Monitoring Windows Systems with WMI

SL1 version 12.2.1

Table of Contents

Chapter 1

Introduction

Overview

This manual describes how to monitor Windows systems in SL1 using SNMP and Windows Management Instrumentation (WMI) credentials and Dynamic Applications.

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

The following sections provide an overview of SNMP and WMI, as well as the PowerPacks you can use to monitor Windows systems SL1:

This chapter covers the following topics:

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

SL1 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 SL1 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.

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. SL1 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***. SL1 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. SL1 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.

WMI Monitoring and System Scalability

SL1 versions 11.2.0, 11.1.3, and 10.2.5 included a new WMI client in response to Microsoft security updates. This change enables WMI Dynamic Applications to collect data from hardened Windows servers, but also has a major impact on system scalability.

This change significantly decreases the number of Microsoft Windows servers that can be supported on each Data Collector in your SL1 system compared to releases prior to the ones listed above. Users who need to

monitor Windows devices using WMI should analyze their system resources and capacity to ensure that they have the resources they need for the devices they want to monitor. For guidance about sizing, see ScienceLogic's Collector Sizing guidelines for WMI endpoints.

To avoid this impact, ScienceLogic recommends using SNMP collection for two-core Windows servers and PowerShell collection for four-core Windows servers. For more information, see this Support Knowledge Base article.

PowerPacks

This manual describes content from the following PowerPacks:

- *Microsoft Base Pack* PowerPack, version 110
- *Windows Restart Automatic Services* PowerPack, version 101

Chapter 2

Configuring Windows Systems for Monitoring with SNMP

Overview

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

The following sections describe how to configure Windows Server 2022, 2019, 2016, 2012, 2012r2, and Windows desktop systems for monitoring by SL1 using SNMP:

This chapter covers the following topics:

Configuring SNMP for Windows Server 2022, 2019, 2016, 2012, and 2012r2

To configure SNMP on a Windows 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 SL1 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, SL1 scans TCP ports 21, 22, 23, 25, and 80.

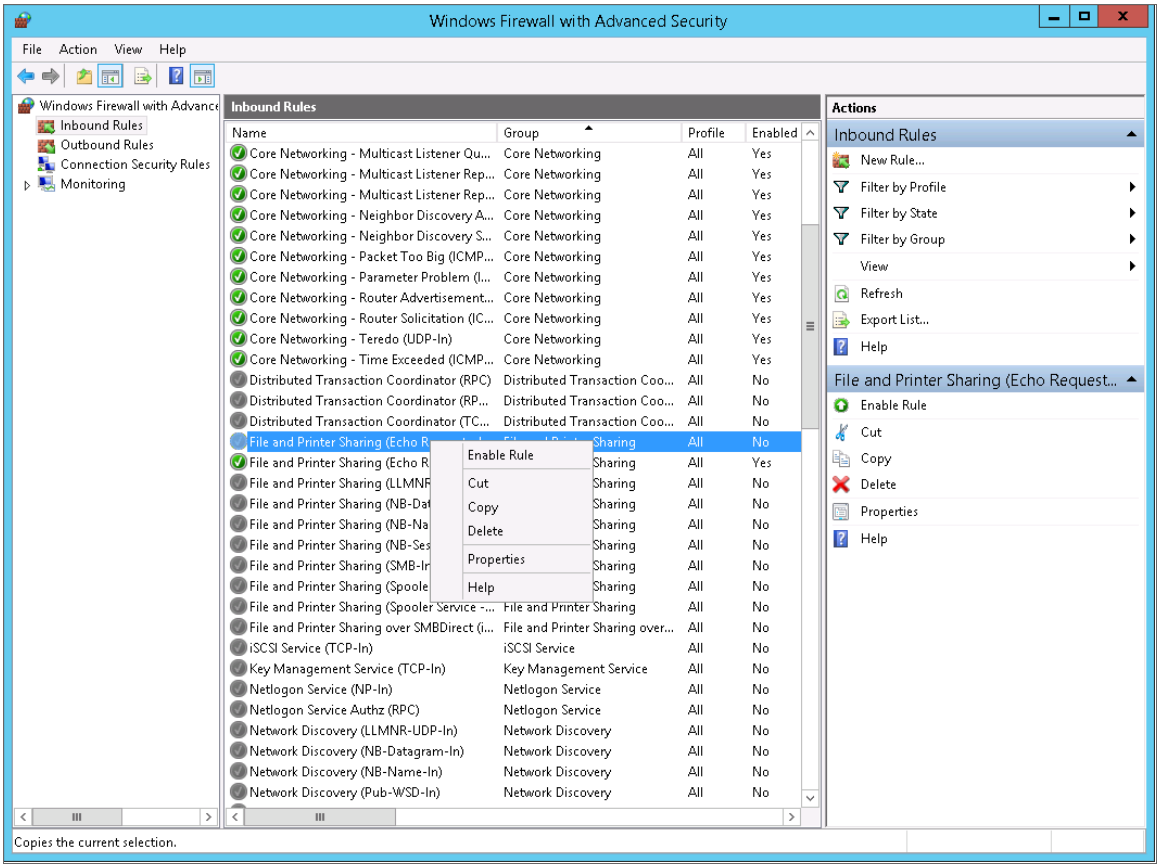
The default configuration for a Windows Server does not allow ICMP "Ping" requests and does not allow connections to TCP ports 21, 22, 23, 25, or 80. Therefore, to discover a Windows Server in SL1, you must perform one of the following tasks:

- 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 SL1 to discover your Windows Server using an IPv4 address, locate the *File and Printer Sharing (Echo Request - ICMPv4-In)* rule.
4. If you want SL1 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*:

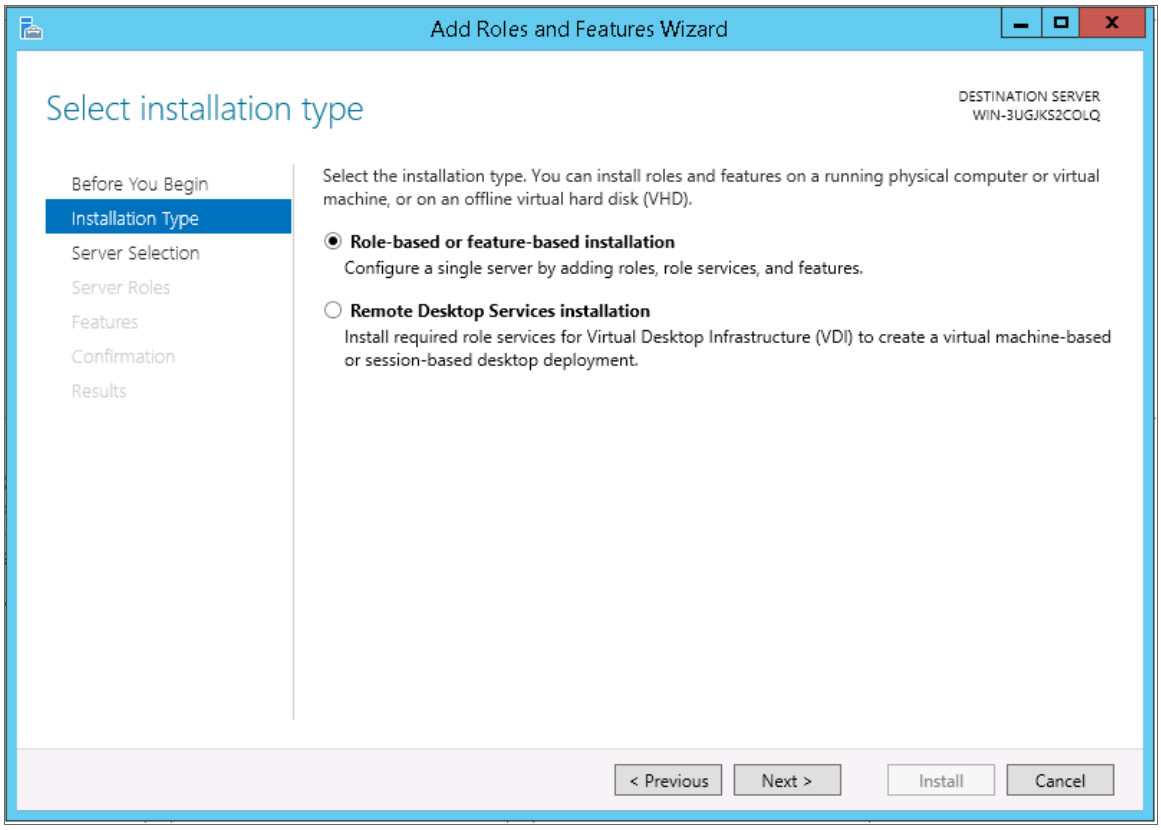


Installing the SNMP Service

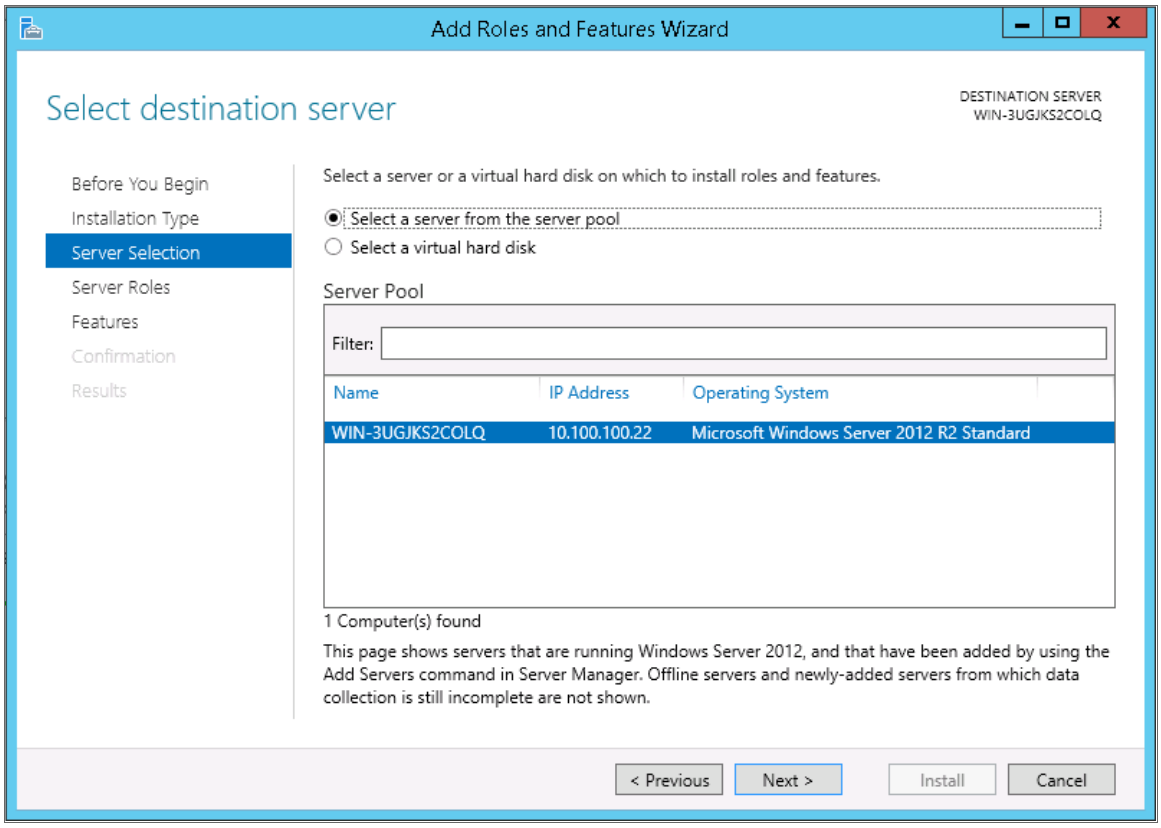
To install the SNMP service on a Windows 2012 Server or Windows 2016 Server, perform the following steps:

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.

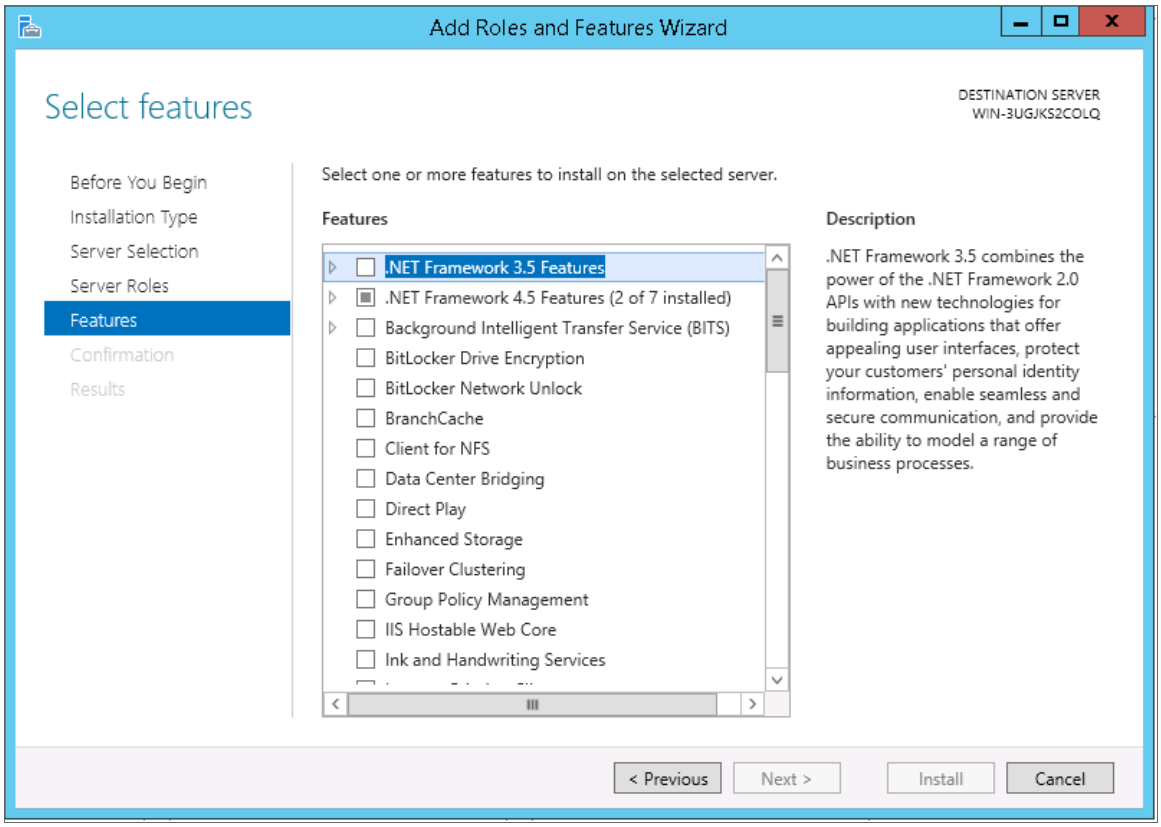
3. If the server does not skip the **Before you begin** page, click the **[Next >]** button to manually skip it. The **Select installation type** page is displayed:



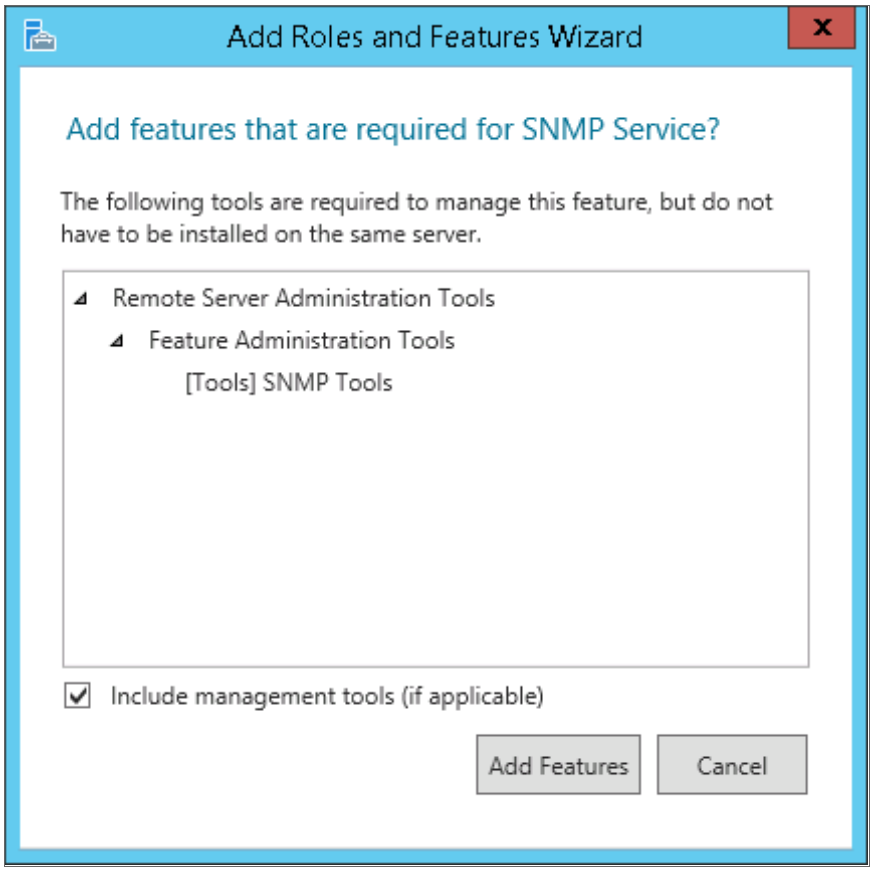
4. Click the **[Next >]** button to continue with *Role-based or feature-based installation*. The **Select destination server** page is displayed:



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:

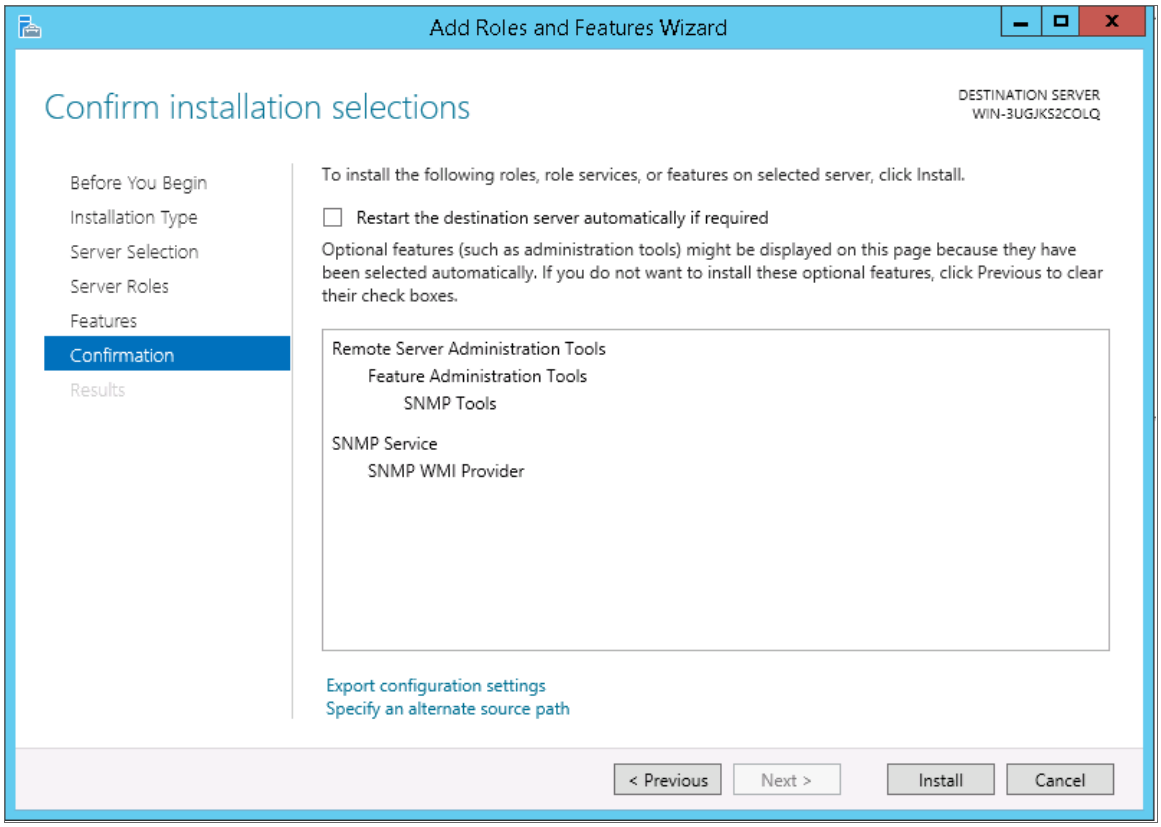


7. Select the *SNMP Service* checkbox. The following confirmation window is displayed:



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.

