ScienceLogic

Monitoring Windows Systems with WMI

SL1 version 12.2.1

Table of Contents

Introduction	5
Monitoring Windows Devices in the ScienceLogic Platform	6
What is SNMP?	6
What is WMI?	6
WMI Monitoring and System Scalability	6
PowerPacks	7
Configuring Windows Systems for Monitoring with SNMP	
Configuring SNMP for Windows Server 2022, 2019, 2016, 2012, and 2012r2	8
Configuring Ping Responses	9
Installing the SNMP Service	10
Configuring the SNMP Service	15
Configuring the Firewall to Allow SNMP Requests	
Configuring Device Classes for Windows Server 2016 and Windows 10	20
Manually Align the Device Class	21
Edit the Registry Key	21
Configuring SNMP for Windows Desktop Systems	21
Enabling SNMP on Windows Desktop Systems	
Additional Steps for Configuring SNMP for Windows 10	
Configuring Windows Systems for Monitoring with WMI	
Configuring WMI on Windows 2012 and Later Servers	
Step 1: Configuring Services	31
Step 2: Configuring the Windows Firewall	
Step 3: Configuring a User Account and Permissions	
Configuring Namespace and DCOM Security Permissions	
Configuring User Account Control to Allow Elevated Permissions	41
Step 4: Configuring a Fixed Port for WMI	
Configuring WMI for Windows Desktop Systems	
Step 1: Configuring Services	44
Step 2: Configuring Windows Firewall	
Step 3: Setting the Default Namespace Security	
Step 4: Setting the DCOM Security Level	54

Step 5: Disabling User Account Control	61
Step 6: Configuring a fixed port for WMI	62
SNMP and WMI Dynamic Applications for Windows Devices	63
SNMP Dynamic Applications	63
WMI Dynamic Applications	64
Microsoft Base Pack	64
Relationships with Other Types of Component Devices	65
Creating SNMP and WMI Credentials for Windows Devices	66
Creating an SNMP Credential	66
Creating an SNMP Credential in the SL1 Classic User Interface	69
Creating a WMI Credential	71
Creating a WMI Credential in the SL1 Classic User Interface	73
Testing Windows Credentials	74
SNMP Credential Test	74
Basic/Snippet Credential Test	74
Running a Windows Credential Test	74
Running a Windows Credential Test in the SL1 Classic User Interface	75
Monitoring a Windows Cluster	77
Monitoring Windows Clusters in the ScienceLogic Platform	77
Discovering Cluster Nodes	78
Aligning a Dynamic Application with a Cluster Node	78
Disabling Collection of a Dynamic Application on a Device	79
Discovering the Cluster IP Address	80
Discovering the Cluster IP Address in the SL1 Classic User Interface	81
Aligning Dynamic Applications with the Cluster Device	82
Using a Device Template to Configure Dynamic Applications	
Automatically Restarting Windows Services	85
What is the Windows Restart Automatic Services PowerPack?	85
Configuring the Windows Restart Automatic Services PowerPack	86
Excluding Automatic Services	
Viewing the List of Excluded Services	
Adding an Excluded Service for All Devices	87

Adding an Excluded Service for a Single Device	88
Removing an Excluded Service	88

Chapter

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 (三).
- 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:

Monitoring Windows Devices in the ScienceLogic Platform	6
What is SNMP?	6
What is WMI?	6
PowerPacks	7

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 <u>Collector Sizing guidelines for WMI endpoints</u>.

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 <u>Support Knowledge Base</u> <u>article</u>.

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 (三).
- 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	. 8
Configuring SNMP for Windows Desktop Systems	21

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*:

2	Wind	dows Firewall wit	h Advanced S	ecurity		_ D X
File Action View Help						
🗢 🄿 🙇 🖬 🗟 🖬						
🔗 Windows Firewall with Advance	Inbound Rules					Actions
📖 Inbound Rules	Name	Group	^	Profile	Enabled ^	Inbound Rules
Cutbound Rules	🖉 Core Networking - Multicast Listener	Qu Core Network	ing	All	Yes	May Rule
Connection Security Rules	🕜 Core Networking - Multicast Listener	Rep Core Network	ing	All	Yes	
p 🛬 Moniconing	🕜 Core Networking - Multicast Listener	Rep Core Network	ing	All	Yes	Y Filter by Profile
	🕜 Core Networking - Neighbor Discove	ry A Core Network	ing	All	Yes	T Filter by State
	🕜 Core Networking - Neighbor Discove	ry S Core Network	ing	All	Yes	🕎 Filter by Group 🕨 🕨
	🔮 Core Networking - Packet Too Big (IC	MP Core Network	ing	All	Yes	View
	🔮 Core Networking - Parameter Probler	n (I Core Network	ing	All	Yes	
	🔮 Core Networking - Router Advertiserr	ient Core Network	ing	All	Yes	Q Refresh
	Ore Networking - Router Solicitation	I (IC Core Network	ing	All	Yes ≡	📑 Export List
	Core Networking - Teredo (UDP-In)	Core Network	ing	All	Yes	👔 Help
	Core Networking - Time Exceeded (IC	MP Core Network	ing o	All	Yes	
	Distributed Transaction Coordinator (RPC) Distributed Ir	ansaction Coo	All	No	File and Printer Sharing (Echo Request 🔺
	Distributed Transaction Coordinator (RP Distributed In	ansaction Coo	All	No	O Enable Rule
	Ele and Drinter Sharing (Echo P	IC Distributed in	ansaction Coo	All	No	of Cut
	File and Printer Sharing (Echo R	Enable Rule	Sharing	All	Vec	🗈 Сору
	File and Printer Sharing (LLMNE	Cut	Sharing	All	No	Y Delete
	File and Printer Sharing (NB-Dat	Comu	Sharing	All	No	
	File and Printer Sharing (NB-Na	Сору	Sharing	All	No	Properties
	File and Printer Sharing (NB-Ses	Delete	Sharing	All	No	👔 Help
	File and Printer Sharing (SMB-Ir	Properties	Sharing	All	No	
	File and Printer Sharing (Spoole	Help	Sharing	All	No	
	File and Printer Sharing (Spooler Servi	ce File and Printe	er Sharing	All	No	
	File and Printer Sharing over SMBDire	ct (i File and Printe	er Sharing over	All	No	
	🔘 iSCSI Service (TCP-In)	iSCSI Service		All	No	
	🔘 Key Management Service (TCP-In)	Key Managen	nent Service	All	No	
	💿 Netlogon Service (NP-In)	Netlogon Sen	/ice	All	No	
	🜑 Netlogon Service Authz (RPC)	Netlogon Sen	/ice	All	No	
	Whetwork Discovery (LLMNR-UDP-In)	Network Disc	overy	All	No	
	🔮 Network Discovery (NB-Datagram-In)	Network Disc	overy	All	No	
	Network Discovery (NB-Name-In)	Network Disc	overy	All	No	
	Wetwork Discovery (Pub-WSD-In)	Network Disc	overy	All	No 🗸	
< III >	< III				>	
Copies the current selection.						

