Monitoring New Relic

New Relic: APM PowerPack version 103

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:

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

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.

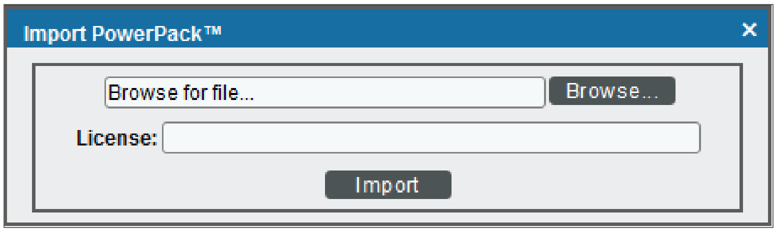
NOTE: Ensure that you do not have the *New Relic: APM Pro* PowerPack installed before installing the *New Relic: APM* PowerPack. These PowerPacks are not compatible. If you have the *New Relic: APM Pro* PowerPack installed, it will need to be uninstalled prior to installing the *New Relic: APM* PowerPack. 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 ***System Administration*** manual.)

To download and install a PowerPack:

1. Download the PowerPack from the ScienceLogic Support Site.
2. Go to the **PowerPack Manager** page (System > Manage > PowerPacks).
3. In the **PowerPack Manager** page, click the **[Actions]** button, then select *Import PowerPack*.

4. The **Import PowerPack** dialog box appears:



5. Click the **[Browse]** button and navigate to the PowerPack file.
6. When the **PowerPack Installer** modal appears, click the **[Install]** button to install the PowerPack.

NOTE: If you exit the **PowerPack Installer** modal without installing the imported PowerPack, the imported PowerPack will not appear in the **PowerPack Manager** 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:

Prerequisites for Monitoring New Relic Services

To configure the SL1 system to 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.

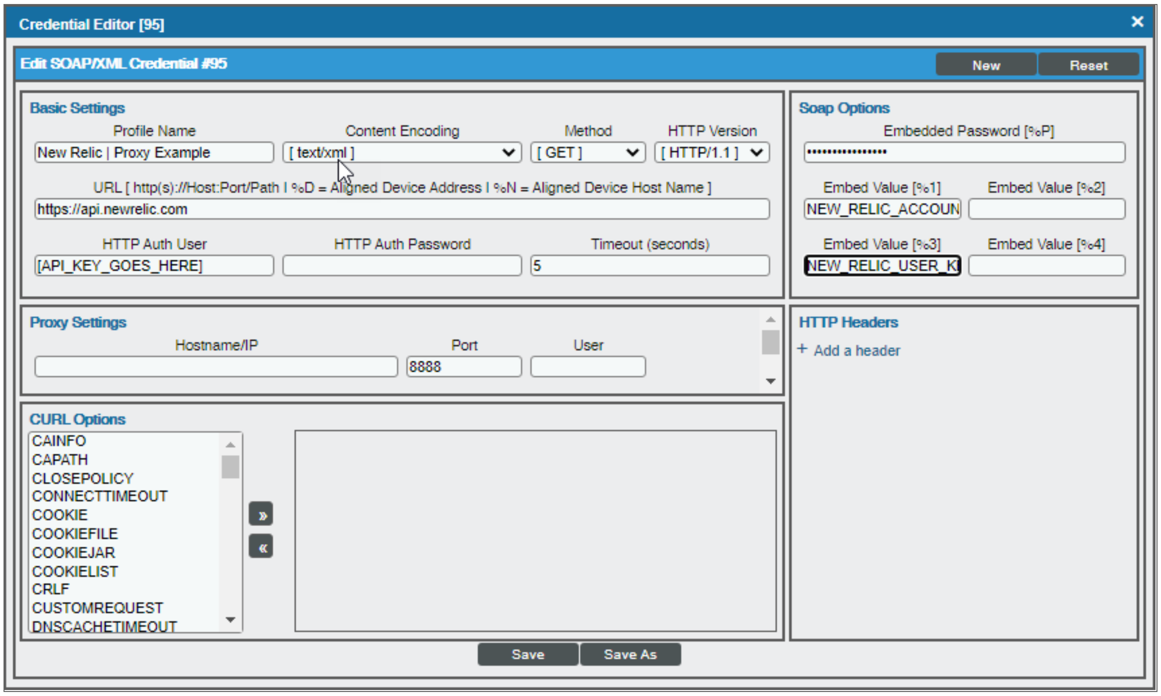
Creating a SOAP/XML Credential for New Relic

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:



Profile Name: New Relic | Proxy Example

Content Encoding: [text/xml]

Method: [GET]

HTTP Version: [HTTP/1.1]

URL [http(s)://Host:Port/Path | %D = Aligned Device Address | %N = Aligned Device Host Name]: https://api.newrelic.com

HTTP Auth User: [API_KEY_GOES_HERE]

HTTP Auth Password:

Timeout (seconds): 5

Embedded Password [%P]: ••••••••••••••••

Embed Value [%1]: NEW_RELIC_ACCOUN

Embed Value [%2]:

Embed Value [%3]: NEW_RELIC_USER_K

Embed Value [%4]:

Hostname/IP:

Port: 8888

User:

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]***. To collect data with New Relic object tags, you must enter a New Relic user key into this field. New Relic user keys begin with "NRAK-" followed by an alpha-numeric value. Leave this field blank if you do not wish to collect tags.

