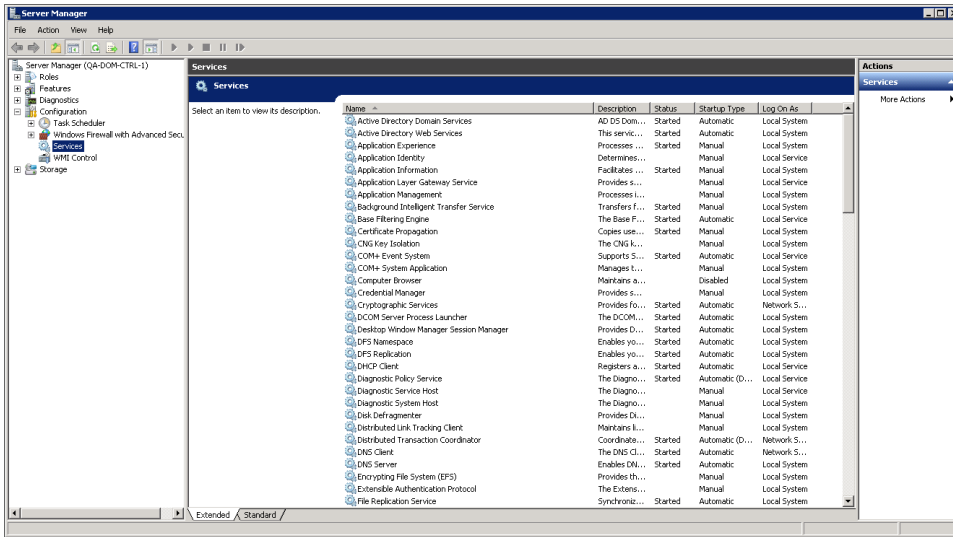
The following services must be running for a Windows device to respond to remote WMI requests:

NOTE: ScienceLogic recommends you set all these services to automatically start.

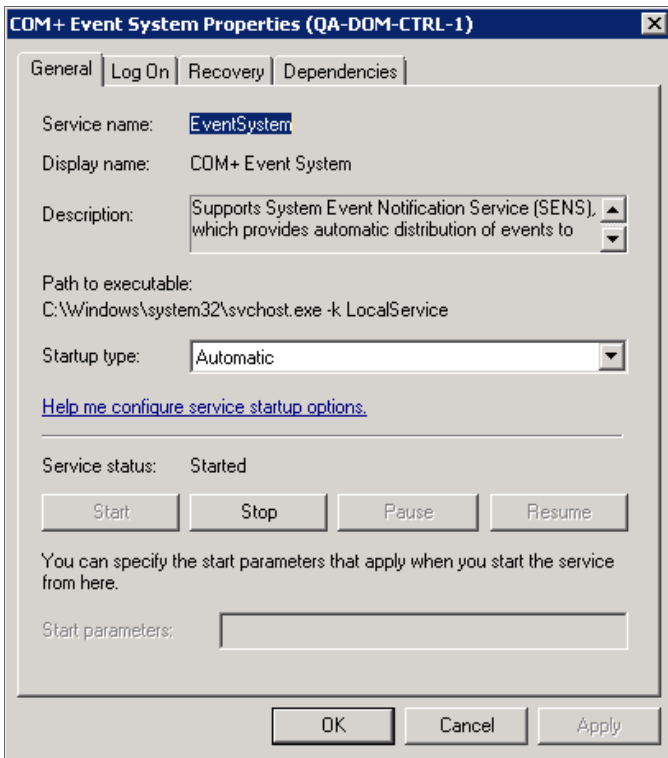
- COM+ Event System
- DCOM Server Process Launcher
- Remote Procedure Call (RPC)
- Remote Registry
- Server
- Windows Management Instrumentation

To ensure a service is running, perform the following steps:

1. In the left pane of the **Server Manager** window, expand the *Configuration* section, and then select *Services*.



2. For each required service, the **Startup Type** column should display *Automatic*. If a service does not have a **Startup Type** of *Automatic*, double-click on that service. The Properties window for that service is displayed:



3. In the **Startup Type** field, select *Automatic*.
4. Click the **[Apply]** button.
5. If the service has not already started, click the **[Start]** button.

Step 2: Configuring the Windows Firewall

To configure Windows Firewall to accept remote WMI requests, execute the following two commands at the console:

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

Step 3: Configuring a User Account and Permissions

There are three ways to configure the user account that the ScienceLogic platform will use to perform WMI requests:

1. To monitor the Windows 2008 server using WMI Dynamic Applications that require **standard permissions**, you can configure a standard user account for use by the ScienceLogic platform. The user account for use by the ScienceLogic platform must be included in the **Distributed COM Users** and **Performance Monitor Users** groups. (For more information, consult Microsoft's documentation.)
2. To monitor the Windows 2008 server using WMI Dynamic Applications that require **elevated permissions**, you can use the default "Administrator" user account. If you use the "Administrator" user account, you do not need to make changes to the User Account Control settings.
3. To monitor the Windows 2008 server using WMI Dynamic Applications that require **elevated permissions**, you can also use a user account that is included in the **Administrators** group. However, you must perform **one** of the following additional steps to use this type of user account:
 - **Option 1:** Make the user a member of the **Distributed COM Users** and **Performance Monitor Users** groups, in addition to the **Administrator** group. (For more information, consult Microsoft's documentation.)
 - **Option 2:** [Configure User Access Control to allow elevated permissions.](#)

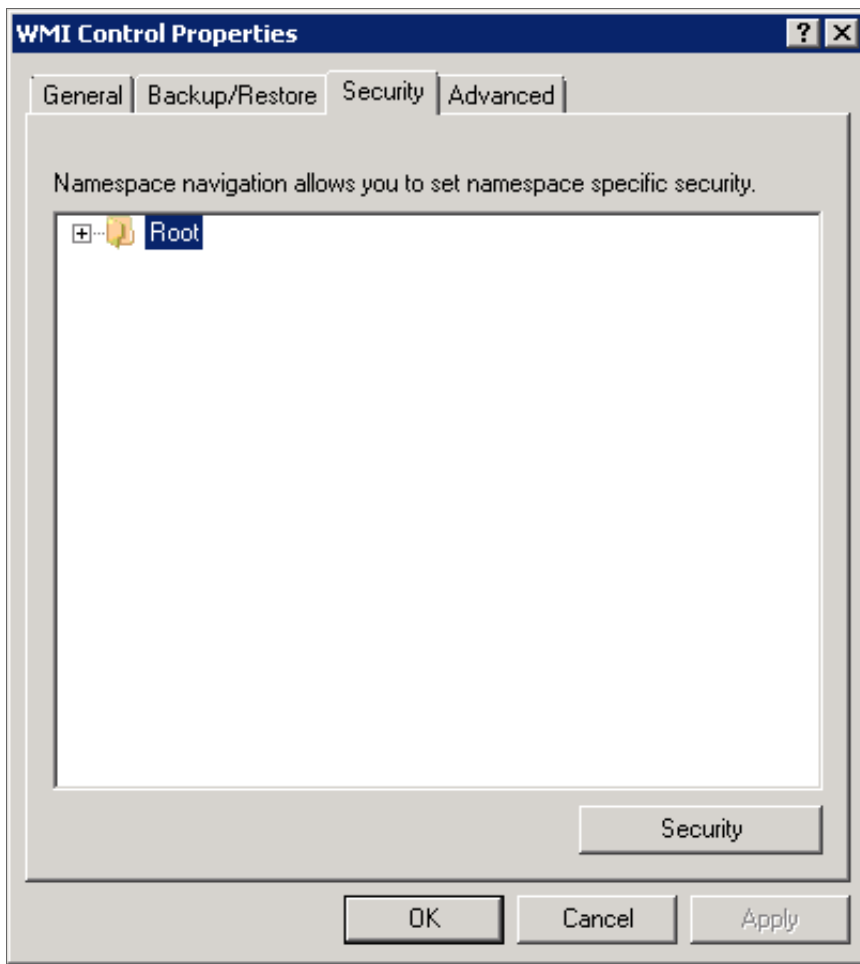
Configuring Namespace and DCOM Security Permissions

For each of these methods, you must ensure that the configured Namespace and DCOM security permissions allow that user to perform remote requests.

To configure the Namespace and DCOM security permissions:

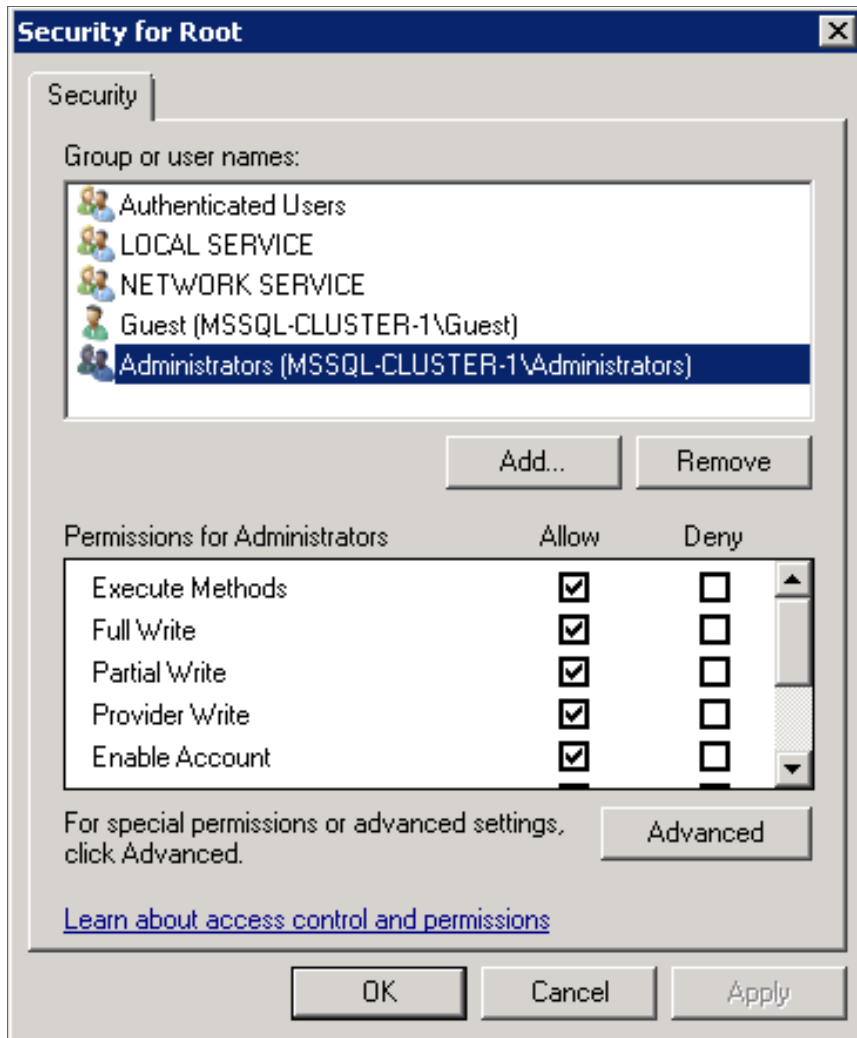
1. In the left pane of the **Server Manager** window, expand the *Configuration* section.
2. Right-click on the *WMI Control* entry and then select *Properties*.

3. In the **WMI Control Properties** window, click the **[Security]** tab:

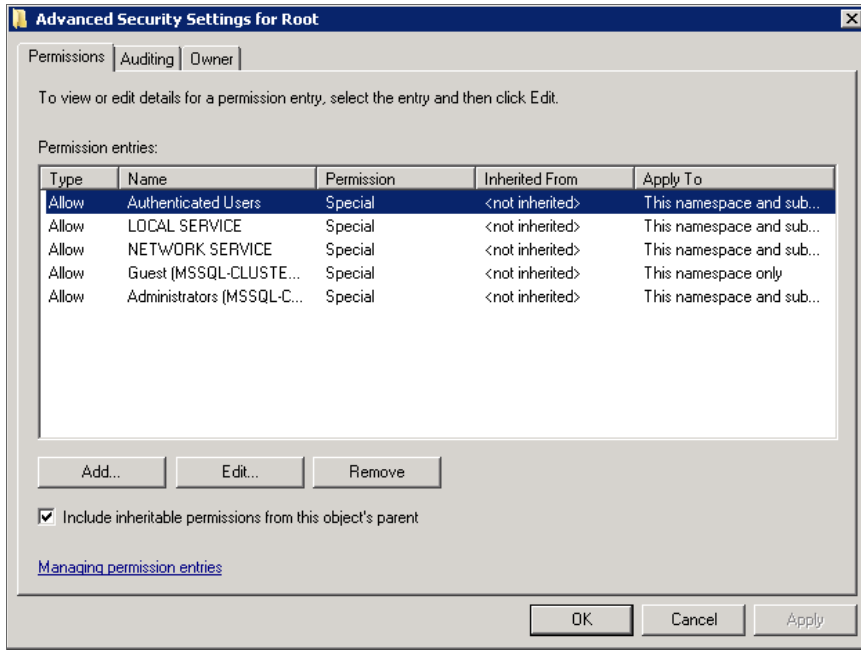


4. In the Security tab, select the *Root* entry from the navigation pane and then select the **[Security]** button. The **Security for Root** window appears.

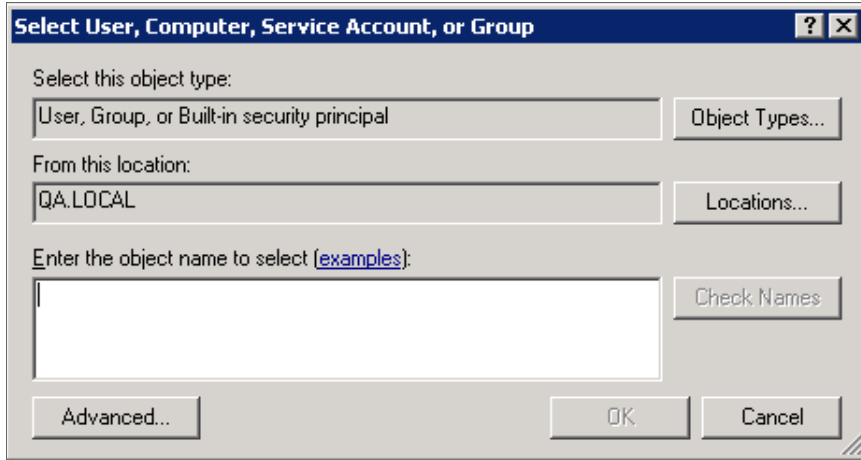
5. In the **Security for Root** window, select the **[Advanced]** button. The **Advanced Security Settings for Root** window is displayed:



- In the **Advanced Security Settings for Root** window, click the **[Add]** button. The **Select User, Computer, Service Account, or Group** window appears.