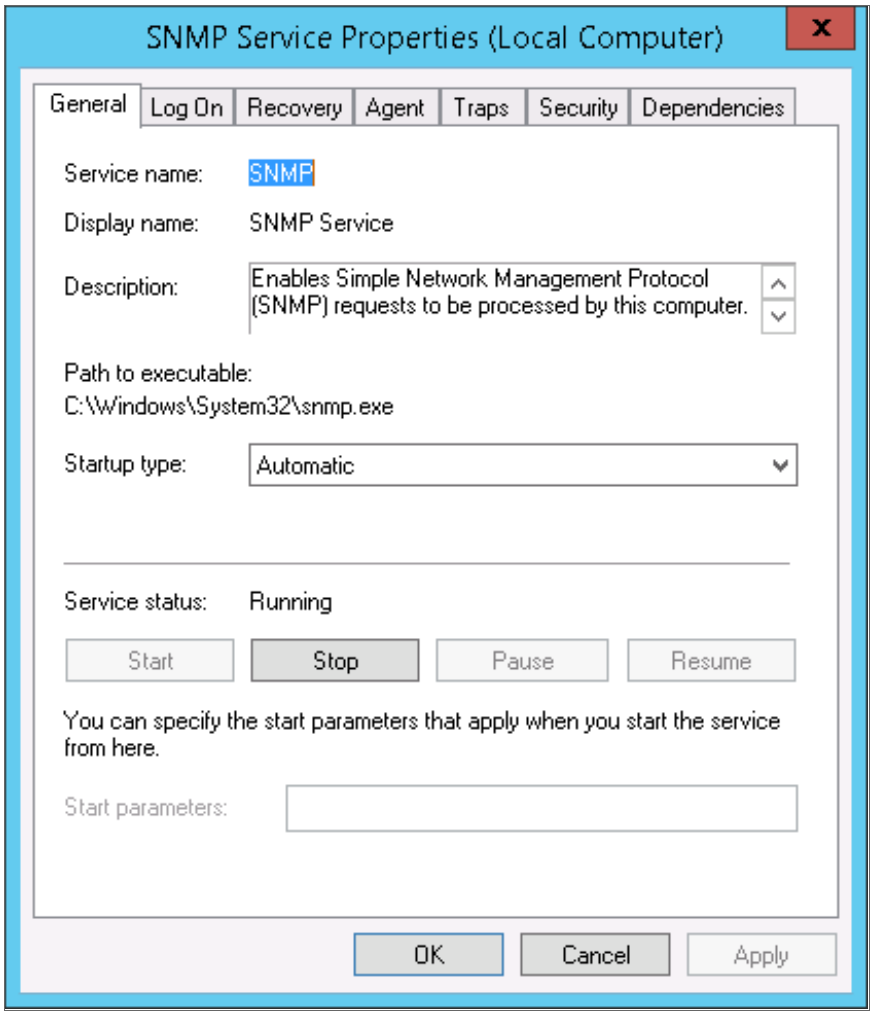
Configuring the SNMP Service

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**.

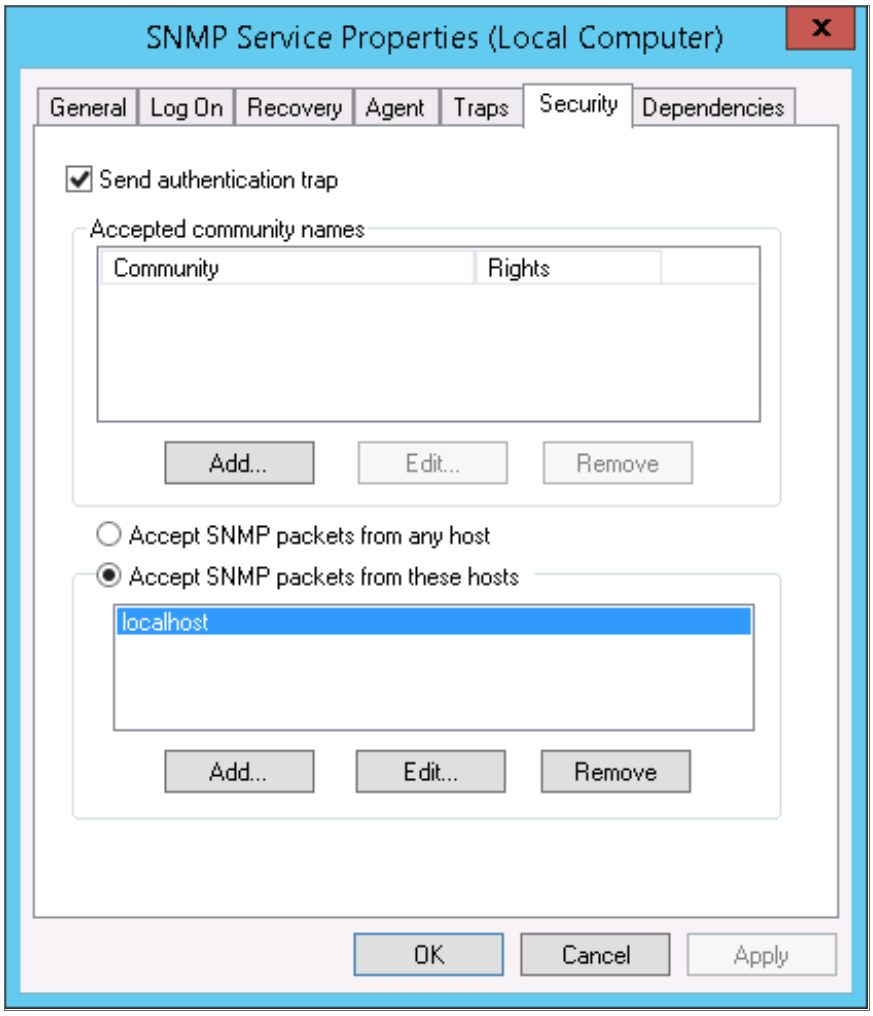
1. In the upper-right of the **Server Manager** window, select **[Tools]** > *Services*. The **Services** window is displayed.

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

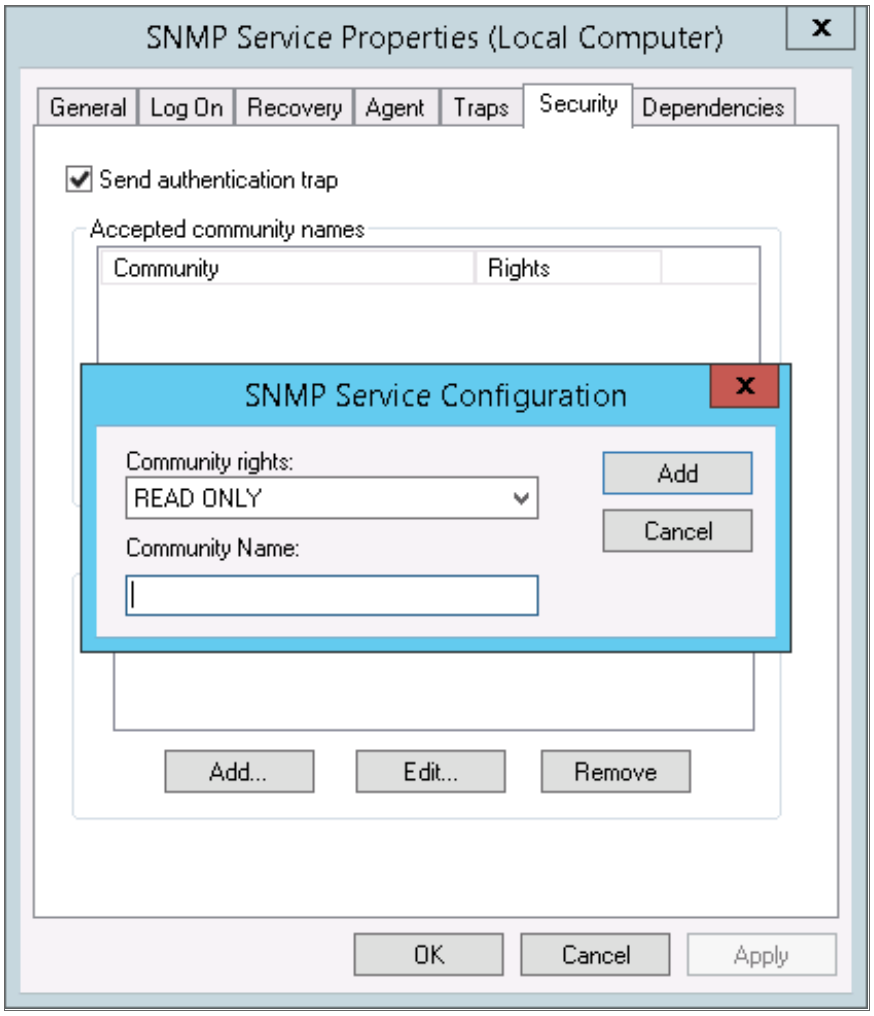


3. In the ***Startup type:*** field, select *Automatic*.

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



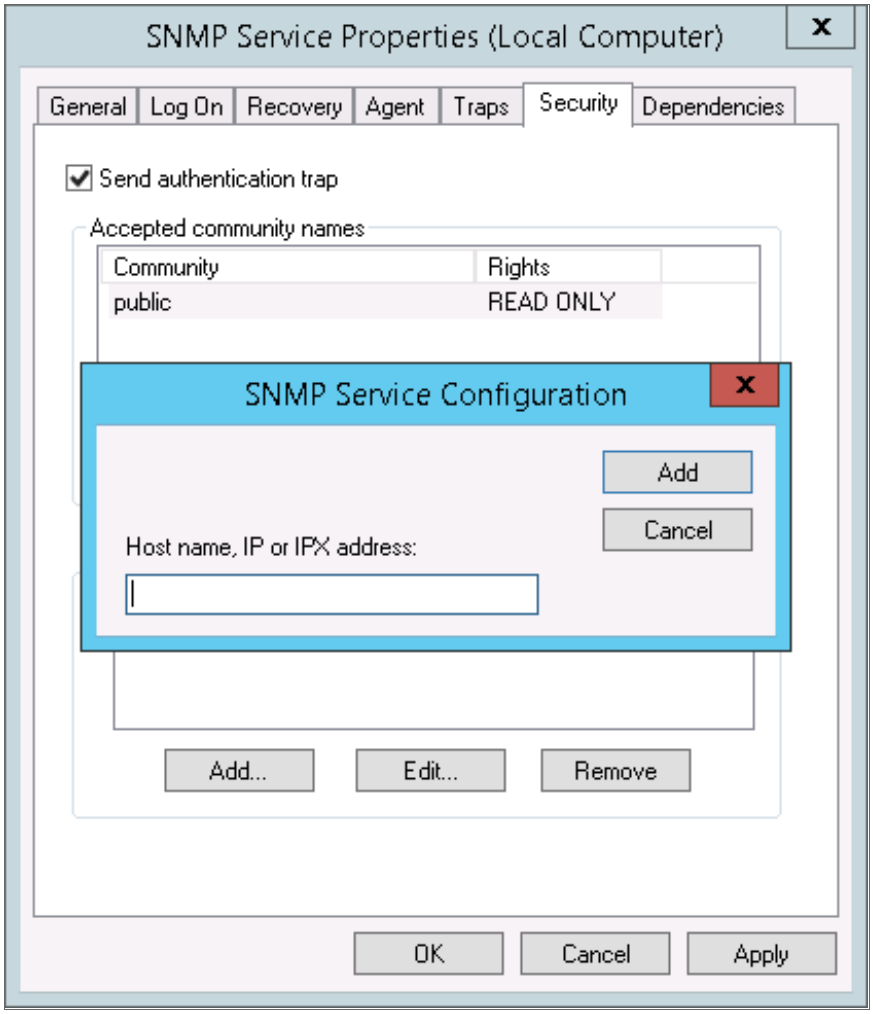
5. In the **Accepted community names** panel, click the **[Add...]** button. The **SNMP Service Configuration** pop-up window is displayed:



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 SL1 to request information from this Windows 2012 Server or Windows 2016 Server using this SNMP community string. This option does not allow SL1 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 SL1 to request information from this Windows 2012 Server or Windows 2016 Server and to perform write operations on this Windows 2012 Server or a Windows 2016 Serve using this SNMP community string.

- ***Community name***. Enter the SNMP community string that SL1 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 SL1, 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:



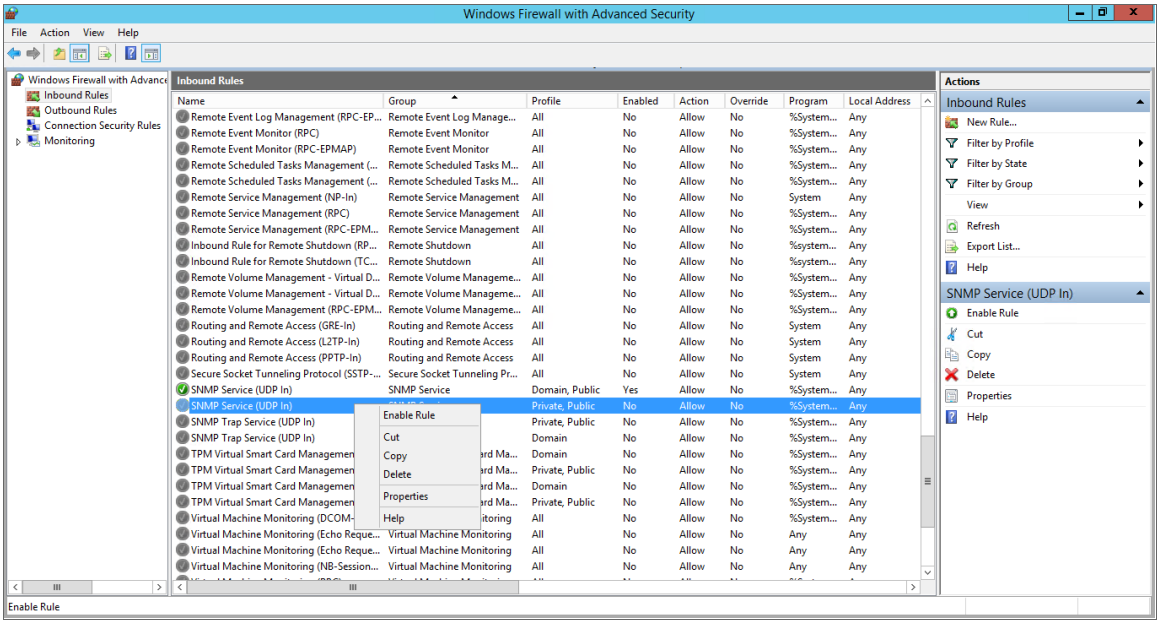
9. In the ***Host name, IP or IPX address*** field, enter the IP address of the All-In-One Appliance or Data Collector that will monitor this server.
10. Click the **[Add]** button to add the appliance to the list of authorized devices.

11. If you are using SL1 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 operating system. This problem prevents SL1 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 Desktop Systems

This section describes how to configure devices that are running a desktop version of the Windows operating system for monitoring by SL1 using SNMP.

Before performing the tasks described in this section, you must know the IP address of each SL1 appliance in your network. If you have not installed a SL1 appliance, you must know the future IP address that will be used by each SL1 appliance.

NOTE: To be monitored by SL1, 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.

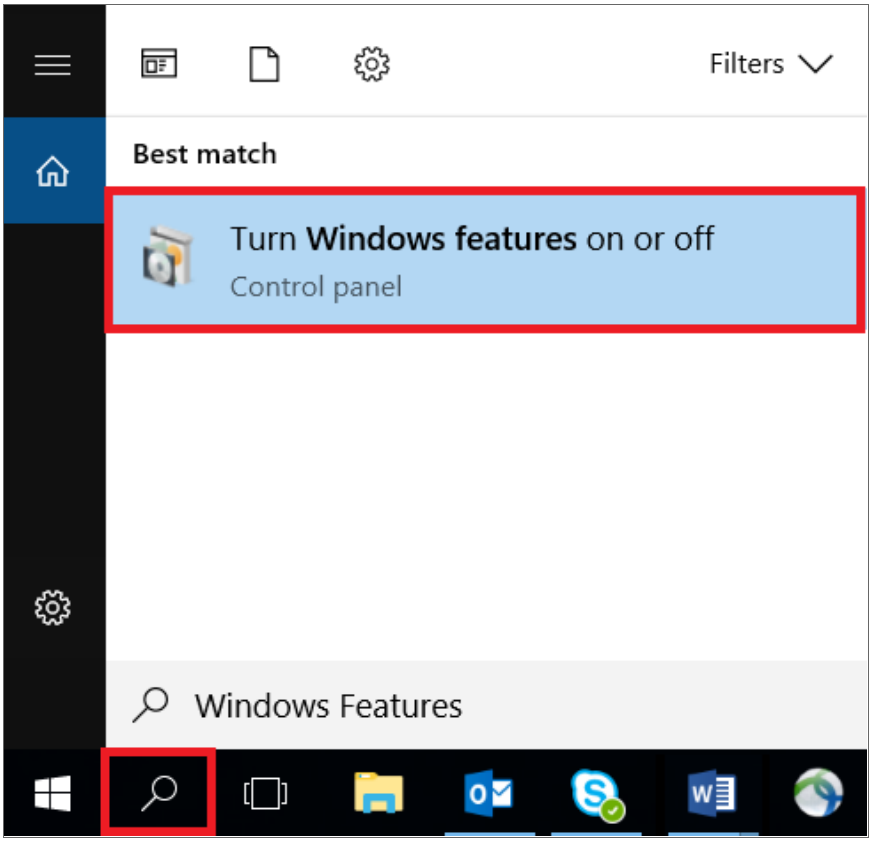
Enabling SNMP on Windows Desktop Systems

You must enable SNMP on each Windows device that you want to monitor with SL1.

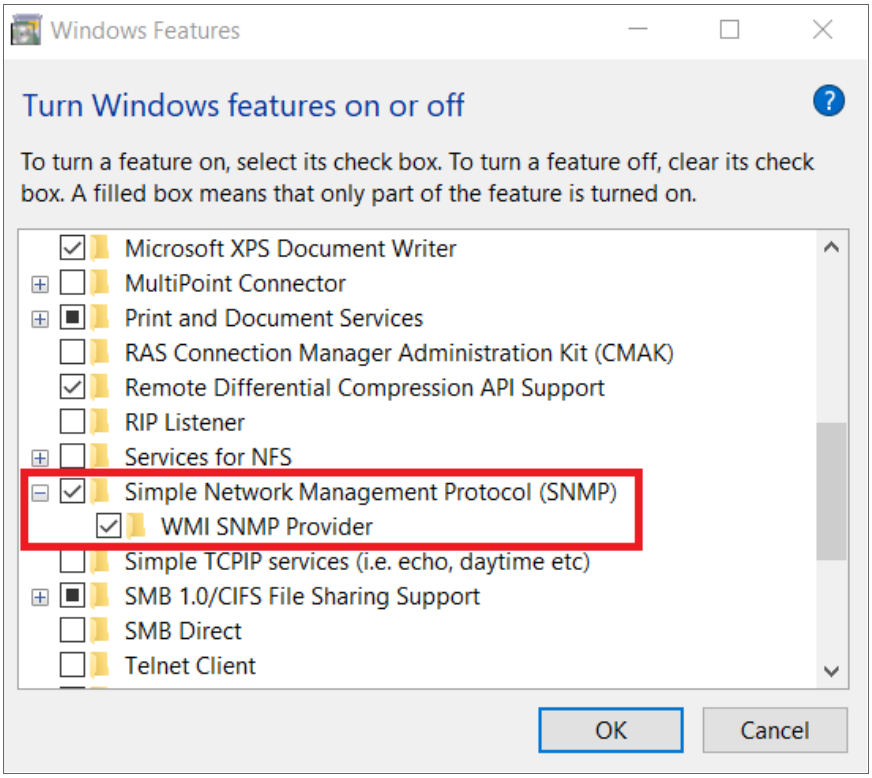
NOTE: The following instructions describe how to enable SNMP on devices running a desktop version of the Windows 10 operating system. For instructions on how to enable SNMP on earlier Windows versions, consult Microsoft's documentation.

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**.

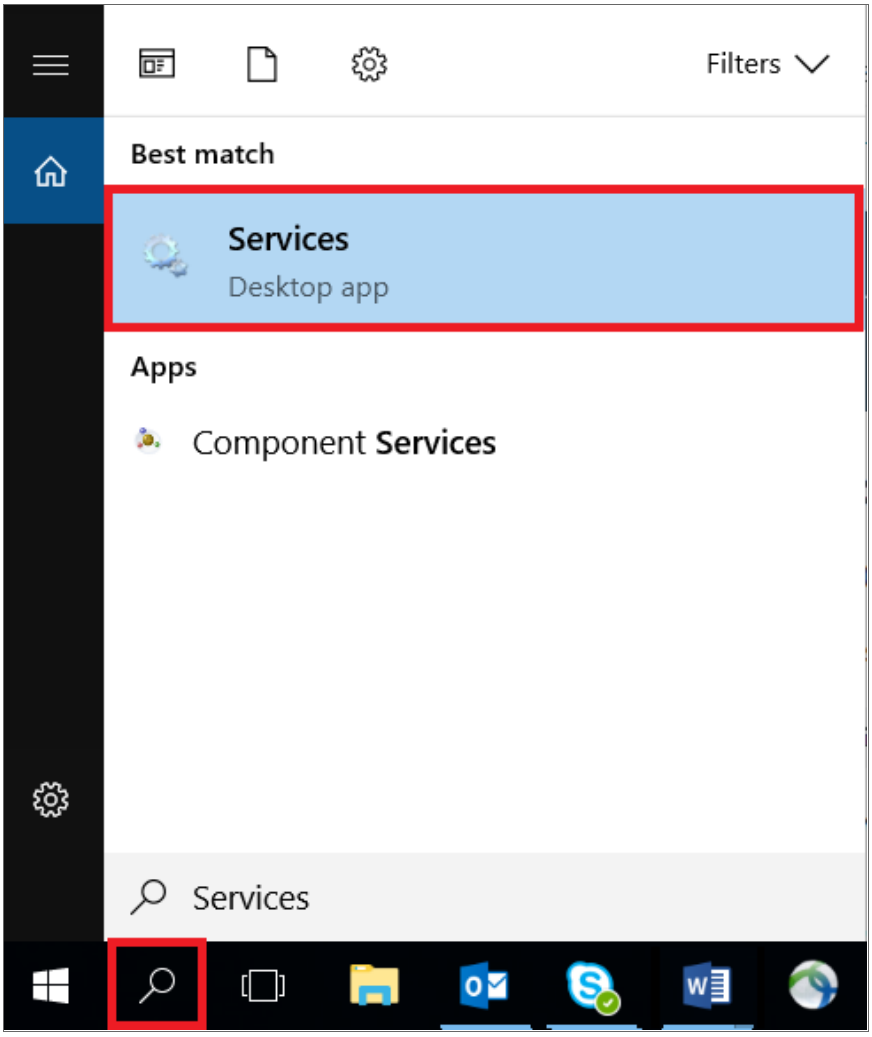


3. In the **Turn Features on or off window**, expand the ***Simple Network Management Protocol (SNMP)*** folder and then select the ***WMI SNMP Provider*** checkbox.