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 model and monitor your New Relic devices, you must run a discovery session to discover your New Relic services.

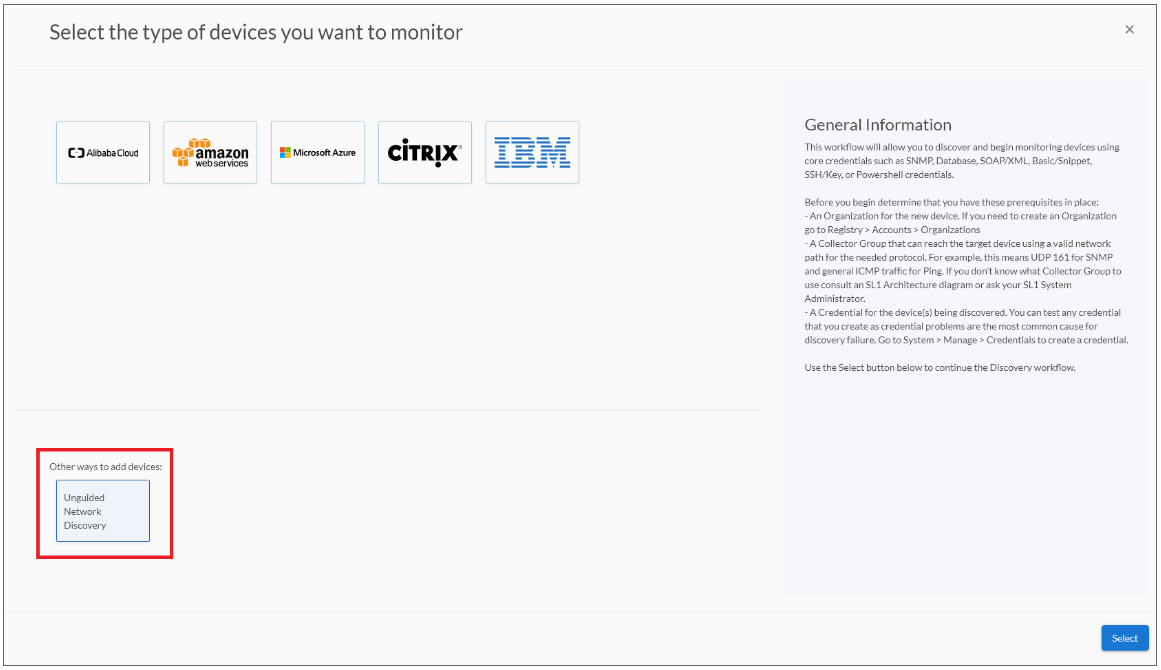
WARNING: If you have multiple New Relic accounts and sub-accounts to discover, follow the steps in the *Discovering Additional New Relic Accounts* section.

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

Several minutes after the discovery session has completed, the Dynamic Applications in the *New Relic: APM* PowerPack should automatically align to the services and then discover, model, and monitor the remaining New Relic component devices.

To discover the New Relic service that you want to monitor, perform the following steps:

1. On the **Devices** page (🖥) or the **Discovery Sessions** page (Devices > Discovery Sessions), click the **[Add Devices]** button. The **Select** page appears:



Select the type of devices you want to monitor

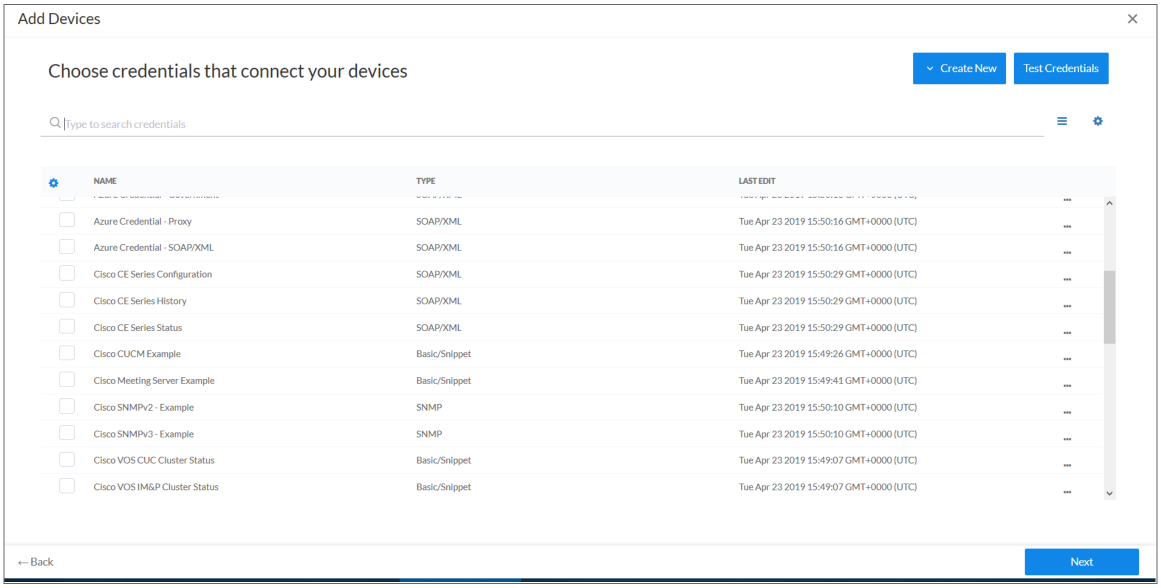
General Information

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

Before you begin determine that you have these prerequisites in place:
- An Organization for the new device. If you need to create an Organization go to Registry > Accounts > Organizations
- A Collector Group that can reach the target device 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 don't know what Collector Group to use consult an SL1 Architecture diagram or ask your SL1 System Administrator.
- A Credential for the device(s) being discovered. You can test any credential that you create as credential problems are the most common cause for discovery failure. Go to System > Manage > Credentials to create a credential.

Use the Select button below to continue the Discovery workflow.

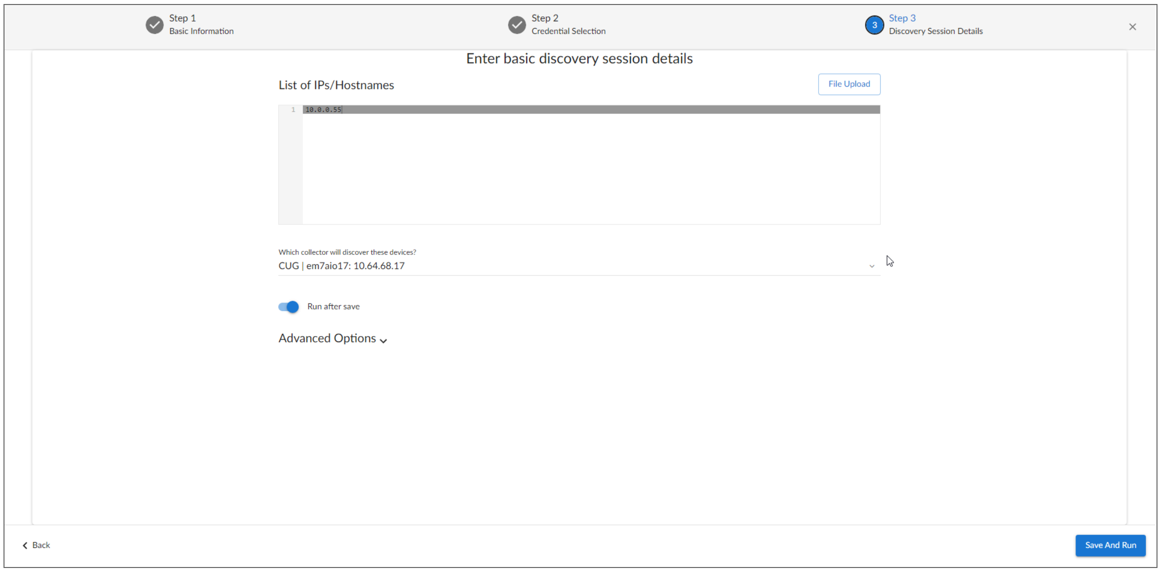
2. Click the **[Unguided Network Discovery]** button. Additional information about the requirements for discovery appears in the **General Information** pane to the right.
3. Click **[Select]**. The **Add Devices** page appears:
4. Complete the following fields:
    - ***Name***. Type a unique name for this discovery session. This name is displayed in the list of discovery sessions on the **[Discovery Sessions]** tab.
    - ***Description***. 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 **Credentials** page of the **Add Devices** wizard appears:



Choose credentials that connect your devices

	NAME	TYPE	LAST EDIT	
□	Azure Credential - Proxy	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)	...
□	Azure Credential - SOAP/XML	SOAP/XML	Tue Apr 23 2019 15:50:16 GMT+0000 (UTC)	...
□	Cisco CE Series Configuration	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CE Series History	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CE Series Status	SOAP/XML	Tue Apr 23 2019 15:50:29 GMT+0000 (UTC)	...
□	Cisco CUCM Example	Basic/Snippet	Tue Apr 23 2019 15:49:26 GMT+0000 (UTC)	...
□	Cisco Meeting Server Example	Basic/Snippet	Tue Apr 23 2019 15:49:41 GMT+0000 (UTC)	...
□	Cisco SNMPv2 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)	...
□	Cisco SNMPv3 - Example	SNMP	Tue Apr 23 2019 15:50:10 GMT+0000 (UTC)	...
□	Cisco VOS CUC Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)	...
□	Cisco VOS IM&P Cluster Status	Basic/Snippet	Tue Apr 23 2019 15:49:07 GMT+0000 (UTC)	...