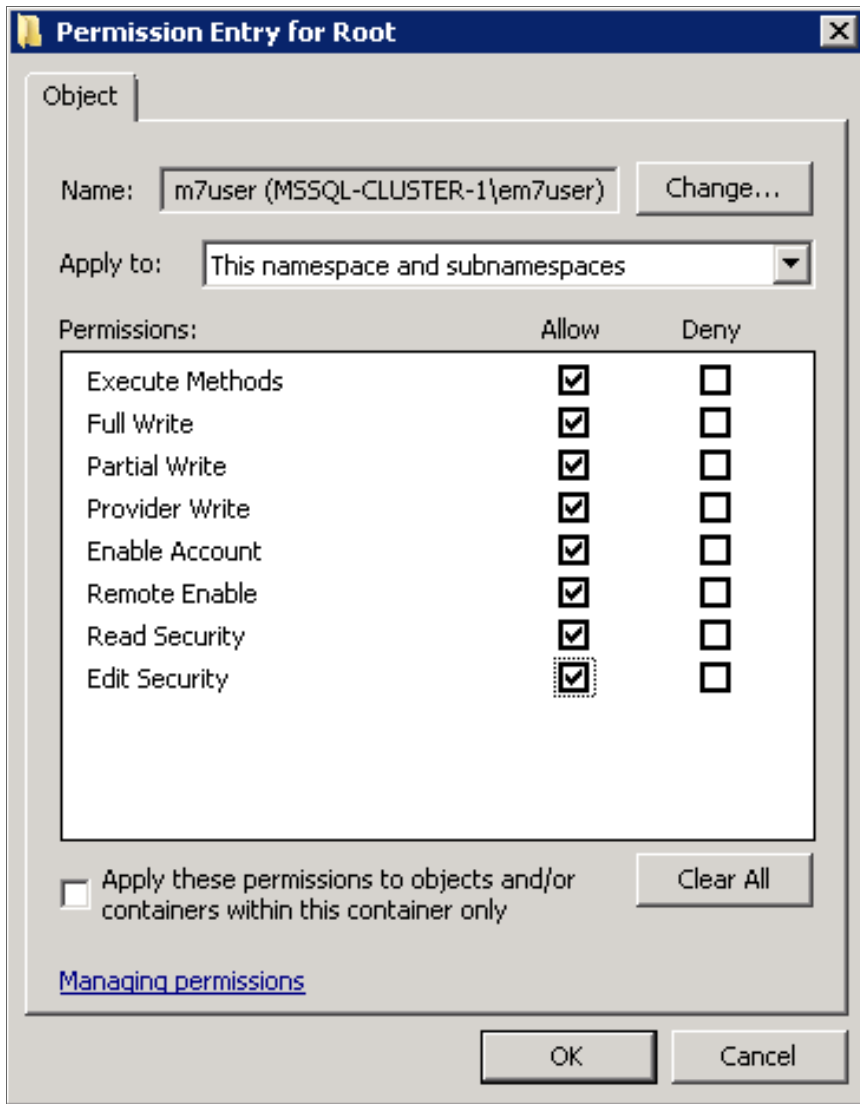


- In the **Select User, Computer, Service Account, or Group** window :



- In the **Enter the object name to select** field, enter the name of the user account that the ScienceLogic platform will use to perform WMI requests or the name of a group that includes that user account.
- Click the **[Check Names]** button to verify the name and then click the **[OK]** button.

8. The **Permission Entry for Root** window is displayed:



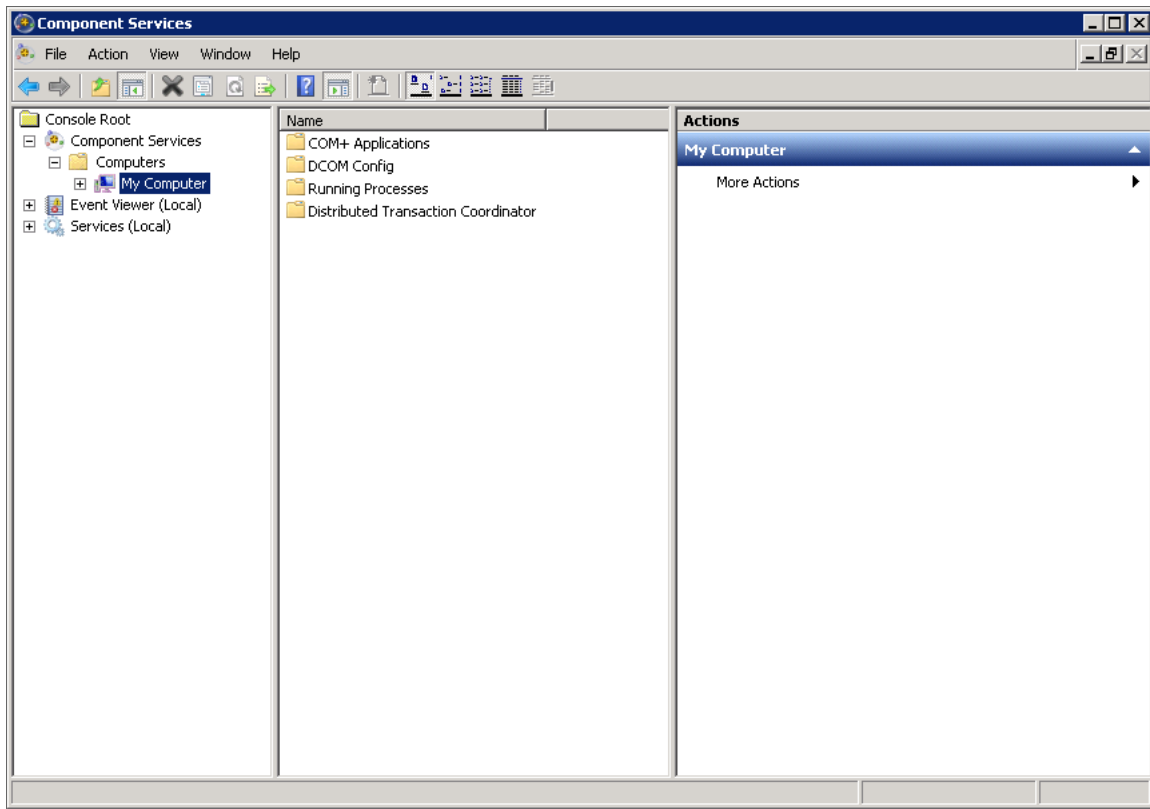
- Select *This namespace and subnamespaces* in the **Apply to** field and select the **Allow** checkbox for all permissions.
- Click the **[OK]** button.

9. In the **Advanced Security Settings for Root** window, click the **[Apply]** button.

10. Click the **[OK]** button in each open window to exit.

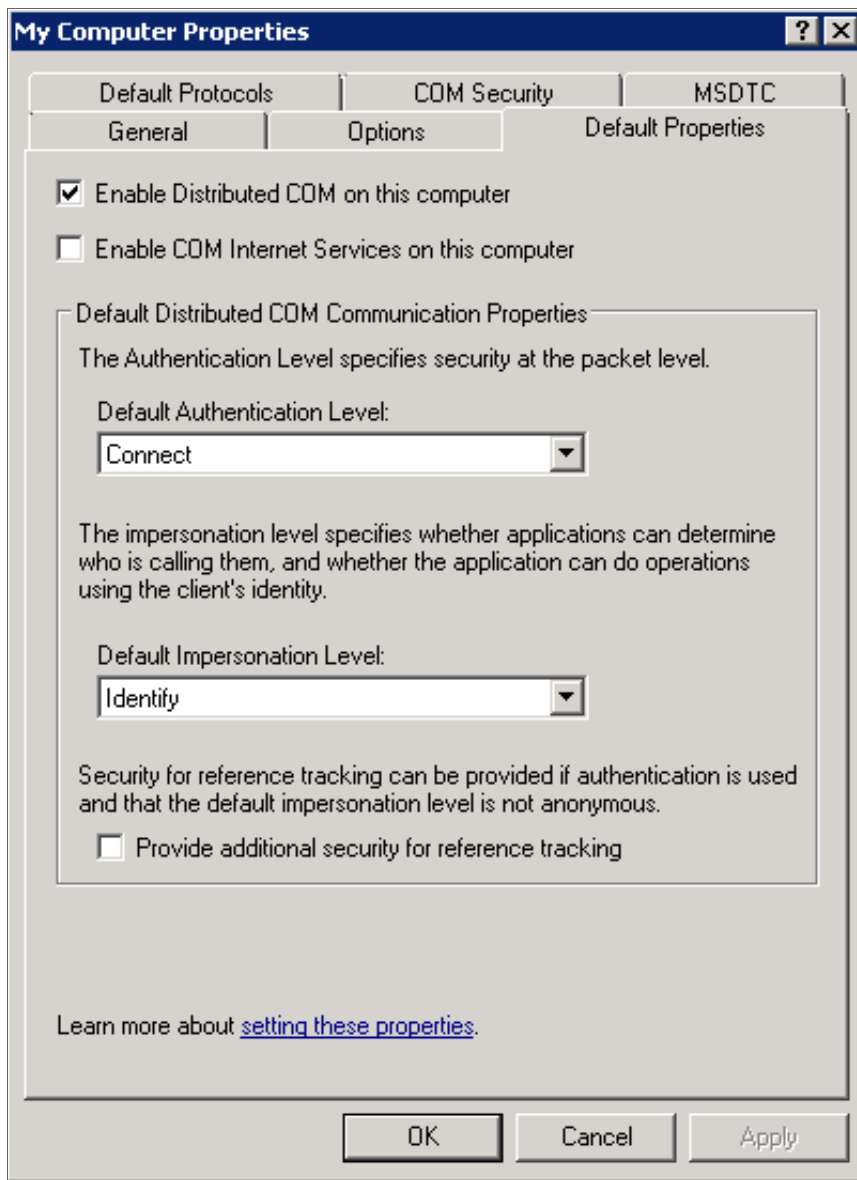
11. Go to the Start menu and select **[Run]**.

12. In the **Run** window, enter "dcomcnfg" and click **[OK]**. The **Component Services** window is displayed:



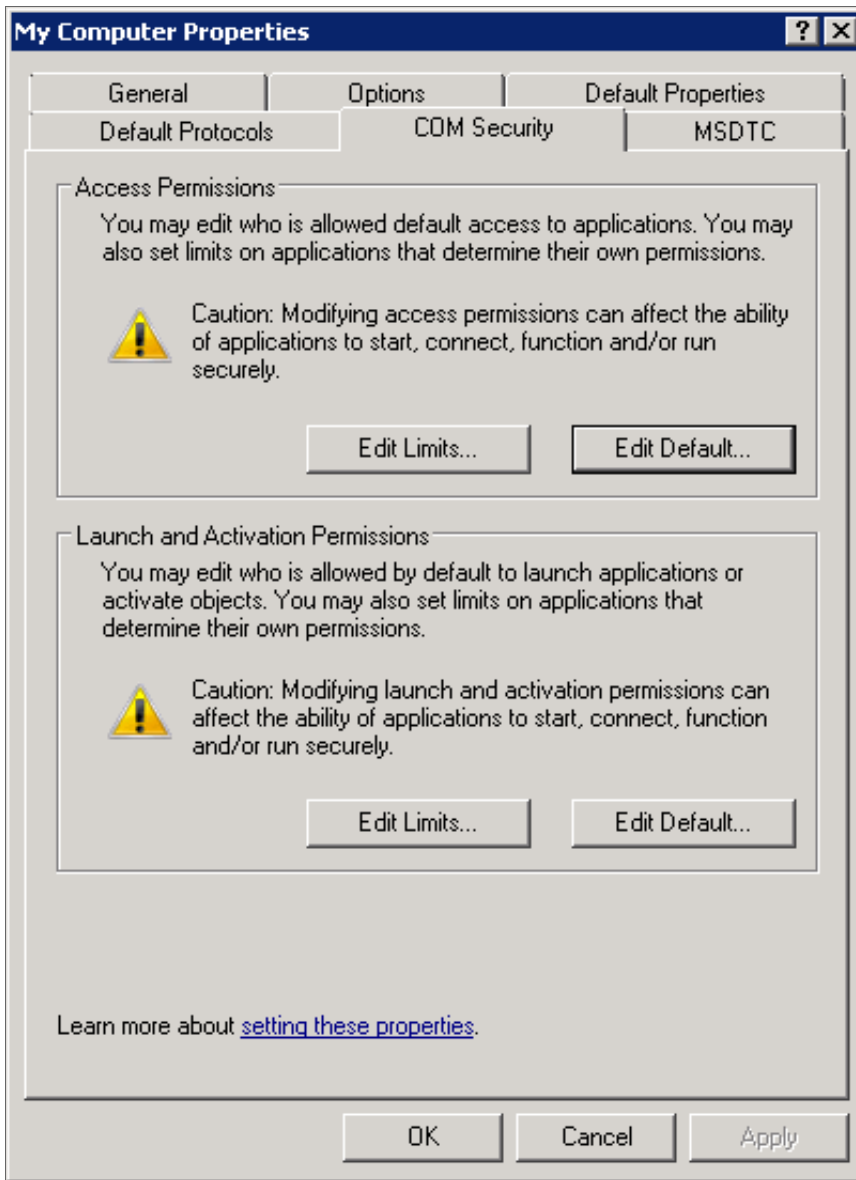
13. In the left pane, expand **Component Services > Computers**. Right-click on **My Computer** and select **Properties**. The **My Computer Properties** window is displayed.

14. In the **My Computer Properties** window, select the **[Default Properties]** tab:



- Ensure that the **Enable Distributed COM on this computer** checkbox is selected.
- Select **Connect** in the **Default Authentication Level** drop-down list.
- Select **Identify** in the **Default Impersonation Level** drop-down list.
- If you made changes in the **[Default Properties]** tab, click the **[Apply]** button.

15. Select the [COM Security] tab:



16. Select the [Edit Limits...] button in the **Access Permissions** pane.
17. In the window that appears, click the [Add...] button. The **Select Users, Computers, Service Accounts, or Groups** window is displayed.
- Enter the name of the user account that the ScienceLogic platform will use to perform WMI requests or the name of a group that includes that user account.
 - Click the **Check Names** button to verify the name and then click the [OK] button.

18. Select the group or user you added in the **Group or user names** pane and then select the **Allow** checkbox for all permissions.
19. Click the **[OK]** button.
20. Click the **[Edit Default...]** button in the **Access Permissions** pane, then repeat steps 16 - 19.
21. Click the **[Edit Limits...]** button in the **Launch and Activation Permissions** pane, then repeat steps 16 - 19.
22. Click the **[Edit Default...]** button in the **Launch and Activation Permissions** pane, then repeat steps 16 - 19.
23. Click the **[Apply]** button.
24. Click **[Yes]** in the confirmation window.

Configuring User Account Control to Allow Elevated Permissions

If you want to use WMI Dynamic Applications that require elevated permissions to monitor a Windows 2008 server and you are using a user account other than the default "Administrator" user account, you must perform **one** of the following two tasks:

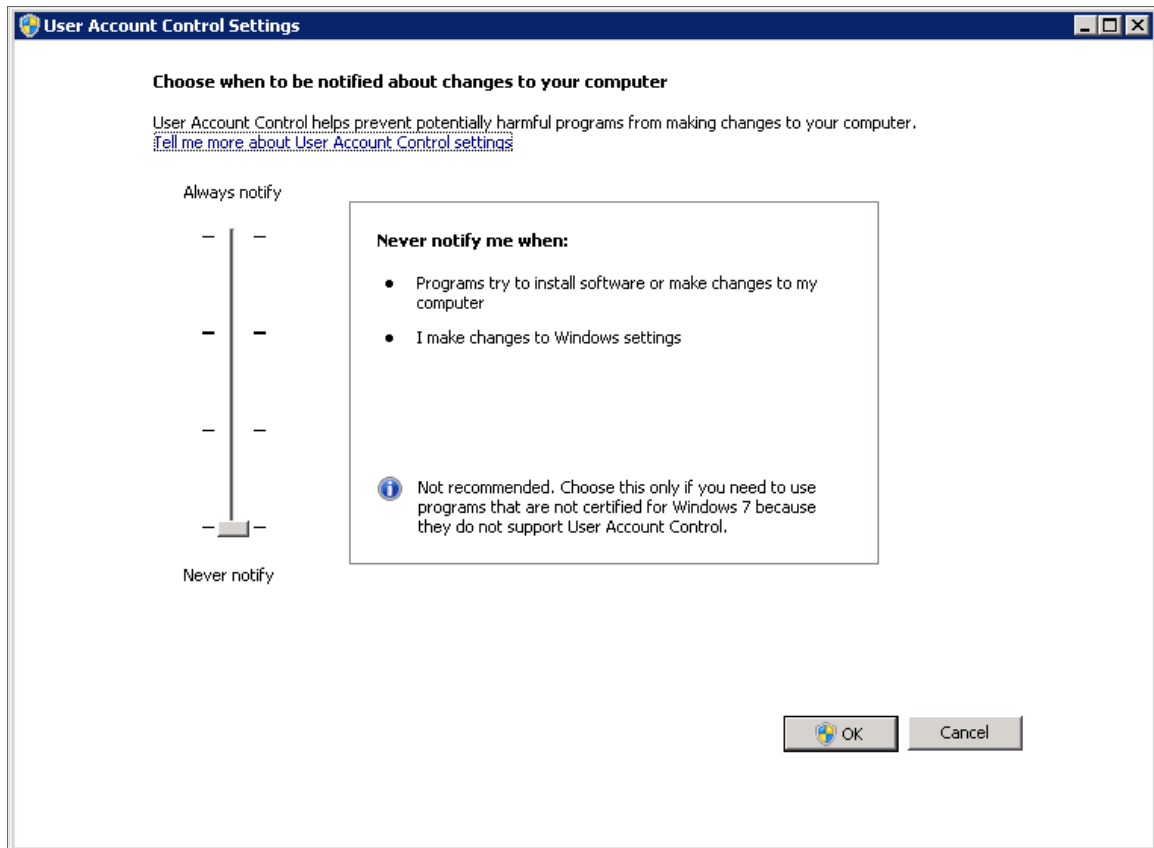
- **Option 1:** [Disable User Account Control](#).
- **Option 2:** [Add a registry entry that disables remote User Account Control filtering](#).

