ScienceLogic

Monitoring New Relic

New Relic: APM PowerPack version 105

Table of Contents

Chapter

1

Introduction

Overview

This manual describes how to monitor New Relic web services in SL1 using the *New Relic: APM* PowerPack.

The following sections provide an overview of New Relic and the *New Relic: APM* PowerPack:

This chapter covers the following topics:

NOTE: ScienceLogic provides this documentation for the convenience of ScienceLogic customers. Some of the configuration information contained herein pertains to third-party vendor software that 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.

What is New Relic?

New Relic is an Application Performance Tool (APM) that captures data and information about web-based applications. Users can measure the performance of their applications, which helps determine potential service delivery issues.

What Does the New Relic: APM PowerPack Monitor?

To monitor New Relic web services using SL1, you must install the *New Relic: APM* PowerPack. This PowerPack enables you to discover, model, and collect data about New Relic web services.

The *New Relic: APM* PowerPack includes:

- A sample credential you can use as a template to create SOAP/XML credentials to connect to the New Relic services you want to monitor
- Dynamic Applications to discover, model, and monitor performance metrics, and to collect configuration data for New Relic services
- Device Classes for each of the New Relic services SL1 monitors
- Event Policies and corresponding alerts that are triggered when New Relic services meet certain status criteria
- Device dashboards that display information about New Relic services
- A "universal" type credential for discovering New Relic Services

NOTE: The PowerPack does not model applications with "reporting: false" statuses.

Installing the New Relic: APM PowerPack

Before completing the steps in this manual, you must import and install the latest version of the *New Relic: APM* PowerPack.

NOTE: Ensure that you do not have the *New Relic: APM Pro* PowerPack installed before installing the *New Relic: APM* PowerPack. These PowerPacks are not compatible. If you have the *New Relic: APM Pro* PowerPack installed, it will need to be uninstalled prior to installing the *New Relic: APM* PowerPack. The historical data from the *New Relic: APM Pro* PowerPack will be deleted when it is uninstalled.

TIP: By default, installing a new version of a PowerPack overwrites all content from a previous version of that PowerPack that has already been installed on the target system. You can use the ***Enable Selective PowerPack Field Protection*** setting in the **Behavior Settings** page (System > Settings > Behavior) to prevent new PowerPacks from overwriting local changes for some commonly customized fields. For more information, see the section on ***Global Settings***.

NOTE: For details on upgrading SL1, see the relevant ***SL1 Platform Release Notes***.

To download and install the PowerPack:

1. Search for and download the PowerPack from the **PowerPacks** page (Product Downloads > PowerPacks & SyncPacks) at the ScienceLogic Support Site.
2. In SL1, go to the **PowerPacks** page (System > Manage > PowerPacks).
3. Click the **[Actions]** button and choose *Import PowerPack*. The **Import PowerPack** dialog box appears.
4. Click **[Browse]** and navigate to the PowerPack file from step 1.
5. Select the PowerPack file and click **[Import]**. The **PowerPack Installer** modal displays a list of the PowerPack contents.
6. Click **[Install]**. The PowerPack is added to the **PowerPacks** page.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPackwill not appear in the **PowerPacks** page. However, the imported PowerPack will appear in the **Imported PowerPacks** modal. This page appears when you click the **[Actions]** menu and select *Install PowerPack*.

Chapter 2

Configuration and Discovery

Overview

The following sections describe how to configure and discover New Relic services for monitoring by SL1 using the *New Relic: APM* PowerPack:

This chapter covers the following topics:

Prerequisites for Monitoring New Relic Services

To configure the SL1 systemto monitor New Relic services using the *New Relic: APM* PowerPack, you must first have the following information about the New Relic services that you want to monitor *for each account and sub-account*:

- A New Relic REST API key. To generate the REST API key, go to the Account Settings page for your New Relic account.
- The username and password for your New Relic service.
- Insights Query Key. This is optional. Add this to the credential if you want to discover infrastructure groups used for server monitoring. You can generate this from your Insights account.

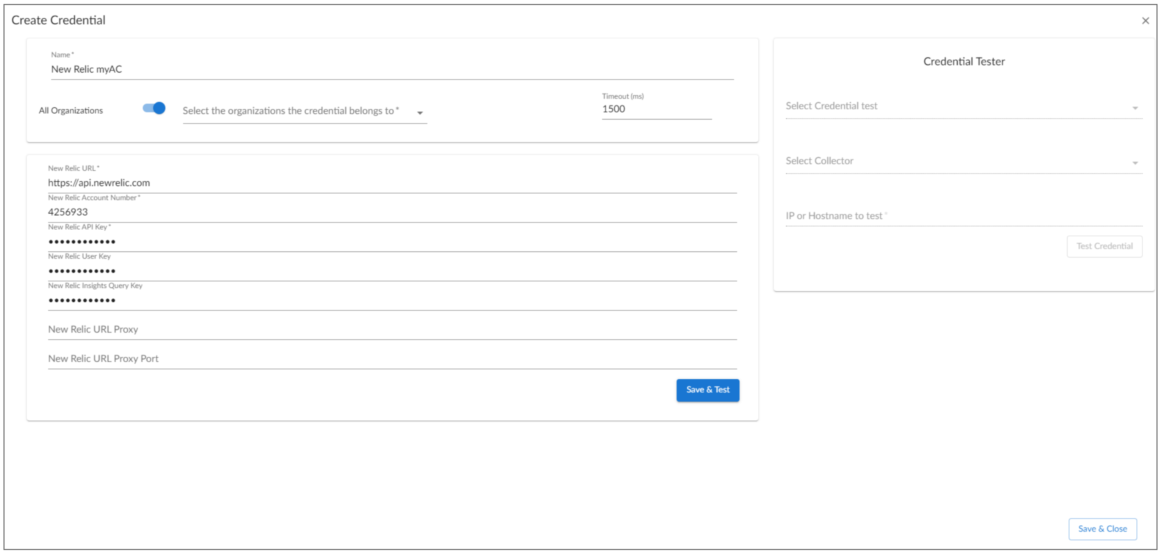
> **NOTE:** Ensure that you do not have the *New Relic: APM Pro* PowerPack installed before installing the *New Relic: APM* PowerPack. These PowerPacks are not compatible. If you have the *New Relic: APM Pro* PowerPack installed, it will need to be uninstalled prior to installing the *New Relic: APM* PowerPack. The historical data from the *New Relic: APM Pro* PowerPack will be deleted when it is uninstalled.