6. On the **Credentials** page, locate and select the SOAP/XML credentials you created for the New Relic service.
7. Click **[Next]**. The **Discovery Session Details** page of the **Add Devices** wizard appears:



Enter basic discovery session details

List of IPs/Hostnames

```
10.0.0.55
```

Which collector will discover these devices?
CUG | em7aio17: 10.64.68.17

● Run after save

8. Complete the following fields:

    - ***List of IPs/Hostnames***. Type "api.newrelic.com".
    - ***Which collector will monitor these devices?***. Select an existing collector to monitor the discovered devices. Required.
    - ***Run after save***. Select this option to run this discovery session as soon as you click **[Save and Close]**.

      In the **Advanced options** section, click the down arrow icon (⌄) to complete the following fields:

        - ***Discover Non-SNMP***. Enable this setting.
        - ***Model Devices***. Enable this setting.

9. Click **[Save and Close]** to save the discovery session. The **Discovery Sessions** page (Devices > Discovery Sessions) displays the new discovery session.
10. If you selected the **Run after save** option on this page, the discovery session runs, and the **Discovery Logs** page displays any relevant log messages. If the discovery session locates and adds any devices, the **Discovery Logs** page includes a link to the **Device Investigator** page for the discovered device.

Discovering New Relic Component Devices in the SL1 Classic User Interface

To model and monitor your New Relic devices, you must run a discovery session to discover your New Relic services.

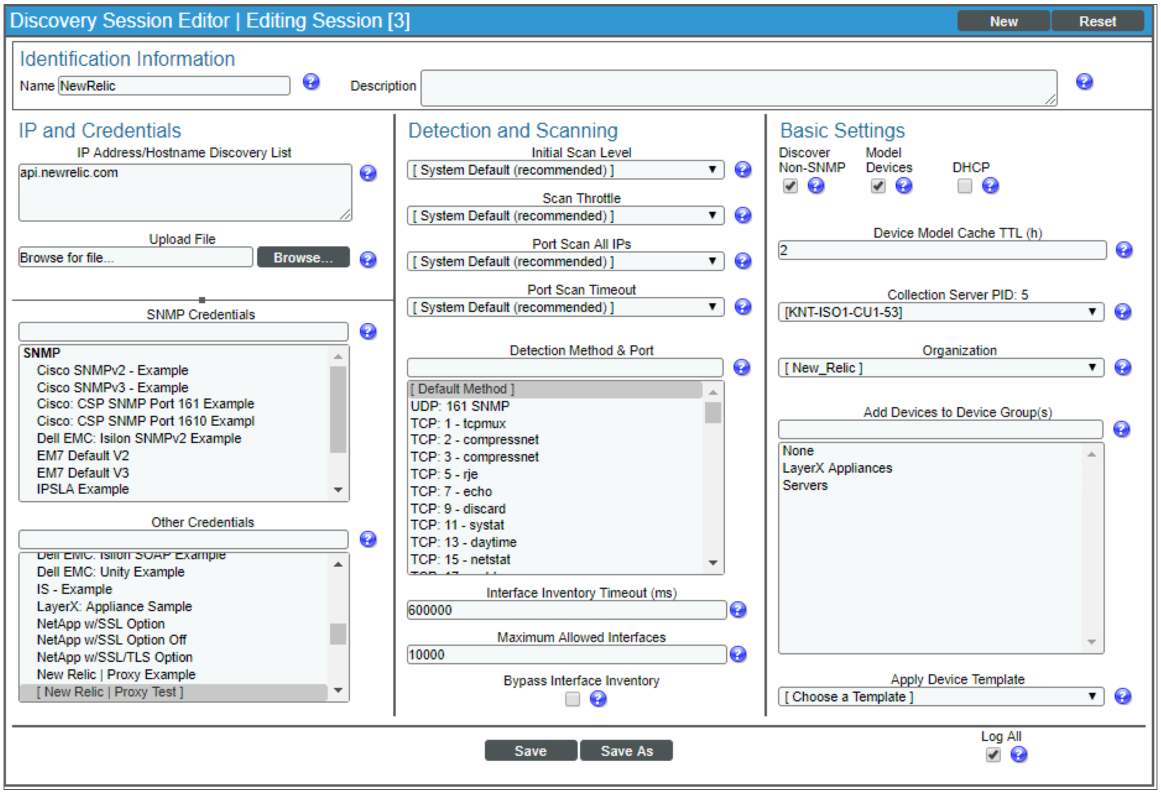
> **WARNING:** If you have multiple New Relic accounts and sub-accounts to discover, follow the steps in the *Discovering Additional New Relic Accounts* section.