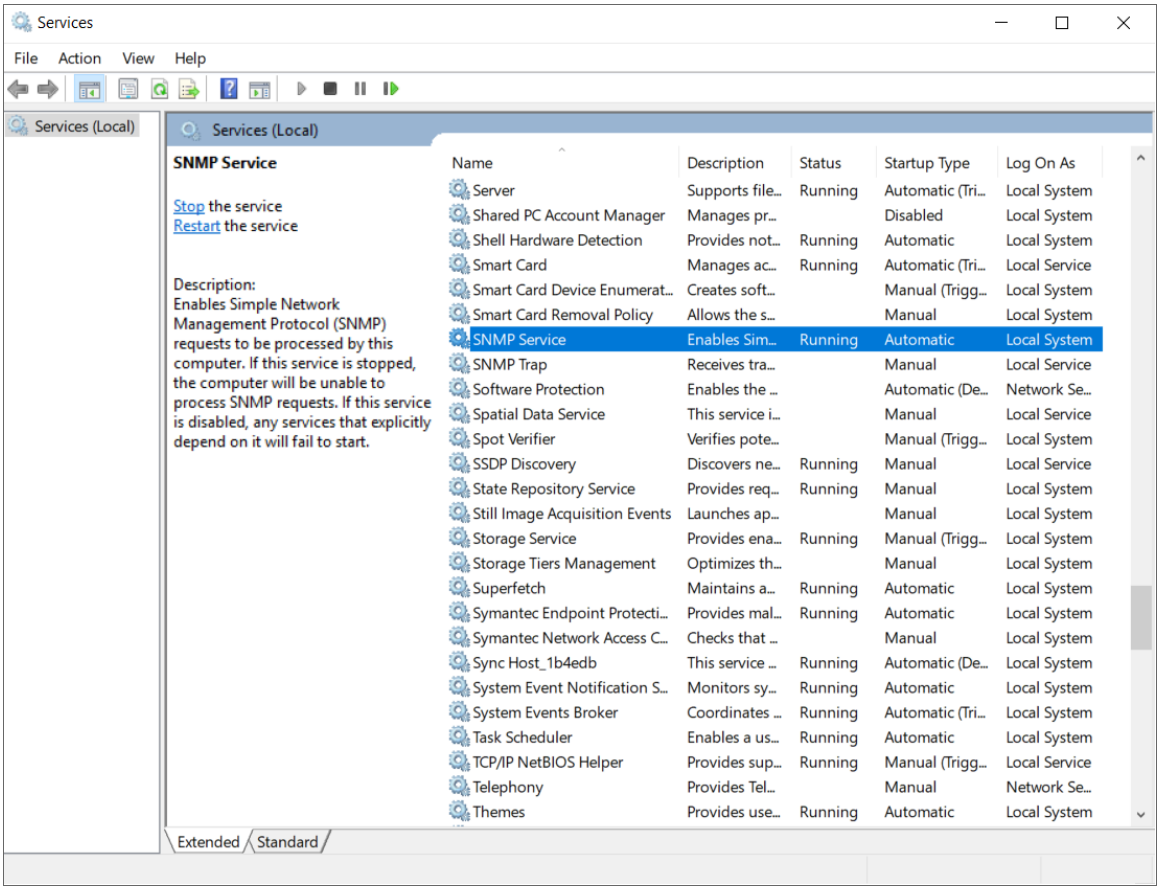


4. Click **[OK]**, and then click **[Close]** after the confirmation message appears.
5. Click the magnifying glass icon in the bottom-left corner and type "Services" in the ***Search Windows*** field.

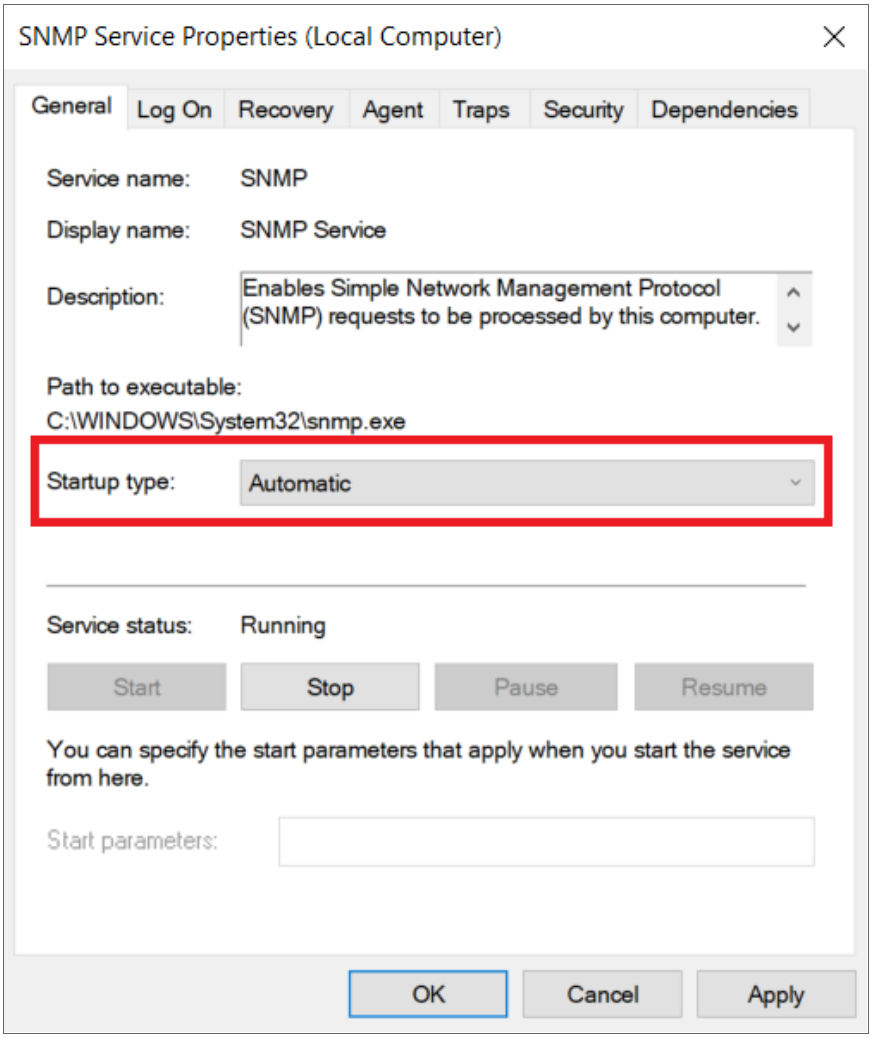
6. Click the **Services** Desktop app.



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

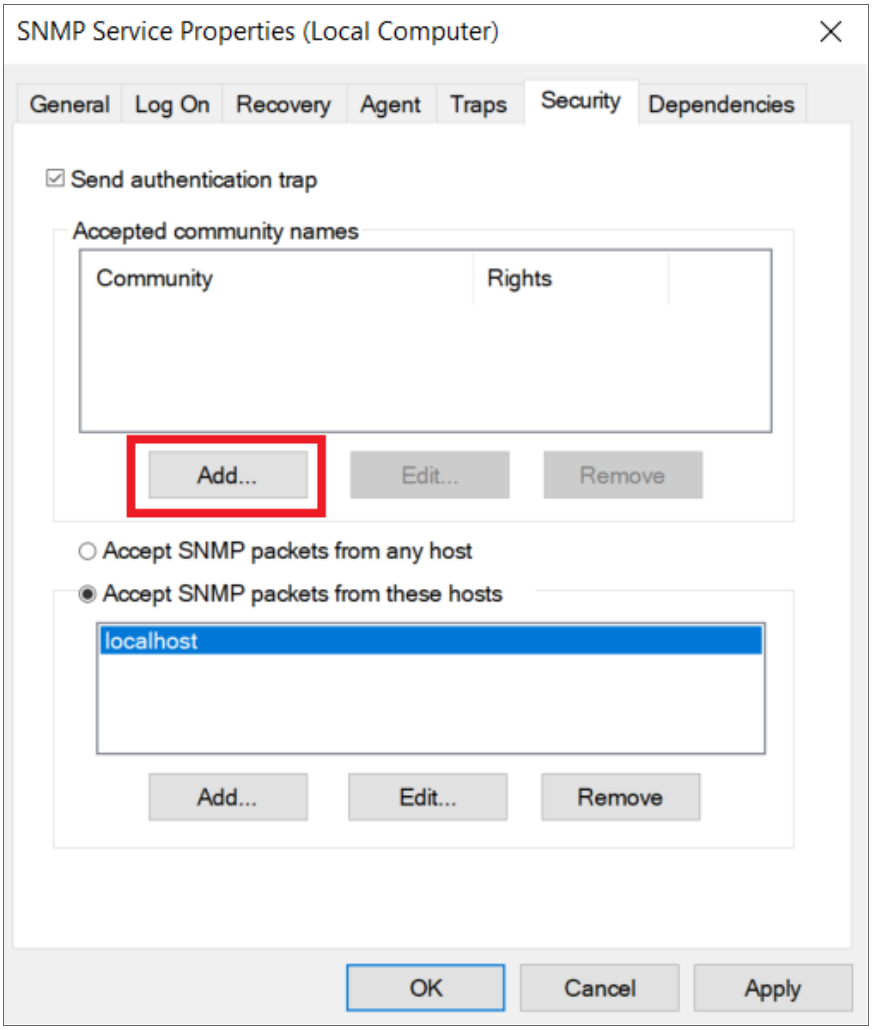


8. In the **SNMP Service Properties** dialog box, click the **[General]** tab and enter the following:

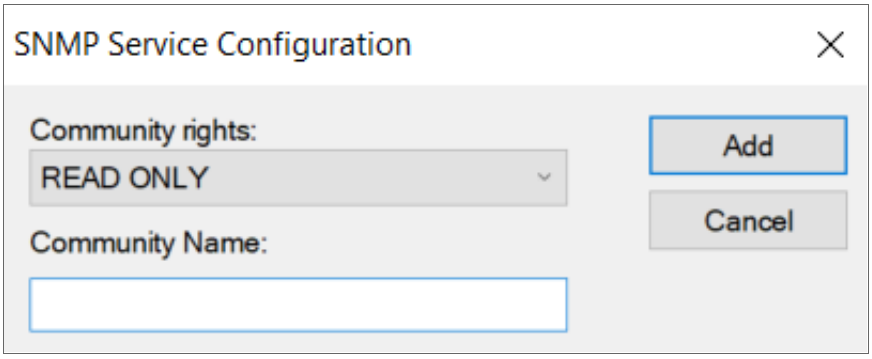


- ***Startup type***. Select *Automatic*.

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

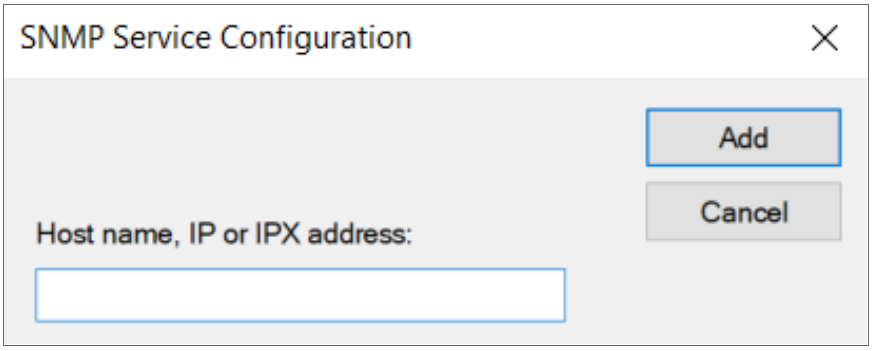


11. In the **SNMP Service Configuration** dialog box, complete the following fields:



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

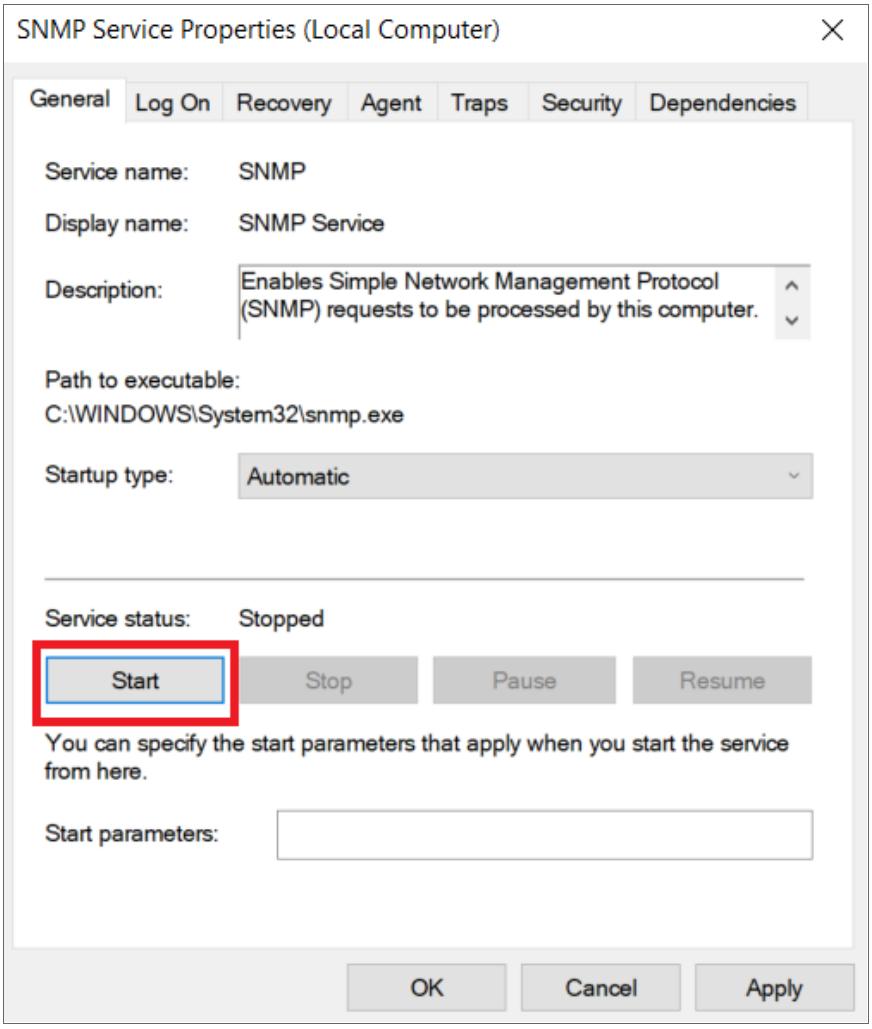
12. Click the **[Add]** button.
13. In the **SNMP Service Properties** dialog box, in the **[Security]** tab, select the *Accept SNMP packets from these hosts* checkbox and then click **[Add]**.
14. In the **SNMP Service Configuration** dialog box, complete the following field:



- ***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*.

Chapter 3

Configuring Windows Systems for Monitoring with WMI

Overview

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

The following sections describe how to configure Windows Server 2012 and later and Windows desktop systems for monitoring by SL1 using SNMP:

This chapter covers the following topics:

Configuring WMI on Windows 2012 and Later 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 SL1.

To configure a Windows 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*
4. *Configuring a fixed port for WMI*

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 SL1 to a Windows server, the following users have elevated permissions:

- The default "Administrator" user account.
- A user account in the **Administrators** group on a Windows server that has User Account Control disabled.
- A user account in the **Administrators** group on a Windows 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

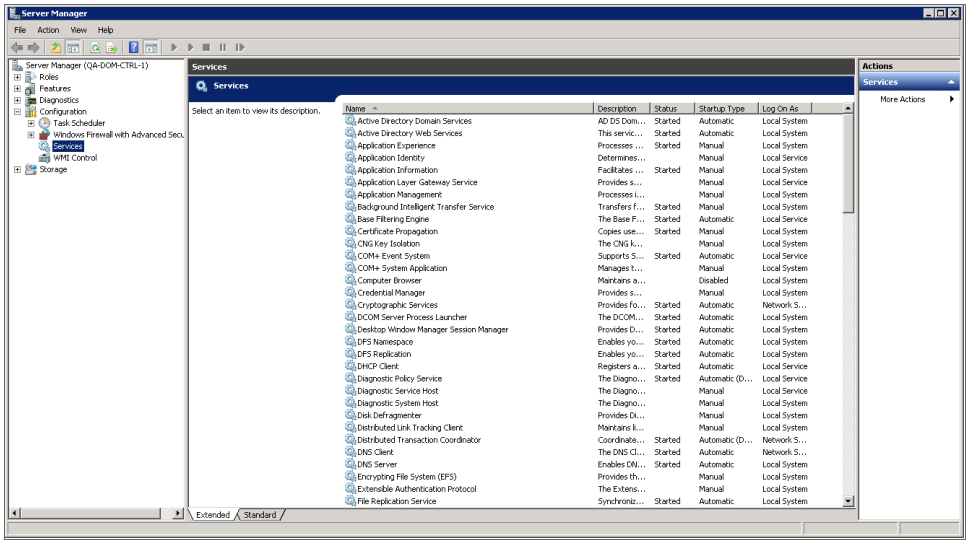
The following services must be running for a Windows device to respond to remote WMI requests:

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

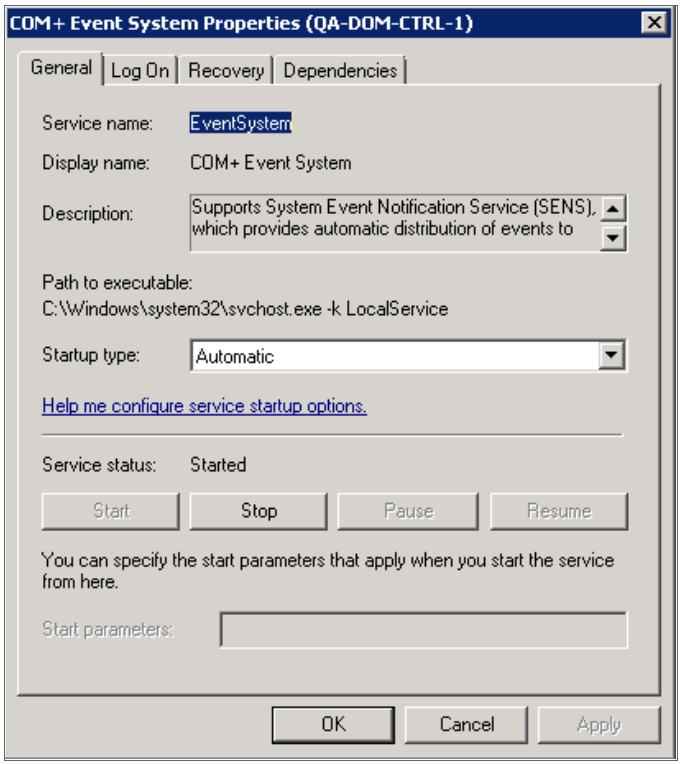
- COM+ Event System
- DCOM Server Process Launcher
- Remote Procedure Call (RPC)
- Remote Registry
- Server
- Windows Management Instrumentation

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:

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: Configuring a User Account and Permissions

There are three ways to configure the user account that SL1 will use to perform WMI requests:

1. To monitor the Windows server using WMI Dynamic Applications that require ***standard permissions***, you can configure a standard user account for use by SL1. The user account for use by SL1 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 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 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*.