Creating a Universal Type Credential for New Relic

To configure SL1 to monitor New Relic services, you must create a either a universal type credential or a SOAP/XML credential. These credentials allow the Dynamic Applications in the "New Relic: APM"PowerPack to communicate with your New Relic service.

To define a "universal" type credential to access New Relic:

1. Go to the **Credentials** page (Manage > Credentials).
2. Click **[Create New]** and select "Create Newrelic Credential". The **Create Credential** modal page appears.



Create Credential

Name *
New Relic myAC

All Organizations

Timeout (ms)
1500

New Relic URL *
https://api.newrelic.com

New Relic Account Number *
4256933

New Relic API Key *
••••••••••••

New Relic User Key
••••••••••••

New Relic Insights Query Key
••••••••••••

3. Supply values in the following fields:
   - ***Name***. Type a name for your credential.
   - ***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 from the ***What organization manages this service?*** drop-down field to align the credential with those specific organizations.
   - ***Timeout (ms)***. Keep the default value of 1500.
   - ***New Relic URL***. Keep the default URL (https://api.newrelic.com).
   - ***New Relic Account Number***. Type the ID number for your New Relic account.
   - ***New Relic API Key***.Type your New Relic API key.

- ***New Relic User Key***. Type your New Relic User Key. New Relic user keys begin with "NRAK-" followed by an alpha-numeric value.

  > **NOTE:** Version 105 and later requires that you use the New Relic User Key.

- ***New Relic Insights Query Key***. Type the Insights Query Key if you want to discover infrastructure groups for server monitoring. If you do not have an Insights account, leave this field blank.

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

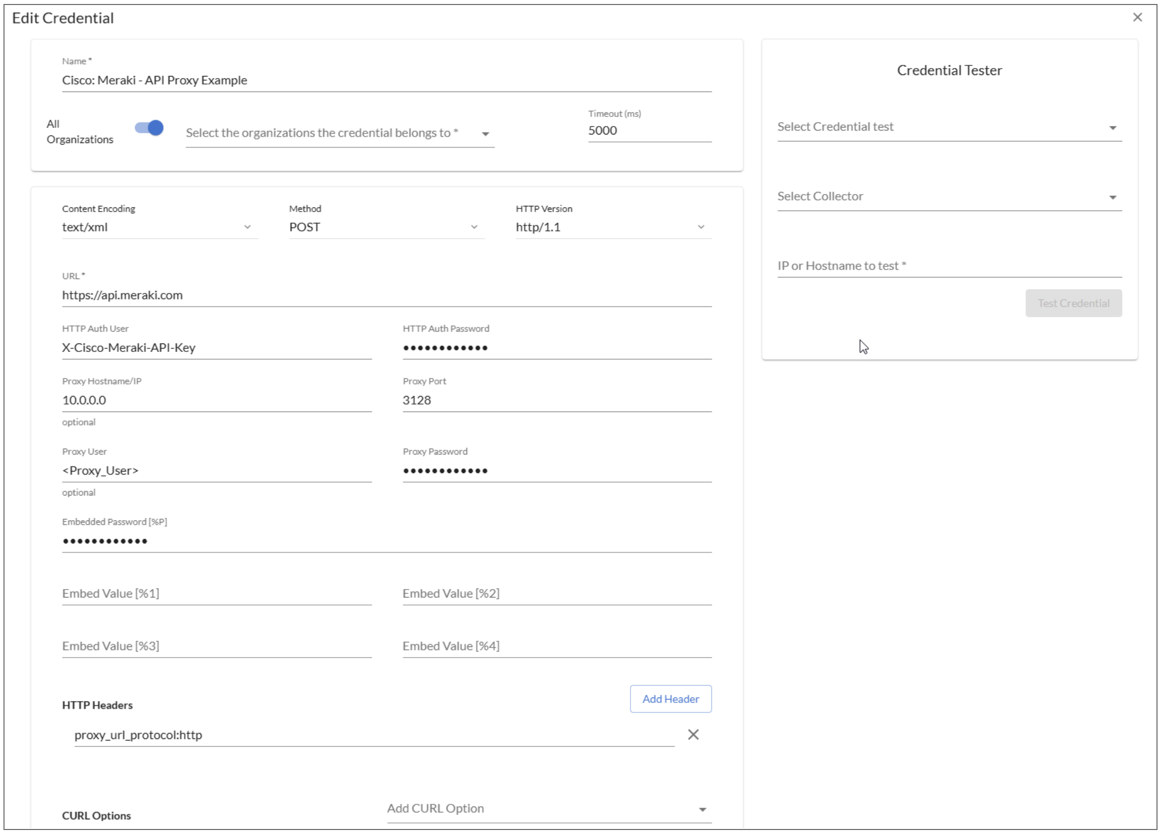
Creating a SOAP/XML Credential for New Relic

To configure SL1 to monitor New Relic services, you can create a SOAP/XML credential. This credential allows the Dynamic Applications in the "New Relic: APM" PowerPack to communicate with your New Relic service.

> **NOTE**: If you are using an SL1 system prior to version 11.1.0, the new user interface does not include the ***Duplicate*** option for sample credential(s). ScienceLogic recommends that you use ***the classic user interface and the Save As button*** to create new credentials from sample credentials. This will prevent you from overwriting the sample credential(s).

To define a SOAP/XML credential:

1. Go to the **Credentials** page (Manage > Credentials).
2. Locate the "New Relic | Proxy Example" credential, then click its **[Actions]** icon (⋮) and select ***Duplicate***. A copy of the credential, called "New Relic | Proxy Example - copy" appears.
3. Click the **[Actions]** icon (···) for the credential copy and select ***Edit***. The **Edit Credential** modal page appears.