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

Several minutes after the discovery session has completed, the Dynamic Applications in the *New Relic: APM* PowerPack should automatically align to the services and then discover, model, and monitor the remaining New Relic component devices.

To discover the New Relic service that you want to monitor, perform the following steps:

1. Go to the **Discovery Control Panel** page (System > Manage > Classic Discovery).
2. In the **Discovery Control Panel**, click the **[Create]** button.
3. The **Discovery Session Editor** page appears. In the **Discovery Session Editor** page, define values in the following fields:



Discovery Session Editor | Editing Session [3]

Identification Information

Name: NewRelic

Description:

IP and Credentials

IP Address/Hostname Discovery List: api.newrelic.com

Upload File: Browse for file...

Other Credentials: [New Relic | Proxy Test]

Detection and Scanning

Initial Scan Level: [System Default (recommended)]

Scan Throttle: [System Default (recommended)]

Port Scan All IPs: [System Default (recommended)]

Port Scan Timeout: [System Default (recommended)]

Detection Method & Port: [Default Method]

Interface Inventory Timeout (ms): 600000

Maximum Allowed Interfaces: 10000

Bypass Interface Inventory: ☐

Basic Settings

Discover Non-SNMP: ☑

Model Devices: ☑

DHCP: ☐

Device Model Cache TTL (h): 2

Collection Server PID: 5: [KNT-ISO1-CU1-53]

Organization: [New_Relic]

Add Devices to Device Group(s):

Apply Device Template: [Choose a Template]

Log All: ☑

- ***Name***. Type a name for the discovery session.
- ***IP Address/Hostname Discovery List***. Type "api.newrelic.com".
- ***Other Credentials***. Select the SOAP/XML credentials you created for the New Relic service.
- ***Discover Non-SNMP***. Select this checkbox.
- ***Model Devices***. Select this checkbox.

4. Optionally, you can enter values in the other fields on this page. For more information about the other fields on this page, see the ***Discovery & Credentials*** manual.
5. Click the **[Save]** button to save the discovery session and then close the **Discovery Session Editor** window.
6. The discovery session you created appears at the top of the **Discovery Control Panel** page. Click its lightning bolt icon (⚡) to run the discovery session.
7. The **Discovery Session** window appears. When the device is discovered, click the device icon (🖥) to view the **Device Properties** page for each device.

Discovering Additional New Relic Accounts

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

Create Credentials

Using the steps outlined in the ***Creating a SOAP/XML Credential for New Relic*** section, create a credential for each additional New Relic account you want to discover.

Edit the Device Template

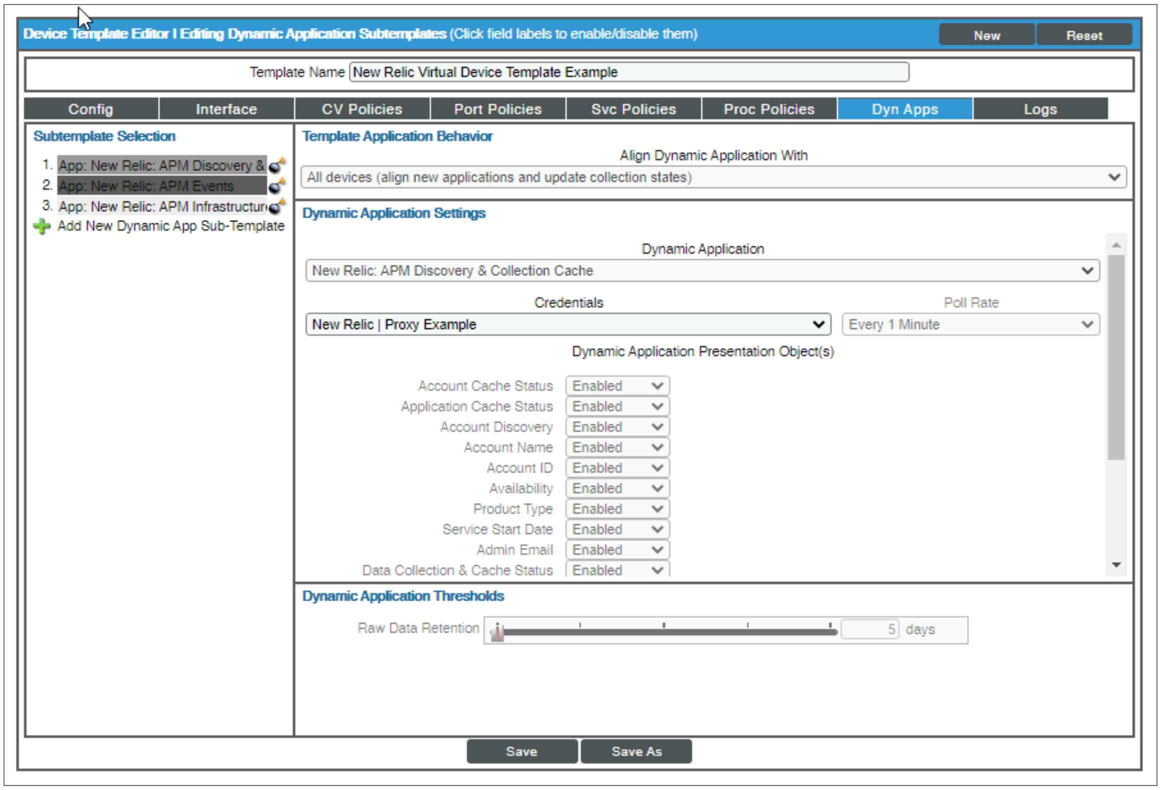
A ***device template*** allows you to save a device configuration and apply it to multiple devices. The *New Relic: APM*PowerPack includes the "New Relic Virtual Device Template Example". You must configure a device template for each additional New Relic account you want to discover.