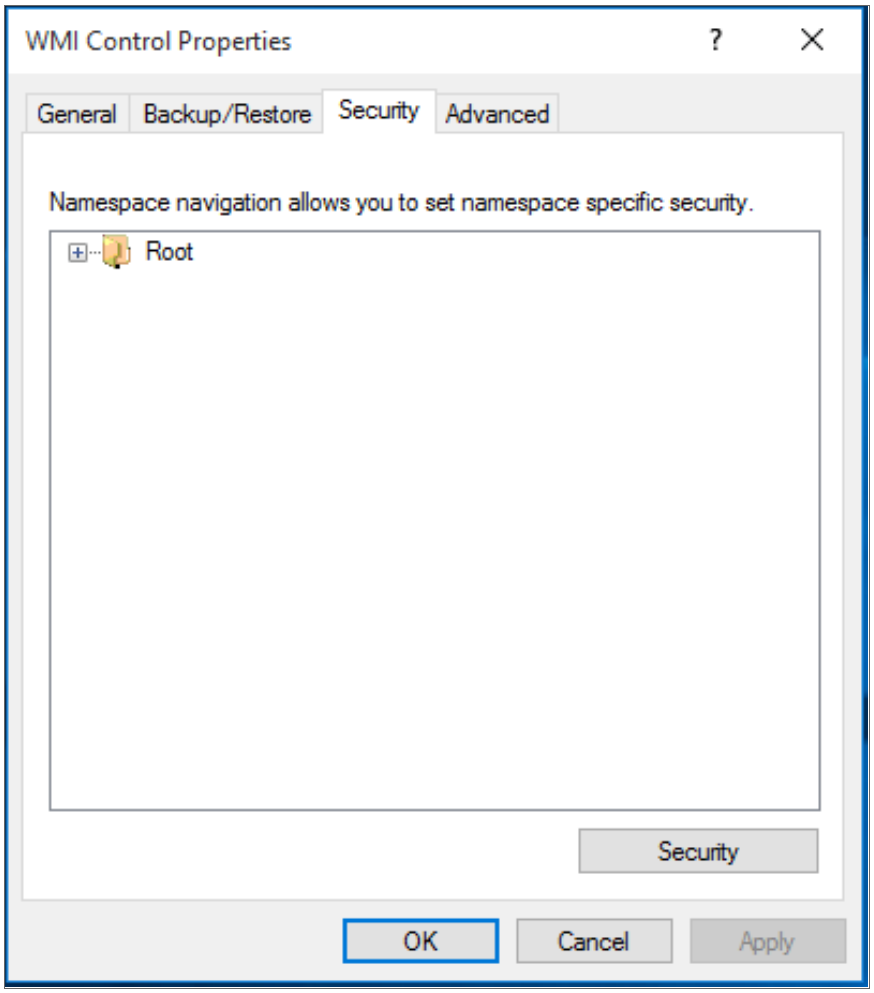
Configuring Namespace and DCOM Security Permissions

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:

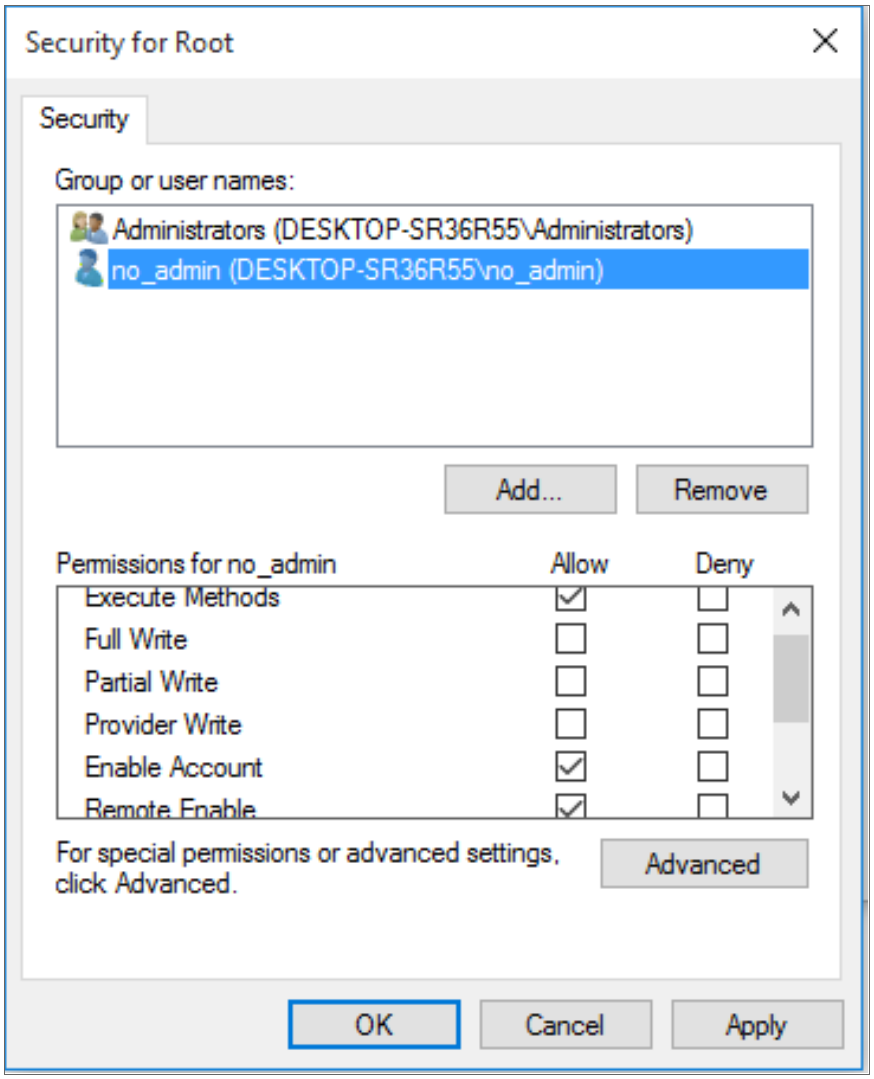
1. In the left pane of the **Server Manager** window, expand the *Configuration* section.
2. Right-click on the *WMI Control* entry and then select *Properties*.

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

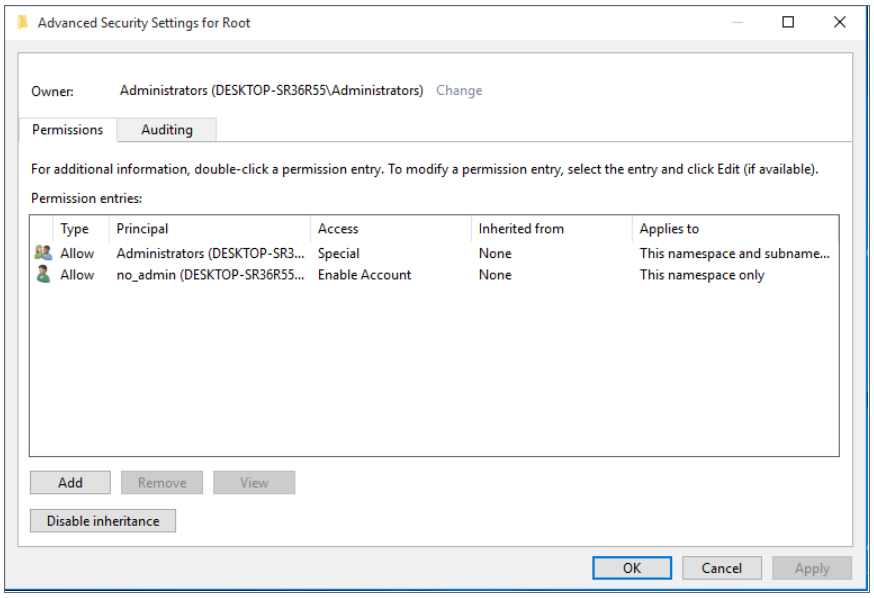


4. In the Security tab, select the *Root* entry from the navigation pane and then select the **[Security]** button. The **Security for Root** window appears.

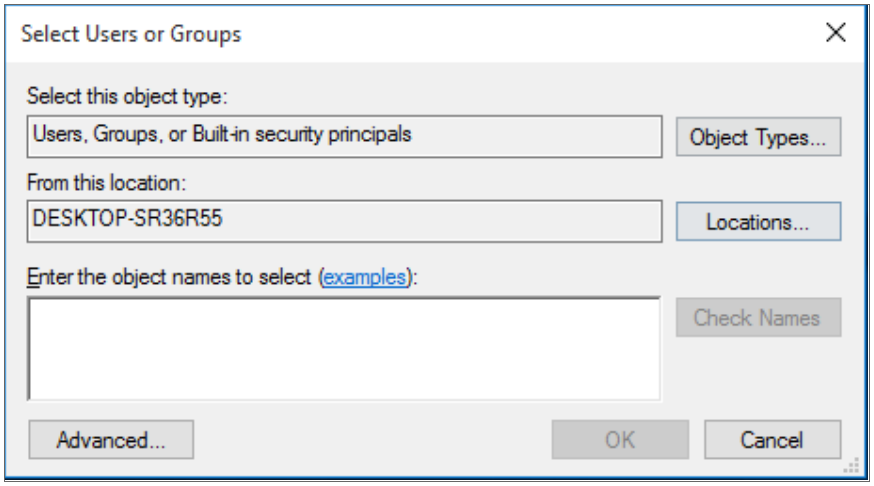
5. In the **Security for Root** window, select the **[Advanced]** button. The **Advanced Security Settings for Root** window is displayed:



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

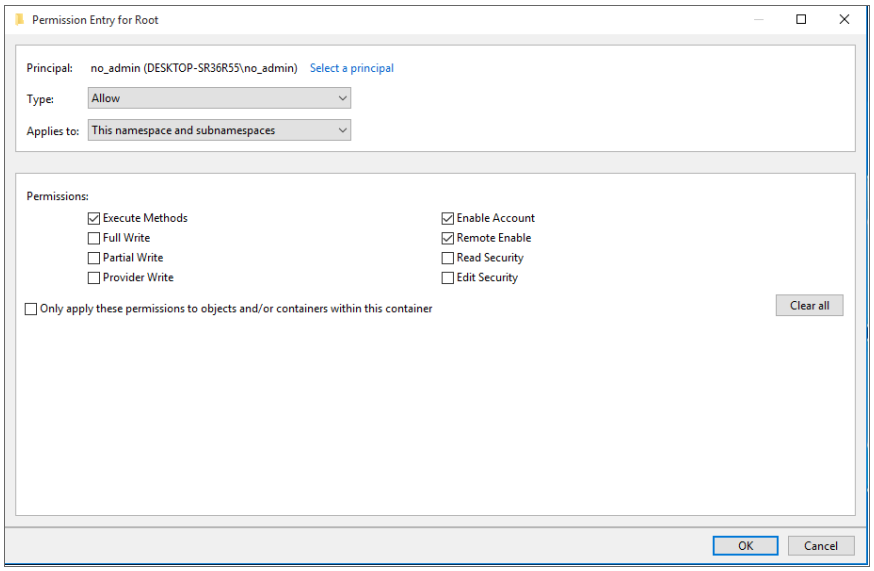


7. In the **Select User, Computer, Service Account, or Group** window :



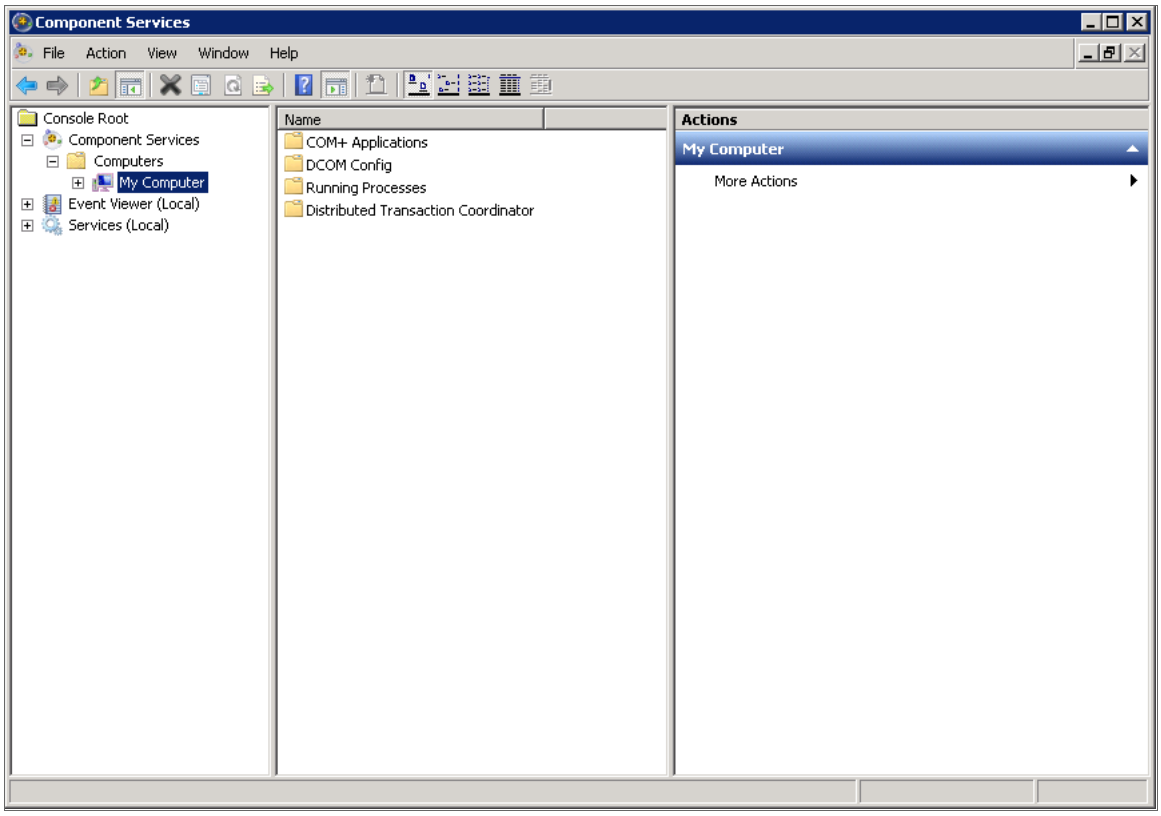
- In the ***Enter the object name to select*** field, enter the name of the user account that SL1 will use to perform WMI requests or the name of a group that includes that user account.
- Click the **[Check Names]** button to verify the name and then click the **[OK]** button.

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



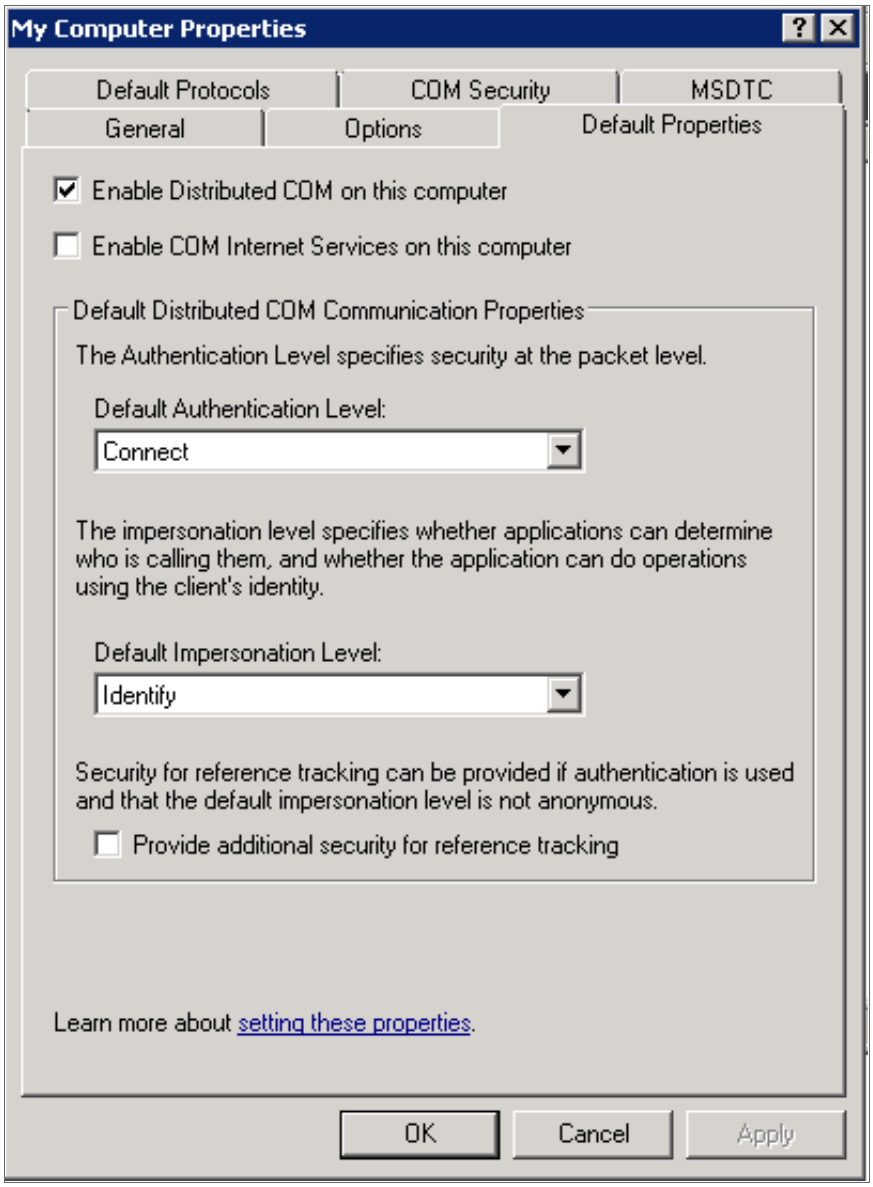
   - Select *This namespace and subnamespaces* in the ***Apply to*** field and select the ***Allow*** checkbox for all permissions.
   - Click the **[OK]** button.
9. In the **Advanced Security Settings for Root** window, click the **[Apply]** button.
10. Click the **[OK]** button in each open window to 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:



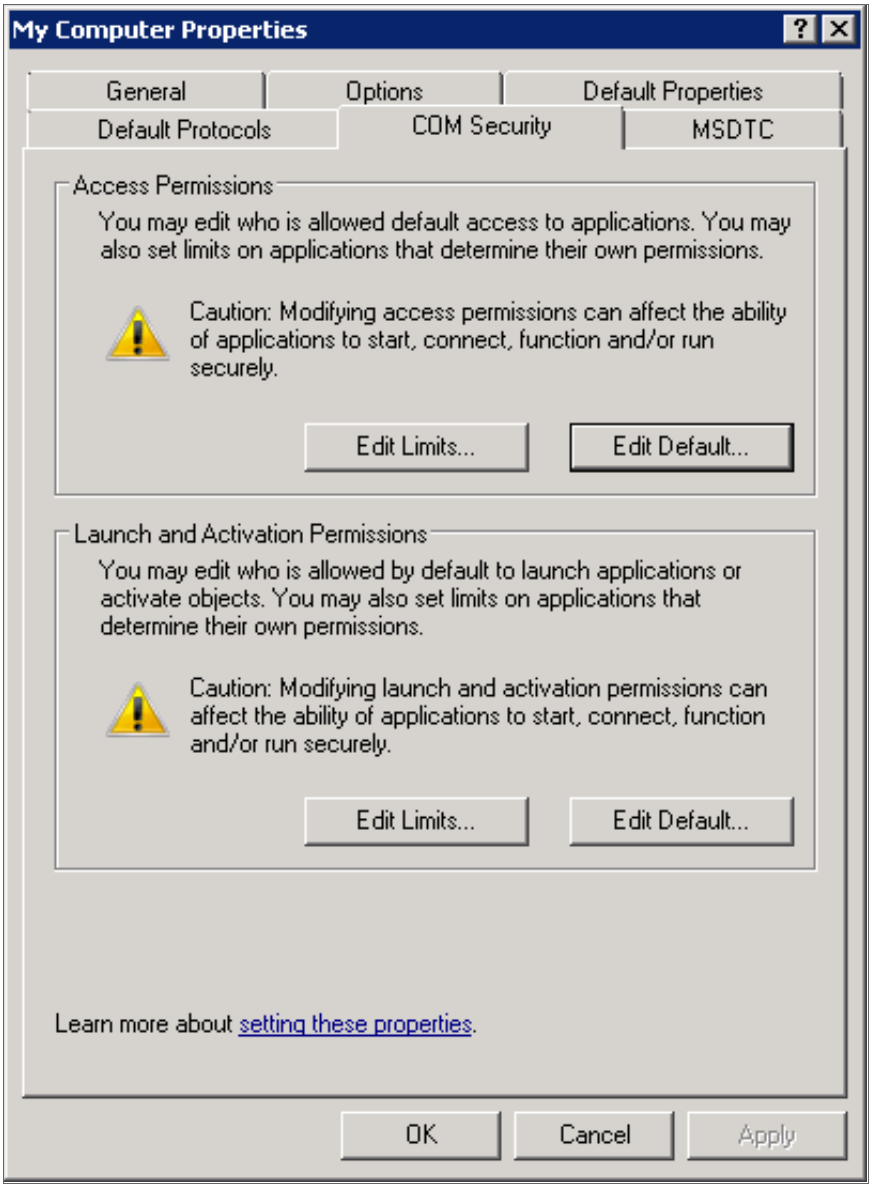
13. In the left pane, expand **Component Services > Computers**. Right-click on **My Computer** and select *Properties*. The **My Computer Properties** window is displayed.