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:

à	Add Roles and Features Wizard	- 🗆 X
Select installation	type	NATION SERVER I-3UGJKS2COLQ
Before You Begin Installation Type	Select the installation type. You can install roles and features on a running physical comp machine, or on an offline virtual hard disk (VHD).	uter or virtual
Server Selection	Configure a single server by adding roles, role services, and features.	
Features	 Remote Desktop Services installation Install required role services for Virtual Desktop Infrastructure (VDI) to create a virtual 	machine-based
Confirmation Results	or session-based desktop deployment.	
	< Previous Next > Install	Cancel

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

Ē.	Add Role	es and Features V	Vizard	_ D X
Select destinatior	n server			DESTINATION SERVER WIN-3UGJKS2COLQ
Before You Begin Installation Type Server Selection Server Roles Features	Select a server or a virtua Select a server from t Select a virtual hard of Server Pool Filter:	al hard disk on which he server pool disk	to install roles and features.	
Confirmation Results	Name WIN-BUGJKS2COLQ	IP Address 10:100.100.22	Operating System Microsoft Windows Server 20	D12 R2 Standard
	This page shows servers Add Servers command in collection is still incomple	that are running Wind I Server Manager. Off ete are not shown. < Pre	dows Server 2012, and that have line servers and newly-added se vious Next >	e been added by using the ervers from which data Install Cancel

- 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:

B	Add Roles and Features Wizard	_ _ X
Select features		DESTINATION SERVER WIN-3UGJKS2COLQ
Before You Begin Installation Type	Select one or more features to install on the selected server. Features	Description
Server Selection Server Roles	INET Framework 3.5 Features Image: Interpretent state Image:	.NET Framework 3.5 combines the power of the .NET Framework 2.0 APIs with new technologies for
Confirmation Results	Background Intelligent Transfer Service (BITS) BitLocker Drive Encryption BitLocker Network Unlock	building applications that offer appealing user interfaces, protect your customers' personal identity information, enable seamless and
	BranchCache Client for NFS Data Center Bridging	secure communication, and provide the ability to model a range of business processes.
	Direct Play Enhanced Storage	
	Failover Clustering Group Policy Management IIS Hostable Web Core	
	Ink and Handwriting Services	
1	< Previous Next >	Install

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

b	Add Roles and Features Wizard	x
Ad The hay	dd features that are required for SNMP Service? e following tools are required to manage this feature, but do not ve to be installed on the same server.	
⊿	Remote Server Administration Tools	
	▲ Feature Administration Tools	
	[Tools] SNMP Tools	
Y	Include management tools (if applicable) Add Features Cancel	

- 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:

B	🚡 Add Roles and Features Wizard 🗕 🗖 🗙			
Confirm installati	on selections	DESTINATION SERVER WIN-3UGJKS2COLQ		
Before You Begin	To install the following roles, role services, or features on selected server, click In	istall.		
Installation Type	Restart the destination server automatically if required			
Server Selection	Optional features (such as administration tools) might be displayed on this page	because they have		
Server Roles	been selected automatically. If you do not want to install these optional features their check boxes.	, click Previous to clear		
Features				
Confirmation Results	Remote Server Administration Tools Feature Administration Tools SNMP Tools SNMP Service SNMP WMI Provider			
	Export configuration settings Specify an alternate source path			
	< Previous Next >	ıstall Cancel		

- 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:

SNMP	Service Properties (Local Computer)
General Log On	Recovery Agent Traps Security Dependencies
Service name:	SNMP
Display name:	SNMP Service
Description:	Enables Simple Network Management Protocol (SNMP) requests to be processed by this computer.
Path to executable C:\Windows\Syst	e: em32\snmp.exe
Startup type:	Automatic
Service status:	Running
Start	Stop Pause Resume
You can specify th from here.	ne start parameters that apply when you start the service
Start parameters:	
	OK Cancel Apply

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

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

SNI	MP Service	Propert	ties (Lo	cal Con	nputer) 🛛 🗙					
General Log	On Recovery	Agent	Traps	Security	Dependencies					
Send authentication trap										
Accepted	community nam	es								
Commu	nity		Rig	nts						
	۵dd	Edi	ŀ	Benc	ive					
	Add			rione						
O Accep	ot SNMP packet	s from any	y host							
 Accept 	ot SNMP packet	s from the	se hosts							
localho	ost									
	Add	Edi	t	Remo	ve					
		Ok	(Cancel	Apply					

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

SNMP Service Properties (Local Computer)
General Log On Recovery Agent Traps Security Dependencies
Send authentication trap
Accepted community names
Community Rights
SNMP Service Configuration
Community rights: Add READ ONLY Community Name:
Add Edit Remove
OK Cancel Apply

- 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:

SNMP	Service Prope	rties (Lo	ocal Con	nputer)	x			
General Log On	Recovery Agent	Traps	Security	Dependencies				
Send authenti	cation trap							
- Accepted com	munity names							
Community		Rig	hts					
public		REA	AD ONLY					
	SNMP Service	e Config	juration	x				
Host name,	Add Host name, IP or IPX address:							
Ad	ld E	jit	Remo	ive				
	(IK	Cancel	Apply				

- 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:

Windows Firewall with Advanced Security									_ 0 ×
File Action View Help									
🗢 🌩 🙇 📰 📑 🖬 🖬									
🔗 Windows Firewall with Advanc	Inbound Rules								Actions
🗱 Inbound Rules	Name	Group	Profile	Enabled	Action	Override	Program	Local Address ^	Inbound Rules
Cutbound Rules	Remote Event Log Management (RPC-EP	Remote Event Log Manage	All	No	Allow	No	%System	Any	May Rule
Connection Security Rules	Remote Event Monitor (RPC)	Remote Event Monitor	All	No	Allow	No	%System	Any	
p 🖏 Wontoning	Remote Event Monitor (RPC-EPMAP)	Remote Event Monitor	All	No	Allow	No	%System	Any	Y Filter by Profile
	Remote Scheduled Tasks Management (Remote Scheduled Tasks N	I All	No	Allow	No	%System	Any	Tilter by State
	Remote Scheduled Tasks Management (Remote Scheduled Tasks N	I All	No	Allow	No	%System	Any	🐨 Filter by Group
	Remote Service Management (NP-In)	Remote Service Manageme	nt All	No	Allow	No	System	Any	View
	Remote Service Management (RPC)	Remote Service Manageme	nt All	No	Allow	No	%System	Any	
	Remote Service Management (RPC-EPM	Remote Service Manageme	nt All	No	Allow	No	%System	Any	Q Refresh
	Inbound Rule for Remote Shutdown (RP	Remote Shutdown	All	No	Allow	No	%system	Any	🔿 Export List
	Inbound Rule for Remote Shutdown (TC	Remote Shutdown	All	No	Allow	No	%system	Any	Help
	Remote Volume Management - Virtual D	Remote Volume Managem	e All	No	Allow	No	%System	Any	
	Remote Volume Management - Virtual D	Remote Volume Managem	e All	No	Allow	No	%System	Any	SNMP Service (UDP In)
	Remote Volume Management (RPC-EPM	Remote Volume Managem	e All	No	Allow	No	%System	Any	O Enable Rule
	Routing and Remote Access (GRE-In)	Routing and Remote Acces	s All	No	Allow	No	System	Any	🔏 Cut
	Routing and Remote Access (L2TP-In)	Routing and Remote Acces	s All	No	Allow	No	System	Any	Ph. Com
	W Routing and Remote Access (PPTP-In)	Routing and Remote Acces	s All	No	Allow	No	System	Any	Le copy
	Secure Socket Tunneling Protocol (SSTP	Secure Socket Tunneling Pi	All	No	Allow	No	System	Any	X Delete
	SNMP Service (UDP In)	SNMP Service	Domain, Public	Yes	Allow	No	%System	Any	Properties
	SNMP Service (UDP In)	Enable Rule	Private, Public	NO	Allow	NO	%System	Any	7 Help
	SIMP Trap Service (UDP In)	Cut	Private, Public	NO	Allow	NO	%System	Any	
	TDM/Gt ul Court Coul Management	Cut	Domain	NO	Allow	NO No	%System	Any	
	TPM Virtual Smart Card Managemen	Copy and Ma	Domain	NO	Allow	NO No	%System	Any	
	TDM Virtual Smart Card Managemen	Delete and Ma	Private, Public	No	Allow	No	%System	Any =	
	TDM Virtual Smart Card Managemen	Properties and Ma	Domain Drivate Dublic	No	Allow	No	%System	Any	
	Widual Machine Menitering (DCOM	Hele iterie	Flivate, Fublic	Ne	Allow	Ne	%System	Any	
	Wittual Machine Monitoring (Eccow-	Virtual Machine Monitoring		No	Allow	No	Any	Any	
	Wittual Machine Monitoring (Echo Reque	Virtual Machine Monitoring		No	Allow	No	Any	Any	
	Virtual Machine Monitoring (NB-Session	Virtual Machine Monitoring		No	Allow	No	Any	Any	
								···· · · ·	
								>	1
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.



Services						- 🗆	×
File Action View	Help						
	à 🔒 👔 🖬 🕨 🔳 🕪						
🤹 Services (Local)	Services (Local)						
	SNMP Service	Name	Description	Status	Startup Type	Log On As	^
		🏟 Server	Supports file	Running	Automatic (Tri	Local System	
	Stop the service	🎑 Shared PC Account Manager	Manages pr		Disabled	Local System	
	<u>Restart</u> the service	🌼 Shell Hardware Detection	Provides not	Running	Automatic	Local System	
		🏟 Smart Card	Manages ac	Running	Automatic (Tri	Local Service	
	Description:	🆏 Smart Card Device Enumerat	Creates soft		Manual (Trigg	Local System	
	Management Protocol (SNMP)	🌼 Smart Card Removal Policy	Allows the s		Manual	Local System	
	requests to be processed by this	SNMP Service	Enables Sim	Running	Automatic	Local System	
	computer. If this service is stopped,	🏟 SNMP Trap	Receives tra		Manual	Local Service	
	the computer will be unable to process SNMP requests. If this service is disabled, any services that explicitly depend on it will fail to start.	🍓 Software Protection	Enables the		Automatic (De	Network Se	
		🍓 Spatial Data Service	This service i		Manual	Local Service	
		🆏 Spot Verifier	Verifies pote		Manual (Trigg	Local System	
		🖏 SSDP Discovery	Discovers ne	Running	Manual	Local Service	
		🍓 State Repository Service	Provides req	Running	Manual	Local System	
		Still Image Acquisition Events	Launches ap		Manual	Local System	
		Storage Service	Provides ena	Running	Manual (Trigg	Local System	
		🍓 Storage Tiers Management	Optimizes th		Manual	Local System	
		🍓 Superfetch	Maintains a	Running	Automatic	Local System	- 10
		🍓 Symantec Endpoint Protecti	Provides mal	Running	Automatic	Local System	
		🍓 Symantec Network Access C	Checks that		Manual	Local System	
		🆏 Sync Host_1b4edb	This service	Running	Automatic (De	Local System	
		🆏 System Event Notification S	Monitors sy	Running	Automatic	Local System	
		🎑 System Events Broker	Coordinates	Running	Automatic (Tri	Local System	
		🍓 Task Scheduler	Enables a us	Running	Automatic	Local System	
		🍓 TCP/IP NetBIOS Helper	Provides sup	Running	Manual (Trigg	Local Service	
		🎑 Telephony	Provides Tel		Manual	Network Se	
		🔍 Themes	Provides use	Running	Automatic	Local System	~
	Extended Standard						

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:

SNMP Se	NMP Service Properties (Local Computer)										
General	General Log On Recovery Agent Traps Security Dependencie										
Service											
Display	name:	SNMP Ser	vice								
Descript	tion:	Enables Si (SNMP) re	mple Ne quests to	twork Ma be proce	nagement essed by th	Protocol is compu	iter.				
Path to C:\WIN	executabl DOWS\Sy	e: stem32\snm	p.exe								
Startup	type:	Automatic					~				
Service	Service status: Running										
S	Start	Stop)	Pau	ise	Res	ume				
You car from he	You can specify the start parameters that apply when you start the service from here.										
Start pa	rameters:										
			Oł	(Cance	I	Apply				

• 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].