Option 1: Disabling User Account Control

To disable User Account Control:

1. Open the **Control Panel** in Large Icon or Small Icon view.
2. Select **User Accounts**.

3. Select **Change User Account Control Settings**. The **User Account Control Settings** window is displayed:



4. Move the slider to **Never Notify**.
5. Click the [OK] button.
6. Restart the Windows 2008 Server.

Option 2: Adding a Registry Entry that Disables Remote User Account Control Filtering

To add a registry entry that disables remote User Account Control filtering:

1. To disable the filter, open a text editor and add the following lines to a new file:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"LocalAccountTokenFilterPolicy"=dword:00000001
```

2. Save the file with a ".reg" extension.
3. In Windows Explorer, double click on the .reg file.
4. Select [Yes] in the pop-up window.

Configuring WMI for Windows Desktop Systems

This section describes how to configure devices that are running a desktop version of the Windows operating system for monitoring by the ScienceLogic platform using WMI.

Before performing the tasks described in this section, you must know the IP address of each ScienceLogic appliance in your network. If you have not installed a ScienceLogic appliance, you must know the future IP address that will be used by each ScienceLogic appliance.

NOTE: To be monitored by the ScienceLogic platform, a Windows device must be running the Windows 7 operating system or later.

NOTE: TCP/IP must be installed and configured before you can install SNMP on a Windows device.

Windows Management Instrumentation (WMI) is the infrastructure that provides information about operations and management on Windows-based operating systems. WMI can be configured to respond to remote requests from the ScienceLogic platform. To configure a device running a desktop version of the Windows operating system to respond to remote requests, you must perform the following steps:

1. [Configure Services](#)
2. [Configure the Windows Firewall](#)
3. [Set Default Namespace Security](#)
4. [Set the DCOM Security Level](#)
5. [Disable User Account Control](#)

NOTE: The following instructions describe how to configure WMI on devices running a desktop version of the Windows 10 operating system. For instructions on how to configure WMI on earlier Windows versions, consult Microsoft's documentation.

Step 1: Configuring Services

The following services must be running for a Windows device to respond to remote WMI requests:

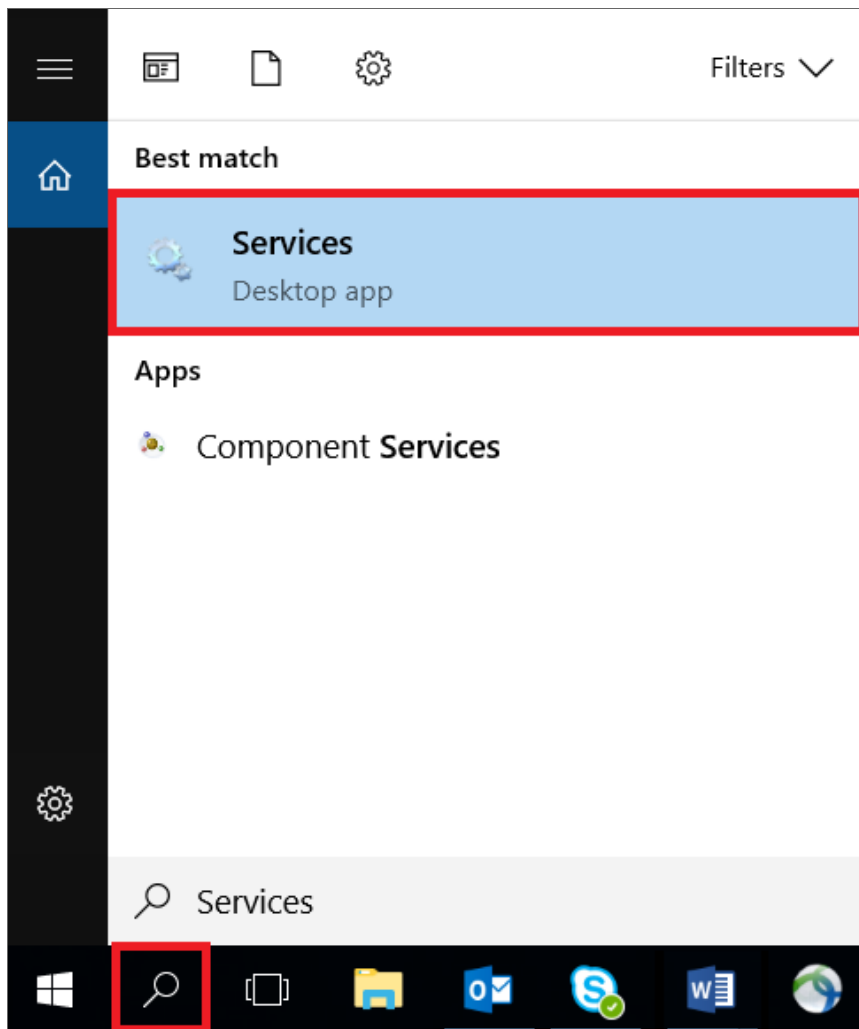
NOTE: ScienceLogic recommends you set all these services to start automatically.

- COM+ Event System
- Remote Access Auto Connection Manager
- Remote Access Connection Manager

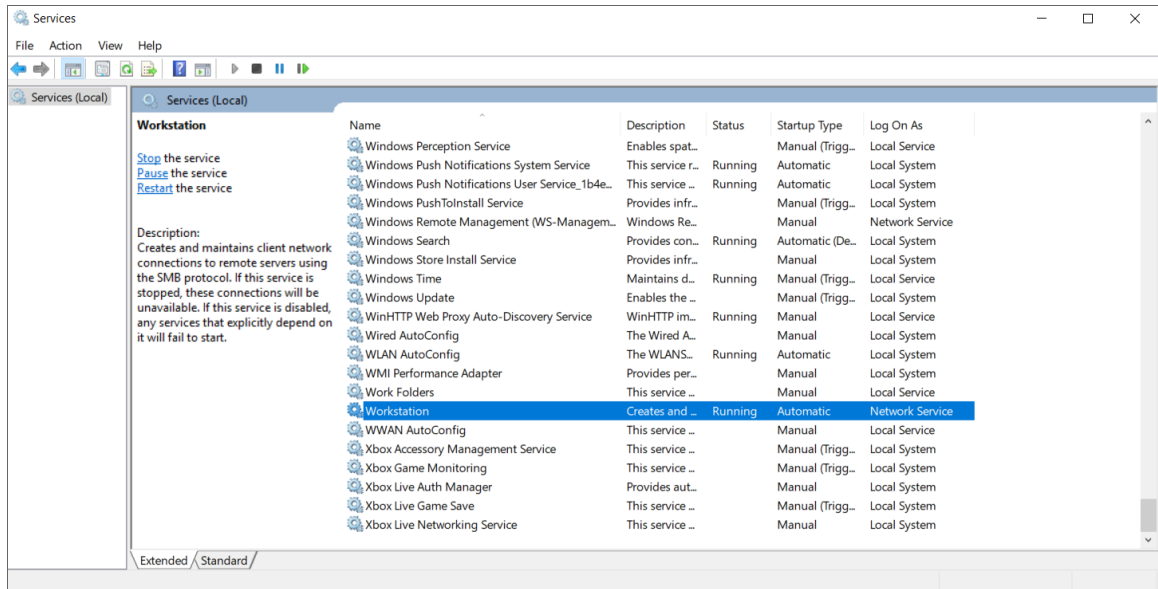
- Remote Procedure Call (RPC)