Edit Credential ×

Name *
Cisco: Meraki - API Proxy Example

All Organizations
Select the organizations the credential belongs to *

Timeout (ms)
5000

Content Encoding
text/xml

Method
POST

HTTP Version
http/1.1

URL *
https://api.meraki.com

HTTP Auth User
X-Cisco-Meraki-API-Key

HTTP Auth Password
••••••••••••

Proxy Hostname/IP
10.0.0.0
optional

Proxy Port
3128

Proxy User
<Proxy_User>
optional

Proxy Password
••••••••••••

Embedded Password [%P]
••••••••••••

Embed Value [%1]

Embed Value [%2]

Embed Value [%3]

Embed Value [%4]

HTTP Headers
Add Header
proxy_url_protocol:http ×

CURL Options
Add CURL Option

Credential Tester

Select Credential test

Select Collector

IP or Hostname to test *

Test Credential

4. Supply values in the following fields:
   - ***Name***. Type a new name for your Meraki credential.
   - ***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)***. Keep the default value.
   - ***Content Encoding***.Keep the default value.
   - ***Method***. Keep the default value.
   - ***HTTP Version***. Keep the default value.
   - ***URL***. Leave this field as the default ("https://api.newrelic.com").
   - ***HTTP Auth User***. Type your New Relic API key in this field.
   - ***HTTP Auth Password***. Leave this field blank.

- ***Embedded Password [%P]***. Type the Insights Query Key in this field if you want to discover infrastructure groups for server monitoring. If you do not have an Insights account, leave this field blank.
- ***Embed Value [%1]***. Type the ID number for your New Relic account.
- ***Embed Value [%3]***. Type your New Relic User Key. New Relic user keys begin with "NRAK-" followed by an alpha-numeric value.

NOTE: Version 105 and later requires that you use the New Relic User Key.

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

Creating a SOAP/XML Credential for New Relic in the SL1 Classic User Interface

To configure SL1 to monitor New Relic services, you must create a SOAP/XML credential. This credential allows the Dynamic Applications in the *New Relic: APM* PowerPack to communicate with your New Relic service.

To configure a SOAP/XML credential to access New Relic:

1. Go to the **Credential Management** page (System > Manage > Credentials).
2. Locate the "New Relic | Proxy Example" credential, and then click its wrench icon (🔧). The **Edit SOAP/XML Credential** modal page appears.
3. Enter values in the following fields.

Basic Settings

- ***Profile Name***. Type a new name for the credential.
- ***URL***. Leave this field as the default ("https://api.newrelic.com").
- ***HTTP Auth User***. Type your New Relic API key in this field.
- ***HTTP Auth Password***. Leave this field blank.

SOAP Options

- ***Embedded Password [%P]***. Type the Insights Query Key in this field if you want to discover infrastructure groups for server monitoring. If you do not have an Insights account, leave this field blank.
- ***Embed Value [%1]***. Type the ID number for your New Relic account.
- ***Embed Value [%3]***. Type your New Relic User Key. New Relic user keys begin with "NRAK-" followed by an alpha-numeric value.

NOTE: Version 105 and later requires that you use the New Relic User Key.

NOTE: There are several system-defined tags that are automatically applied by New Relic. To avoid duplicate data, SL1 does not collect these tags and will collect only user-defined tags.

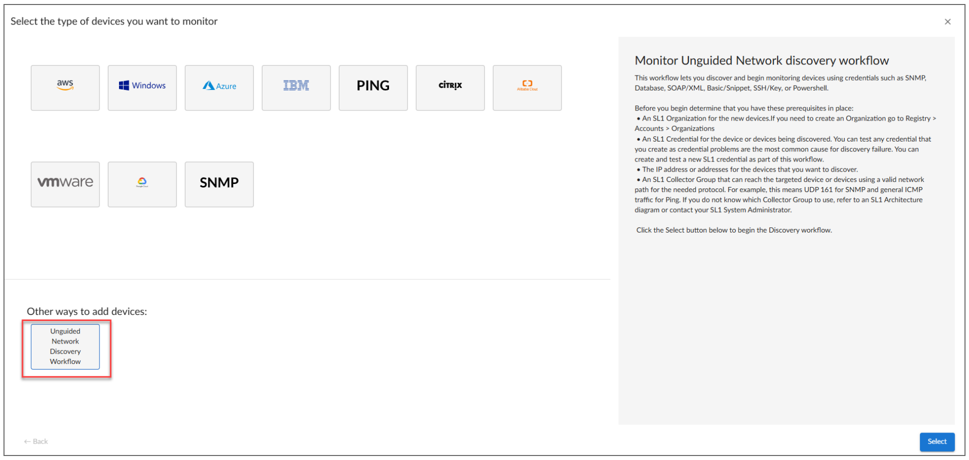
4. For all other fields, use the default values.
5. Click the **[Save As]** button.

Discovering New Relic Component Devices

To monitor your New Relic system, you must run a discovery session to discover the server on which New Relic is installed.

To create and run a discovery session that will discover a New Relic appliance:

1. Go to the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions) and click the **[Add Devices]** button.
2. Click the **[Unguided Network Discovery Workflow]** button. Additional information about that requirements for discovery appears in the **General Information** pane to the right.


Select the type of devices you want to monitor
×
aws
Windows
Azure
IBM
PING
citrix
Alibaba Cloud
vmware
Google Cloud
SNMP
Other ways to add devices:
Unguided Network Discovery Workflow
← Back
Select

Monitor Unguided Network discovery workflow

This workflow lets you discover and begin monitoring devices using credentials such as SNMP, Database, SOAP/XML, Basic/Snippet, SSH/Key, or Powershell.

Before you begin determine that you have these prerequisites in place:

- An SL1 Organization for the new devices.If you need to create an Organization go to Registry > Accounts > Organizations
- An SL1 Credential for the device or devices being discovered. You can test any credential that you create as credential problems are the most common cause for discovery failure. You can create and test a new SL1 credential as part of this workflow.
- The IP address or addresses for the devices that you want to discover.
- An SL1 Collector Group that can reach the targeted device or devices using a valid network path for the needed protocol. For example, this means UDP 161 for SNMP and general ICMP traffic for Ping. If you do not know which Collector Group to use, refer to an SL1 Architecture diagram or contact your SL1 System Administrator.