SNMP Se	rvice Pro	perties (Loo	al Comp	outer)			\times					
General	Log On	Recovery	Agent	Traps	Security	Dependencies						
Send authentication trap												
Acce	Accepted community names											
Co	mmunity			Rigi	nts							
	Ad	ld	Edit		Remo	ove						
	ccept SNN	IP packets fr	om any h	ost								
• A	ccept SNM	IP packets fr	om these	hosts								
lo	calhost											
L												
	Ad	ld	Edit		Remo	ve						
			OK	(Cancel	Apply						

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

SNMP Service Configuration		×
Community rights:		Add
READ ONLY ~		Cancel

- 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:

SNMP Service Configuration	×
	Add
Host name IP or IPX address	Cancel

- 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.

S	SNMP Service Properties (Local Computer)										
	General	Log On	Recovery	Recovery Agent Traps Security Dependencies							
	Service	name:	SNMP								
	Display name: SNMP Service										
	Descript	tion:	Enables Si (SNMP) re	mple Nei quests to	twork Ma be proce	nagement essed by th	Protocol is computer	. ^			
	Path to executable: C:\WINDOWS\System32\snmp.exe										
	Startup	type:	Automatic					×			
	Service	status:	Stopped						.		
	S	Start	Stop)	Pau	lse	Resum	е			
You can specify the start parameters that apply when you start the service from here.											
	Start pa	rameters:]		
						Canad		Ameli	_		
				Or	`	Cancel	/	-фріу			

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 (三).
- 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	. 30
Configuring WMI for Windows Desktop Systems	43

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 <u>http://msdn.microsoft.com/en-us/library/windows/desktop/aa826699%28v=vs.85%29.aspx</u>

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.

Server Manager							
File Artison View Help							
Server Manager (QA-DOM-CTRL-1)	Services						
E Roles	Ö Services					Services 🔺	
E Preatures	- services					More Actions	
Configuration	Select an item to view its description.	Name	Description Status	Startup Type Log C	n As 🔺	1	
Task Scheduler		Active Directory Domain Services	AD D5 Dom Started	Automatic Local	System		
Windows Firewall with Advanced Secu	1	Active Directory Web Services	This servic Started	Automatic Local	System	1	
Services	1	Application Experience	Processes Started	Manual Local	System		
🚔 WMI Control	1	Application Identity	Determines	Manual Local	Service	1	
🗉 🔠 Storage	1	Application Information	Facilitates Started	Manual Local	System	1	
	1	Application Layer Gateway Service	Provides s	Manual Local	Service	1	
	1	Application Management	Processes i	Manual Local	System		
	1	Background Intelligent Transfer Service	Transfers f Started	Manual Local	System	1	
	1	🔄 Base Filtering Engine	The Base F Started	Automatic Local	Service	1	
	1	Certificate Propagation	Copies use Started	Manual Local	System	1 1	
	1	💁 CNG Key Isolation	The CNG k	Manual Local	System		
	1	🔍 COM+ Event System	Supports S Started	Automatic Local	Service	1 1	
	1	🖾 COM+ System Application	Manages t	Manual Local	System	4 1	
	1	🖾 Computer Browser	Maintains a	Disabled Local	System	1 1	
	1	🚳 Credential Manager	Provides s	Manual Local	System		
	1	Cryptographic Services	Provides fo Started	Automatic Netwo	ork S	1 1	
	1	COM Server Process Launcher	The DCOM Started	Automatic Local	System	1 1	
	1	💁 Desktop Window Manager Session Manager	Provides D Started	Automatic Local	System	1 1	
	1	OFS Namespace	Enables yo Started	Automatic Local	System		
	1	OFS Replication	Enables yo Started	Automatic Local	System	1 1	
	1	C DHCP Client	Registers a Started	Automatic Local	Service	1 1	
	1	Q Diagnostic Policy Service	The Diagno Started	Automatic (D Local	Service		
	1	Chagnostic Service Host	The Diagno	Manual Local	Service		
	1	Diagnostic System Host	The Diagno	Manual Local	System		
	1	🖾 Disk Defragmenter	Provides Di	Manual Local	System	4 I	
	1	🖾 Distributed Link Tracking Client	Maintains I	Manual Local	System		
	1	Substributed Transaction Coordinator	Coordinate Started	Automatic (D Netwo	ek S	1 1	
	1	🖾 DNS Client	The DNS Cl Started	Automatic Netwo	ark S	4 I	
	1	QDNS Server	Enables DN Started	Automatic Local	System		
	1	Encrypting File System (EFS)	Provides th	Manual Local	System		
	1	Extensible Authentication Protocol	The Extens	Manual Local	System		
	1	File Replication Service	Synchroniz Started	Automatic Local	System 💌	1	
•	Extended / Standard /					1	

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:

COM+ Event Syste	m Properties (QA-DOM-CTRL-1)	×			
General Log On	Recovery Dependencies				
Service name:	EventSystem				
Display name:	COM+ Event System				
Description:	Description: Supports System Event Notification Service (SENS), which provides automatic distribution of events to				
Path to executable: C:\Windows\system32\svchost.exe -k LocalService					
Startup type:	Automatic				
Help me configure service startup options.					
Service status:	Started				
Start	Stop Pause Resume				
You can specify the start parameters that apply when you start the service from here.					
Start parameters:					
	Cancel Apply				

- 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:

- 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:

WMI Con	trol Properties			?	×		
General	Backup/Restore	Security	Advanced				
Namesp	Namespace navigation allows you to set namespace specific security.						
±	Root						
				Security			
		Ok	Cancel	Арг	oly		

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.