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 SL1 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 server and you are using a user account other than the default "Administrator" user account, you must perform **one** of the following two tasks:

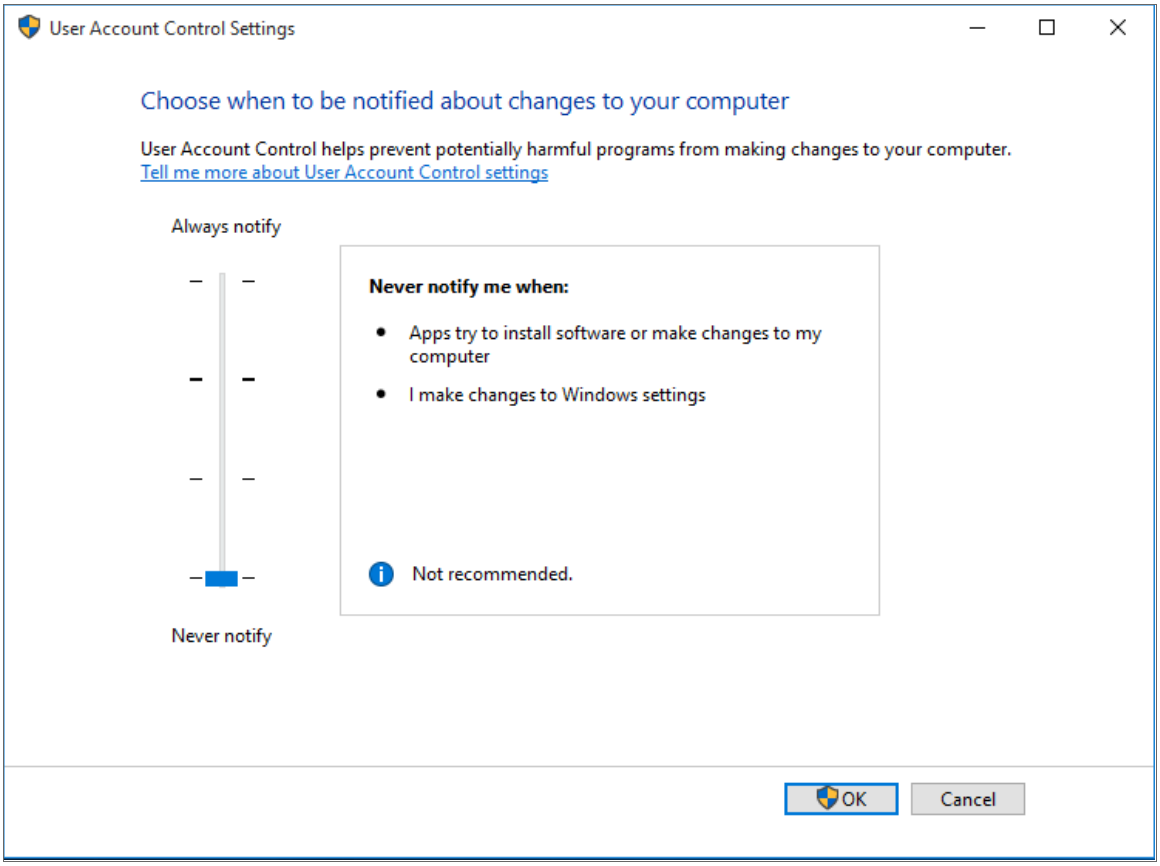
- **Option 1**: *Disable User Account Control*.
- **Option 2**: *Add a registry entry that disables remote User Account Control filtering*.

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 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.

Step 4: Configuring a Fixed Port for WMI

Specific ports must be opened to allow WMI monitoring when there is a separate firewall between the Data Collector and the device. This can occur when the default configuration of the Windows Firewall blocks incoming network traffic for the Windows Management Instrumentation (WMI) connection.

For the WMI connection to succeed, the remote machine must permit incoming network traffic on TCP ports 135, 445, and additional dynamically-assigned ports, typically in the range of 1025 to 5000 and 49152 to 65535.

To set up a fixed port for WMI, see the Microsoft documentation on Setting Up a Fixed Port for WMI.

To set up a fixed port for WMI:

1. At the command prompt, type `winmgmt -standalonehost`
2. Stop the WMI service by typing the command `net stop "Windows Management Instrumentation"`, or use the shorter cpmmand of `net stop winmgmt`
3. Restart the WMI service in a new service host by typing `net start "Windows Management Instrumentation"` or `net start winmgmt`
4. Establish a new port number for the WMI service by typing `netsh firewall add portopening TCP 24158 WMIFixedPort`

To undo any changes you make to WMI, type `winmgmt /sharedhost`, then stop and start the winmgmt service again.

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 SL1 using WMI.

Before performing the tasks described in this section, you must know the IP address of each SL1 appliance in your network. If you have not installed a SL1 appliance, you must know the future IP address that will be used by each SL1 appliance.

NOTE: To be monitored by SL1, 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 SL1. 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*
6. *Configuring a fixed port for WMI*

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:

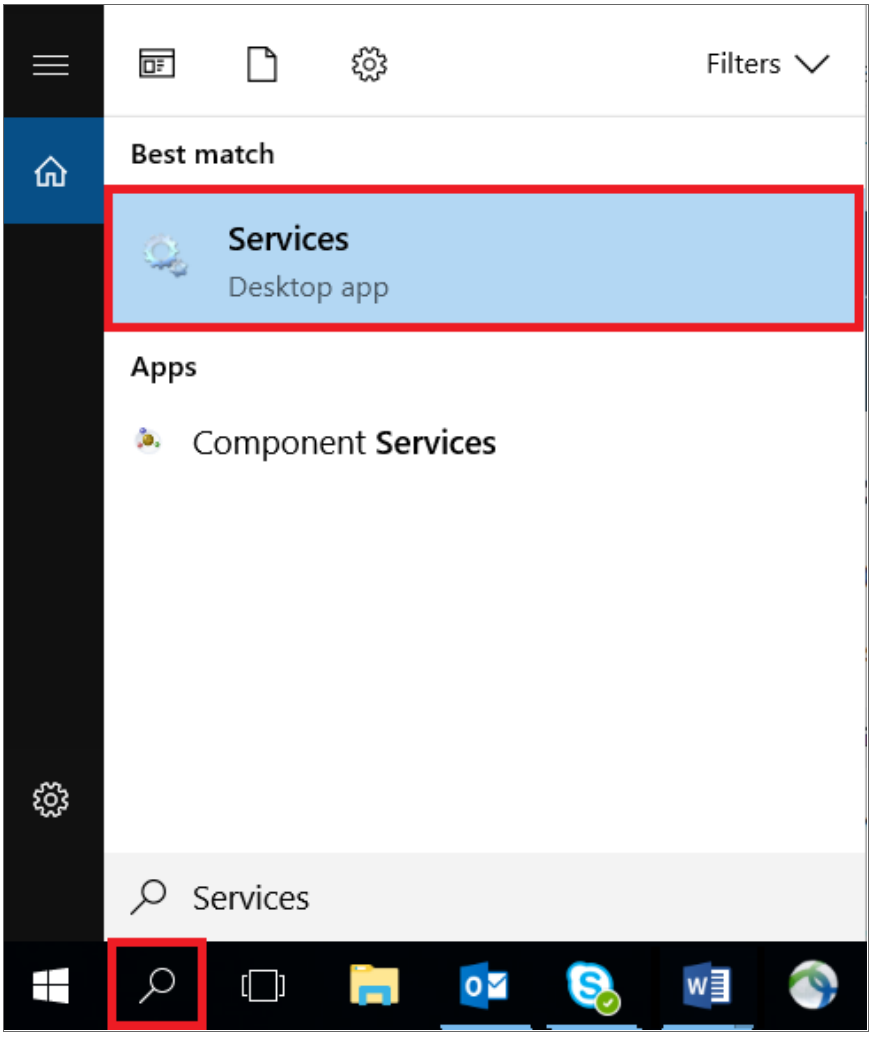
NOTE: ScienceLogic recommends you set all these services to start automatically.

- 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

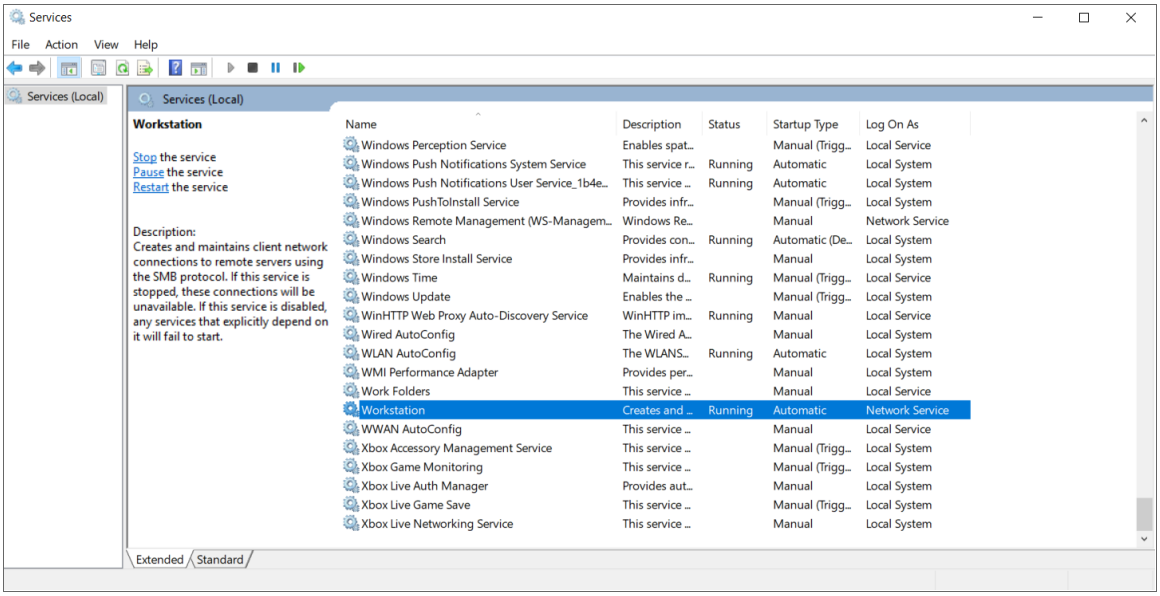
To ensure a service is running, perform the following steps:

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.

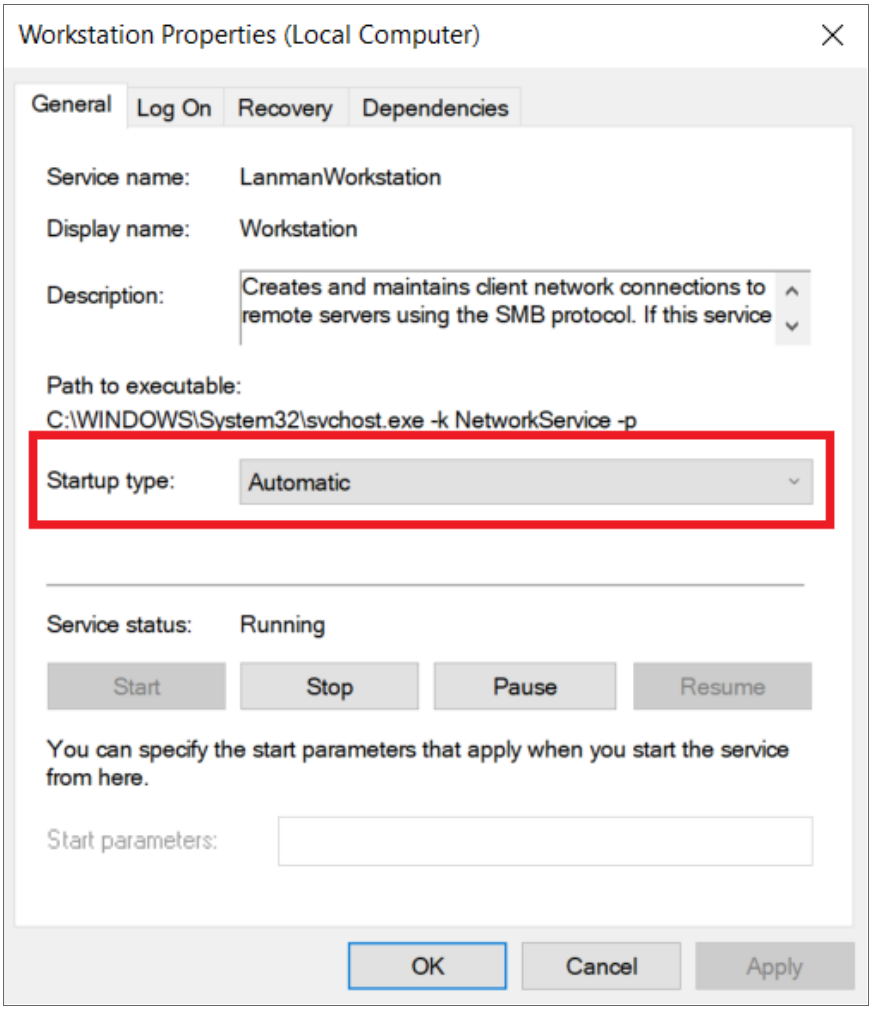


3. From the list of services in the right pane, perform the remaining steps for ***each*** of the services you want to check. This example uses **Workstation**. However, you should check each of the following services:



- 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
```

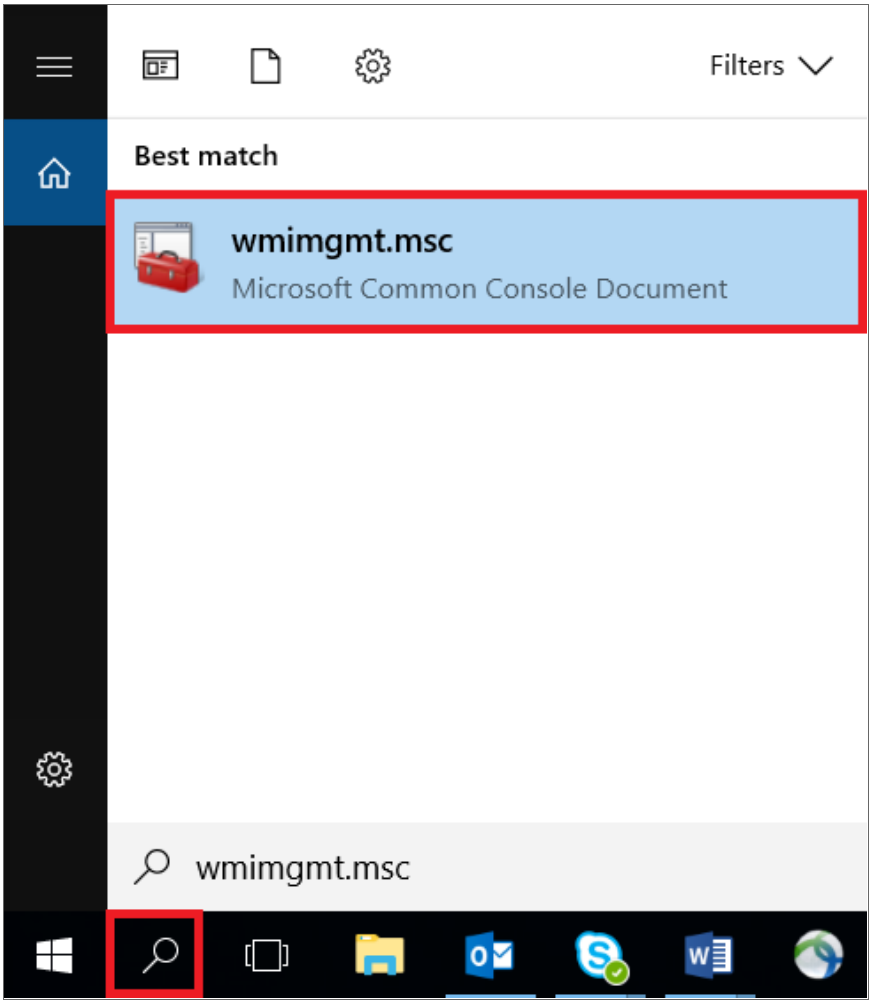
```
netsh advfirewall firewall set rule group="remote administration" new
enable=yes
```

Step 3: Setting the Default Namespace Security

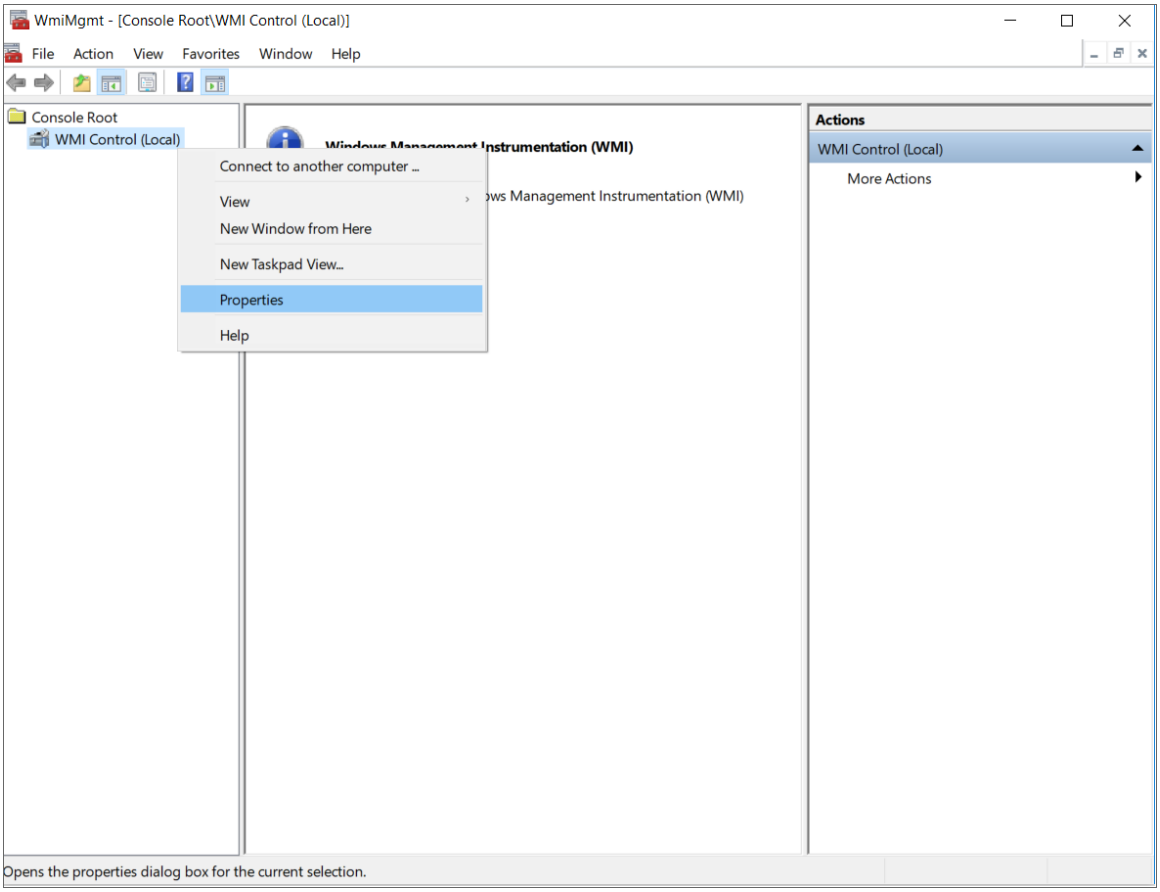
To set the default namespace security, perform the following steps:

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

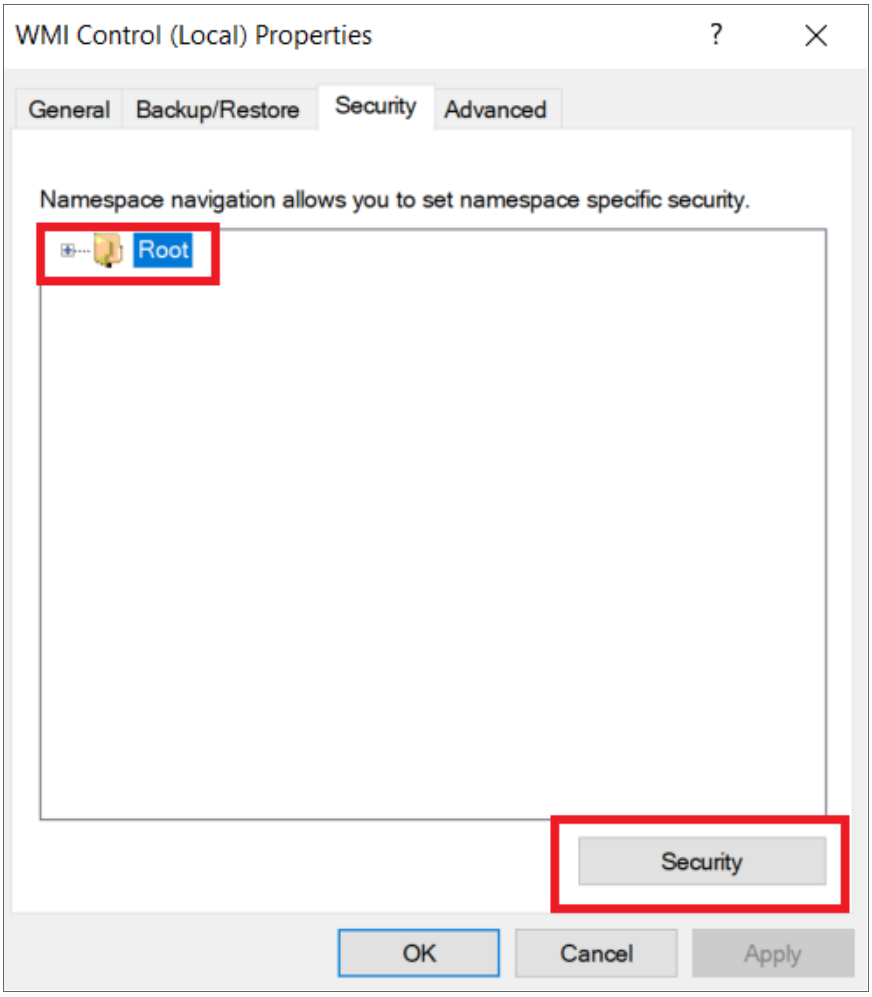
2. Click the **wmimgmt.msc** Microsoft Common Console Document.



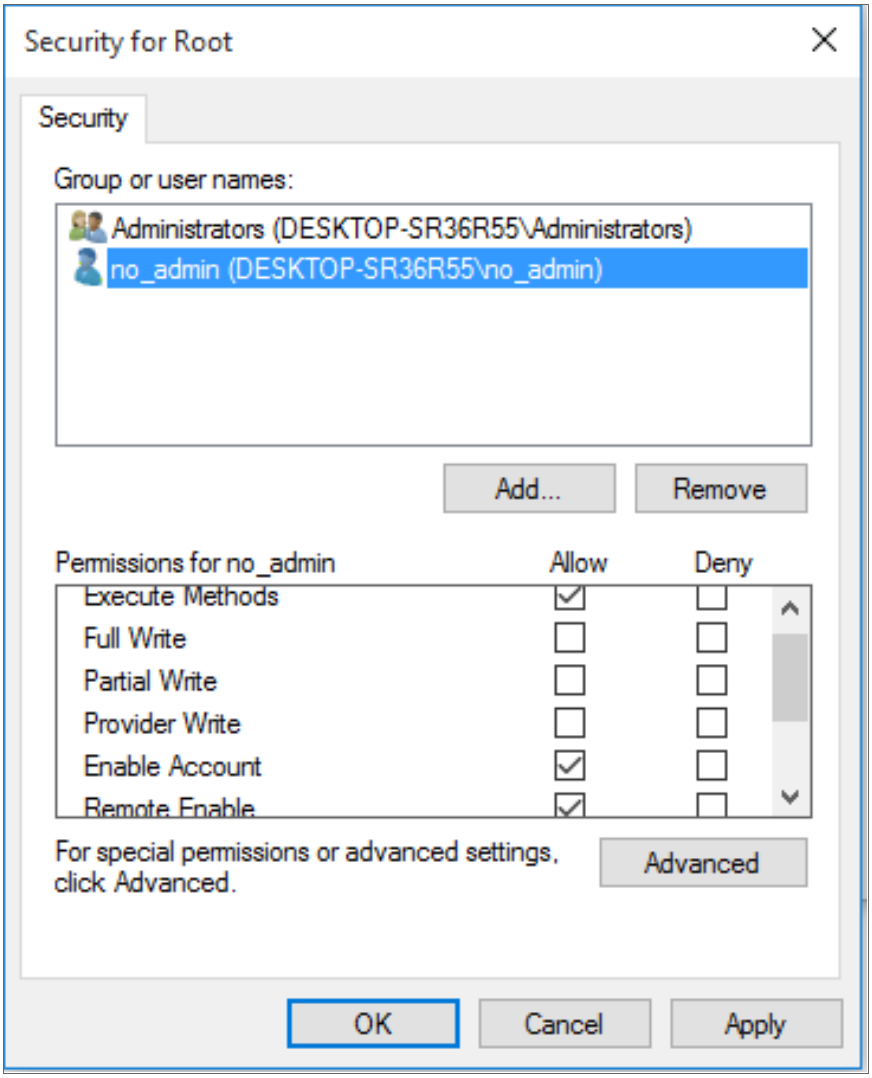
3. In the **WmiMgmt** window, right click **WMI Control (Local)** and select *Properties*.



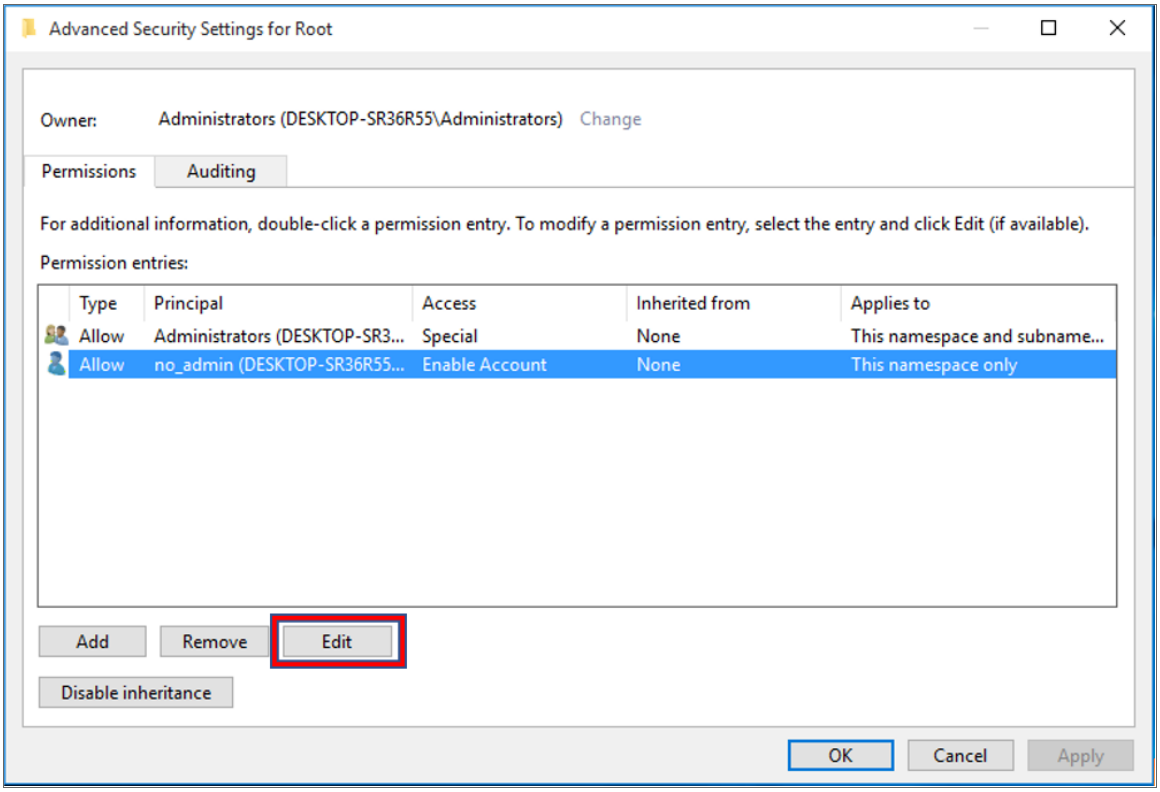
4. In the **WMI Control (Local) Properties** window, click the **[Security]** tab, click **Root**, and then click the **[Security]** button.



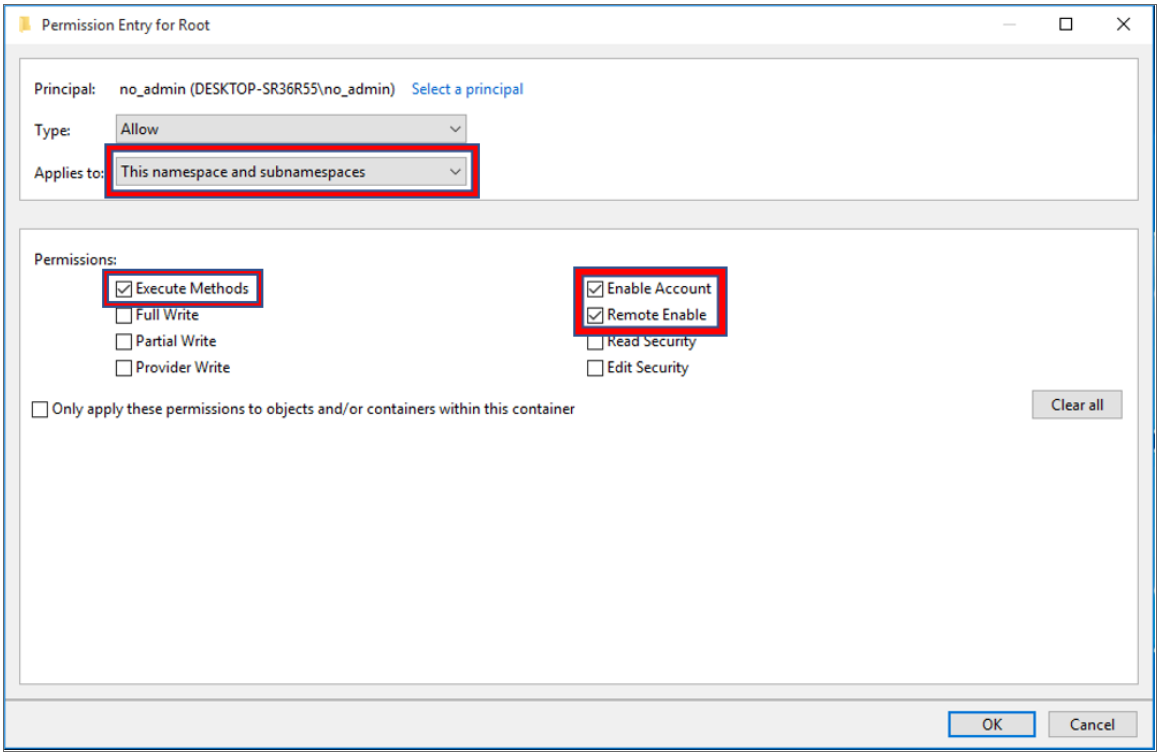
5. In the **Security for Root** window, click **Administrators**, and then click the **[Advanced]** button.



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:



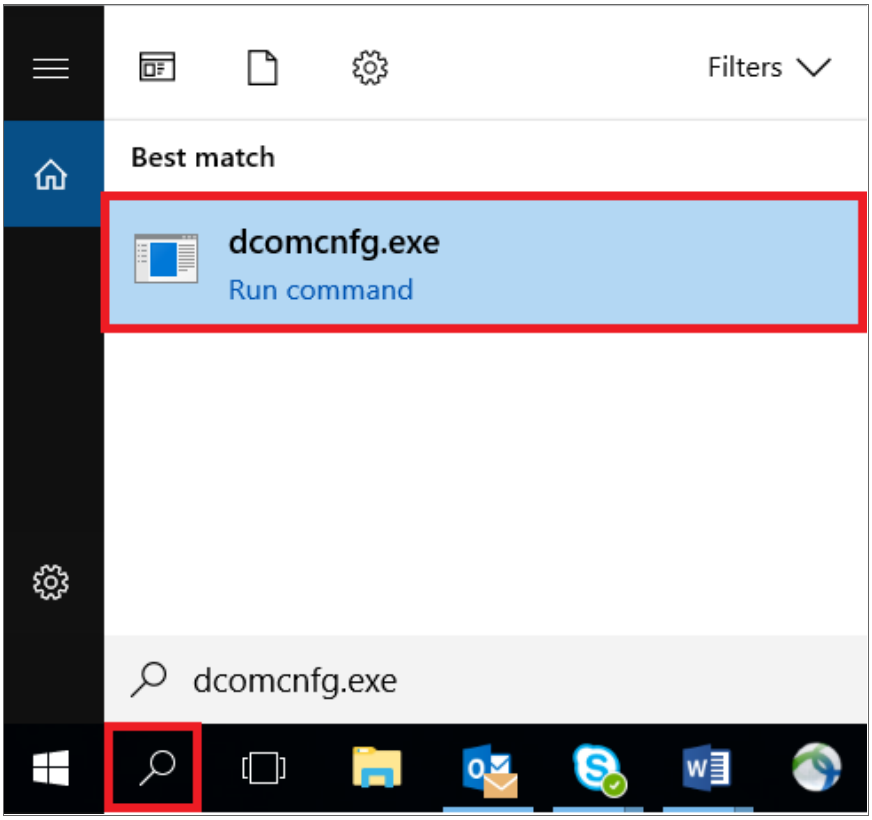
   - ***Type***. Select *Allow*.
   - ***Applies to***. Select *This namespace and subnamespaces*.
   - ***Permissions***. Select the *Execute Methods*, *Full Write*, *Partial Write*, *Provider Write*, *Enable Account*, *Remote Enable*, *Read Security*, and *Edit Security* checkboxes.
8. Click **OK** in this window and the following windows, and then close the **WmiMgmt** window.

Step 4: Setting the DCOM Security Level

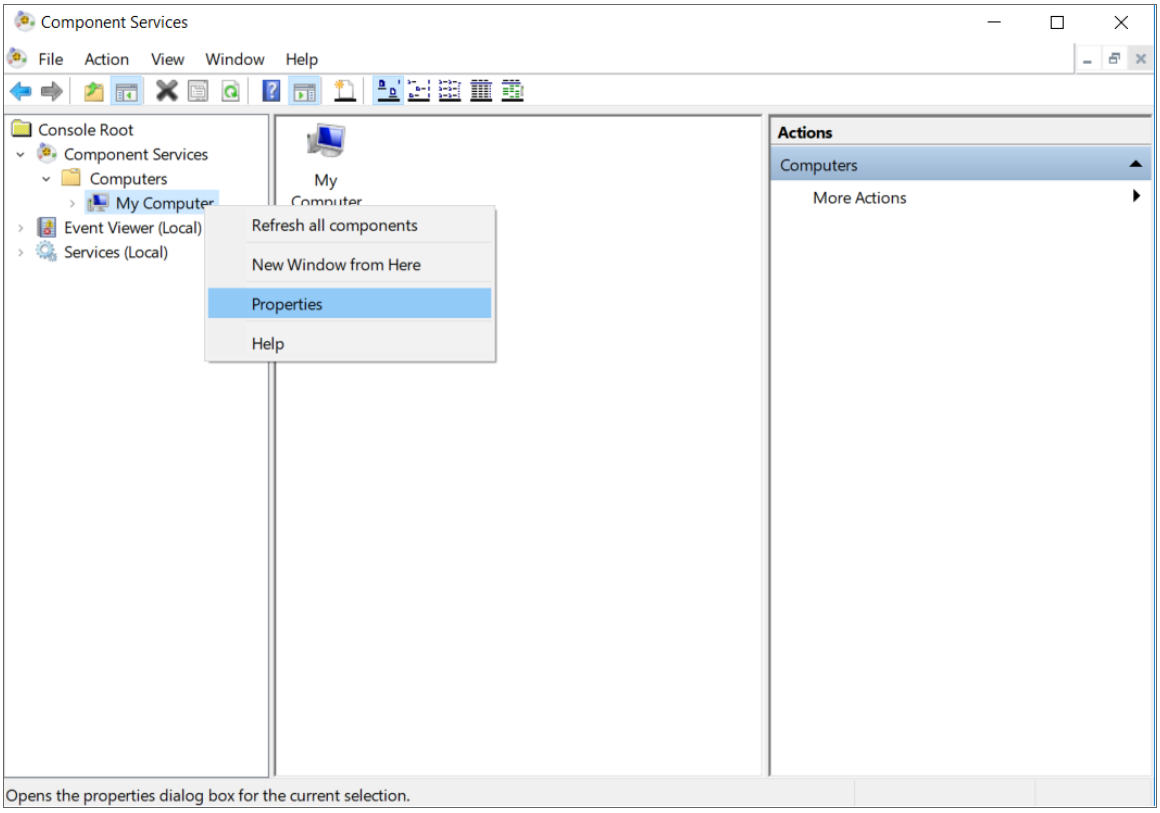
To set the DCOM Security Level, perform the following steps:

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

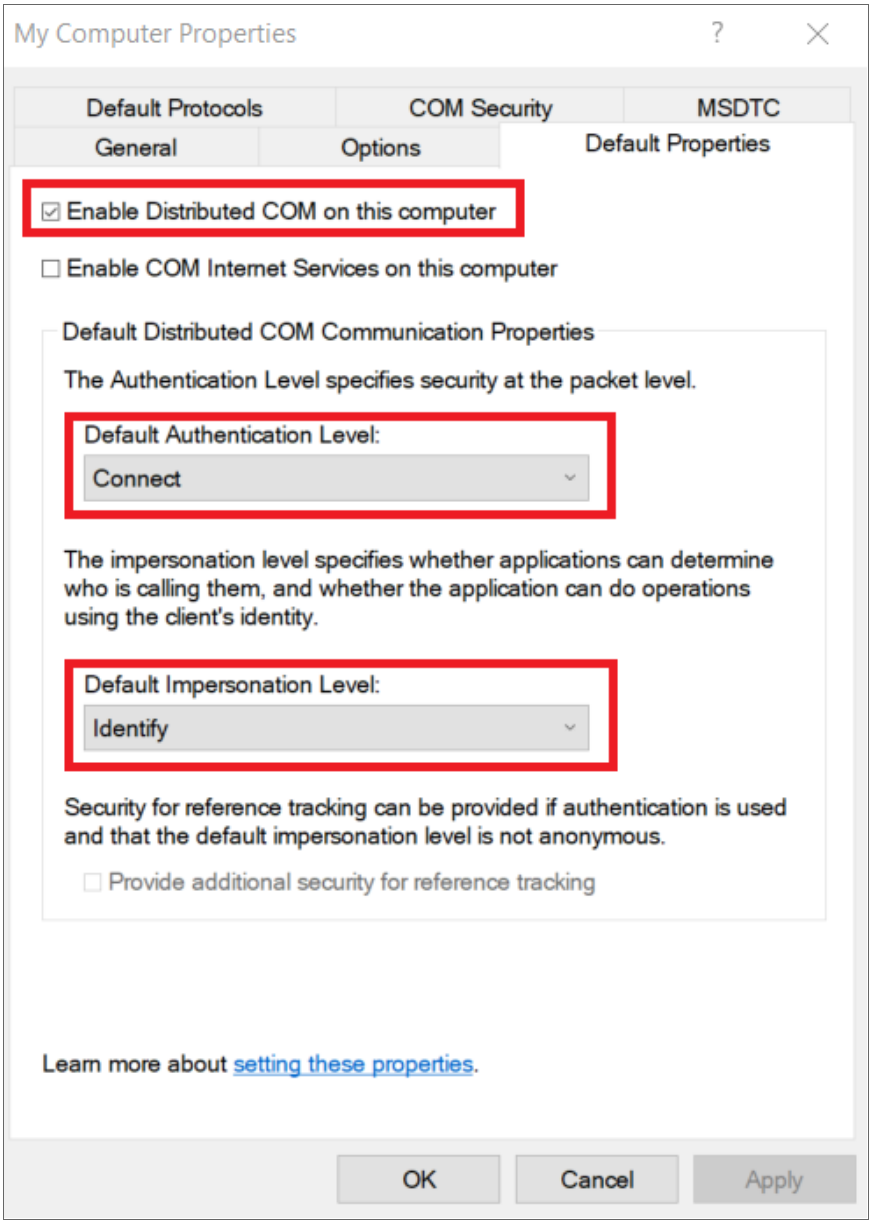
2. Click the **dcomcnfg.exe** command.



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

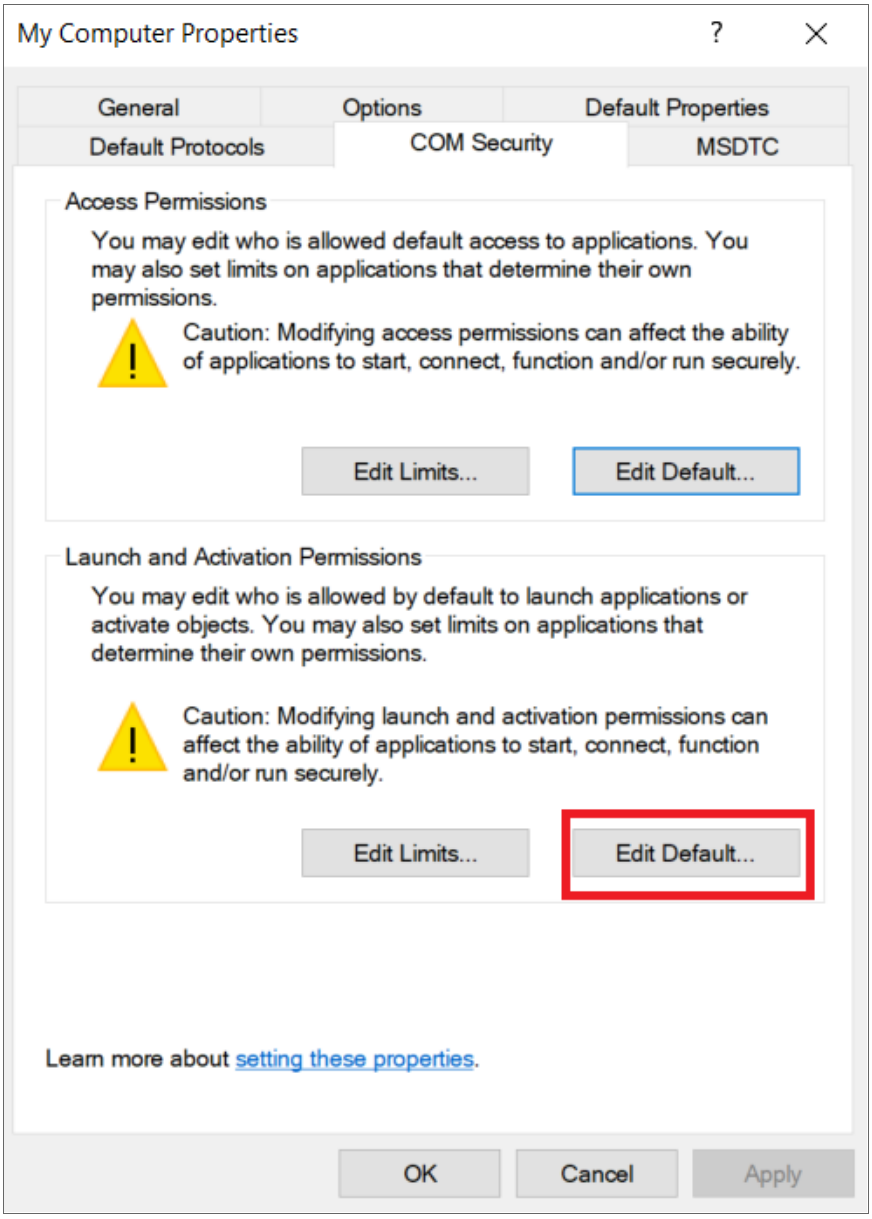


4. In the **My Computer Properties** window, click the **[Default Properties]** tab and then complete the following fields:

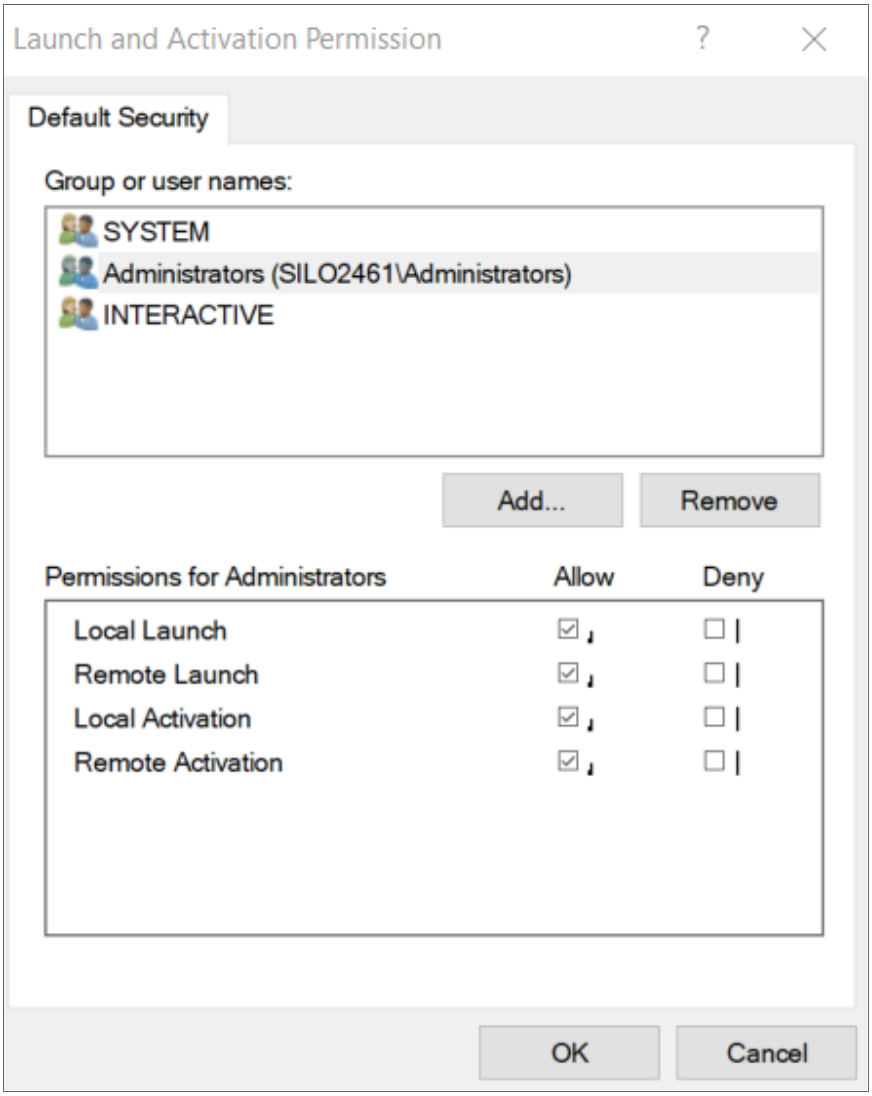


- ***Enable Distributed COM on this computer***. Select this checkbox.
- ***Default Authentication Level***. Select *Connect*.
- ***Default Impersonation Level***. Select *Identify*.

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



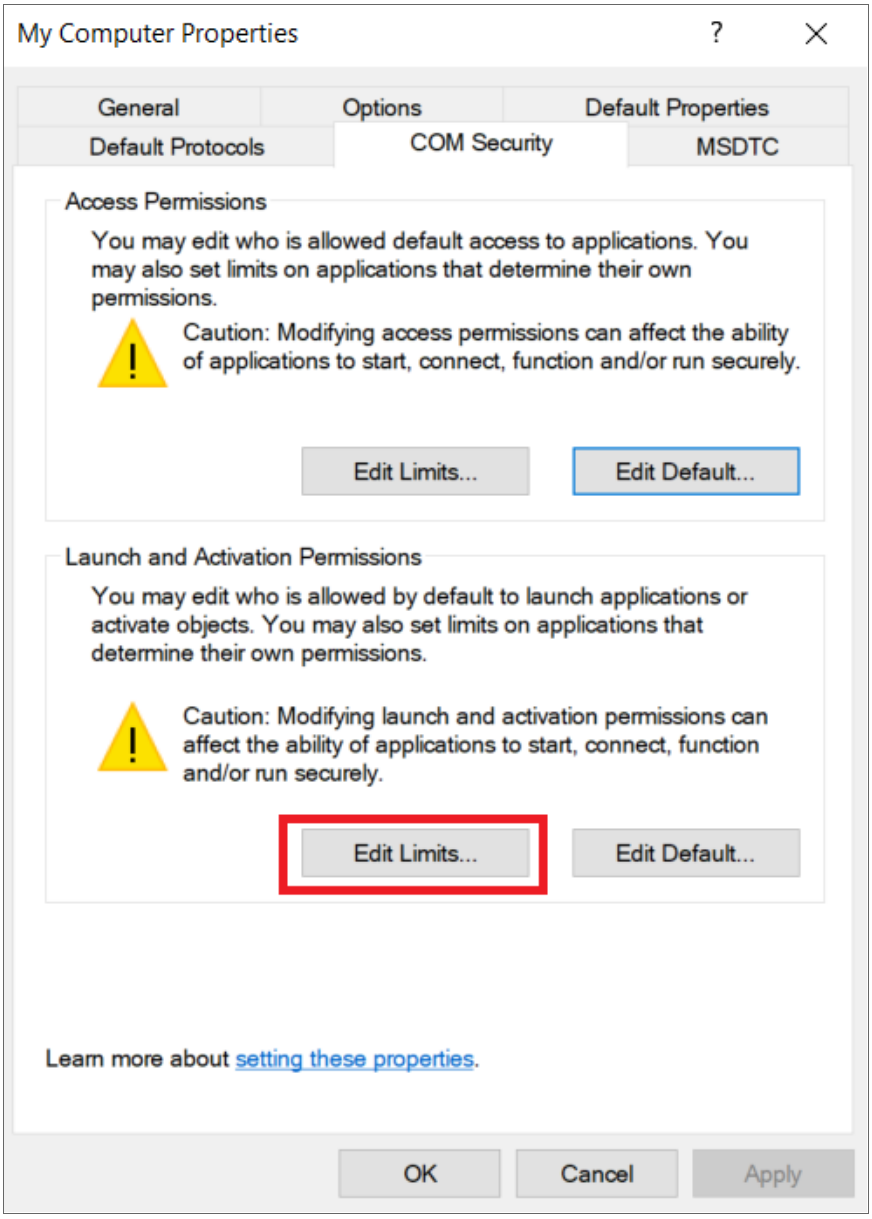
6. In the **Launch and Activation Permission** window, select the following:



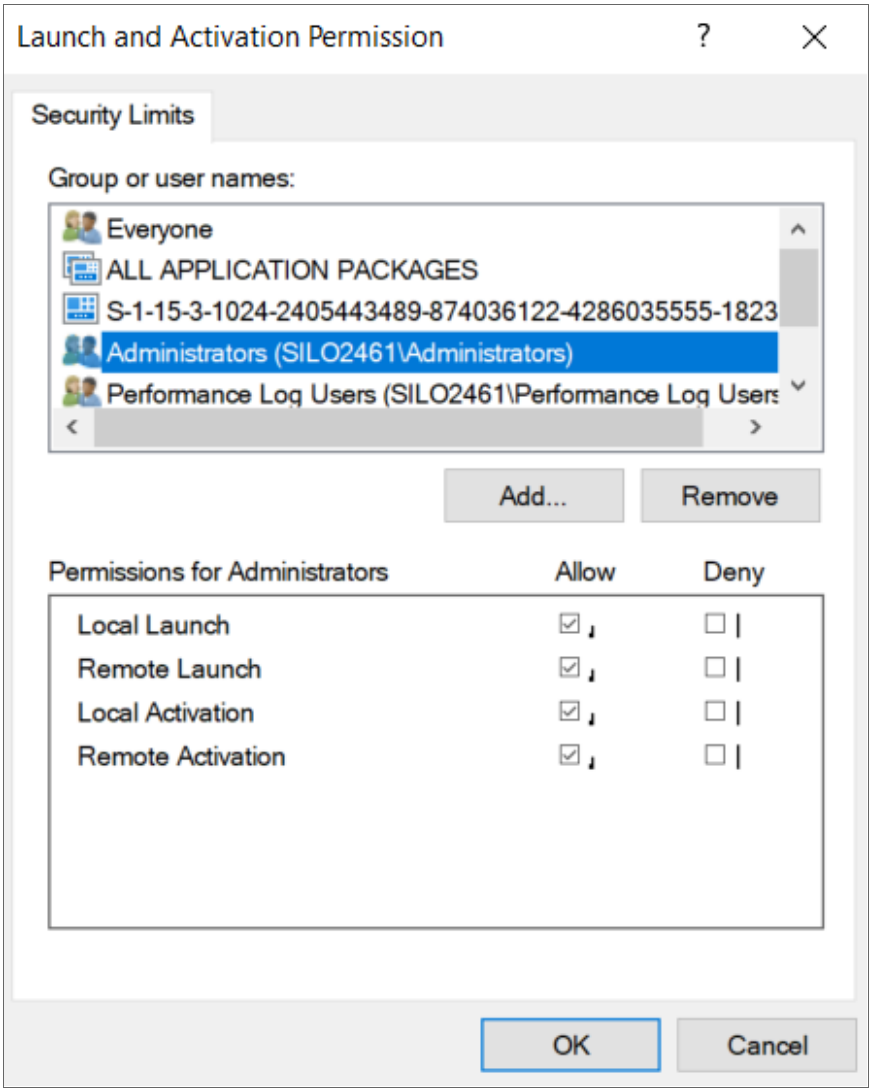
- ***Group or user names***. Select *Administrators*.
- ***Permissions for Administrators***. Set **Local Launch, Remote Launch, Local Activation**, and **Remote Activation**to ***Allow***.

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.

Step 6: Configuring a fixed port for WMI

Specific ports must be opened to allow WMI monitoring when there is a separate firewall between the Data Collector and the device. This can occur when the default configuration of the Windows Firewall blocks incoming network traffic for the Windows Management Instrumentation (WMI) connection.

For the WMI connection to succeed, the remote machine must permit incoming network traffic on TCP ports 135, 445, and additional dynamically-assigned ports, typically in the range of 1025 to 5000 and 49152 to 65535.

To set up a fixed port for WMI, see the Microsoft documentation on Setting Up a Fixed Port for WMI.

To set up a fixed port for WMI:

1. At the command prompt, type `winmgmt -standalonehost`
2. Stop the WMI service by typing the command `net stop "Windows Management Instrumentation"`, or use the shorter cpmmand of `net stop winmgmt`
3. Restart the WMI service in a new service host by typing `net start "Windows Management Instrumentation"` or `net start winmgmt`
4. Establish a new port number for the WMI service by typing `netsh firewall add portopening TCP 24158 WMIFixedPort`

To undo any changes you make to WMI, type `winmgmt /sharedhost`, then stop and start the winmgmt service again.

Chapter 4

SNMP and WMI Dynamic Applications for Windows Devices

Overview

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

The following sections describe the SNMP and WMI Dynamic Applications that SL1 uses to monitor Windows devices:

This chapter covers the following topics:

SNMP Dynamic Applications

If you configure your Windows system to respond to SNMP requests from SL1, you can discover your Windows system as an SNMP device. When SL1 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 SL1, you can use WMI Dynamic Applications to collect information from your Windows system.

NOTE: Although the SL1 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, SL1 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 2012, 2012r2, 2016, 2019, and 2022, 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

Relationships with Other Types of Component Devices

Additionally, the Dynamic Applications in the *Microsoft Base Pack* PowerPack can automatically build relationships between Windows servers and other associated devices:

- If you discover Dynatrace devices using the Dynamic Applications in the *Dynatrace* PowerPack, SL1 will automatically create relationships between Windows servers and Dynatrace hosts.
- If you discover Cisco AppDynamics devices using the Dynamic Applications in the *Cisco: AppDynamics* PowerPack, SL1 will automatically create relationships between Windows servers and AppDynamics nodes.
- If you discover New Relic devices using the Dynamic Applications in the *New Relic APM Pro* PowerPack, SL1 will automatically create relationships between Windows servers and New Relic servers.

Chapter 5

Creating SNMP and WMI Credentials for Windows Devices

Overview

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon (•••).

The following sections describe how to create SNMP and WMI credentials for Windows devices that you want to monitor with SL1:

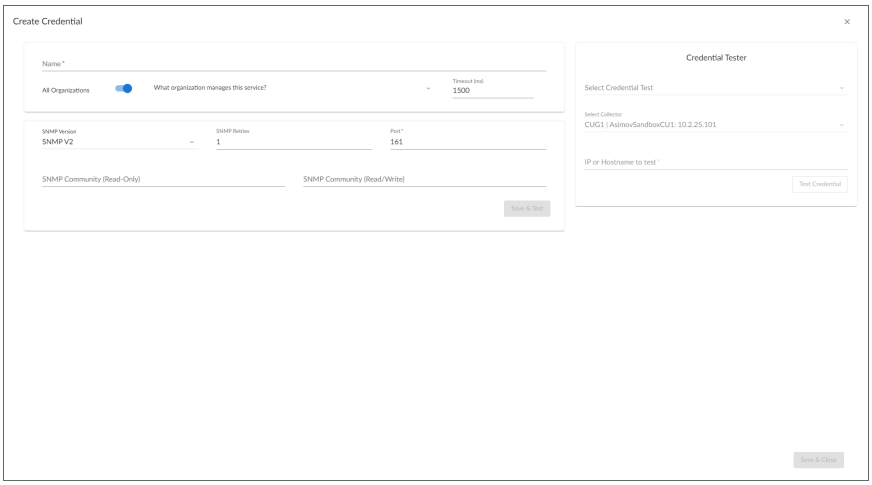
This chapter covers the following topics:

Creating an SNMP Credential

SNMP credentials allow SL1 to access SNMP data on a managed device. SL1 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 **Credentials** page (Manage > Credentials).
2. Click the **[Create New]** button and then select *Create SNMP Credential*. The **Create Credential** modal page appears:



3. Supply values in the following fields:
    - ***Name***. Name of the credential. Can be any combination of alphanumeric characters, up to 64 characters. This is a required field.
    - ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations. This field is required.

NOTE: To learn more about credentials and organizations, see the section *Aligning Organizations With a Credential*.

- ***Timeout (ms)***. Time, in milliseconds, after which SL1 will stop trying to communicate with the device. The default value is *1500*.