Click the Select button below to begin the Discovery workflow.

3. Click **[Select]**. The three-step wizard appears starting with the **[Step 1 Basic Information]** tab.
4. Complete the following fields:
   - ***Discovery Session 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***.Optional. 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.
   - ***Select the organization to add discovered devices to***. Select the name of the organization to which you want to add the discovered devices.

5. Click **[Next]**. The **[Step 2 Credential Selection]** tab of the wizard appears.
6. On the **[Credential Selection]** tab, locate and select the SOAP/XML credential you created for New Relic appliances.
7. Click **[Next]**. The **[Step 3 Discovery Session Details]** tab of the wizard appears.
8. Complete the following fields:
   - ***List of IP/Hostnames***. Type the IP address for the New Relic appliance.
   - ***Which collector will discover these devices?***. Required. Select an existing collector to monitor the discovered devices.
   - ***Run after save***. Toggle on (blue) to run this discovery session as soon as you save the session.
   - ***Advanced options***. Click the down arrow (⌄) to complete the following fields:
     - ***Discover Non-SNMP***. Toggle on (blue) to enable this setting.
     - ***Model Devices***. Toggle on (blue) to enable this setting.
     - ***Select Device Template***. If you configured a New Relic device template, select it here. Otherwise, leave the default selection.
9. If you enabled the ***Run after save*** option, click the**[Save and Run]** button. The discovery session will run and the **Discovery Logs** page will display any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page will include a link to the **Device Investigator** page for the discovered device.
10. If you did not enable the ***Run after save*** option, click the **[Save and Close]** button. The **Discovery Sessions** page (Devices > Discovery Sessions) will display the new discovery session.

Discovering New Relic Component Devices in the SL1 Classic User Interface

To discover and monitor your New Relic account in the , you must do the following in the classic user interface:

- Configure the Device Template that is included in the New Relic: APM PowerPack
- Create a virtual device representing the environment and modify, by template, the New Relic virtual device.

NOTE: If you want to discover additional New Relic accounts, you must create a credential for each account you want to discover. Next you must edit the New Relic device template and then create a virtual device to which you will align the template.

NOTE: The PowerPack does not model applications with "reporting: false" statuses.

Configuring the Device Template

A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *New Relic: APM*PowerPack includes the "New Relic Virtual Device Template Example". You must configure a device template for each additional New Relic account you want to discover.

If you configure this device template correctly, once you align the template to the New Relic virtual device, SL1 will use the device template to automatically align the New Relic discovery Dynamic Applications and start collecting data.

To configure the New Relic device template:

1. Go to the **Configuration Templates** page (Devices > Templates, or Devices > Templates, or Registry > Devices > Templates in the classic SL1 user interface in the SL1 classic user interface).
2. Locate the "New Relic Virtual Device Template Example" and click its wrench icon (🔧). The **Device Template Editor** page appears.
3. Click the **[Dyn Apps]** tab. The **Editing Dynamic Application Subtemplates** page appears.
4. Complete the following fields:
   - **Template Name**. Type a new name for the device template.
   - **Credentials**. Select the "universal" type or SOAP/XML credential that you created for the New Relic account.
5. Click the next Dynamic Application listed in the **Subtemplate Selection** section on the left side of the page and then select the New Relic "universal" type or SOAP/XML credential in the ***Credentials*** field.
6. Repeat step 5 until the you have selected the New Relic "universal" type or SOAP/XML credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.
7. Click **[Save As]**.

NOTE: You must rename the sample **New Relic Virtual Device Template Example** and click **[Save As]** to save it. If you do not rename the device template, then your device template will be overwritten the next time you upgrade the *New Relic: APM*PowerPack.

Creating a Virtual Device and Aligning the Device Template

To discover New Relic account, you must create a ***virtual device*** that represents the New Relic account. A virtual device is a user-defined container that represents a device or service that cannot be discovered by SL1. You can use the virtual device to store information gathered by policies or Dynamic Applications.

To create a virtual device that represents your New Relic account:

1. Go to the **Device Manager** page (Devices > Classic Devices, or Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface in the SL1 classic user interface).
2. Click the **[Actions]** button and select *Create Virtual Device* from the menu. The **Virtual Device** modal page appears.
3. Complete the following fields:
   - ***Device Name***. Type a name for the virtual device.
   - ***Organization***. Select the organization for this device. The organization you associate with the device limits the users that will be able to view and edit the device. Typically, only members of the organization will be able to view and edit the device.

   - ***Device Class***. Select *New Relic, Inc. | Service Device*.
   - ***Collector***. Select the collector group that will monitor the device.

4. Click **[Add]** to create the virtual device.
5. In the **Device Manager** page (Devices > Classic Devices, or Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface in the SL1 classic user interface), select the checkbox (☑) for the virtual device that you just created.
6. Click the ***Select Actions*** drop-down and select *MODIFY By Template* from the menu and click **[Go]**.
7. In the **Device Template Editor**, use the ***Template*** drop-down to select the device template that you created for the New Relic account and click the **[Apply]** button.
8. Click the **[Confirm]** button to save your changes.

To verify that the template has aligned the correct Dynamic Applications:

1. Go to the **Devices** page and select the device for the New Relic service. The **Device Investigator** page appears.
2. On the **Device Investigator** page, click the **Collections** tab. The **Dynamic Applications Collections** page appears.
3. You should see the following Dynamic Applications aligned to the New Relic service:
   - New Relic: APM Discovery & Collection Cache
   - New Relic: APM Events
   - New Relic: APM Infrastructure Group Discovery

To verify the template has aligned the correct Dynamic Applications in the SL1 Classic User Interface:

1. Go to the **Device Manager** page (Registry>Devices>Device Manager) and click the wrench icon (🔧) for the New Relic service.
2. On the **Device Properties** page, click the **Collections** tab. The **Dynamic Applications Collections** page appears.
3. You should see the following Dynamic Applications aligned to the New Relic service:
   - New Relic: APM Discovery & Collection Cache
   - New Relic: APM Events
   - New Relic: APM Infrastructure Group Discovery

Relationships with Other Types of Component Devices

Additionally, the Dynamic Applications in the *New Relic: APM*PowerPack can automatically build relationships between New Relic devices and other associated devices:

- If you discover Linux devices using the Dynamic Applications in the *Linux Base Pack* PowerPack version 102 or later, SL1 will automatically create relationships between New Relic devices and Linux servers.
- If you discover Windows servers using the Dynamic Applications in the *Microsoft Base Pack* PowerPack version 107 or later, SL1 will automatically create relationships between New Relic devices and Windows servers.