1

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

Security for Root	×			
Security				
Group or user names: Administrators (DESKTOP-SR36R55\Administrators) admin (DESKTOP-SR36R55\no_admin)				
Add Remove				
Permissions for no_admin Allow Deny Execute Methods Full Write Partial Write Provider Write Enable Account Remote Enable For special permissions or advanced settings, click Advanced. Advanced	^			
OK Cancel Apply	/			

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

Adv	vanced S	ecurity Settings for Root					2
Owner: Administrators (DESKTOP-SR36R55\Administrators) Change							
Pern	nissions	ssions Auditing					
For additional information, double-click a permission entry. To modify a permission entry, select the entry and click Edit (if available). Permission entries:							
	Туре	Principal	Access	Inherited from	Applies to		_
2	Allow	Administrators (DESKTOP-SR3	Special	None	This namespace and	l subname.	••
4	Allow	no_aumin (DESKTOP-SK50K33	LINDIE ACCOUNT	NOTE	rnis namespace ong	у	
	Add	Remove View					
Di	isable inl	heritance					
				[OK Cancel	Appl	y

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

Select Users or Groups	×
Select this object type: Users, Groups, or Built-in security principals	Object Types
From this location:	
DESKTOP-SR36R55	Locations
Enter the object names to select (<u>examples</u>):	Check Names
Advanced OK	Cancel

- 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:

Permission	Entry for Root		- D X
Principal:	no_admin (DESKTOP-SR36R55\no_admin) Select a	principal	
Туре:	Allow		
Applies to:	This namespace and subnamespaces $\qquad \lor$		
Permissions	: Full Write Partial Write Provider Write	∑ Enable Account ∑ Remote Enable ☐ Read Security ☐ Edit Security	
Only app	ly these permissions to objects and/or containers with	in this container	Clear all
			OK Cancel

- 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:

Component Services				_ 🗆 🗡
🧽 File Action View Window H	Help			_ B ×
🗢 🔿 🖄 📅 🗙 🗒 🙆 🔿	🛛 🖬 🖿 🖿 🏛 🗰	-		
Console Root	Name		Actions	
🖃 💩 Component Services	COM+ Applications		My Computer	_
E Computers	DCOM Config		More Actions	•
Event Viewer (Local)	Running Processes		More Accors	•
🛨 🥁 Services (Local)				
· · · · · · · · · · · · · · · · · · ·	,			

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:

1y Computer Properties ? 🗙						
Default Protocols COM Security MSDTC General Options Default Properties						
 Enable Distributed COM on this computer Enable COM Internet Services on this computer Default Distributed COM Communication Properties The Authentication Level specifies security at the packet level. Default Authentication Level: Connect 						
The impersonation level specifies whether applications can determine who is calling them, and whether the application can do operations using the client's identity. Default Impersonation Level:						
Identify Security for reference tracking can be provided if authentication is used and that the default impersonation level is not anonymous. Provide additional security for reference tracking						
Learn more about <u>setting these properties</u> .						
OK Cancel Apply						

- 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:

My Computer Properties				? ×		
General Default Protocols	Options COM Sec	Def urity	ault Properties			
Access Permissions You may edit who is allowed default access to applications. You may also set limits on applications that determine their own permissions. Caution: Modifying access permissions can affect the ability of applications to start, connect, function and/or run securely.						
	Edit Limits	E	Edit Default			
Launch and Activation Permissions You may edit who is allowed by default to launch applications or activate objects. You may also set limits on applications that determine their own permissions. Caution: Modifying launch and activation permissions can affect the ability of applications to start, connect, function and/or run securely.						
	Edit Limits	E	Edit Default			
Learn more about <u>setting these properties</u> .						
	ОК	Cance	el Apply			

- 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:

User Account Control Settings	_	×
Choose when to be notified about changes to your computer User Account Control helps prevent potentially harmful programs from making changes to <u>Tell me more about User Account Control settings</u>	your computer.	
- - Never notify me when: • Apps try to install software or make changes to my computer - - - - - - - - - - - - - -		
i Not recommended.		
Never notify		
Фок	Cancel	

- 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:0000001

- 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:

Services							-	\times
File Action View Help								
🔶 🤿 🔟 🔟 📰	▶ Ⅲ Ⅱ Ⅰ ▶							
Services (Local)	Local)							
Workstation Stop the service Pause the servic Restart the servi Creates and ma connections to the SMB protoc stopped, these- unavailable. If the any services the it will fail to start	e ce iite remote servers using col. If this service is connections will be his service is disabled, this service is disabled, the seplicitly depend on rt.	Name Windows Pursption Service Windows Push Notifications System Service_1b4e Windows Push Notifications User Service_1b4e Windows Push Notifications User Service_1b4e Windows Push Notifications User Service_1b4e Windows Store Install Service Windows Store Install Service Windows Time Windows Config Wind AutoConfig Wind Performance Adapter Work Folders Work Folders Work Folders Work Config Work AutoConfig Work AutoConf	Description Enables spat This service Provides infr Windows Re Provides com Provides com Provides com Provides the WinHTTP im The WLANS Provides per This service This service This service This service This service This service This service	Status Running Running Running Running Running	Startup Type Manual (frigg., Automatic Automatic Manual (frigg., Manual Manual (frigg., Manual Manual Automatic Manual Automatic Manual	Log On As Local System Local System		^
Evtended Sta	ndard /	······				,		~

- 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:

Workstati	on Prope	rties (Local	l Computer)	×		
General	Log On	Recovery	Dependencies			
Service	name:	LanmanWo	orkstation			
Display	name:	Workstation	n			
Descript	Description:		Creates and maintains client network connections to remote servers using the SMB protocol. If this service			
Path to C:\WINI	executabl DOWS\Sy	e: stem32\svch	nost.exe -k NetworkService -p			
Startup type: Automatic ~						
_				1		
Service	status:	Running				
S	Start	Stop	Pause Resume			
You car from he	n specify tl re.	ne start para	meters that apply when you start the service			
Start pa	rameters:					
			OK Cancel Apply			

- 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.

🔚 WmiMgmt - [Console Root\WMI Control	(Local)]			- 🗆 ×
File Action View Favorites Windo	ow Help			_ 8 ×
🗢 🔿 🙍 🗊 🖺				
Console Root			Actions	
WMI Control (Local)	Windows Managament I	nstrumentation (WMI)	WMI Control (Local)	^
Connect to a	another computer	we Management Instrumentation (M/MI)	More Actions	•
View Minder	, vu from Horo	wisi Management instrumentation (WW)		
New Windo	witomhere			
New laskpa	d View			
Properties				
Help				
Opens the properties dialog box for the curren	it selection.			