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 Registry > Devices > Templates 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:


Device Template Editor I Editing Dynamic Application Subtemplates (Click field labels to enable/disable them)
New
Reset
Config
Interface
CV Policies
Port Policies
Svc Policies
Proc Policies
Dyn Apps
Logs
Subtemplate Selection
Add New Dynamic App Sub-Template
Template Application Behavior
Dynamic Application Settings
Dynamic Application Presentation Object(s)
Dynamic Application Thresholds
Save
Save As

Template Name: New Relic Virtual Device Template Example

Subtemplate Selection:
1. App: New Relic: APM Discovery &
2. App: New Relic: APM Events
3. App: New Relic: APM Infrastructure

Align Dynamic Application With: All devices (align new applications and update collection states)

Dynamic Application: New Relic: APM Discovery & Collection Cache

Credentials: New Relic | Proxy Example

Poll Rate: Every 1 Minute

Account Cache Status	Enabled
Application Cache Status	Enabled
Account Discovery	Enabled
Account Name	Enabled
Account ID	Enabled
Availability	Enabled
Product Type	Enabled
Service Start Date	Enabled
Admin Email	Enabled
Data Collection & Cache Status	Enabled

Raw Data Retention: 5 days

- **Template Name**. Type a new name for the device template.
- **Credentials**. Select the 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 SOAP/XML credential in the ***Credentials*** field.

6. Repeat step 5 until the you have selected the New Relic SOAP/XML credential in the ***Credentials*** field for all of the Dynamic Applications listed in the **Subtemplate Selection** section.

7. Click **[Save As]**.

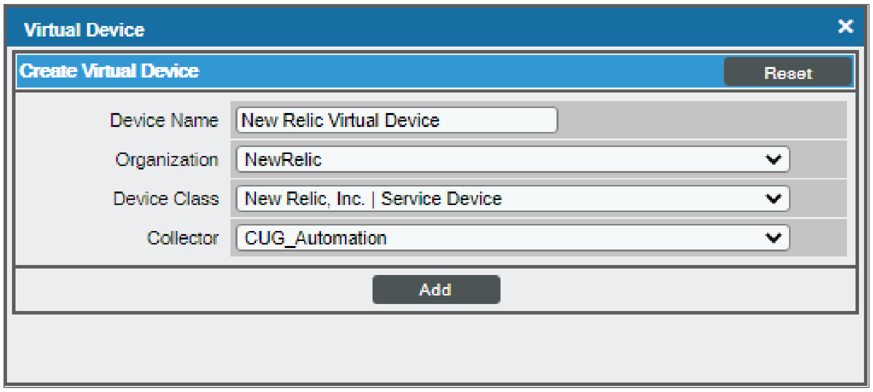
NOTE: You must rename the sample **New Relic Virtual Device Template Example** and click **[Save As]** to save it. If you do not rename the device template, then your device template will be overwritten the next time you upgrade the *New Relic: APM*PowerPack.

Create a Virtual Device

To discover an additional 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.