- If you discover Windows servers using the Dynamic Applications in the *Microsoft: Windows Server* PowerPack version 108 or later, SL1 will automatically create relationships between New Relic devices and Windows servers.

Viewing New Relic Component Devices

In addition to the **Devices** page, you can view the New Relic service and all associated component devices in the following places in the user interface:

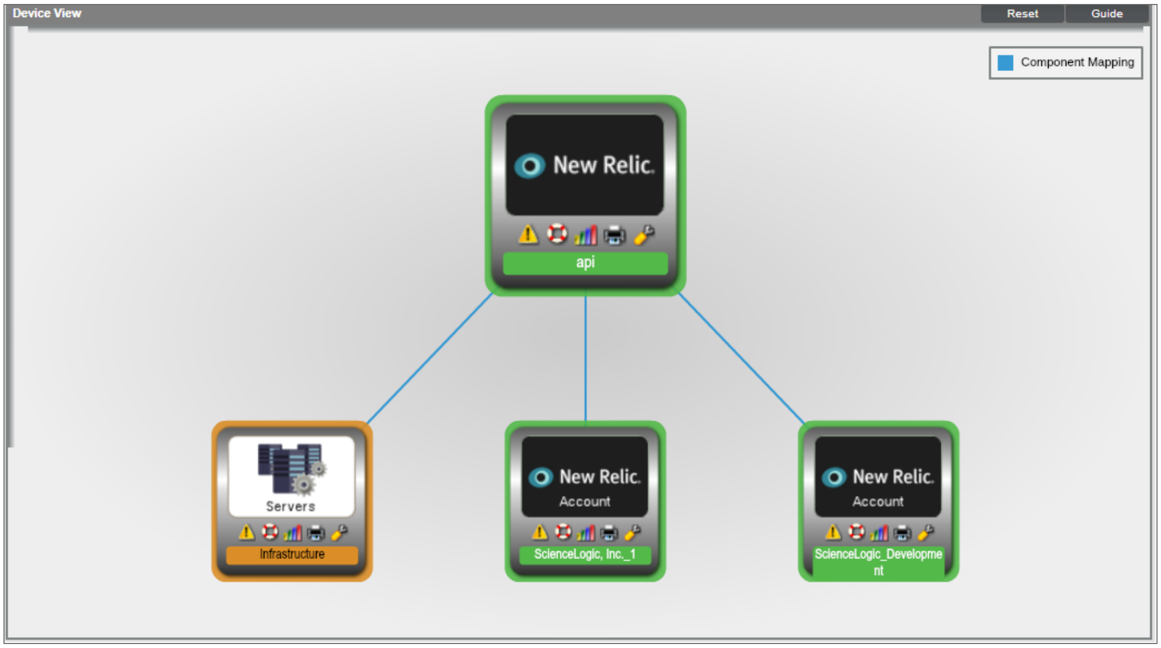
- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a New Relic service, find the New Relic device and click its plus icon (+).
- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. SL1 also updates each map with the latest status and event information. To view the map for a New Relic service, go to Classic Maps > Device Maps > Components, and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.

Viewing New Relic Component Devices in the SL1 Classic User Interface

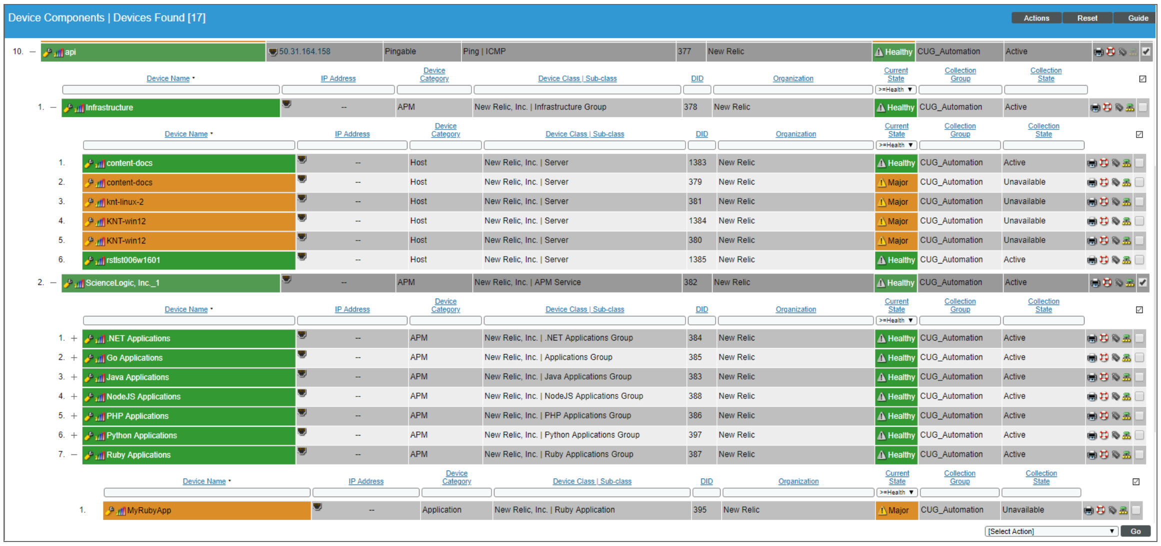
In addition to the **Device Manager** page (Devices > Classic Devices, or Registry > Devices > Device Manager in the classic SL1 user interface), you can view the New Relic service and all associated component devices in the following places in the user interface:

- The **Device View** modal page (click the bar-graph icon [📊] for a device, then click the **Topology** tab) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-click to select any listed device. This reloads the page to make the selected device the primary device.