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

WMI Con	trol (Local) Prope	erties			?	×
General	Backup/Restore	Security	Advanced			
Namesp	ace navigation allo	ws you to s	et namespa	ce specific s	ecurity.	
···· 🔃	Root					
				Se	ecurity	
		Ok	(Cancel	Ap	ply

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

Security for Root		×
Security Group or user names: Administrators (DESKTOP-SR3 no_admin (DESKTOP-SR36R5	6R55\Administra 55\no_admin)	ators)
Permissions for no_admin Execute Methods Full Write Partial Write Provider Write Enable Account Remote Enable For special permissions or advanced click Advanced.	Add Allow	Remove Deny
OK	Cancel	Apply

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

Ad	vanced S	ecurity Settings f	for Root					×
Owr	ner:	Administrators	(DESKTOP-SR36F	855\Administrators) C	hange			
Perr	nissions	Auditing						
For a Pern	additiona nission e	al information, de	ouble-click a perm	nission entry. To modify	y a permission entry, select	the entry and click Edit (if	available).	
	Туре	Principal		Access	Inherited from	Applies to		
97	Allow	Administrators	(DESKTOP-SR3	Special	None	This namespace and	l subname.	
8	Allow	no_admin (DES	KTOP-SR36R55	Enable Account	None	This namespace on	у	
	Add	Remove	Edit					
D	isable inl	heritance						

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

Permission	on Entry for Root	—		×
Principal:	no_admin (DESKTOP-SR36R55\no_admin) Select a principal			
Туре:	Allow			
Applies to:	: This namespace and subnamespaces			
Permission	ns: Execute Methods Full Write Remote Enable			
	Partial Write Read Security			
	Provider Write Edit Security			
Only app	oply these permissions to objects and/or containers within this container		Clear al	I.
		ОК	Can	cel

- 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:

My Computer Properties			?	\times
Default Protocols General	COM Sec Options	urity Default Pr	MSDTC roperties	
☑ Enable Distributed COM o	on this computer]		
Enable COM Internet Ser	vices on this comp	outer		
The Authentication Level	specifies security a	openies at the packet leve	I.	
Default Authentication L	evel:	~		
	necifies whether a	polications can de	etermine	
who is calling them, and v using the client's identity.	whether the applic	ation can do oper	ations	
Default Impersonation L	_evel:			
Identify		~		
Security for reference trac and that the default imper	king can be provid rsonation level is n	ed if authentication of anonymous.	on is used	
Provide additional sec	curity for reference	tracking		
Learn more about <u>setting th</u>	ese properties.			
	ОК	Cancel	Appl	у

- 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.

My Computer Properties	5		?	\times
General	Options	Defa	ult Properties	
Default Protocols	COM Secu	irity	MSDTC	;
Access Permissions				
You may edit who i	s allowed default acce	ss to applica	ations You	
may also set limits o permissions.	on applications that det	termine thei	rown	
Caution: M	lodifying access permis	ssions can a	ffect the abilit	ty
of applicati	ons to start, connect, f	unction and	/or run secure	ely.
	Edit Limits	Ed	lit Default	
Launch and Activation	Permissions			
You may edit who is activate objects. Yo	s allowed by default to	launch app	lications or	
determine their own	permissions.		is that	
A Caution: M	lodifying launch and a	ctivation per	missions can	
affect the a	ability of applications to	start, conn	ect, function	
and/or run	securely.			
	Edit Lippito	E	lit Default	
	Edit Limits		III Delault	
Learn more about setting	g these properties.			
	014	0		
	OK	Cancel	Ap	ply

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

aunch and Activation Permission		? >	×
Default Security			
Group or user names:			_
SYSTEM Administrators (SIL 02461)Adr	ninistrators)		Ŀ
	ninstators)		Ŀ
	Add	Remove	
Permissions for Administrators	Allow	Deny	
Permissions for Administrators	Allow	Deny	7
Permissions for Administrators Local Launch Remote Launch	Allow	Deny	
Permissions for Administrators Local Launch Remote Launch Local Activation	Allow	Deny	
Permissions for Administrators Local Launch Remote Launch Local Activation Remote Activation	Allow	Deny	
Permissions for Administrators Local Launch Remote Launch Local Activation Remote Activation	Allow	Deny	
Permissions for Administrators Local Launch Remote Launch Local Activation Remote Activation	Allow	Deny	
Permissions for Administrators Local Launch Remote Launch Local Activation Remote Activation	Allow	Deny	
Permissions for Administrators Local Launch Remote Launch Local Activation Remote Activation	Allow	Deny	

- 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.

My Computer Propertie	es	? ×
General	Options	Default Properties
Default Protocols	COM Security	MSDTC
Access Permissions		
You may edit who may also set limits permissions.	is allowed default access t on applications that determ	o applications. You nine their own
Caution: of applica	Modifying access permissio tions to start, connect, func	ns can affect the ability tion and/or run securely.
	Edit Limits	Edit Default
Launch and Activatio You may edit who activate objects. Y determine their ow Caution: affect the and/or run	n Permissions is allowed by default to lau ou may also set limits on a in permissions. Modifying launch and activa ability of applications to sta n securely.	anch applications or oplications that ation permissions can art, connect, function
	Edit Limits	Edit Default
Learn more about <u>setti</u>	ng these properties. OK	Cancel Apply

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

Launch and Activation Permission ? $>$							
Security Limits							
Group or user names:							
Everyone ALL APPLICATION PACKAGES S-1-15-3-1024-2405443489-874036122-4286035555-1823 Administrators (SILO2461\Administrators) Performance Log Users (SILO2461\Performance Log Users < > >							
[Add Remove						
Permissions for Administrators	Allow	Denv					
Permissions for Auministrators		Deny					
Local Launch							
Local Launch Remote Launch							
Local Launch Remote Launch Local Activation							
Local Launch Remote Launch Local Activation Remote Activation							

- 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:0000001

- 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 (三).
- 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	63
WMI Dynamic Applications	64
Relationships with Other Types of Component Devices	65

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 (三).
- 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	66
Creating a WMI Credential	71
Testing Windows Credentials	.74

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:

				Credential lester
d Organizations 🛑 What	organization manages this service?	v	Timeout (ma) 1500	Select Credential Test
NMPVersion	SNMP Retries	Port*		Select Collector CUG1 AsimovSandboxCU1: 10.2.25.101
NMP V2	~ 1	161		IP or Hostname to test "
NMP Community (Read-Only)		SNMP Community (Read/Write)		Test C

- 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
 - $^\circ~$ 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.