- Remote Procedure Call (RPC) Locator
- Remote Registry
- Server
- Windows Management Instrumentation
- WMI Performance Adapter
- Workstation

To ensure a service is running, perform the following steps:

1. Click the magnifying glass icon in the bottom-left corner and type "Services" in the **Search Windows** field.
2. Click the **Services** Desktop app.

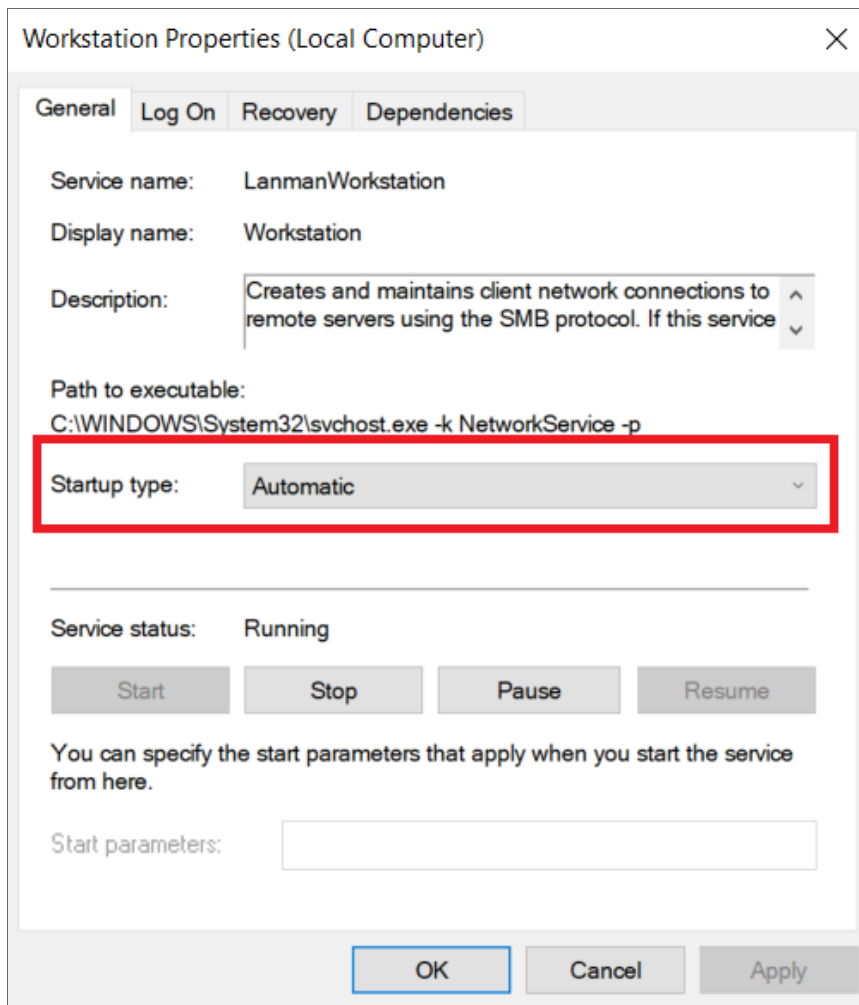


- From the list of services in the right pane, perform the remaining steps for **each** of the services you want to check. This example uses **Workstation**. However, you should check each of the following services:



- COM+ Event System
- Remote Access Auto Connection Manager
- Remote Access Connection Manager
- Remote Procedure Call (RPC)
- Remote Procedure Call (RPC) Locator
- Remote Registry
- Server
- Windows Management Instrumentation
- WMI Performance Adapter
- Workstation

4. Double-click the name of the service. In this example, we double-clicked **Workstation**.
5. In the **Workstation Properties** dialog box, click the **[General]** tab and complete the following field:



- **Startup Type.** Select **Automatic**.

6. Click the **[Apply]** button.
7. If the service has not already started, click the **[Start]** button.
8. Repeat steps 4-7 for each service.

Step 2: Configuring Windows Firewall

To configure Windows Firewall to accept remote WMI requests:

1. Click the magnifying glass icon in the bottom-left corner and type "Command Prompt" in the **Search Windows** field.
2. Execute the following two commands in the Command Prompt window:

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

3. If the result of the second command is "No rules match the specified criteria", run the following two commands:

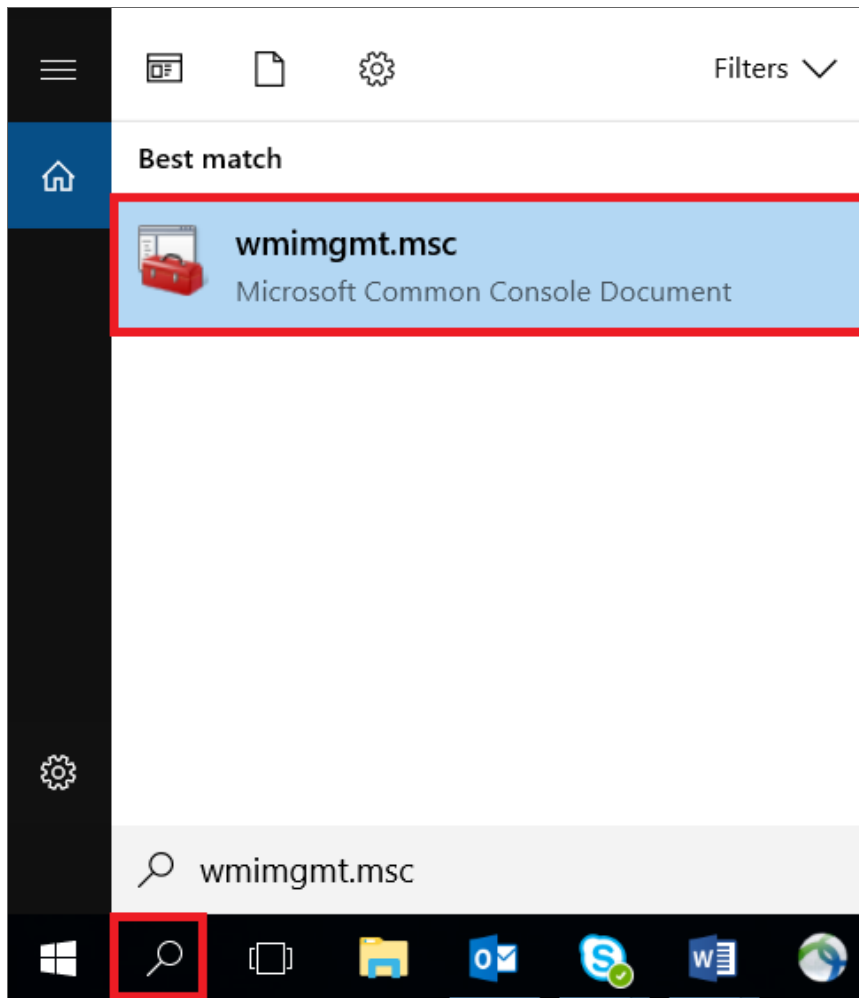
```
netsh firewall set service remoteadmin enable  
netsh advfirewall firewall set rule group="remote administration" new enable=yes
```

Step 3: Setting the Default Namespace Security

To set the default namespace security, perform the following steps:

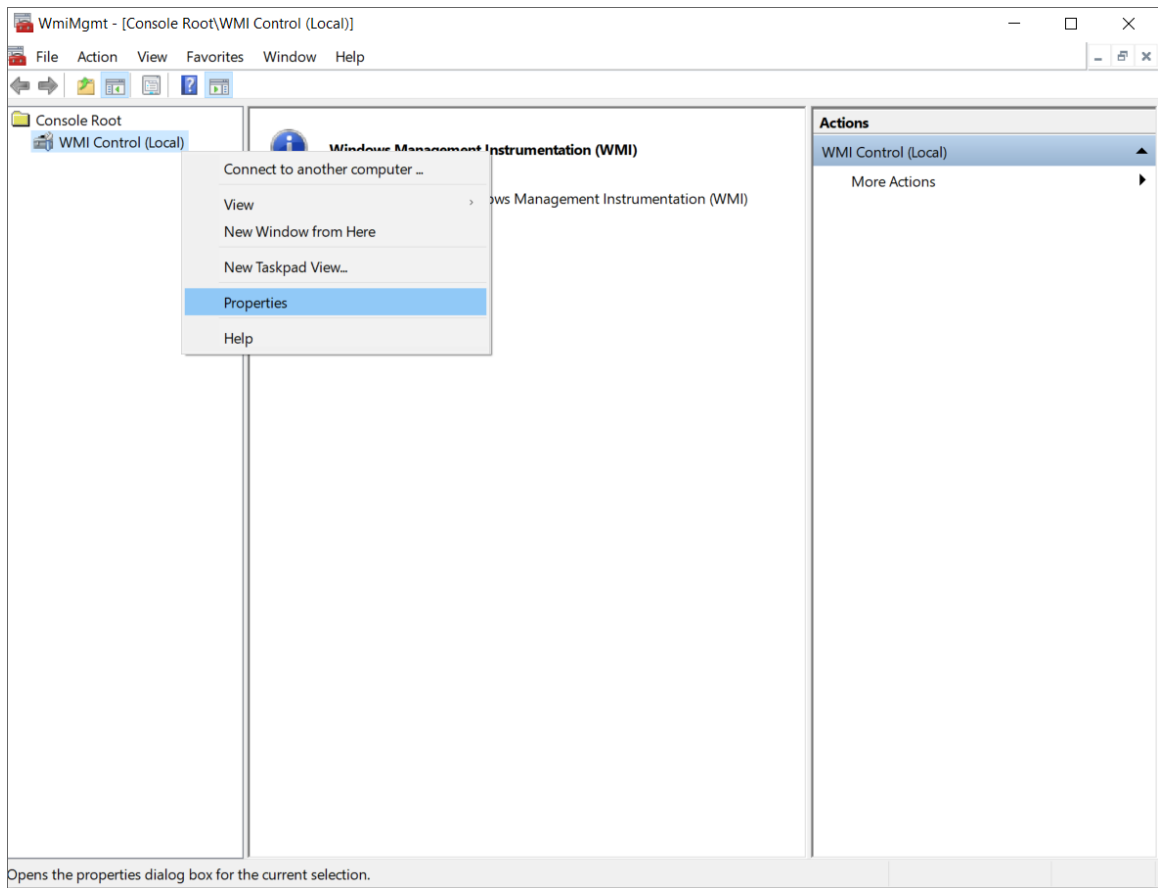
1. Click the magnifying glass icon in the bottom-left corner and type "Services" in the **Search Windows** field.

2. Click the **wmimgmt.msc** Microsoft Common Console Document.

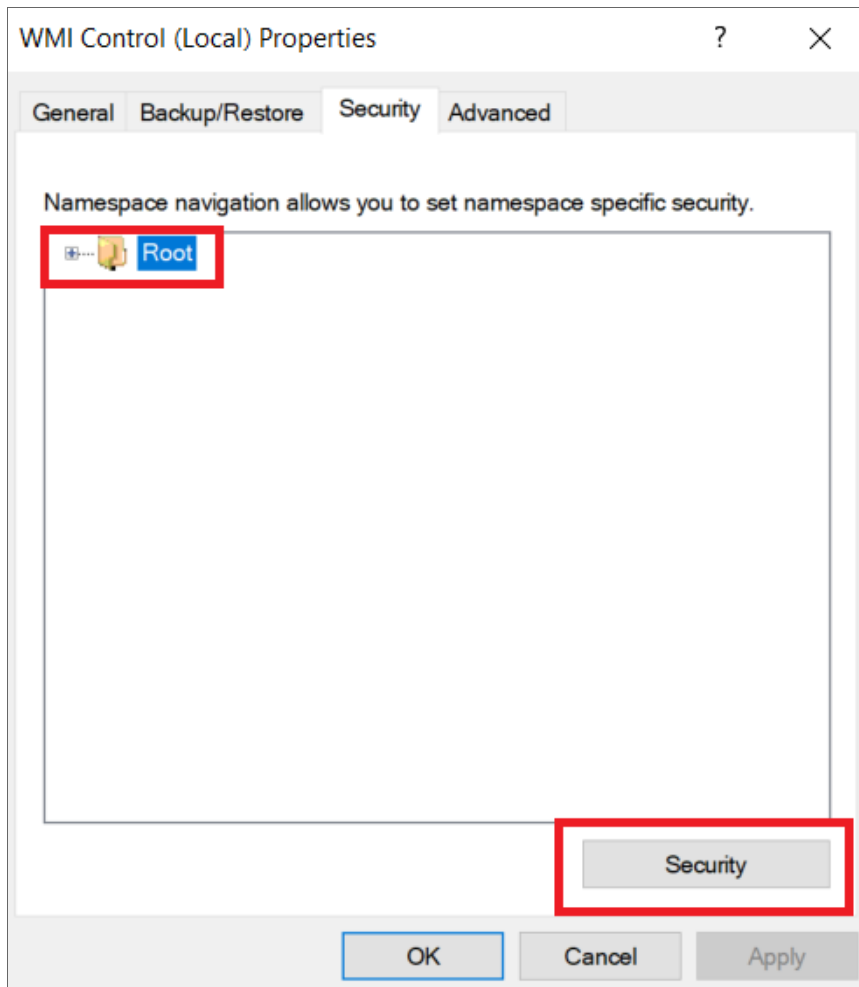


3

3. In the **WmiMgmt** window, right click **WMI Control (Local)** and select *Properties*.

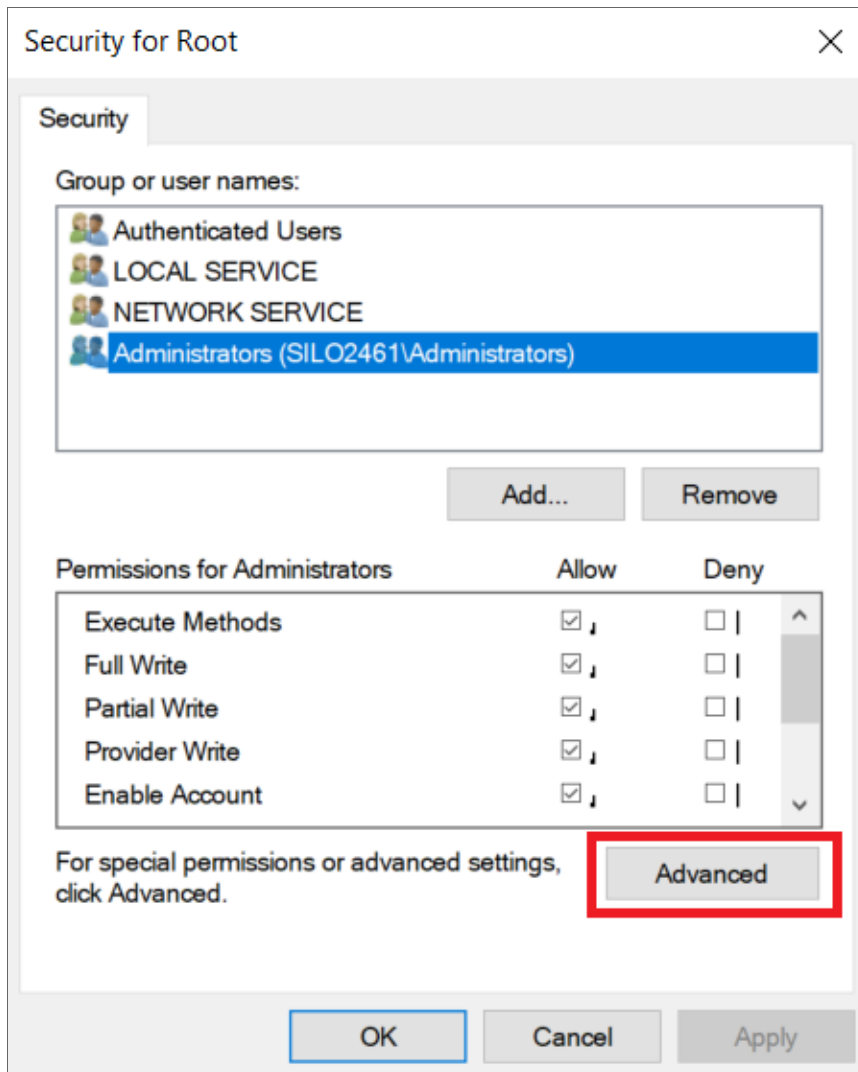


4. In the **WMI Control (Local) Properties** window, click the **[Security]** tab, click **Root**, and then click the **[Security]** button.

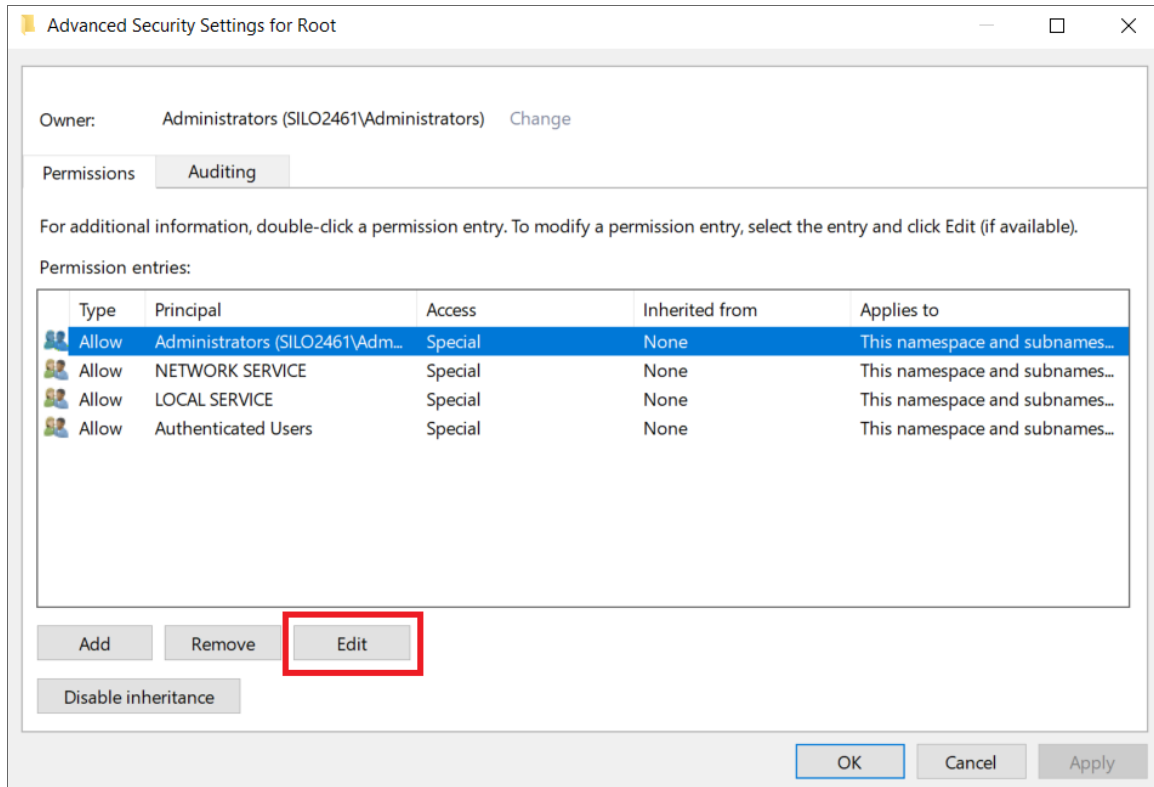


3

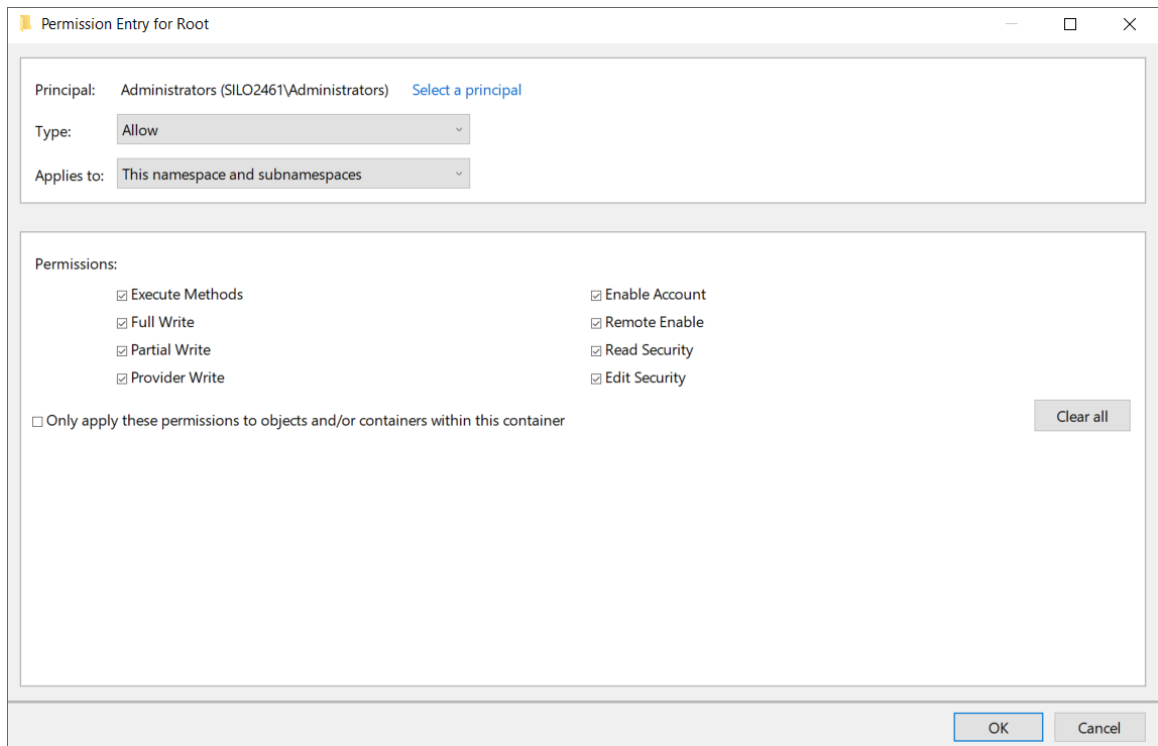
5. In the **Security for Root** window, click **Administrators**, and then click the **[Advanced]** button.