NOTE: When you discover multiple New Relic accounts and sub-accounts, the top level device is shown as "api", which you can change as desired. The figure below shows that we have two different accounts discovered, as well as New Relic servers.



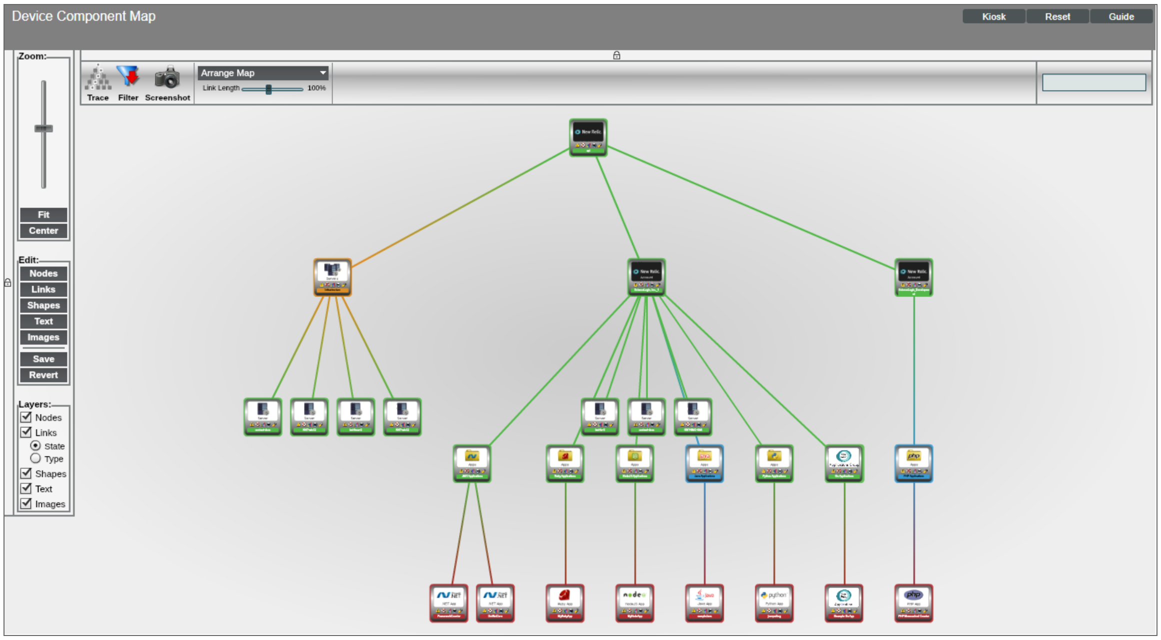
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by SL1 in an indented view, so you can easily view the hierarchy and relationships between child devices, parent devices, and root devices. To view the component devices associated with a New Relic service, find the service and click its plus icon (+):



Device Components | Devices Found [17]

	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State	Collection Group	Collection State
10. —	api	50.31.164.158	Pingable	Ping | ICMP	377	New Relic	Healthy	CUG_Automation	Active
1. —	Infrastructure	--	APM	New Relic, Inc. | Infrastructure Group	378	New Relic	Healthy	CUG_Automation	Active
1.	content-docs	--	Host	New Relic, Inc. | Server	1383	New Relic	Healthy	CUG_Automation	Active
2.	content-docs	--	Host	New Relic, Inc. | Server	379	New Relic	Major	CUG_Automation	Unavailable
3.	knt-linux-2	--	Host	New Relic, Inc. | Server	381	New Relic	Major	CUG_Automation	Unavailable
4.	KNT-win12	--	Host	New Relic, Inc. | Server	1384	New Relic	Major	CUG_Automation	Unavailable
5.	KNT-win12	--	Host	New Relic, Inc. | Server	380	New Relic	Major	CUG_Automation	Unavailable
6.	rstlst006w1601	--	Host	New Relic, Inc. | Server	1385	New Relic	Healthy	CUG_Automation	Active
2. —	ScienceLogic, Inc._1	--	APM	New Relic, Inc. | APM Service	382	New Relic	Healthy	CUG_Automation	Active
1. +	.NET Applications	--	APM	New Relic, Inc. | .NET Applications Group	384	New Relic	Healthy	CUG_Automation	Active
2. +	Go Applications	--	APM	New Relic, Inc. | Applications Group	385	New Relic	Healthy	CUG_Automation	Active
3. +	Java Applications	--	APM	New Relic, Inc. | Java Applications Group	383	New Relic	Healthy	CUG_Automation	Active
4. +	NodeJS Applications	--	APM	New Relic, Inc. | NodeJS Applications Group	388	New Relic	Healthy	CUG_Automation	Active
5. +	PHP Applications	--	APM	New Relic, Inc. | PHP Applications Group	386	New Relic	Healthy	CUG_Automation	Active
6. +	Python Applications	--	APM	New Relic, Inc. | Python Applications Group	397	New Relic	Healthy	CUG_Automation	Active
7. —	Ruby Applications	--	APM	New Relic, Inc. | Ruby Applications Group	387	New Relic	Healthy	CUG_Automation	Active
1.	MyRubyApp	--	Application	New Relic, Inc. | Ruby Application	395	New Relic	Major	CUG_Automation	Unavailable

- The **Component Map** page (Classic Maps > Device Maps > Components) allows you to view devices by root node and view the relationships between root nodes, parent components, and child components in a map. This makes it easy to visualize and manage root nodes and their components. SL1 automatically updates the **Component Map** as new component devices are discovered. The platform also updates each map with the latest status and event information. To view the map for a New Relic service, go to the **Component Map** page and select the map from the list in the left NavBar. To learn more about the **Component Map** page, see the ***Views*** manual.