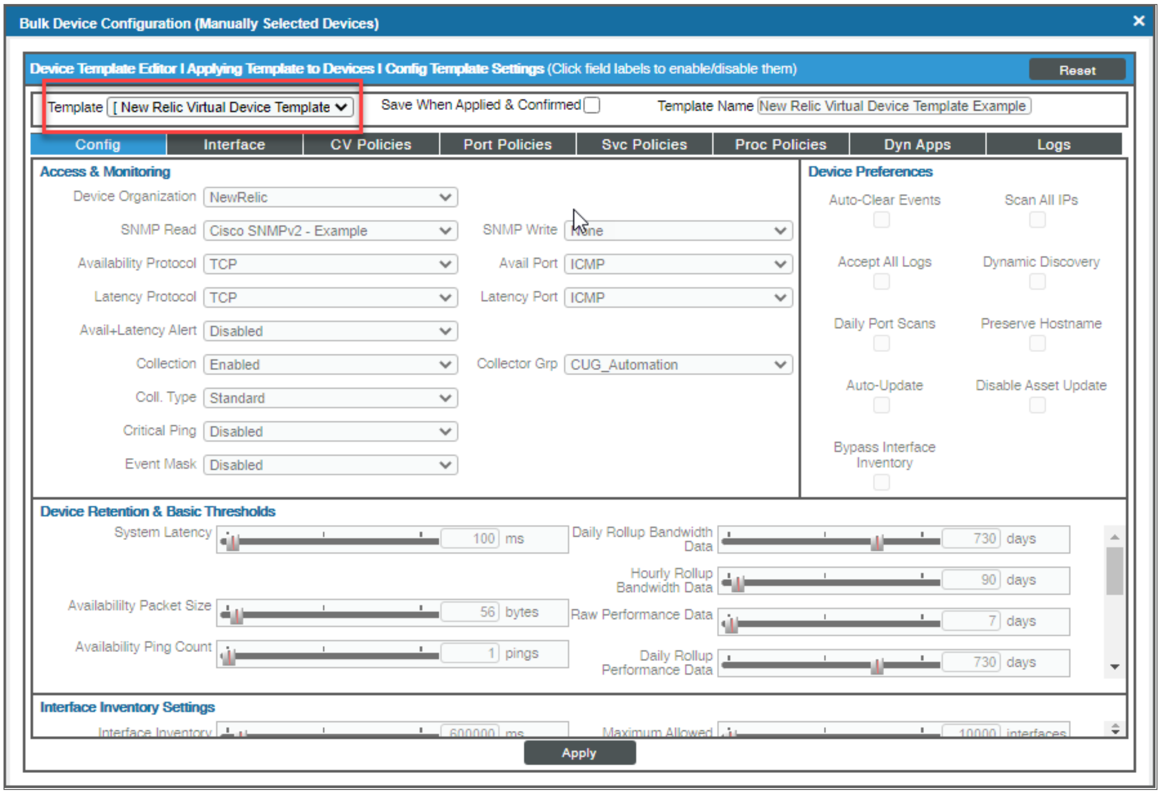
To create a virtual device that represents your New Relic account:

1. Go to the **Device Manager** page (Devices > Device Manager, or Registry > Devices > Device Manager 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:



Device Name: New Relic Virtual Device
Organization: NewRelic
Device Class: New Relic, Inc. | Service Device
Collector: CUG_Automation

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 > Device Manager, or Registry > Devices > Device Manager 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.



Bulk Device Configuration (Manually Selected Devices)

Device Template Editor | Applying Template to Devices | Config Template Settings (Click field labels to enable/disable them)

Template [New Relic Virtual Device Template] Save When Applied & Confirmed □ Template Name New Relic Virtual Device Template Example

Access & Monitoring

Device Organization: NewRelic
SNMP Read: Cisco SNMPv2 - Example
SNMP Write: None
Availability Protocol: TCP
Avail Port: ICMP
Latency Protocol: TCP
Latency Port: ICMP
Avail+Latency Alert: Disabled
Collection: Enabled
Collector Grp: CUG_Automation
Coll. Type: Standard
Critical Ping: Disabled
Event Mask: Disabled

Device Preferences

□ Auto-Clear Events □ Scan All IPs
□ Accept All Logs □ Dynamic Discovery
□ Daily Port Scans □ Preserve Hostname
□ Auto-Update □ Disable Asset Update
□ Bypass Interface Inventory

Device Retention & Basic Thresholds

System Latency: 100 ms
Availability Packet Size: 56 bytes
Availability Ping Count: 1 pings
Daily Rollup Bandwidth Data: 730 days
Hourly Rollup Bandwidth Data: 90 days
Raw Performance Data: 7 days
Daily Rollup Performance Data: 730 days

Interface Inventory Settings

Interface Inventory: 600000 ms
Maximum Allowed: 10000 interfaces

Verifying Discovery and Dynamic Application Alignment

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, go to the **Devices** page and click the device for the New Relic service. From the **Device Investigator** page for the New Relic service, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the service are automatically aligned during discovery.

> **NOTE:** It can take several minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.