6. In the **Advanced Security Settings for Root** window, click **Administrators**, and then click the **[Edit...]** button.



7. In the **Permission Entry for Root** window, enter the following:



- **Type.** Select *Allow*.
- **Applies to.** Select *This namespace and subnamespaces*.
- **Permissions.** Select the *Execute Methods*, *Full Write*, *Partial Write*, *Provider Write*, *Enable Account*, *Remote Enable*, *Read Security*, and *Edit Security* checkboxes.

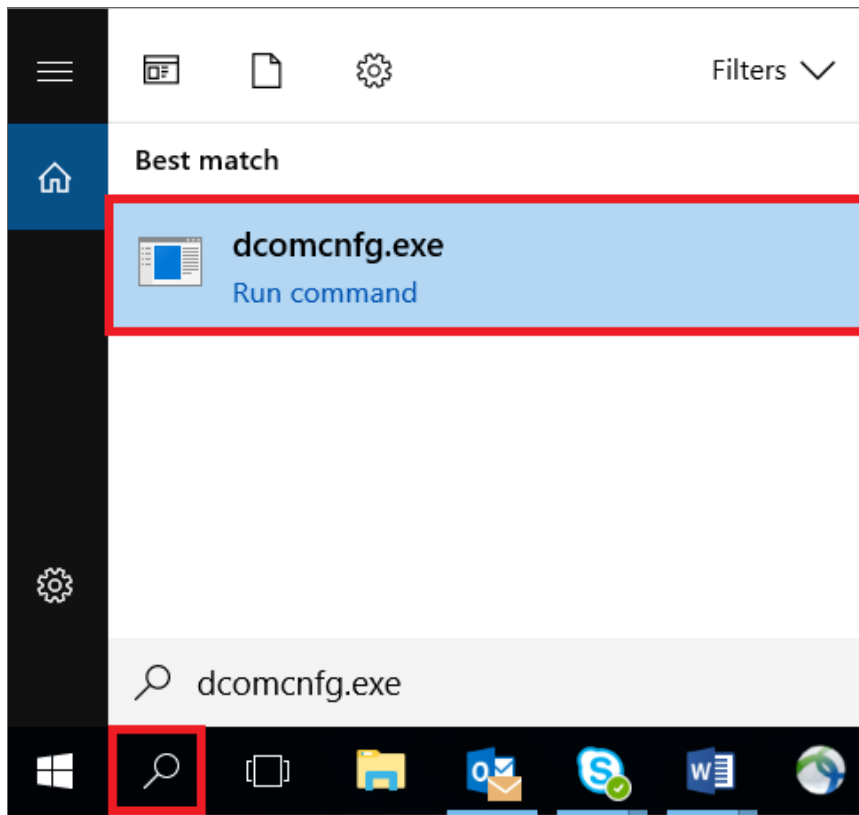
8. Click **OK** in this window and the following windows, and then close the **WmiMgmt** window.

Step 4: Setting the DCOM Security Level

To set the DCOM Security Level, perform the following steps:

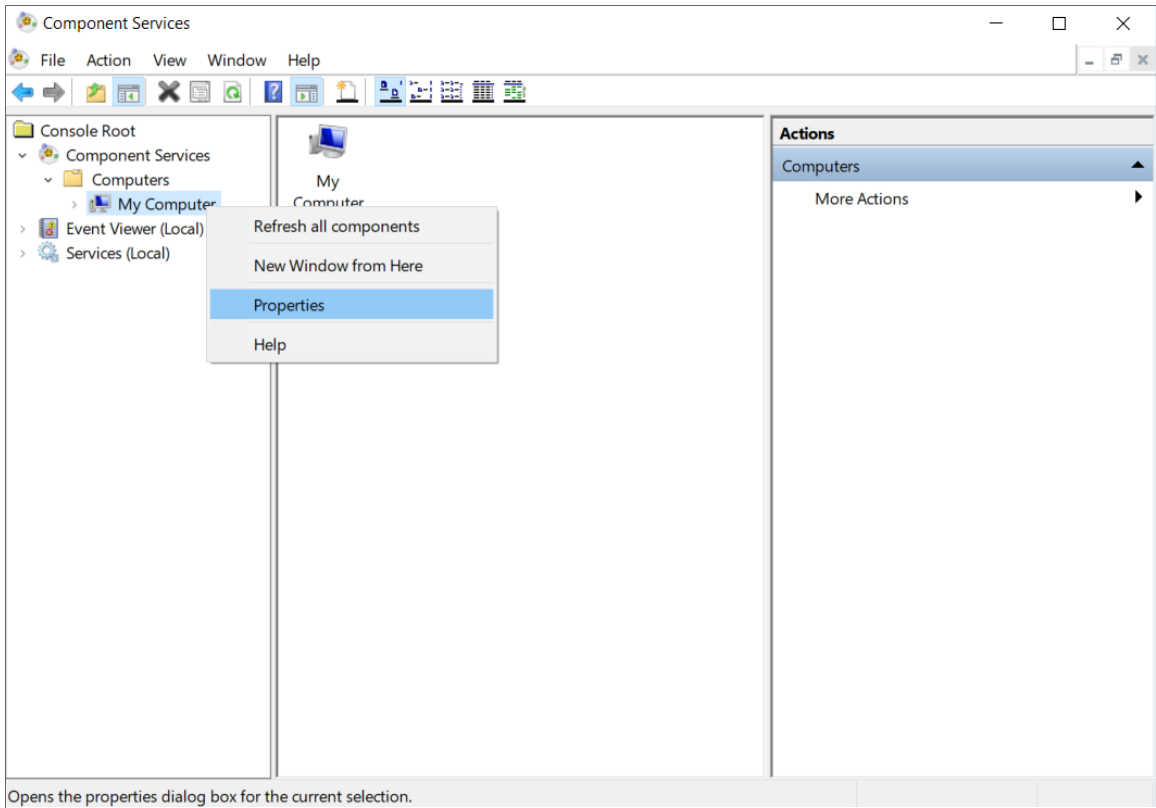
1. Click the magnifying glass icon in the bottom-left corner and type "dcomcnfg.exe" in the **Search Windows** field.

2. Click the **dcomcnfg.exe** command.

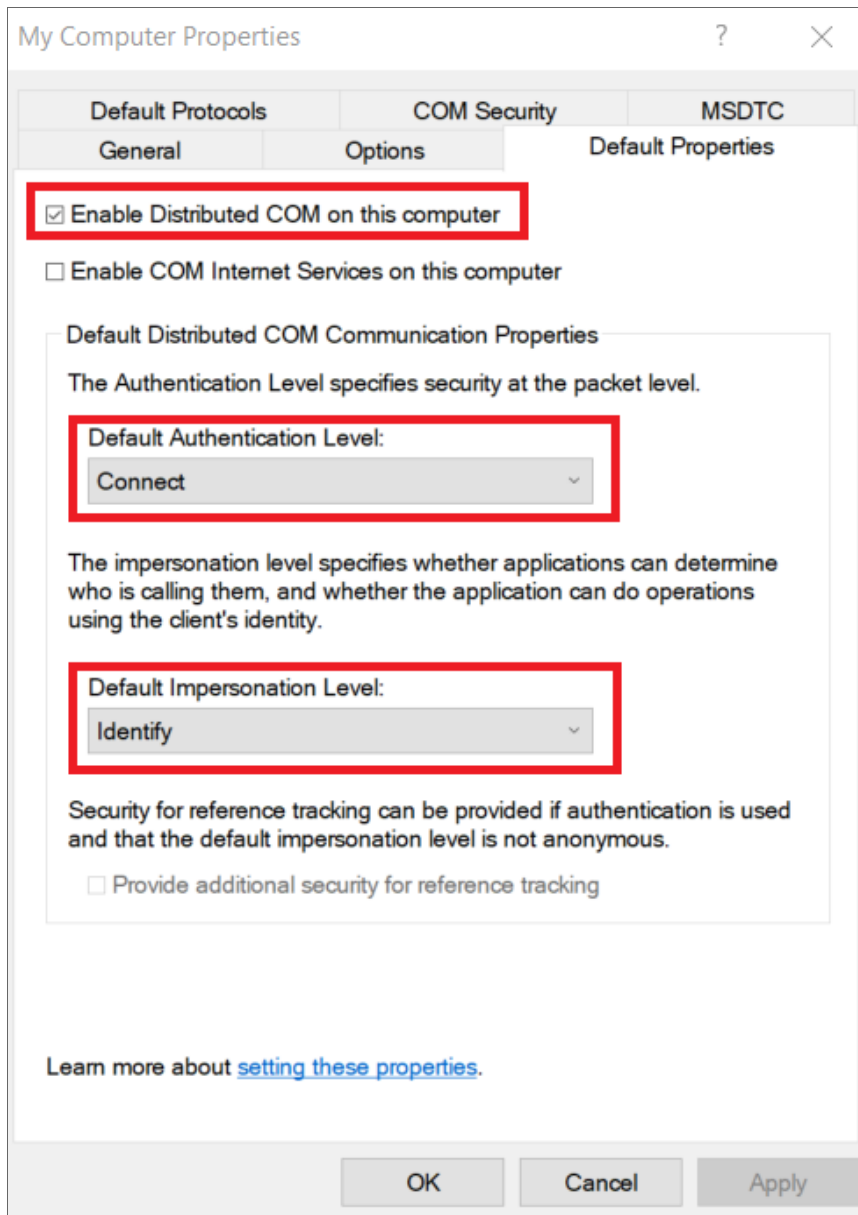


3

3. In the **Component Services** window, expand **Component Services > Computers**, right-click **My Computer**, and then select *Properties*.

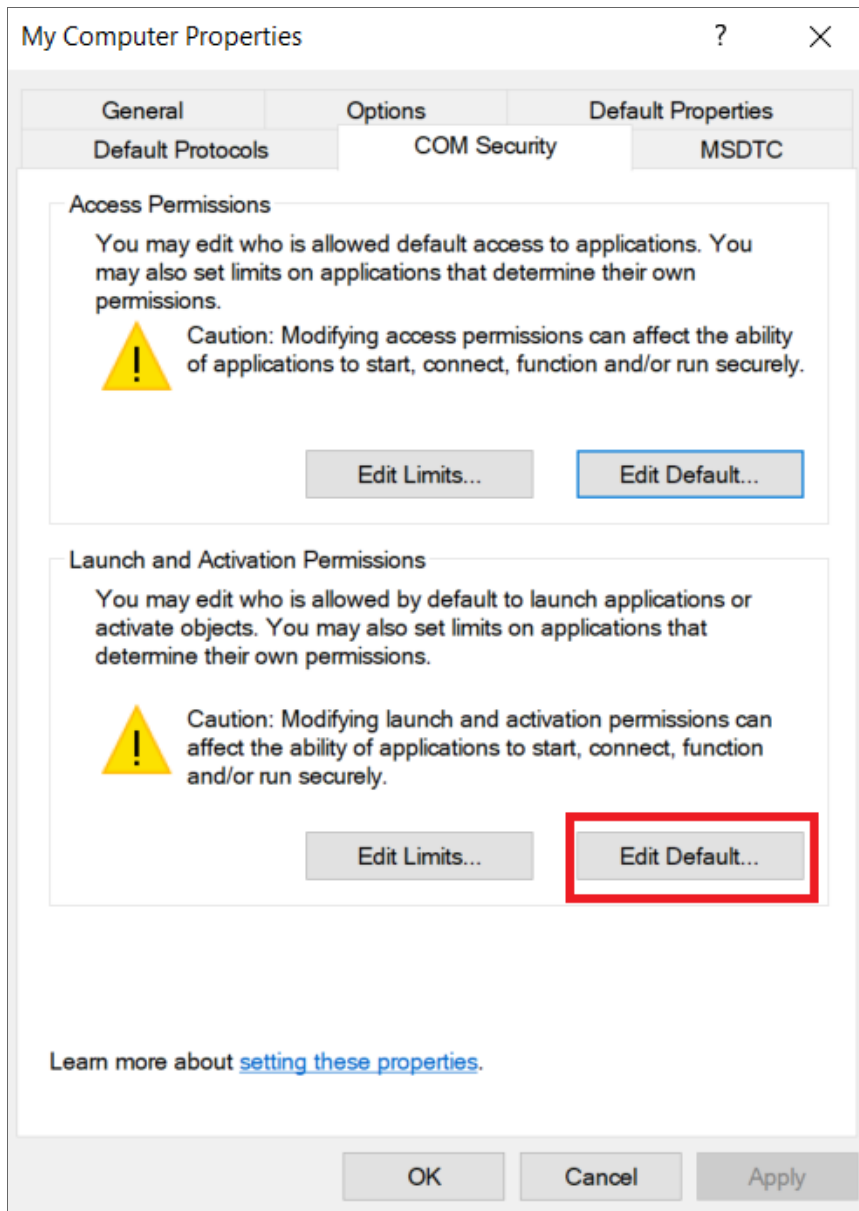


4. In the **My Computer Properties** window, click the **[Default Properties]** tab and then complete the following fields:

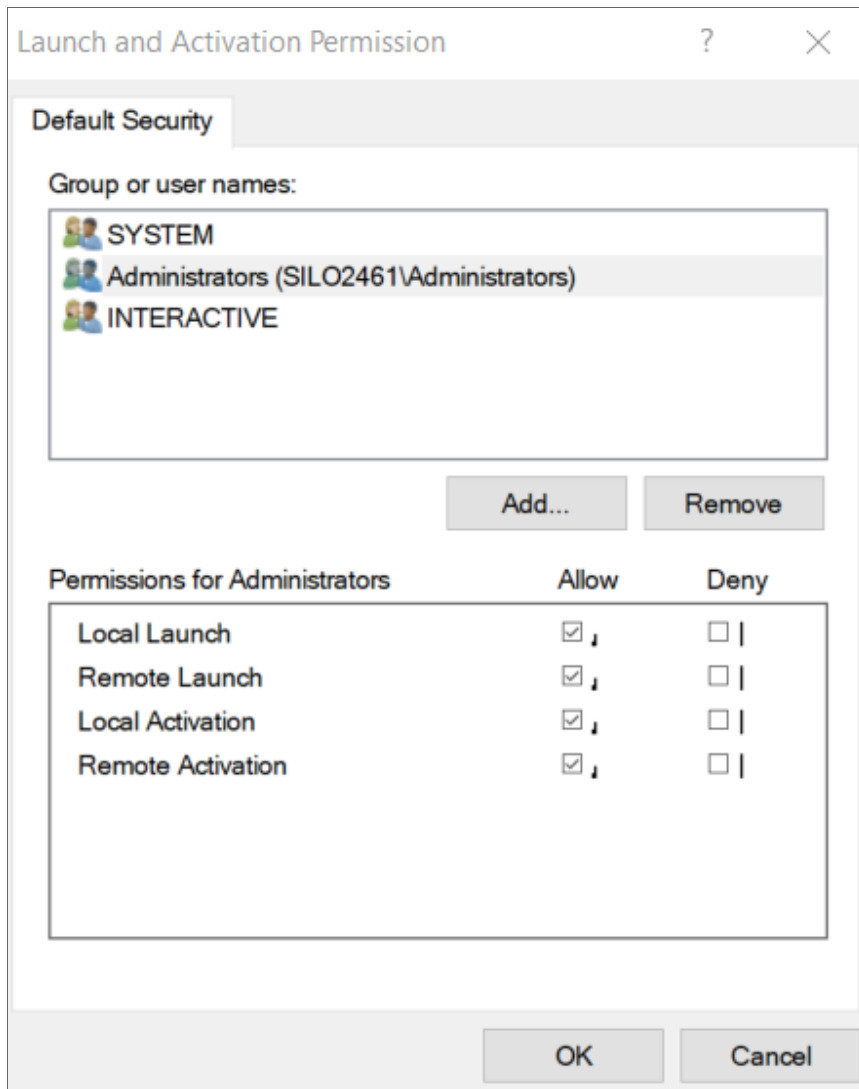


- **Enable Distributed COM on this computer.** Select this checkbox.
- **Default Authentication Level.** Select *Connect*.
- **Default Impersonation Level.** Select *Identify*.

5. In the **My Computer Properties** window, click the **[COM Security]** tab. Under **Launch and Activation Permissions**, click the **[Edit: Default...]** button.



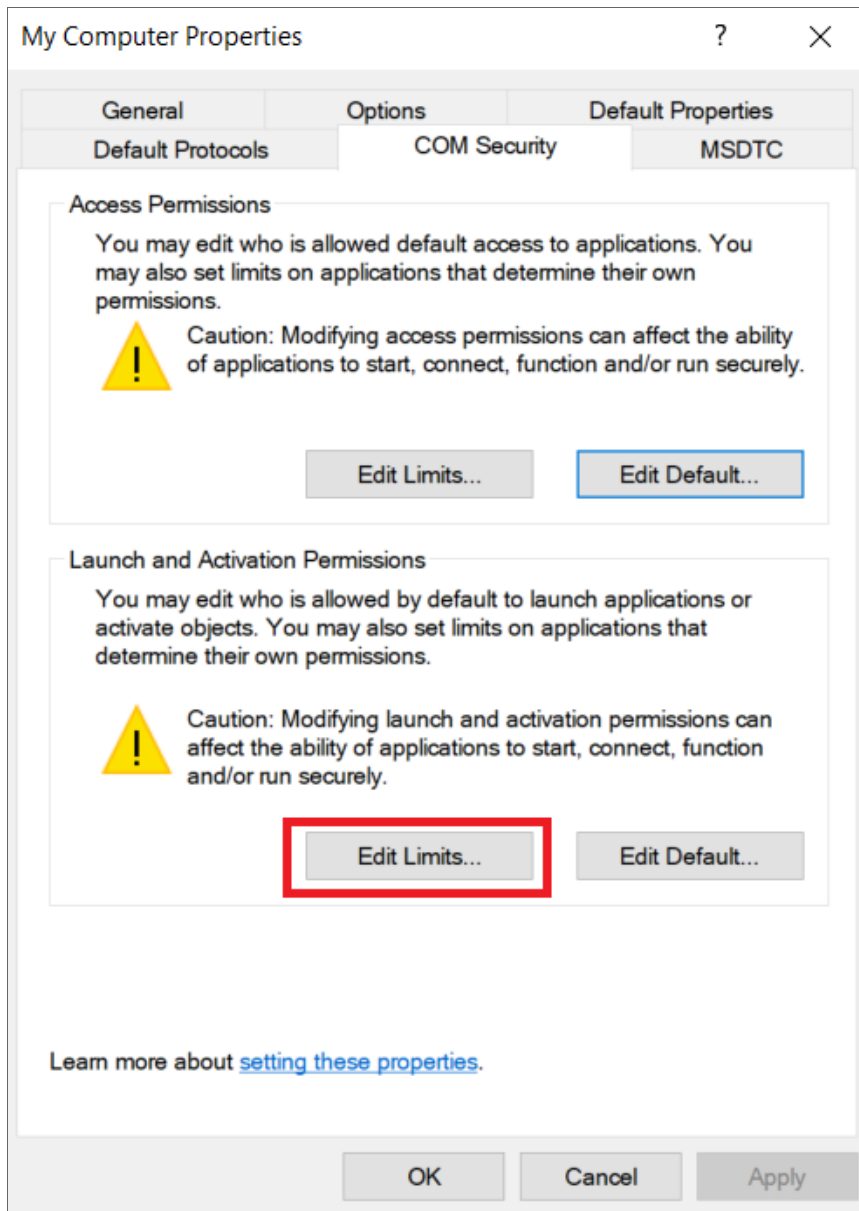
6. In the **Launch and Activation Permission** window, select the following:



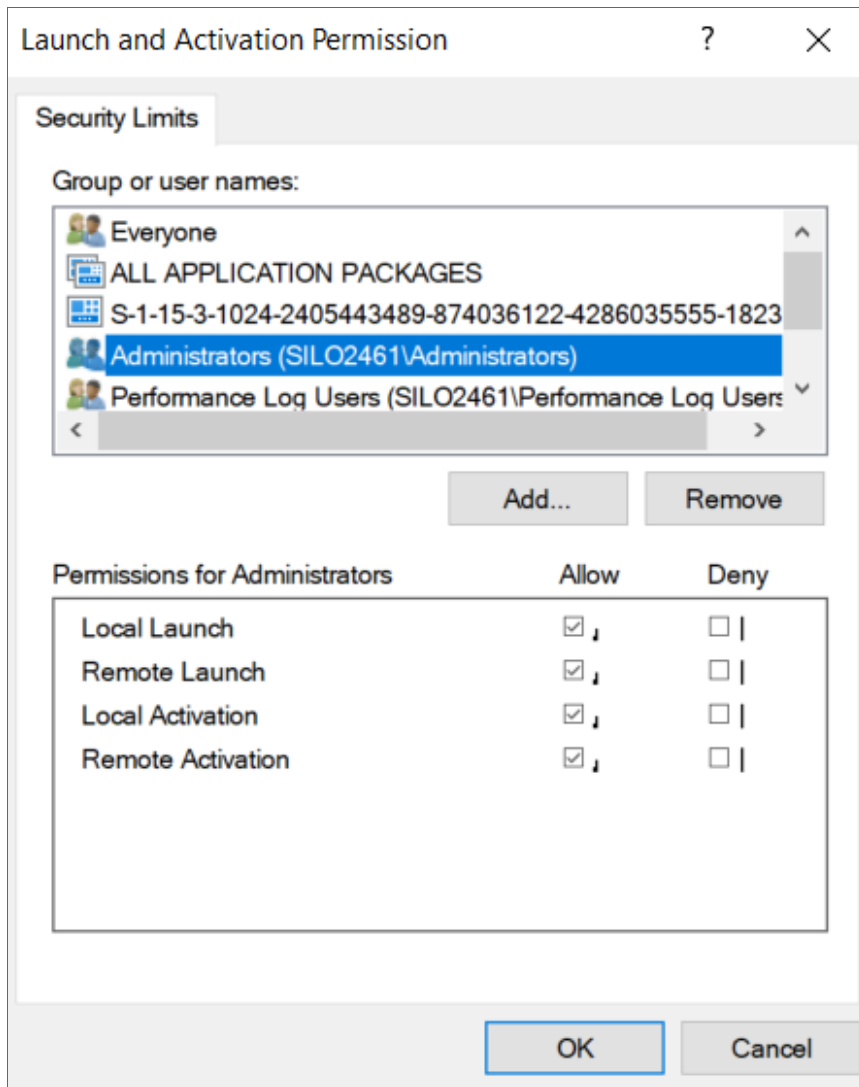
- **Group or user names.** Select *Administrators*.
- **Permissions for Administrators.** Set **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** to *Allow*.

7. Click **[OK]**.

8. In the **My Computer Properties** window, in the **Launch and Activation Permissions** pane, click the [**Edit Limits...**] button.



9. In the **Launch Permission** window, select the following:



- **Group or user names.** Select *Administrators*.
- **Permissions for Administrators.** Set **Local Launch**, **Remote Launch**, **Local Activation**, and **Remote Activation** to *Allow*.

10. Click **OK** in this window and the following windows, and then close the **Component Services** window.

11. Restart the computer to save the settings.

Step 5: Disabling User Account Control

To monitor a device running Windows 7, 8, or 10, you must perform the following additional steps to disable the User Account Control (UAC) filter for remote logins:

1. Use a text editor such as Notepad to create a new file.

2. Include the following in the file.:

```
Windows Registry Editor Version 5.00
[HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\System]
"LocalAccountTokenFilterPolicy"=dword:00000001
```

3. Save the file with a name of your choice, like disableUAC.reg, to the directory of your choice. Make sure to save the new file with the .reg suffix.
4. In Windows Explorer, double click on the .reg file to execute it.

SNMP and WMI Dynamic Applications for Windows Devices

Overview

The following sections describe the SNMP and WMI Dynamic Applications that the ScienceLogic platform uses to monitor Windows devices:

<i>SNMP Dynamic Applications</i>	71
<i>WMI Dynamic Applications</i>	72
<i>Microsoft Base Pack</i>	72

SNMP Dynamic Applications

If you configure your Windows system to respond to SNMP requests from the ScienceLogic platform, you can discover your Windows system as an SNMP device. When the ScienceLogic platform discovers a Windows system as an SNMP device, the platform will automatically collect the same data from the Windows system that the platform collects from most network devices. This data includes interface usage, file system usage, CPU usage, memory usage, and hardware configuration information.

In addition to the common SNMP data collection, you can install an optional agent that reports WMI information through SNMP. The following SNMP Dynamic Applications can be used to collect the information reported by the optional agent:

- MSSQL: General
- MSSQL: Memory
- MSSQL: SQL Stats

WMI Dynamic Applications

If you configure your Windows system to respond to WMI requests from the ScienceLogic platform, you can use WMI Dynamic Applications to collect information from your Windows system.

NOTE: Although the the ScienceLogic platform supports WMI Dynamic Applications, ScienceLogic recommends that you use PowerShell Dynamic Applications where possible. PowerShell is the preferred management platform for Microsoft products.

All of the WMI Dynamic Applications include a discovery object. If you include a credential for WMI Dynamic Applications in the discovery session that includes your Windows system, the ScienceLogic platform will automatically align the appropriate WMI Dynamic Applications to the Windows system. For more information about creating a discovery session, see the *Discovery & Credentials* manual.

The following PowerPack includes WMI Dynamic Applications for Microsoft systems.

Microsoft Base Pack

NOTE: The Dynamic Applications in this PowerPack support Windows Server 2008, 2012, and 2016, as well as Windows XP, 7, 8, and 10 desktop systems.

The following WMI Dynamic Applications can be used to collect performance data from Windows Servers or Windows desktop systems as a user with standard permissions:

- Windows CPU
- Windows Disk
- Windows Interface
- Windows Memory

The following WMI Dynamic Applications can be used to collect configuration data from Windows Servers or Windows desktop systems as a user with standard permissions:

- Windows Asset
- Windows Process List
- Windows Service List
- Windows SMART Status

Creating SNMP and WMI Credentials for Windows Devices

Overview

The following sections describe how to create SNMP and WMI credentials for Windows devices that you want to monitor with the ScienceLogic platform:

<i>Creating an SNMP Credential</i>	73
<i>Creating a WMI Credential</i>	76
<i>Testing Windows Credentials</i>	78
<i>SNMP Credential Test</i>	78
<i>Basic/Snippet Credential Test</i>	78
<i>Running a Windows Credential Test</i>	78

Creating an SNMP Credential

SNMP Credentials (called "community strings" in earlier versions of SNMP) allow the ScienceLogic platform to access SNMP data on a managed device. The platform uses SNMP credentials to perform discovery, run auto-discovery, and gather information from SNMP Dynamic Applications.

To create an SNMP credential:

1. Go to the **Credential Management** page (System > Manage > Credentials).

Profile Name	Organization	RO Use	RW Use	DS Use	Type	Credential User	Host	Port	Timeout (ms)	ID	Last	Actions
1. Amazon Web Services Credential	System	--	--	--	SOAP/XML Host	AWS Account Access	example.com	80	2000	1	2015-05-16	Create SNMP Credential
2. Azure Credential - SOAP/XML	[all orgs]	--	--	--	SOAP/XML Host	<AD_USER>	login.windows.net	443	60000	60	2015-05-14	Create Database Credential
3. Azure Credential - SSH/Key	[all orgs]	--	--	--	SSH/Key	<SUBSCRIPTION_ID_H	%D	22	180000	59	2015-05-14	Create SOAP/XML Host Credential
4. Cisco SNMPv2 - Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	3	2015-05-14	Create LDAP/AD Credential
5. Cisco SNMPv3 - Example	[all orgs]	--	--	--	SNMP	{USER_GOES_HERE}	--	161	1500	2	2015-05-14	Create Basic/Snippet Credential
6. Cisco ACI	[all orgs]	--	--	126	Basic/Snippet	admin	173.36.219.46	443	0	62	2015-05-14 15:05:24	Create SSH/Key Credential
7. Cisco ACI Credential	[all orgs]	--	--	--	Basic/Snippet	admin	198.18.133.200	443	0	61	2015-05-14 14:32:20	Create PowerShell Credential
8. Cloudkick - Example	[all orgs]	--	--	--	Basic/Snippet	{SECURITY KEY GOES}	127.0.0.1	443	5000	9	2015-05-14 11:25:31	
9. GUCM Perfmon/Service 8.0 Example	[all orgs]	--	--	--	SOAP/XML Host	--	%D	8443	2000	4	2015-05-14 11:25:12	
10. EM7 Central Database	[all orgs]	--	--	--	Database	root	localhost	7706	0	51	2015-05-14 11:28:41	
11. EM7 Collector Database	[all orgs]	--	--	--	Database	root	%D	7707	0	14	2015-05-14 11:25:43	
12. EM7 DB	[all orgs]	--	--	--	Database	root	%D	7706	0	35	2015-05-14 11:28:32	
13. EM7 DB - DB Info	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	38	2015-05-14 11:28:32	
14. EM7 DB - My.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	37	2015-05-14 11:28:32	
15. EM7 DB - Ssl.cnf	[all orgs]	--	--	--	SOAP/XML Host	root	%D	80	3000	36	2015-05-14 11:28:32	
16. EM7 Default V2	[all orgs]	--	--	--	SNMP	--	--	161	1500	10	2015-05-14 11:25:42	
17. EM7 Default V3	[all orgs]	--	--	--	SNMP	em7defaultv3	--	161	500	11	2015-05-14 11:25:42	
18. EMC - Example	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	10000	15	2015-05-14 11:25:47	
19. GoGrid - Example	[all orgs]	--	--	--	Basic/Snippet	{SECURITY KEY GOES}	127.0.0.1	443	5000	16	2015-05-14 11:25:51	
20. IP-SLA Example	[all orgs]	--	--	--	SNMP	--	--	161	1500	5	2015-05-14 11:25:14	
21. LifeSize - Endpoint SNMP	[all orgs]	--	--	--	SNMP	control	--	161	3000	16	2015-05-14 11:25:58	
22. LifeSize - Endpoint SSH/CLI	[all orgs]	--	--	--	Basic/Snippet	auto	%D	22	3	17	2015-05-14 11:25:58	
23. Local API	[all orgs]	--	--	--	Basic/Snippet	em7admin	192.0.0.189	80	5000	22	2015-05-14 11:28:11	
24. NetApp 7-mode	[all orgs]	--	--	--	Basic/Snippet	root	%D	443	3000	24	2015-05-14 11:28:20	
25. NetApp w/SSL Option	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	3000	26	2015-05-14 11:28:20	
26. NetApp w/SSL Option Off	[all orgs]	--	--	--	SOAP/XML Host	root	%D	443	10000	25	2015-05-14 11:28:20	
27. Nexus netconf	[all orgs]	--	--	--	Basic/Snippet	--	%D	22	10000	6	2015-05-14 11:25:16	
28. Nexus snmp	[all orgs]	--	--	--	SNMP	--	--	161	10000	7	2015-05-14 11:25:16	
29. Polycom - Advanced	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	28	2015-05-14 11:28:24	
30. Polycom - CDR	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	31	2015-05-14 11:28:24	
31. Polycom - Interface	[all orgs]	--	--	--	SOAP/XML Host	admin	%D	80	20000	29	2015-05-14 11:28:24	

2. Click the **[Actions]** button and select **Create SNMP Credential**. The **Credential Editor** page appears.

Credential Editor X

Create New SNMP Credential Reset

Basic Settings

Profile Name: SNMP Version: [SNMP V2]

Port: Timeout(ms): Retries:

SNMP V1/V2 Settings

SNMP Community (Read-Only): SNMP Community (Read/Write):

SNMP V3 Settings

Security Name: Security Passphrase:

Authentication Protocol: [MD5] Security Level: [Authentication Only] SNMP v3 Engine ID:

Context Name: Privacy Protocol: [DES] Privacy Protocol Pass Phrase:

Save

3. Supply values in the following fields:

- **Profile Name**. Name of the credential. Can be any combination of alphanumeric characters. This field is required.
- **SNMP Version**. SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*. This field is required.

- **Port.** The port the platform will use to communicate with the external device or application. The default value is *161*. This field is required.
- **Timeout (ms).** Time, in milliseconds, after which the platform will stop trying to communicate with the SNMP device. The default value is *1500*. This field is required.
- **Retries.** Number of times the platform will try to authenticate and communicate with the external device. The default value is *1*. This field is required.

SNMP V1/V2 Settings

These fields appear if you selected *SNMP V1* or *SNMP V2* in the **SNMP Version** field. Otherwise, these fields are grayed out.

- **SNMP Community (Read Only).** The SNMP community string (password) required for read-only access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the **SNMP Community (Read/Write)** field.
- **SNMP Community (Read/Write).** The SNMP community string (password) required for read and write access of SNMP data on the remote device or application. For SNMP V1 and SNMP V2 credentials, you must supply a community string, either in this field or in the **SNMP Community (Read Only)** field.

SNMP V3 Settings

These fields appear if you selected *SNMP V3* in the **SNMP Version** field. Otherwise, these fields are grayed out.

- **Security Name.** Name for SNMP authentication. This field is required.
- **Security Passphrase.** Password to authenticate the credential. This value must contain at least 8 characters. This value is required if you use a **Security Level** that includes authentication.
- **Authentication Protocol.** Select an authentication algorithm for the credential. Choices are MD5 or SHA. The default value is *MD5*. This field is required.
- **Security Level.** Specifies the combination of security features for the credentials. This field is required. Choices are:
 - *No Authentication / No Encryption.*
 - *Authentication Only.* This is the default value.
 - *Authentication and Encryption.*
- **SNMP v3 Engine ID.** The unique engine ID for the SNMP agent you want to communicate with. (SNMPv3 authentication and encryption keys are generated based on the associated passwords and the engine ID.) This field is optional.
- **Context Name.** A context is a mechanism within SNMPv3 (and AgentX) that allows you to use parallel versions of the same MIB objects. For example, one version of a MIB might be associated with SNMP Version 2 and another version of the same MIB might be associated with SNMP Version 3. For SNMP Version 3, specify the context name in this field. This field is optional.

- **Privacy Protocol.** The privacy service encryption and decryption algorithm. Choices are *DES* or *AES*. The default value is *DES*. This field is required.
 - **Privacy Protocol Passphrase.** Privacy password for the credential. This field is optional.
4. Click the **[Save]** button to save the new SNMP credential.
 5. Repeat steps 1-4 for each SNMP-enabled device in your network that you want to monitor with the ScienceLogic platform.

NOTE: When you define a SNMP Credential, the ScienceLogic platform automatically aligns the credential with all organizations of which you are a member.

Creating a WMI Credential

NOTE: Although the the ScienceLogic platform supports WMI Dynamic Applications, ScienceLogic recommends that you use PowerShell Dynamic Applications where possible. PowerShell is the preferred management platform for Microsoft products.

If you configure your Windows system to respond to WMI requests from the ScienceLogic platform, you can use WMI Dynamic Applications to collect information from your Windows system.

All of the WMI Dynamic Applications include a discovery object. If you include a credential for WMI Dynamic Applications in the discovery session that includes your Windows system, the ScienceLogic platform will automatically align the appropriate WMI Dynamic Applications to the Windows system. For more information about creating a discovery session, see the **Discovery & Credentials** manual.

You can create a credential for WMI Dynamic Applications from the **Credential Management** page. To create a credential for a WMI Dynamic Application:

1. Go to the **Credential Management** page (System > Manage > Credentials).

2. Select the **[Create]** button in the upper right of the page. Select **Basic/Snippet Credential**.

ID	Name	Type	Host	Status
1	@PS 160	Basic/Snippet	SOAPPX/Host	NO
2	@PS 163	Basic/Snippet	SOAPPX/Host	NO
3	@PS 164	Basic/Snippet	SNMP	NO
4	@PS 165 (Longer Timeout)	Basic/Snippet	SNMP	NO
5	@PS 166	Basic/Snippet	SECURITY KEY GOES HERE 127.0.0.1	NO
6	@PS 167	Basic/Snippet	SOAPPX/Host	em7App
7	@PS 168	Basic/Snippet	SOAPPX/Host	em7App
8	@PS 169 (Performance Service 8.0 Example)	Basic/Snippet	SOAPPX/Host	NO
9	@PS 170 (Collector Database)	Database	root	NO
10	@PS 171 (Default V2)	SNMP	em7DefaultV2	NO
11	@PS 172 (Default V3)	SNMP	em7DefaultV3	NO
12	@PS 173 (Example)	Basic/Snippet	root	NO
13	@PS 174 (Example)	Basic/Snippet	root	NO
14	@PS 175 (Example)	Basic/Snippet	SECURITY KEY GOES HERE 127.0.0.1	NO
15	@PS 176 (Example)	SNMP	em7App	NO
16	@PS 177 (Example)	Basic/Snippet	auto	NO
17	@PS 178 (Example)	Database	sa	NO
18	@PS 179 (Example)	Database	sa	NO
19	@PS 180 (Example)	Database	root	NO
20	@PS 181 (Example)	Basic/Snippet	root	NO
21	@PS 182 (Example)	Basic/Snippet	root	NO
22	@PS 183 (Example)	Basic/Snippet	root	NO
23	@PS 184 (Example)	Database	sa	NO
24	@PS 185 (Example)	Database	sa	NO
25	@PS 186 (Example)	Database	sa	NO
26	@PS 187 (Example)	Database	sa	NO
27	@PS 188 (Example)	Database	sa	NO
28	@PS 189 (Example)	Database	sa	NO
29	@PS 190 (Example)	Database	sa	NO
30	@PS 191 (Example)	Database	sa	NO
31	@PS 192 (Example)	Database	sa	NO
32	@PS 193 (Example)	Database	sa	NO
33	@PS 194 (Example)	Database	sa	NO
34	@PS 195 (Example)	Database	sa	NO
35	@PS 196 (Example)	Database	sa	NO
36	@PS 197 (Example)	Database	sa	NO
37	@PS 198 (Example)	Database	sa	NO
38	@PS 199 (Example)	Database	sa	NO
39	@PS 200 (Example)	Database	sa	NO
40	@PS 201 (Example)	Database	sa	NO
41	@PS 202 (Example)	Database	sa	NO
42	@PS 203 (Example)	Database	sa	NO
43	@PS 204 (Example)	Database	sa	NO
44	@PS 205 (Example)	Database	sa	NO
45	@PS 206 (Example)	Database	sa	NO

3. The **Credential Editor** page appears, where you can define the following fields:

Credential Editor

Create New Basic/Snippet Credential Reset

Basic Settings

Credential Name

Hostname/IP Port Timeout(ms)

Username Password

Save

- **Credential Name.** Name of the credential. Can be any combination of alphanumeric characters.
- **Hostname/IP.** Hostname or IP address of the device from which you want to retrieve data. To use the same WMI default credential for multiple devices, enter %D in this field.
- **Port.** Port number associated with the data you want to retrieve. For WMI Dynamic Applications that perform WBEM requests, supply the port used by the WBEM service on the device. For WMI Dynamic Applications that perform WMI requests, which includes all default WMI Dynamic Applications in the ScienceLogic platform, enter any valid port number in this field; the platform does not specify a port number when performing WMI requests.
- **Timeout (ms).** Time, in milliseconds, after which the platform will stop trying to communicate with the authenticating server.
- **Username.** Username for a user account on the device.

NOTE: To specify a domain user, enter the username in the format DOMAIN\username. In most cases, you should use a domain user in the credential and use the format DOMAIN\username.

- **Password.** Password for a user account on the device.

4. To save the credential, select the **[Save]** button. To clear the values you set, select the **[Reset]** button.

Testing Windows Credentials

Credential Tests define a series of steps that the platform can execute on-demand to validate whether a credential works as expected. This section describes the SNMP and Basic/Snippet Credential Tests that are included in the default installation of the platform.

SNMP Credential Test

The SNMP Credential Test can be used to test an SNMP credential for connectivity. The SNMP Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to the host specified in the credential.
- **Test Port Availability.** Performs an NMAP request to the UDP port specified in the credential on the host specified in the credential.
- **Test SNMP Availability.** Attempts an SNMP getnext request to .1.3.6.1 using the credential.

Basic/Snippet Credential Test

The Basic/Snippet Credential Test can be used to test a Basic/Snippet credential for connectivity. The Basic/Snippet Credential Test performs the following steps:

- **Test Reachability.** Performs an ICMP ping request to the host specified in the credential.
- **Test Port Availability.** Performs an NMAP request to the TCP port specified in the credential on the host specified in the credential.
- **Test Name Resolution.** Performs an nslookup request on the host specified in the credential.

Running a Windows Credential Test

To run a Windows credential test from the **Credential Management** page:

1. Go to the **Credential Management** page (System > Manage > Credentials).

- Click the **[Actions]** menu, and then select *Test Credential*. The **Credential Tester** modal page appears:

- Supply values in the following fields:

- Test Type.** Select a credential test to run.
- Credential.** Select the credential you want to test. This drop-down list includes only credentials that you have access to that can be tested using the selected credential test.
- Hostname/IP.** Enter a hostname or IP address that will be used during the test. For example, if you are testing an SNMP credential, the hostname/IP address you supply will be used to perform a test SNMP request.
- Collector.** Select the All-In-One Appliance or Data Collector that will run the test.

- Click the **[Run Test]** button to run the credential test. The **Test Credential** window appears:

Test Credential Test execution complete					
Step	Description	Log Message	Status		
1	Test Reachability	Check to see if the device is reachable using ICMP	The device is reachable using ICMP. The average response time is 0.397ms	Passed	?
2	Test Port Availability	Check to see if the SNMP port is open	Port 161 is open	Passed	?
3	Test SNMP Availability	Check to see if a walk of SNMP will return results	The SNMP SysName is ScienceLogic EM7 G3 - All-In-One	Passed	?

The **Test Credential** window displays a log entry for each step in the credential test. The steps performed are different for each credential test. The log entry for each step includes the following information:

- Step.** The name of the step.
- Description.** A description of the action performed during the step.
- Log Message.** The result of the step for this execution of the credential test.
- Status.** Whether the result of this step indicates the credential and/or the network environment is configured correctly (Passed) or incorrectly (Failed).
- Step Tip.** Mouse over the question mark icon (?) to display the tip text. The tip text recommends what to do to change the credential and/or the network environment if the step has a status of "Failed".

- Optionally, you can click the **[Execute Discovery Session]** button to run a discovery session using the **Credential**, **Hostname/IP**, and **Collector** you selected in the **Credential Tester** modal page.

Monitoring a Windows Cluster

Overview

The following sections describe how to monitor a Windows Cluster using the ScienceLogic platform:

<i>Monitoring Windows Clusters in the ScienceLogic Platform</i>	80
<i>Discovering Cluster Nodes</i>	81
<i>Aligning a Dynamic Application with a Cluster Node</i>	81
<i>Disabling Collection of a Dynamic Application on a Device</i>	82
<i>Discovering the Cluster IP Address</i>	83
<i>Aligning Dynamic Applications with the Cluster Device</i>	85
<i>Using a Device Template to Configure Dynamic Applications</i>	86

Monitoring Windows Clusters in the ScienceLogic Platform

The general approach for monitoring a Windows Cluster is to discover each cluster node and then discover the shared IP address as an additional, separate, device:

- For each cluster node, configure the ScienceLogic platform to monitor the non-cluster related aspects of the devices. For example, the CPU, memory, and interface utilization for each node. When you configure monitoring for each cluster node, you will ensure that the cluster services are not monitored on each cluster node.

- For the additional device that represents the cluster itself, configure the ScienceLogic platform to monitor the clustered services. For example, you would align the performance Dynamic Applications that collect data about a Windows device to this device record. When you configure monitoring for the device record that represents the clustered services, you will ensure that node-specific data, for example, CPU, memory, and interface utilization, is not monitored through the shared IP.

NOTE: Version 101 of the *Microsoft: SQL Server Enhanced PowerPack* does not support the ability to monitor SQL Server clusters. The SQL Servers that you monitor must not be using Windows Server Failover Clustering (WSFC) or SQL Server Failover Cluster Instances (FCI) for high-availability.

By monitoring the shared IP address separately, the ScienceLogic platform will always poll the active cluster node for information about the clustered service.

Discovering Cluster Nodes

The steps to discover the individual cluster nodes depend on the types of Dynamic Application you will use to monitor the cluster services, i.e. the Dynamic Applications that will be aligned with the device record for the shared IP address. When you discover each cluster node, you must configure the ScienceLogic platform to ensure that the Dynamic Applications for the clustered service are not aligned automatically.

There are several approaches to preventing the Dynamic Applications for the clustered service from being automatically aligned to each cluster node:


- In the discovery session for a cluster node, do not include any credentials that can be used to collect the Dynamic Applications for the clustered service. For example, if you will use WMI Dynamic Applications to monitor the clustered service, do not include a credential that can be used to successfully make WMI requests in the discovery session. By using this method, you might prevent the automatic alignment of Dynamic Applications that you would like to align with the cluster nodes; in this case, you would have to align those Dynamic Applications manually.
- In some cases, you might need or want to include credentials that can be used to collect Dynamic Applications for the clustered service in the discovery session for a cluster node. This typically occurs when the Dynamic Applications for the clustered service use the SNMP protocol. If you need to include any credential that can be used to collect Dynamic Applications for the clustered service in the discovery session for a cluster node, you can allow the Dynamic Applications for the clustered service to align with the device records for the cluster nodes, then manually disable collection for those Dynamic Applications on those devices. The ScienceLogic platform will not re-enable collection for those Dynamic Applications.

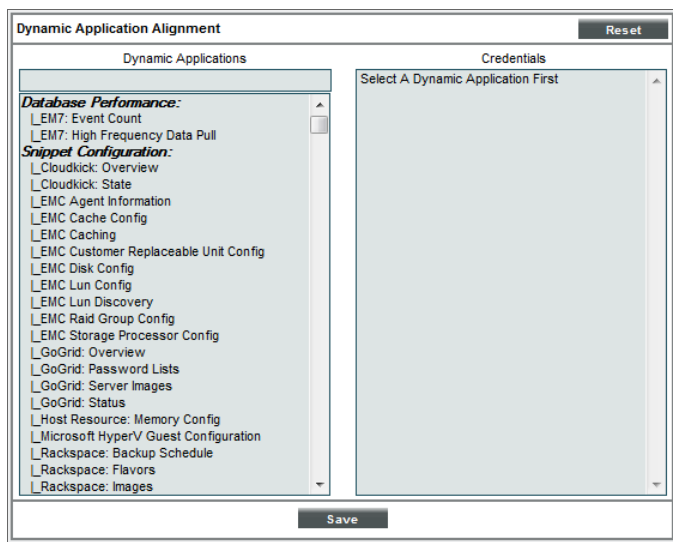
The following sub-sections describe how to manually align a Dynamic Application with a cluster node and how to disable collection of a Dynamic Application on a device. If you are configuring the ScienceLogic platform to monitor multiple clusters that provide the same service, you can speed up both of these tasks by [creating and applying device templates](#).

Aligning a Dynamic Application with a Cluster Node

If you need to manually align a Dynamic Application to a cluster node, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).


2. Select the wrench icon () for the cluster node. The **Device Properties** page is displayed.
3. Select the [**Collections**] tab. The **Dynamic Application Collections** page is displayed.
4. Select the [**Action**] button.
5. Select **Add Dynamic Application**. The **Dynamic Application Alignment** page appears:



6. In the **Dynamic Application Alignment** page, select the Dynamic Application you want to align in the **Dynamic Applications** field.
7. In the **Credentials** field, select the credential for the Dynamic Application.
8. Select the [**Save**] button.

Disabling Collection of a Dynamic Application on a Device

If you need to manually disable collection for a Dynamic Application on a device, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Select the wrench icon () for the device record for the cluster. The **Device Properties** page is displayed.

3. Select the **[Collections]** tab. The **Dynamic Application Collections** page is displayed:

Close		Properties	Thresholds	Collections	Monitors			
Schedule		Logs	Toolbox	Interfaces	Relationships	Tickets	Redirects	Notes
Device Name	MSSQL-CLUSTER-1.QA.LOCAL			Managed Type	Physical Device			 MSSQL-CLUSTER-1.QA
IP Address / ID	10.168.44.206 38			Category	Servers			
Class	Microsoft			Sub-Class	Windows 2008 Server R2			
Organization	DC - Servers			Uptime	2 days, 17:24:26			
Collection Mode	Active			Collection Time	2012-03-19 18:45:00			
Description	Hardware: Intel® Family 6 Model 46 Stepping 6 AT/AT COMPATIBLE - S			Group / Collector	CUG em7_a0			

Dynamic Application™ Collections							Expand	Action	Reset	Guide
	ID	Poll Frequency	Type	Credential						
+ Informant: Memory	312	5 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>					
+ Informant: Volumes	314	5 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>					
+ MSSQL: General	84	10 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>					
+ MSSQL: Memory	83	10 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>					
+ MSSQL: SQL Stats	82	10 mins	SNMP Performance	Default SNMP Credential	<input type="checkbox"/>					
+ Host Resource: CPU Config	12	1440 mins	SNMP Configuration	Default SNMP Credential	<input type="checkbox"/>					
+ Host Resource: Software	9	120 mins	SNMP Configuration	Default SNMP Credential	<input type="checkbox"/>					
+ Host Resource: CPU	10	5 mins	Snippet Performance	Default SNMP Credential	<input type="checkbox"/>					
+ Host Resource: Memory	8	5 mins	Snippet Performance	Default SNMP Credential	<input type="checkbox"/>					
+ Host Resource: Memory Config	11	1440 mins	Snippet Configuration	Default SNMP Credential	<input type="checkbox"/>					

[Select Action]

4. Select the checkbox for each Dynamic Application you want to disable.
5. In the **Select Action** drop-down list, select *Disable All Collection Objects*.
6. Select the **[Go]** button.

Discovering the Cluster IP Address

To discover the additional device that represents the cluster, you must run a discovery session to discover a shared IP address for the cluster as a pingable device. By discovering the shared IP address as a cluster, you will prevent the ScienceLogic platform from automatically collecting node-specific data using SNMP. After discovering the cluster as a pingable device, you can manually align the Dynamic Applications that will monitor the clustered service with the device record for the cluster.

If you are configuring the ScienceLogic platform to monitor multiple clusters that provide the same service, you can [create a device template](#) to speed up the manual configuration of Dynamic Applications.


To discover the virtual IP of the cluster as a pingable device:

1. Go to the **Discovery Control Panel** page (System > Manage > Discovery).

2. Select the **[Create]** button. The **Discovery Session Editor** page appears:


3. Supply values in the following fields:

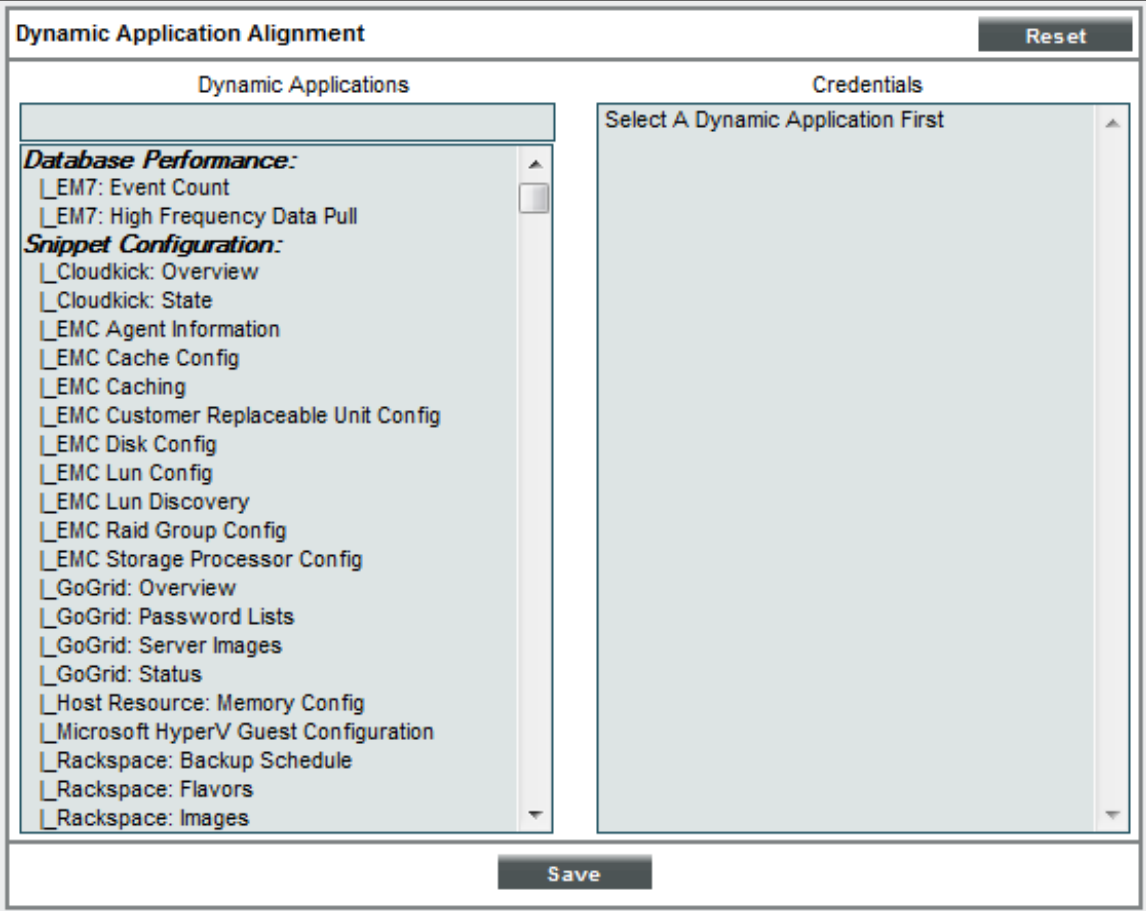
- **IP Address Discovery List.** Enter the shared IP address for the cluster.
- **SNMP Credentials.** Do not select any credentials.
- **Other Credentials.** Do not select any credentials.
- **Discover Non-SNMP.** Select this checkbox.
- **Duplication Protection.** Deselect this checkbox. If you discovered the cluster nodes as SNMP devices, the ScienceLogic platform will have associated the shared IP address for the cluster with one of those nodes. You must disable duplication protection for the ScienceLogic platform to discover the shared IP address as a new device.
- **Apply Device Template.** If you are [using a device template to configure Dynamic Applications](#), select the device template in this field.

4. For the other fields in this page, you can use the default values or select different values based on your operating procedures.
5. Select the **[Save]** button.
6. In the **Discovery Control Panel** page, select the lightning bolt icon () for the new discovery session.

Aligning Dynamic Applications with the Cluster Device

To manually align a Dynamic Application to the device record for the cluster, perform the following steps:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Select the wrench icon () for the device record for the cluster. The **Device Properties** page is displayed.
3. Select the [**Collections**] tab. The **Dynamic Application Collections** page is displayed.
4. Select the [**Action**] button.
5. Select **Add Dynamic Application**. The **Dynamic Application Alignment** page appears:



Dynamic Application Alignment Reset

Dynamic Applications	Credentials
<p>Database Performance:</p> <ul style="list-style-type: none">EM7: Event CountEM7: High Frequency Data Pull <p>Snippet Configuration:</p> <ul style="list-style-type: none">Cloudkick: OverviewCloudkick: StateEMC Agent InformationEMC Cache ConfigEMC CachingEMC Customer Replaceable Unit ConfigEMC Disk ConfigEMC Lun ConfigEMC Lun DiscoveryEMC Raid Group ConfigEMC Storage Processor ConfigGoGrid: OverviewGoGrid: Password ListsGoGrid: Server ImagesGoGrid: StatusHost Resource: Memory ConfigMicrosoft HyperV Guest ConfigurationRackspace: Backup ScheduleRackspace: FlavorsRackspace: Images	Select A Dynamic Application First

Save

6. In the **Dynamic Application Alignment** page, select the Dynamic Application you want to align in the **Dynamic Applications** field.
7. In the **Credentials** field, select the credential for the Dynamic Application.
8. Select the [**Save**] button.

Using a Device Template to Configure Dynamic Applications

If you are configuring the ScienceLogic platform to monitor multiple clusters that provide the same service, you can create a device template to speed up the manual configuration of Dynamic Applications on the cluster nodes and/or the device record that represents the cluster.

To create a device template that configures a Dynamic Application on a device:

1. Go to the **Configuration Templates** page (Registry > Devices > Templates).
2. Select the **[Create]** button. The **Device Template Editor** page is displayed.
3. Select the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page is displayed:

4. Select *Add New Dynamic App Sub-Template* in the left pane.
5. Supply values in the following fields:
 - **Align Dynamic Application With.** Select *All devices*.
 - **Dynamic Application.** Select the Dynamic Application that you want to configure.
 - **Credentials.** If you want to use the device template to align Dynamic Applications with a device, enable this field by clicking on the field name. Select the credential you want to align with the Dynamic Application on all devices to which this template is applied. If you want to use the device template to disable collection for this Dynamic Application, do not enable this field.

6. If you want to use the device template to disable collection for this Dynamic Application, select the name of each object that appears in the **Dynamic Application Settings** page. The object names appear below the **Credentials** field. In the drop-down list for each object, select *Disabled*.
7. If you want to configure multiple Dynamic Applications with this device template, repeat steps 4–6 for each additional Dynamic Application.
8. Select the **[Save]** button.

You can apply the device template to all devices in a discovery session by selecting the device template in the **Apply Device Template** field in the discovery session. To apply a device template to one or more devices after discovery:

1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
2. Select the checkbox for each device to which you want to apply the device template.
3. In the **Select Action** drop-down list, select *Modify By Template*.
4. Select the **[Go]** button. The **Device Template Editor** page is displayed:

The screenshot shows the 'Device Template Editor' interface with the following sections:

- Header:** 'Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)' and a 'Reset' button.
- Template Selection:** A dropdown menu set to 'New / One-off Template', a 'Save When Applied & Confirmed' checkbox, and a 'Template Name' input field.
- Navigation Tabs:** 'Config', 'Interface', 'CV Policies', 'Port Policies', 'Svc Policies', 'Proc Policies', and 'Dyn Apps'.
- Access & Monitoring:**
 - Device Organization: Acme Corporation
 - SNMP Read: c0sm0s, SNMP Write: None
 - Availability Protocol: TCP, Avail Port: ICMP
 - Latency Protocol: TCP, Latency Port: ICMP
 - Avail+Latency Alert: Disabled
 - Collection: Enabled, Collector Grp: CUG
 - Coll. Type: Standard
 - Critical Ping: Disabled
 - Event Mask: Disabled
- Device Preferences:**
 - Auto-Clear Events:
 - Scan All IPs:
 - Accept All Logs:
 - Dynamic Discovery:
 - Daily Port Scans:
 - Preserve Hostname:
 - Auto-Update:
 - Disable Asset Update:
- Device Retention & Basic Thresholds:**
 - System Latency: 500 ms
 - Bandwidth Data: 30 days
 - Normalized BW Data: 30 days
 - Performance Data: 30 days
 - Normalized Perf Data: 30 days
 - Device Logs Max: 5000 records
 - Log Age Max: 30 days
 - Ping Packet Size: 100 %
 - Number of Availability Pings: 1
- Footer:** An 'Apply' button.

5. Select the device template that you want to apply in the **Template** field.
6. Select the **[Apply]** button. A summary of the changes you are about to make is displayed.
7. Select the **[Confirm]** button.

Automatically Restarting Windows Services

Overview

The following sections describe how to use the *Windows Restart Automatic Services PowerPack* in the ScienceLogic platform:

<i>What is the Windows Restart Automatic Services PowerPack?</i>	88
<i>Configuring the Windows Restart Automatic Services PowerPack</i>	89
<i>Excluding Automatic Services</i>	90
<i>Viewing the List of Excluded Services</i>	90
<i>Adding an Excluded Service for All Devices</i>	90
<i>Adding an Excluded Service for a Single Device</i>	91
<i>Removing an Excluded Service</i>	91

What is the Windows Restart Automatic Services PowerPack?

The *Windows Restart Automatic Services PowerPack* can be used to:

- Monitor the state of Windows services with a startup type of "Automatic" using WMI.
- Automatically start failed services by making an RPC over SMB request.

Configuring the Windows Restart Automatic Services PowerPack

To configure the content in the *Windows Restart Automatic Services* PowerPack:

1. [Configure your Windows device to respond to remote WMI requests.](#)
2. [Create a WMI credential for your Windows device .](#)
3. Align the "Windows Find Automatic Services Not Running" Dynamic Application to the device with the WMI credential. If you include the WMI credential you created in the discovery session for your Windows device, this Dynamic Application will be aligned automatically.

The Dynamic Application collects the status of all services with a startup type of "Automatic" that are not on the [exclusion list](#):

The screenshot shows a configuration report for 'Windows Find Automatic Services Not Running'. The interface includes a top navigation bar with tabs for Close, Summary, Performance, Configs, Journals, Interfaces, and Logs. Below this is a detailed view of the device information, including the device name (TL008-HQ-AP-01.MSTL008.local), IP address (10.0.6.38), class (Microsoft), organization (System), and hardware details (Intel i4 Family 6 Model 44). A Windows 2008 logo is also present.

The main section of the report is a table titled 'Automatic Services' with columns for 'Display Name', 'Name', and 'State'. The table lists 30 services, with their current status indicated in the 'State' column. Most services are in a 'Running' state, but two are 'Stopped': 'Microsoft .NET Framework NGEN v4.0.30319_X64' and 'Microsoft .NET Framework NGEN v4.0.30319_X86'.

Display Name	Name	State
1. Windows Management Instrumentation	Winmgmt	Running
2. Hyper-V Guest Shutdown Service	vmicshutdow	Running
3. Shell Hardware Detection	ShellHWDetection	Running
4. IP Helper	iphlpvc	Running
5. Application Host Helper Service	AppHostSvc	Running
6. Windows Firewall	MpsSvc	Running
7. DHCP Client	Dhcp	Running
8. Windows Font Cache Service	FontCache	Running
9. Netlogon	Netlogon	Running
10. Network Store Interface Service	nsi	Running
11. Remote Procedure Call (RPC)	RpcSs	Running
12. User Profile Service	ProfSvc	Running
13. Power	Power	Running
14. COM+ Event System	EventSystem	Running
15. World Wide Web Publishing Service	W3SVC	Running
16. Microsoft .NET Framework NGEN v4.0.30319_X64	clr_optimization_v4.0.30319_64	Stopped
17. NetPipe Listener Adapter	NetPipeActivator	Running
18. Windows Event Log	eventlog	Running
19. None	None	None
20. Microsoft .NET Framework NGEN v4.0.30319_X86	clr_optimization_v4.0.30319_32	Stopped
21. DCOM Server Process Launcher	DcomLaunch	Running
22. Software Protection	spsvc	Running
23. Base Filtering Engine	BFE	Running
24. Hyper-V Data Exchange Service	vmickvexchange	Running
25. Workstation	LanmanWorkstation	Running
26. Hyper-V Time Synchronization Service	vmictimesync	Running
27. Net.Tcp Listener Adapter	NetTcpActivator	Running
28. Distributed Link Tracking Client	TrkWks	Running
29. Server	LanmanServer	Running
30. Print Spooler	Spooler	Running

If a service with a startup type of "Automatic" is in a non-running state, the platform will generate a major event. By default, this event will trigger the "Start Required Windows Services" automation policy, which will execute an RPC over SMB request to start the failed service. No additional configuration is required to configure this automation.

Excluding Automatic Services

The `master.definitions_service_autostart_exclude` database table specifies service with a type of "Automatic" that should not be monitored by the "Windows Find Automatic Services Not Running" Dynamic Application, either for a single device or all devices. The following services are defined as excluded for all devices by default:

- ATI HotKey Poller
- Distributed Transaction Coordinator
- Performance Logs and Alerts
- Removable Storage
- TPM Base Services
- Windows Service Pack Installer update service
- VSS

Viewing the List of Excluded Services

You can view the list of excluded services by performing the following steps:

1. Go to the **Database Tool** page (System > Tools > DB Tool).
2. In the **SQL Query** field, type the following query:

```
SELECT * FROM master.definitions_service_autostart_exclude;
```

3. Click **[Go]**.
4. The output includes the following fields:
 - **service_name**. The name of the excluded service.
 - **did**. The ID for the device for which the service is excluded. If this value is 0, the exclusion applies to all devices.

Adding an Excluded Service for All Devices

You can exclude a service for all devices by performing the following steps:

1. Go to the **Database Tool** page (System > Tools > DB Tool).
2. In the **SQL Query** field, type the following query, supplying the service name where indicated:

```
INSERT INTO master.definitions_service_autostart_exclude VALUES ("<service name>", 0);
```

3. Click **[Go]**.

Adding an Excluded Service for a Single Device

You can exclude a service for a single device by performing the following steps:

1. Go to the **Database Tool** page (System > Tools > DB Tool).
2. In the **SQL Query** field, type the following query:
 - Replace "X" with the device ID for which you want to exclude the service.
 - Supply the service name where indicated.

```
INSERT INTO master.definitions_service_autostart_exclude VALUES ("<service name>", X);
```

3. Click **[Go]**.

Removing an Excluded Service

You can remove an entry from the list of exclusions by performing the following steps:

1. Go to the **Database Tool** page (System > Tools > DB Tool).
2. In the **SQL Query** field, type the following query:
 - Replace "X" with the device ID associated with the entry that you want to delete.
 - Supply the service name where indicated.

```
DELETE FROM master.definitions_service_autostart_exclude WHERE service_name="<service name>" AND did=X;
```

3. Click **[Go]**.

© 2003 - 2019, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

ALL INFORMATION AVAILABLE IN THIS GUIDE IS PROVIDED "AS IS," WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED. SCIENCELOGIC™ AND ITS SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE OR NON-INFRINGEMENT.

Although ScienceLogic™ has attempted to provide accurate information on this Site, information on this Site may contain inadvertent technical inaccuracies or typographical errors, and ScienceLogic™ assumes no responsibility for the accuracy of the information. Information may be changed or updated without notice. ScienceLogic™ may also make improvements and / or changes in the products or services described in this Site at any time without notice.

Copyrights and Trademarks

ScienceLogic, the ScienceLogic logo, and EM7 are trademarks of ScienceLogic, Inc. in the United States, other countries, or both.

Below is a list of trademarks and service marks that should be credited to ScienceLogic, Inc. The ® and ™ symbols reflect the trademark registration status in the U.S. Patent and Trademark Office and may not be appropriate for materials to be distributed outside the United States.

- ScienceLogic™
- EM7™ and em7™
- Simplify IT™
- Dynamic Application™
- Relational Infrastructure Management™

The absence of a product or service name, slogan or logo from this list does not constitute a waiver of ScienceLogic's trademark or other intellectual property rights concerning that name, slogan, or logo.

Please note that laws concerning use of trademarks or product names vary by country. Always consult a local attorney for additional guidance.

Other

If any provision of this agreement shall be unlawful, void, or for any reason unenforceable, then that provision shall be deemed severable from this agreement and shall not affect the validity and enforceability of any remaining provisions. This is the entire agreement between the parties relating to the matters contained herein.

In the U.S. and other jurisdictions, trademark owners have a duty to police the use of their marks. Therefore, if you become aware of any improper use of ScienceLogic Trademarks, including infringement or counterfeiting by third parties, report them to Science Logic's legal department immediately. Report as much detail as possible about the misuse, including the name of the party, contact information, and copies or photographs of the potential misuse to: legal@sciencelogic.com



800-SCI-LOGIC (1-800-724-5644)

International: +1-703-354-1010