Credentials			🔧 Act	ivity Em7admin ~ 迎 _{Scien}	ncelogic
Q. Type to search credentials			≡ ¢	✓ Create New Test Crede	antials
¢		THEFT	1.447.8797	Create SNMP Credential	
			00700	Create Database Credential	
AppDynamics Example	SOAP/XML	2000	Jul 6, 2020, 11:35 AM	Create SOAP/XML Credential	
AppDynamics Example - Proxy	SOAP/XML	2000	Jul 6, 2020, 11:35 AM	Create LDAP Credential	
AWS Credential	SOAP/XML	2000	Ail 6, 2020, 11:33 AM		· ·
AWS Credential - Proxy	SOAP/XML	2000	Jul 6, 2020, 11:33 AM	Create Basic/Snippet Credential	
AWS Credential - Specific Region	SOAP/XML	2000	Jul 6, 2020, 11:33 AM	Create SSH/Key Credential	
Azure Classic Credential SOAP	SOAP/XML	60000	Jul 6, 2020, 11:32 AM	Create Powershell Credential	
Azure Credential - China	SQAP/XML	120000	Jul 6, 2020, 11:34 AM		
Azure Credential - Germany	SOAP/XML	120000	Jul 6, 2020, 11:34 AM	Create Aliyun Credential	
Azure Credential - Government	SOAP/XML	120000	Ail 6, 2020, 11:34 AM	Create Aws Credential	
Azure Credential - Proxy	SOAP/XML	120000	Jul 6, 2020, 11:34 AM	Create Azure Credential	
Azure Gredential - SOAP/30ML	SQAP/XML	120000	Jul 6. 2020. 11:34 AM	Create Citrixien Credential	
Cisco CE Series Configuration	SOAP/XML	15000	Jul 6. 2020. 11:34 AM	Create Ibm Credential	
Cisco CE Series History	SDAP/XML	15000	Jul 6, 2020, 11:34 AM		
Cisco CE Series Status	SOAP/XML	15000	Jul 6, 2020, 11:34 AM		
Cisco CUCM Example	Basic/Snippet	30000	Jul 6. 2020. 11:32 AM		
Cisco Meeting Server Example	Basic/Srippet	15000	Jul 6, 2020, 11:33 AM		
Cisco SNMPv2 - Example	SNMP	1500	Jul 6, 2020, 11:33 AM		
Cisco SNMPv3 - Example	SNMP	1500	Jul 6, 2020, 11:33 AM		
Cisco VOS CUC Cluster Status	Basic/Srippet	10000	Jul 6, 2020, 11:32 AM		
Cisco VOS IM&P Cluster Status	Basic/Snippet	10000	Jul 6, 2020, 11:32 AM		
Cisco VOS SOAP - Example	SOAP/XML	5000	Jul 6. 2020. 11:32 AM		
Cisco: ACI Sample Credential	Basic/Srippet	30000	Jul 6, 2020, 11:33 AM		

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

Create Credential		N		×
Name*		ю	Credential Tester	
All Organizations	×	Timeout (ms) 1500	Select Credential Test	
			Select Collector CUG1 jchristianson-sl1-cu-42: 10.2.17.42	
Hostname/IP*	Port*		IP or Hostname to test "	
Username	Password			Test Credential
				Save & Close

- 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



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 (三).
- 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	. 77
Discovering Cluster Nodes	. 78
Discovering the Cluster IP Address	. 80
Using a Device Template to Configure Dynamic Applications	. 82

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 (*P*) for the cluster node. The **Device Properties** page is displayed.
- 3. Select the [Collections] tab. The Dynamic Application Collections page is displayed.
- 4. Select the [Action] button.
- 5. Select Add Dynamic Application. The Dynamic Application Alignment page appears.
- 6. In the **Dynamic Application Alignment** page, select the Dynamic Application you want to align in the **Dynamic Applications** field.
- 7. In the Credentials field, select the credential for the Dynamic Application.
- 8. Select the [Save] button.

Disabling Collection of a Dynamic Application on a Device

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

- 1. Go to the **Device Manager** page (Registry > Devices > Device Manager).
- 2. Select the wrench icon (🎤) for the device record for the cluster. The **Device Properties** page is displayed.
- 3. Select the [Collections] tab. The Dynamic Application Collections page is displayed:

Close	Properties	T <u>h</u> resholds	<u>C</u> ollections	<u>M</u> onitors				
<u>S</u> chedule	Logs	T <u>o</u> olbox	<u>I</u> nterfaces	Relationships	<u>T</u> ickets	Redirects	Notes	
Device Name	MSSQL-CLUSTER-1.Q	A.LOCAL		Managed Ty	/pe Physical Device			
IP Address / ID	10.168.44.206 38			Categ	ory Servers			
Class	Microsoft			Sub-Cla	windows 2008 S	erver R2		<u> </u>
Organization	DC - Servers			Upti	me 2 days, 17:24:26		Windo	ows2008
Collection Mode	Active			Collection Ti	me 2012-03-19 18:45	5:00	🔺 😂 ,	all 🖶 🥜 👘
Description	Hardware: Intel64 Fam	ilv 6 Model 46 Steppin	6 AT/AT COMPATIBLE	Group / Coller	tor CUG Lem7 an		MSSOL-CI	USTER-1.QA.LO
		ing of model to otopping	,		an occitorTao		Į	
	TH					Evened	Anting Depart	Cuida
Dynamic Applica	tion ^{1M} Collections					Expand	Action Reset	Guide
I Information Management	<u> </u>	Ovnamic Application		<u>D</u>	Poll Frequency	Type	Credential	
+ Informant: Mem	огу			312	5 mins	SNMP Performance	Default SNMP Credential	
+ Informant: Volu	mes			314	5 mins	SNMP Performance	Default SNMP Credential	
+ MSSQL: Gener	al			84	10 mins	SNMP Performance	Default SNMP Credential	
+ MSSQL: Memor	У			83	10 mins	SNMP Performance	Default SNMP Credential	
+ MSSQL: SQL S	tats			82	10 mins	SNMP Performance	Default SNMP Credential	/
+ Host Resource	CPU Config			12	1440 mins	SNMP Configuration	Default SNMP Credential	/ 🗖
+ Host Resource	Software			9	120 mins	SNMP Configuration	Default SNMP Credential	1
+ Host Resource	CPU			10	5 mins	Snippet Performance	Default SNMP Credential	1
+ Host Resource	Memory			8	5 mins	Snippet Performance	Default SNMP Credential	1 1
+ Host Resource	Memory Config			11	1440 mins	Snippet Configuration	Default SNMP Credential	1
						[Select Act	ion]	→ Go
				Sav	e			

- 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 (\square) 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:

	1 Step 1 Basic Information	Step 2 Credential Selection	3 Step 3 Discovery Session Details	×
	Name*			
	Description (Optional)			
	Select the organization to add discovered devices to *		·	
← Back				Next >