- ***SNMP Version***. SNMP version. Choices are *SNMP V1*, *SNMP V2*, and *SNMP V3*. The default value is *SNMP V2*.
- ***Port***. The port SL1 will use to communicate with the external device or application. The default value is *161*. This field is required.
- ***SNMP Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

SNMP V1/V2 Settings

If you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field, complete these fields. These fields are inactive if you selected *SNMP V3*.

- ***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

If you selected *SNMP V3* in the ***SNMP Version*** field, complete these fields. These fields are inactive if you selected *SNMP V1* or *SNMP V2*.

- ***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.

  In addition to alphanumeric characters, you ***can*** also use the following special characters in an SNMP V3 security passphrase: ? - _ = , . : # + % $ [ ] { } & ! ( ) | /

  You ***cannot*** use the following special characters in an SNMP V3 security passphrase: " ' \
- ***Authentication Protocol***. Select an authentication algorithm for the credential. This field is required. Choices are:
  - *MD5*. This is the default value.
  - *SHA*
  - *SHA-224*
  - *SHA-256*
  - *SHA-384*
  - *SHA-512*

NOTE: The *SHA* option is SHA-128.

- ***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*.
- ***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***. 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. This field is required. Choices are:
  - *DES*. This is the default value.
  - *AES-128*
  - *AES-192*
  - *AES-256*
  - *AES-256-C*. This option is for discovering Cisco devices only.
- ***Privacy Protocol Passphrase***. Privacy password for the credential. This field is optional.

4. Click **[Save & Close]**.

NOTE: If you would like to test your credential using the Credential Tester panel, click **[Save & Test]**. For detailed instructions on using the Credential Tester panel, see the *Using the Credential Tester Panel* section.

Creating an SNMP Credential in the SL1 Classic User Interface

SNMP Credentials allow SL1 to access SNMP data on a managed device. SL1 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).
2. Click the **[Actions]** button and select *Create SNMP Credential*. The **Credential Editor** page appears.
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*.
   - ***Port***. The port SL1 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 SL1 will stop trying to communicate with the SNMP device. The default value is *1500*.
   - ***Retries***. Number of times SL1 will try to authenticate and communicate with the external device. The default value is *1*.

   SNMP V1/V2 Settings

These fields appear if you selected *SNMP V1* or *SNMP V2* in the ***SNMP Version*** field. The fields are inactive if you selected SNMP V3.

- ***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. These fields are inactive if you selected SNMP V1 or SNMP V2.

- ***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. This field is required. Choices are:
  - *MD5*. This is the default value.
  - *SHA*
  - *SHA-224*
  - *SHA-256*
  - *SHA-384*
  - *SHA-512*

NOTE: The *SHA* option is SHA-128.

- ***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. This field is required. Choices are:
  - *DES*. This is the default value.
  - *AES-128*
  - *AES-192*
  - *AES-256*
  - *AES-256-C*. This option is for discovering Cisco devices only.
- ***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 SL1.

NOTE: When you define an SNMP Credential, SL1 automatically aligns the credential with all organizations of which you are a member.

Creating a WMI Credential

NOTE: Although SL1 supports WMI Dynamic Applications, ScienceLogic recommends that you use PowerShell Dynamic Applications where possible. PowerShell is the preferred management platform for Microsoft products.

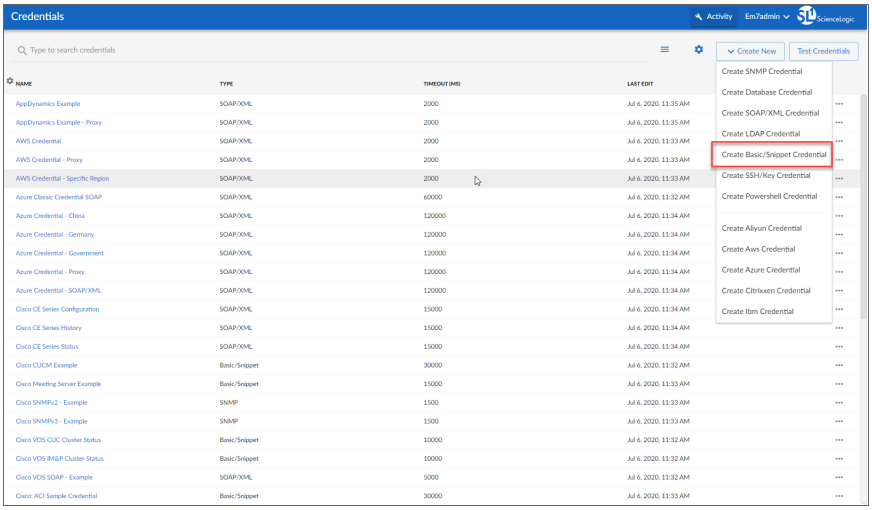
If you configure your Windows system to respond to WMI requests from SL1, you can use WMI Dynamic Applications to collect information from your Windows system.

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, SL1 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.

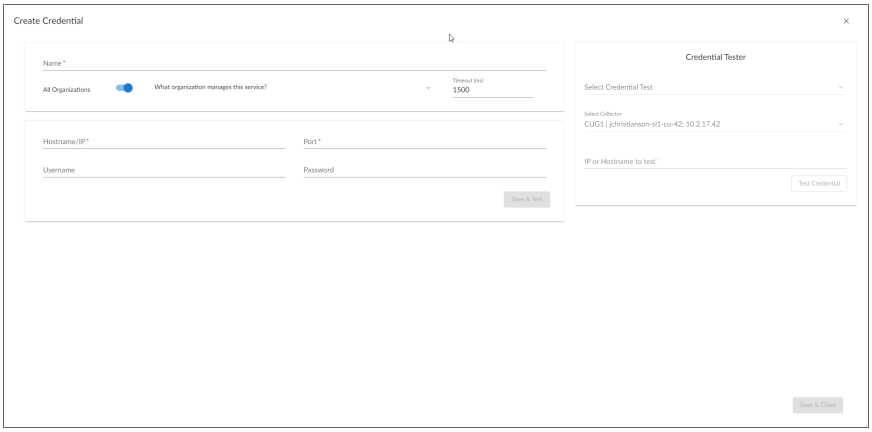
You can create a credential for WMI Dynamic Applications from the **Credentials** page. To create a credential for a WMI Dynamic Application:

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

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



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



- ***Credential Name***. Name of the credential. Can be any combination of alphanumeric characters.
- ***All Organizations***. Toggle on (blue) to align the credential to all organizations, or toggle off (gray) and then select one or more specific organizations from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
- ***Timeout (ms)***. Time, in milliseconds, after which the platform will stop trying to communicate with the authenticating server.
- ***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 SL1, enter any valid port number in this field; the platform does not specify a port number when

performing WMI requests.

- ***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 & Close]** button.

Creating a WMI Credential in the SL1 Classic User Interface

NOTE: Although SL1 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 SL1, 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, SL1 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*.
3. The **Credential Editor** page appears, where you can define the following fields:
    - ***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 SL1, 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. 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 SL1 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 SL1.

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.

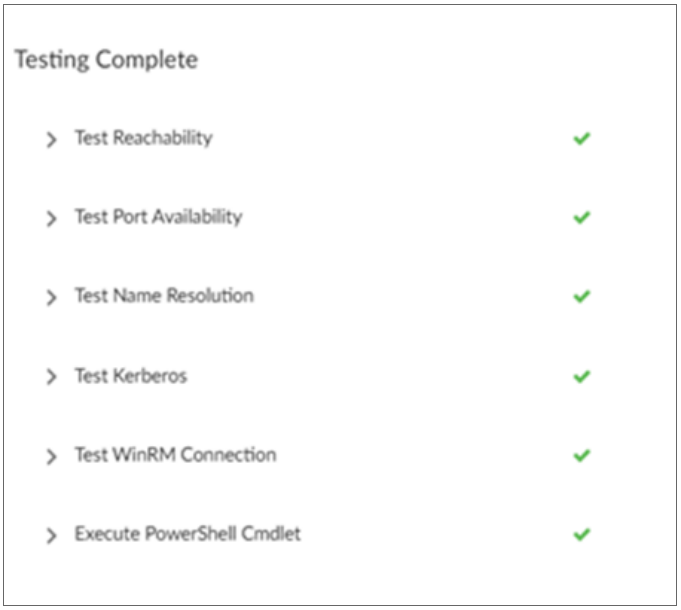
Running a Windows Credential Test

You can test a credential from the **Credentials** page using a predefined credential test.

To run a credential test from the **Credentials** page:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click the **Actions** button (⋯) of the credential that you want to test, and then select *Edit/Test*.
3. The **Credential Tester** modal page appears. Fill out the following fields on this page:
    - ***Select Credential Test***. Select a credential test to run. This drop-down list includes the *ScienceLogic Default Credential Tests*, credential tests included in any PowerPacks that have been optionally installed on your system, and credential tests that users have created on your system.
    - ***Collector***. Select the All-In-One Appliance or Data Collector that will run the test.