Device Component Map

Chapter 3

Dashboards

Overview

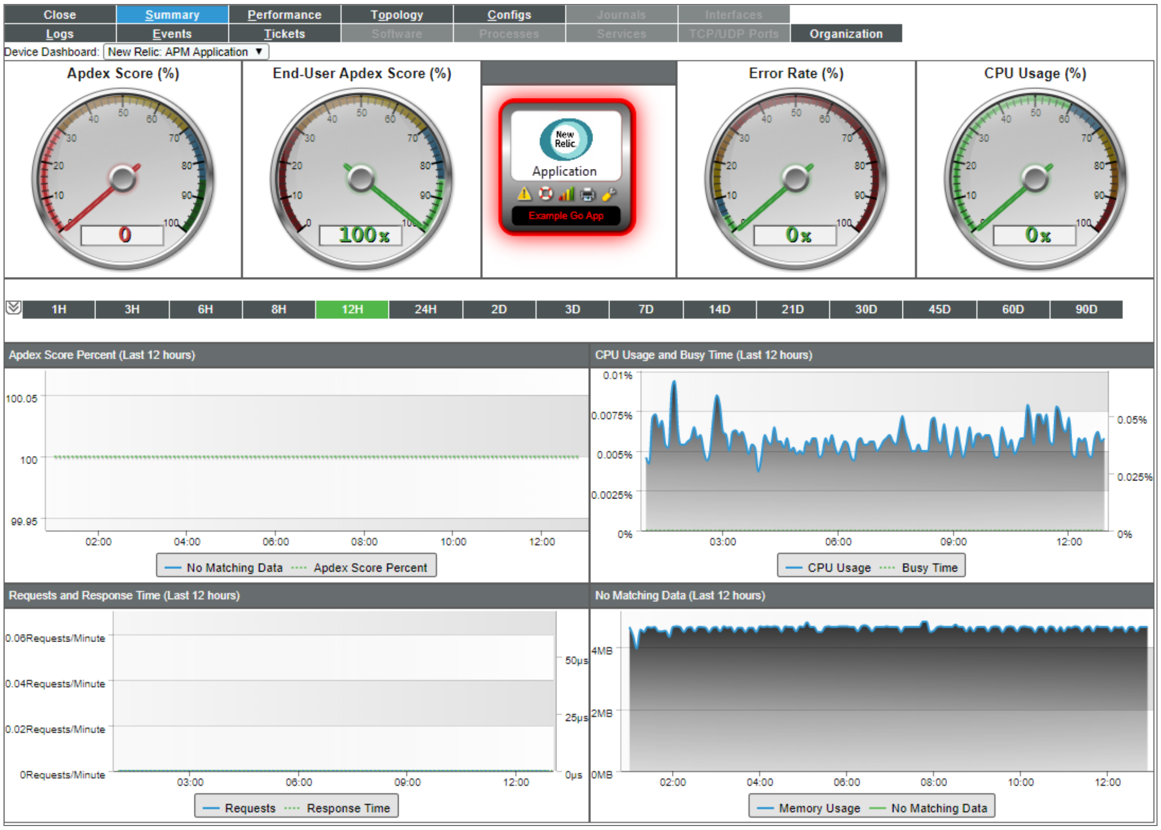
The following section describes the device dashboards that are included in the *New Relic: APM* PowerPack:

This chapter covers the following topics:

Device Dashboards

The *New Relic: APM* PowerPack includes device dashboards that provide summary information for New Relic applications and applications groups.

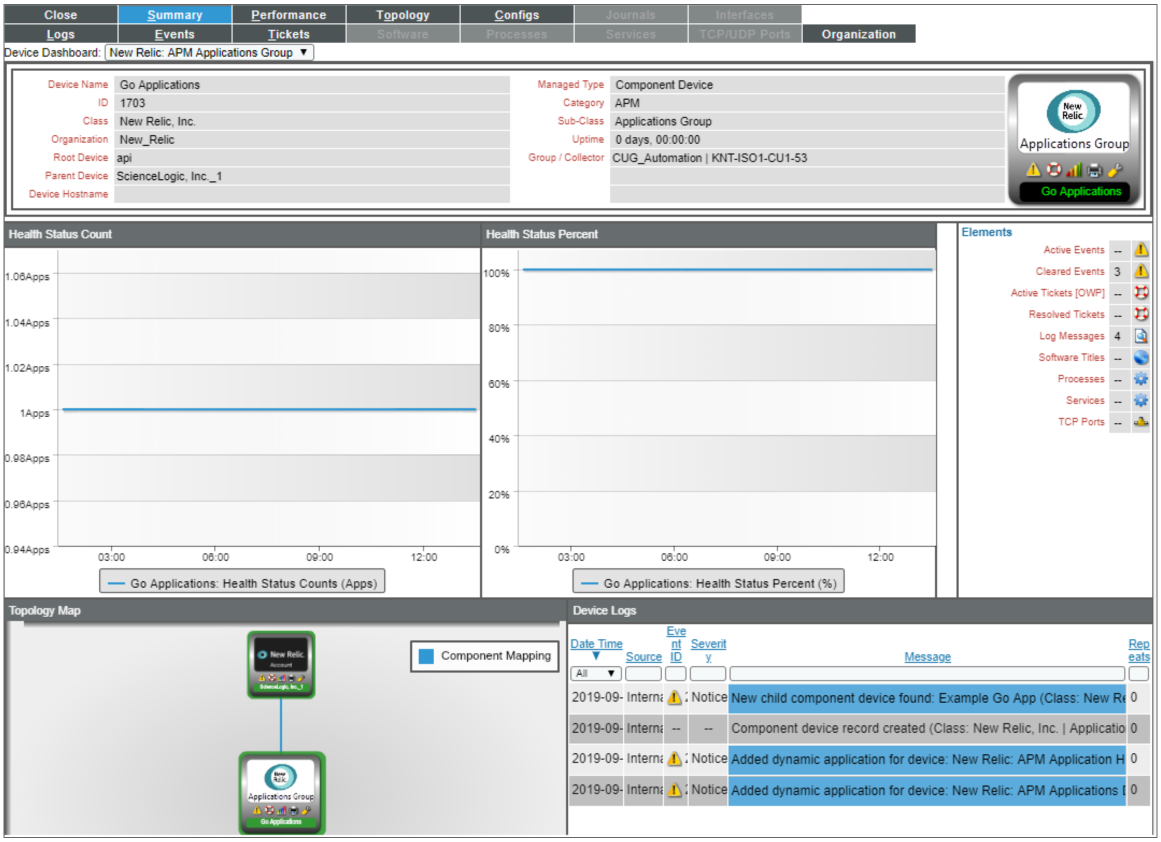
New Relic: APM Application



The New Relic: APM Application device dashboard displays the following information:

- Apdex Score
- End-User Apdex Score
- Error Rate
- CPU Usage
- Apdex Score Percent over a period of time
- CPU Usage and Busy Time over a period of time
- Requests and Response Time over a period of time
- Memory Usage over a period of time

New Relic: APM Applications Group



Device Dashboard: New Relic: APM Applications Group ▼

Device Name: Go Applications
ID: 1703
Class: New Relic, Inc.
Organization: New_Relic
Root Device: api
Parent Device: ScienceLogic, Inc._1
Device Hostname:

Managed Type: Component Device
Category: APM
Sub-Class: Applications Group
Uptime: 0 days, 00:00:00
Group / Collector: CUG_Automation | KNT-ISO1-CU1-53

Go Applications

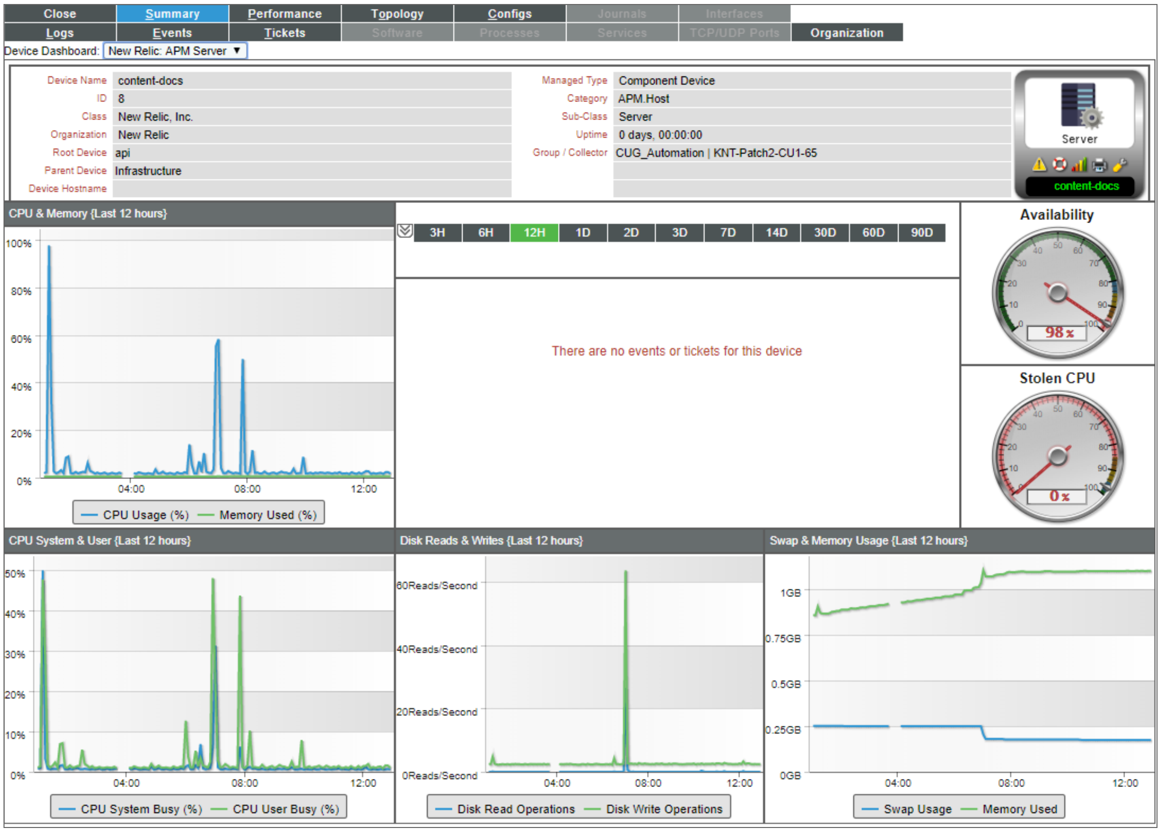
Elements		
Active Events	--	⚠
Cleared Events	3	⚠
Active Tickets [OWP]	--	
Resolved Tickets	--	
Log Messages	4	
Software Titles	--	
Processes	--	
Services	--	
TCP Ports	--	

Date Time ▼	Source	Event ID	Severity	Message	Repeats
All ▼					
2019-09-	Interna	⚠ :	Notice	New child component device found: Example Go App (Class: New Re	0
2019-09-	Interna	--	--	Component device record created (Class: New Relic, Inc. | Applicatio	0
2019-09-	Interna	⚠ :	Notice	Added dynamic application for device: New Relic: APM Application H	0
2019-09-	Interna	⚠ :	Notice	Added dynamic application for device: New Relic: APM Applications [	0

The New Relic: APM Applications Group device dashboard displays the following information:

- Health Status Count over a period of time
- Health Status Percent over a period of time
- Device Logs

New Relic: APM Server



Device Dashboard: New Relic: APM Server

Device Name	content-docs	Managed Type	Component Device
ID	8	Category	APM.Host
Class	New Relic, Inc.	Sub-Class	Server
Organization	New Relic	Uptime	0 days, 00:00:00
Root Device	api	Group / Collector	CUG_Automation | KNT-Patch2-CU1-65
Parent Device	Infrastructure		
Device Hostname			

There are no events or tickets for this device

The New Relic: APM Server device dashboard displays the following information:

- CPU and Memory over a period of time
- Events associated with the server
- Availability
- Stolen CPU
- CPU System & User over a period of time
- Disk Reads & Writes over a period of time
- Swap & Memory Usage over a period of time

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/company/legal.

ScienceLogic

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

International: +1-703-354-1010