- **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 (\checkmark) 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 (*I*) 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 (*P*) 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:

Device Template Editor Editing Dynam	ic Application Subtemplates (Click field labels	to enable/disable them)	Nev	v Reset
Ten	nplate Name			
Config Interface CV Policie	s Port Policies Svc Policies Proc Policie	s Dyn Apps		
Subtemplate Selection	Template Application Behavior All devices (align new applications and update of	Align Dynamic Application With collection states)		Ŧ
	Dynamic Application Settings	Dynamic Application		
	Alteon: Load Trending	-A		-
	Crea	dentials	Poll Rate	3
	Default SNMP credential		 Every 15 Minutes 	-
	ARP Entries Concurrent Connections Per Port Connection Rate Per Virtual Server Port Bindings Real Server Current Sessions	Enabled - Enabled - Enabled - Enabled -		
	Dynamic Application Thresholds No thresholds available for selected application.	m		•

- 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:

Device Template Editor Applying Template to Devices Config Template Settings (Click field labels to enable/disable them)								
Template New / One-off Template	Save Wh	en Applied & Confirm	med Template Name					
Config Interface CV Policies Port Policies Svc Policies Proc Policies Dyn Apps								
Access & Monitoring				Device Preferences				
Device Organization Acme Corpo	ration	-		Auto-Clear Events	Scan All IPs			
SNMP Read c0sm0s		SNMP Write	None 🚽					
Availability Protocol TCP		 Avail Port 	ICMP 💂	Accept All Logs	Dynamic Discovery			
Latency Protocol TCP		Latency Port	ICMP -					
Avail+Latency Alert Disabled		w.		Daily Port Scans	Preserve Hostname			
Collection Enabled		- Collector Grp	CUG					
Coll. Type Standard		Ŧ		Auto-Update	Disable Asset Update			
Critical Ping Disabled		-						
Event Mask Disabled		v						
Device Retention & Basic Threshole	ls			1				
System Latency	1	500 ms	Bandwidth Data	1 1	30 days			
			Normalized BW Data	1	30 days			
Device Logs Max 📊	1 1	5000 records	Performance Data		30 days ⋿			
Log Age Max	1 1	30 days	Normalized Perf Data	1	30 days			
Number of Availability	1 1	1 pings	Ping Packet Size	1	100 %			
riliys								

- 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 (三).
- 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?	. 85
Configuring the Windows Restart Automatic Services PowerPack	. 86
Excluding Automatic Services	. 87

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**:

Close	<u>S</u> ummary	Performance	<u>C</u> onfigs	Journals	Interfaces	<u>L</u> ogs			
<u>E</u> vents	Tickets	Software	Processes	Se rvice s	TCP Ports	Organization			
1									
Device Name	TL008-HQ-AP-01.MS	TL008.local		Managed Type	Physical Device				
IP Address / ID	10.0.6.38 1085			Category	Servers				- 111
Class	Microsoft			Sub-Class	Windows Server	r 2008 R2			- 111
Organization	System			Untime	0 days 00:08:44			Windows 2008	8
Collection Mode	Active			Collection Time	2014-03-07 17:3	0.00		🔺 💭 📶 📾 🍐	9
Description	Hardwara: Intal®4 Eau	mily & Madal 44 Stanning		Collection rime	2014-03-01 17.5	0.00 m. 220		TL008-HO-AP	
Desorption Hardware: Intel64 Family 6 Model 44 Stepping 2 ATIAL COMPATIBLE - So Group / Collector CUG_236 [em/_Cu_238									
Luis		Configuration Dana	et Mindous Find As	stematic Consider No	t Dunning		0-41	Decet Outle	
Host Resource:	CPU Config	Configuration Repo	IL WINDOWS FIND AL	Itomatic Services No	t Running		Actions	Reset Guide	•
Host Resource	Memory Config	Snap-Shot Date [2	014-03-07 16:50:00	0]				Snap-Sh	iots
Host Resource	Software								
-Windows Find	Automatic Services No	Automatic Servi	ces						In!
				DisplayName		100 1	Name	State	
		1. Windows Ma	nagement instrumentat	ion		vvinmgmt		Running	
		2. hyper-v Gue	st Shutdown Service			ChalleW/Detection		Running	
		3. Sheii Hardwa	re Detection			ShellHvvDetection		Running	
		4. IP neiper	ant University			ipnipsvc AcellectCus		Running	
		5. Application H	ost Helper Service			AppHostSVC		Running	
		6. WINDOWS FIR	ewai			MpsSVC		Running	
		7. DHCP Client	7. DHCP Client			Uncp		Running	
		8. Windows For	9 Netlogon			FontCache		Running	E
		9. Netiogon	- Interferen Grenden			Netiogon		Running	
		10. Network Store Interface Service 11. Demote Procedure Call (DDC)				nsi DeeCe		Running	
		11. Remote Procedure Call (RPC)				RpcSs		Running	
		12. User Profile Service				ProtSVC		Running	
		13. Power				Power		Running	
		14. COM+ Event System Eve				EventSystem		Running	
		15. World Wide Web Publishing Service W3SVC						Running	
		16. Microsoft .NE	I Framework NGEN v4	.0.30319_X64		cir_optimization_v4.0.	30319_64	Stopped	
		17. Net.Pipe Liste	ner Adapter			NetPipeActivator		Running	
		18. Windows Eve	ent Log			eventiog		Running	
		19. None				None		None	
		20. Microsoft .NE	I Framework NGEN v4	.0.30319_X86		cir_optimization_v4.0.	30319_32	Stopped	
		21. DCOM Serve	Process Launcher			DcomLaunch		Running	
		22. Software Pro	tection			sppsvc		Running	
		23. Base Filtering	Engine			BFE		Running	
		24. Hyper-V Data	Exchange Service			vmickvpexchange		Running	
		25. Workstation				LanmanWorkstation		Running	
		26. Hyper-V Time	Synchronization Serv	ice		vmictimesync		Running	
		27. Net.Tcp Liste	ner Adapter			NetTcpActivator		Running	
		28. Distributed Li	nk Tracking Client			TrkWks		Running	
		29. Server				LanmanServer		Running	
	Find	30. Print Spooler				Spooler		Running	

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].

© 2003 - 2025, ScienceLogic, Inc.

All rights reserved.

LIMITATION OF LIABILITY AND GENERAL DISCLAIMER

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

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

Copyrights and Trademarks

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

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

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

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

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

Other

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

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



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

International: +1-703-354-1010