    - ***IP or Hostname to Test***. Type 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.

4. Click **[Test Credential]** button to run the credential test. The Credential Test starts and the Testing Completed modal displays the results.



The **Testing Completed** window displays a log entry for each step in the credential test. The steps performed are different for each credential test.

Running a Windows Credential Test in the SL1 Classic User Interface

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

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Click the **[Actions]** menu, and then select *Test Credential*. The **Credential Tester** modal page appears.
3. 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.
4. Click the **[Run Test]** button to run the credential test. The **Test Credential** window appears.

   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".

5. 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.

Chapter 6

Monitoring a Windows Cluster

Overview

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

The following sections describe how to monitor a Windows Cluster using SL1:

This chapter covers the following topics:

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 SL1 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 SL1 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, SL1 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 SL1 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. SL1 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 SL1 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:

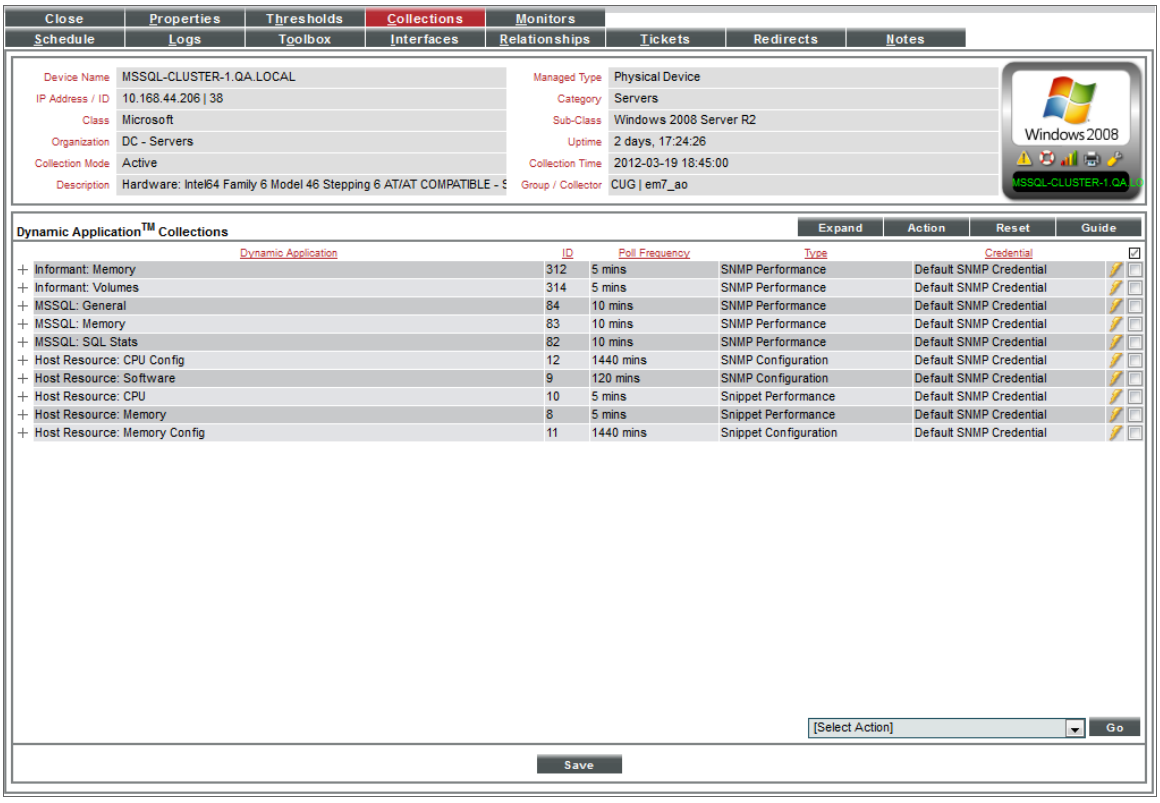
1. Go to the **Device Manager** page (Registry > Devices > Device Manager).

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:



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.

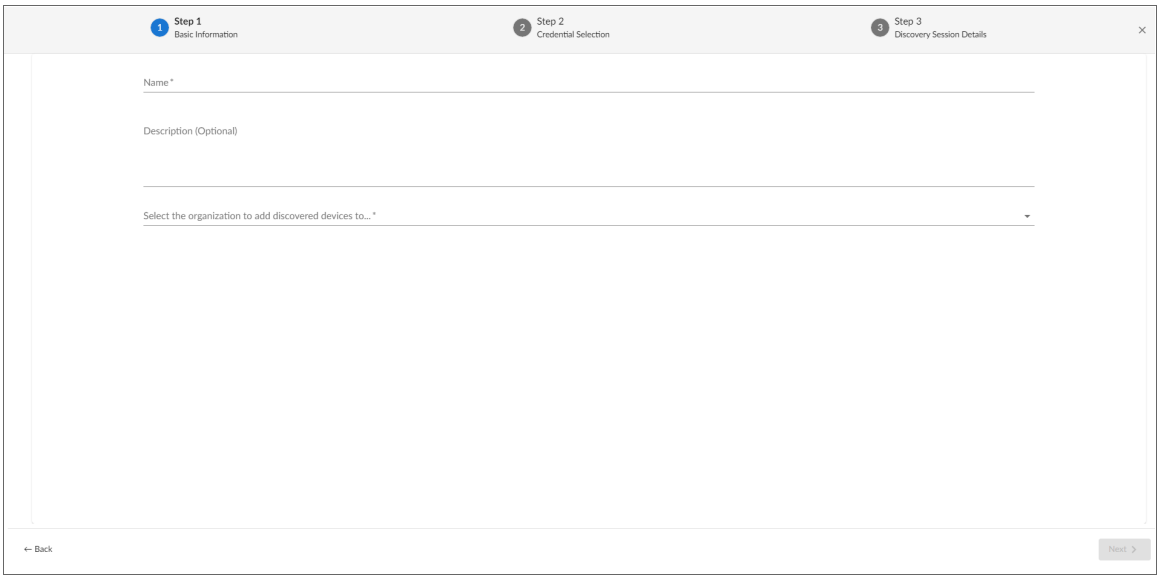
Discovering the Cluster IP Address

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 SL1 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 SL1 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 **Devices** page ( ) or the **Discovery Sessions** page Devices > Discovery Sessions).
2. Click the **[Add Devices]** button.
3. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the General Information page to the right.
4. Click **[Select]**. The **Add Devices** page appears.
5. Complete the following fields:



   - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the Discovery Sessions tab.
   - ***Description***. Type a short description of the discovery session. You can use the text in this description to search for the discovery session on the Discovery Sessions tab. Optional.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.
6. Click **[Next]**. The **Credentials** page of the **Add Devices** wizard appears.

7. Do not select anything in the **Credentials** page. Click **[Next]**.
8. In the **Discovery Session Details** page, click the down arrow icon ( ) next to ***Advanced Options*** to complete the following fields:
    - ***List of IPs/Hostnames***. Enter the shared IP address for the cluster.
    - ***Discover Non-SNMP***. Enable this setting (blue).
    - ***Select Device Template***. If you are *using a device template to configure Dynamic Applications*, select the device template in this field.
9. For the other fields in this page, you can use the default values or select different values based on your operating procedures.
10. Select the **[Save And Run]** button.

Discovering the Cluster IP Address in the SL1 Classic User Interface

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 SL1 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 SL1 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, SL1 will have associated the shared IP address for the cluster with one of those nodes. You must disable duplication protection for SL1 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.
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.

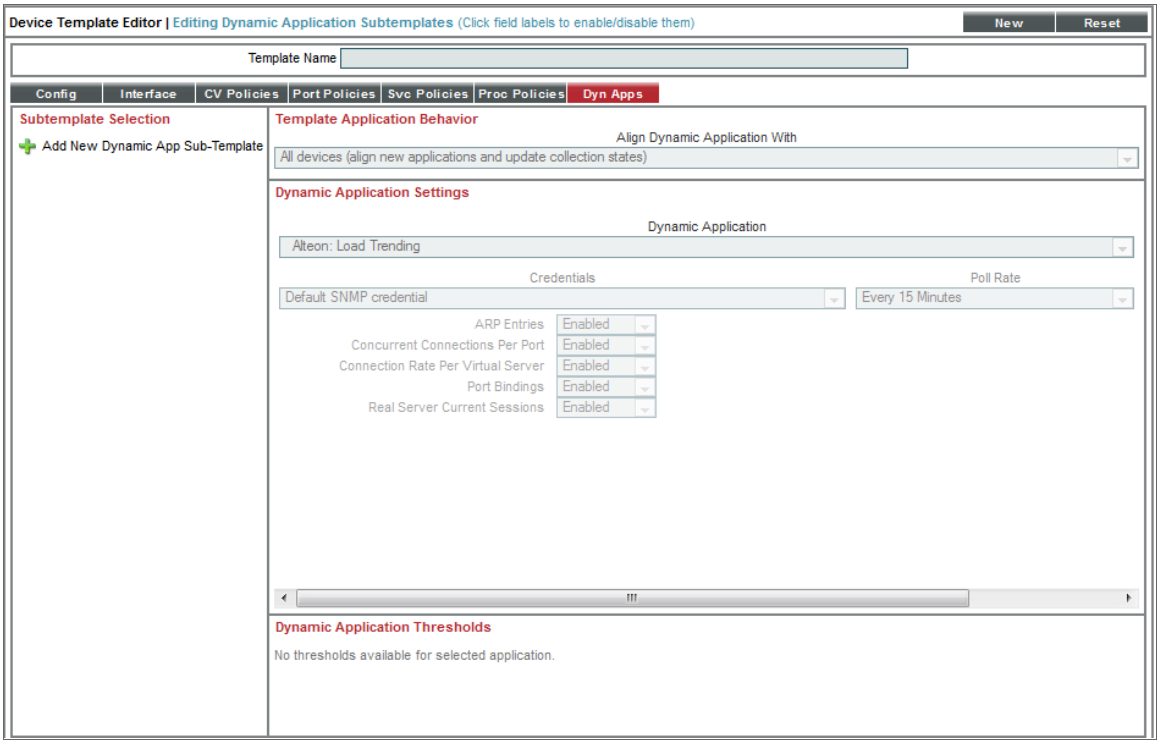
Using a Device Template to Configure Dynamic Applications

If you are configuring SL1 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 (Devices > Templates or Registry > Devices > Templates in the SL1 classic user interface).
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:

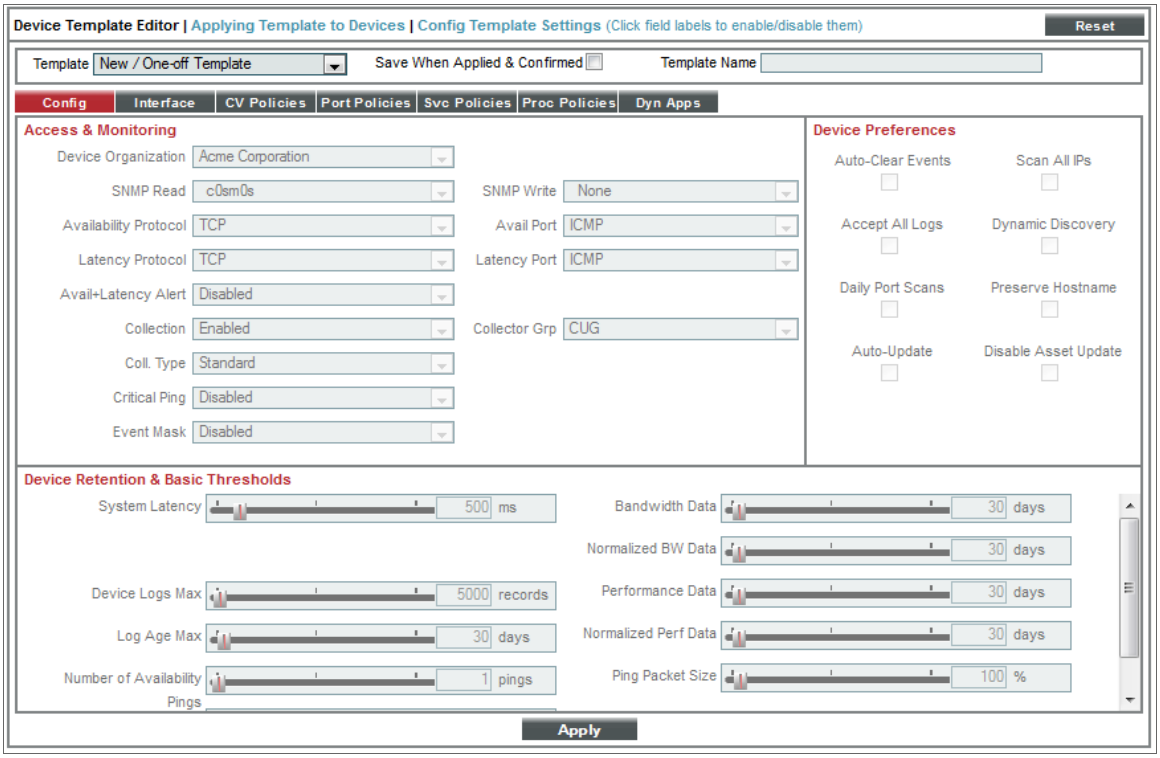
- ***Align Dynamic Application With***. Select *All devices*.
- ***Dynamic Application***. Select the Dynamic Application that you want to configure.
- ***Credentials***. If you want to use the device template to align Dynamic Applications with a device, enable this field by clicking on the field name. 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:



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.

Chapter 7

Automatically Restarting Windows Services

Overview

Use the following menu options to navigate the SL1 user interface:

- To view a pop-out list of menu options, click the menu icon ( ).
- To view a page containing all of the menu options, click the Advanced menu icon ( ).

The following sections describe how to use the *Windows Restart Automatic Services* PowerPack in SL1:

This chapter covers the following topics:

What is the Windows Restart Automatic Services PowerPack?

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

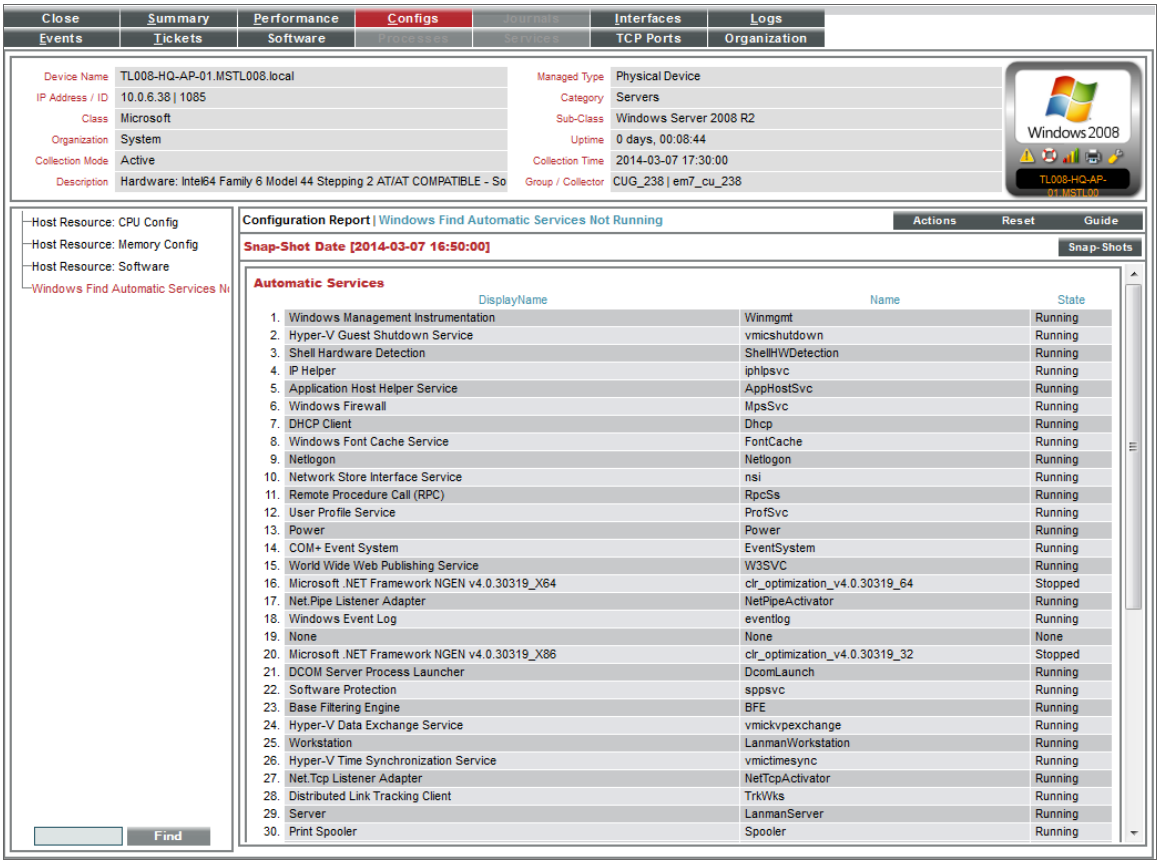
- Monitor the state of Windows services with a startup type of "Automatic" using WMI.
- Automatically start failed services by making an RPC over SMB request.

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*:



If a service with a startup type of "Automatic" is in a non-running state, SL1 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).

> **NOTE:** The **Database Tool** page is available only in versions of SL1 prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

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).

> **NOTE:** The **Database Tool** page is available only in versions of SL1 prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

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).

> **NOTE:** The **Database Tool** page is available only in versions of SL1 prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

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).

> **NOTE:** The **Database Tool** page is available only in versions of SL1 prior to 12.2.1 and displays only for users that have sufficient permissions to access the page.

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]**.

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. For more information, see https://sciencelogic.com/company/legal.

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

International: +1-703-354-1010