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

If the listed Dynamic Applications have not been automatically aligned during discovery, or you want to align more Dynamic Applications, you can align them manually. To do so, perform the following steps:

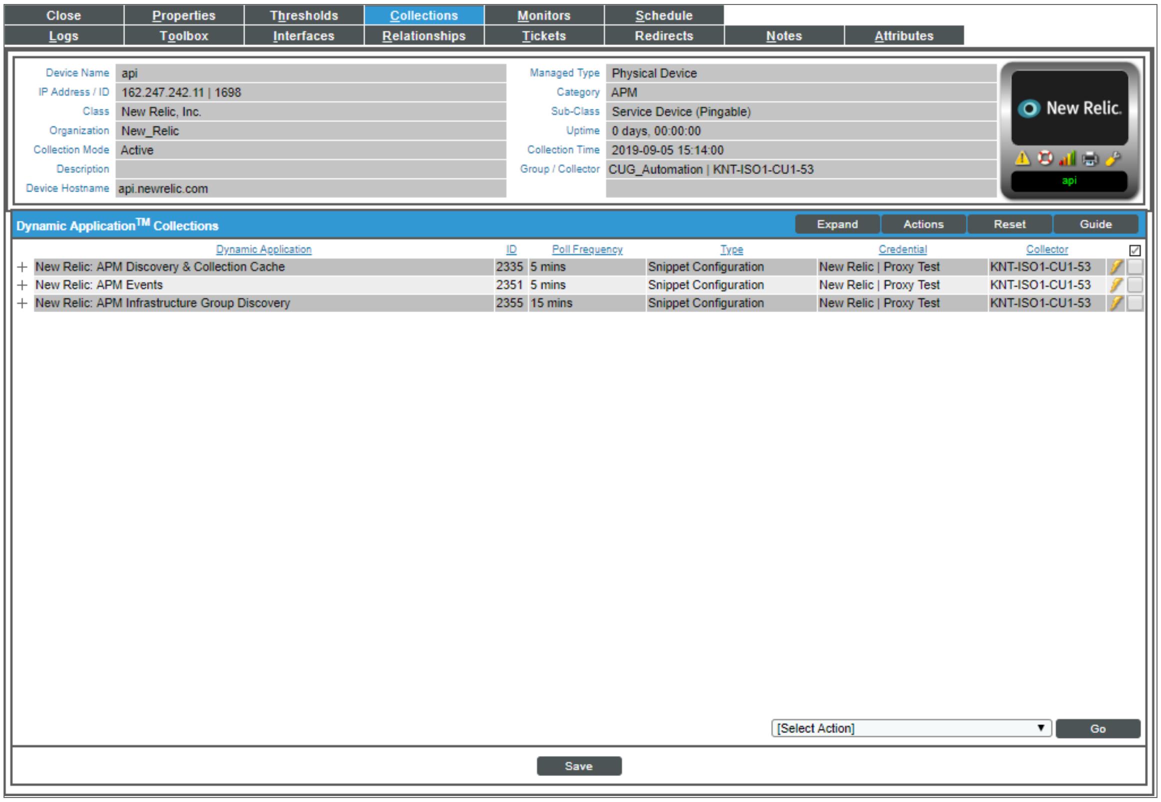
1. Click the **[Edit]** button, and then select **[Align Dynamic App]**. The **Align Dynamic Application** window appears.
2. Click *Choose Dynamic Application*. The **Choose Dynamic Application** window appears.
3. Select the Dynamic Application you want to align and click **[Select]**. The name of the selected Dynamic Application appears in the **Align Dynamic Application** window.
4. If a default credential is listed below the Dynamic Application and you want to use that credential, skip ahead to step 7. Otherwise, uncheck the box next to the credential name.
5. Click *Choose Credential*. The **Choose Credential** window appears.
6. Select the credential for the Dynamic Application and click the **[Select]** button. The name of the selected credential appears in the **Align Dynamic Application** window.
7. Click the **[Align Dynamic App]** button. When the Dynamic Application is successfully aligned, it is added to the **[Collections]** tab, and a confirmation message appears at the bottom of the tab.
8. Repeat steps 1-7 for any other unaligned Dynamic Applications.

Verifying Discovery and Dynamic Application Alignment in the SL1 Classic User Interface

To verify that SL1 has automatically aligned the correct Dynamic Applications during discovery:

1. After discovery has completed, click the device icon for the New Relic service (). From the **Device Properties** page for the New Relic service, click the **[Collections]** tab. The **Dynamic Application Collections** page appears.
2. All applicable Dynamic Applications for the service are automatically aligned during discovery.

> **NOTE:** It can take several minutes after the discovery session has completed for Dynamic Applications to appear in the **Dynamic Application Collections** page.



Device Name	api	Managed Type	Physical Device
IP Address / ID	162.247.242.11 | 1698	Category	APM
Class	New Relic, Inc.	Sub-Class	Service Device (Pingable)
Organization	New_Relic	Uptime	0 days, 00:00:00
Collection Mode	Active	Collection Time	2019-09-05 15:14:00
Description		Group / Collector	CUG_Automation | KNT-ISO1-CU1-53
Device Hostname	api.newrelic.com		

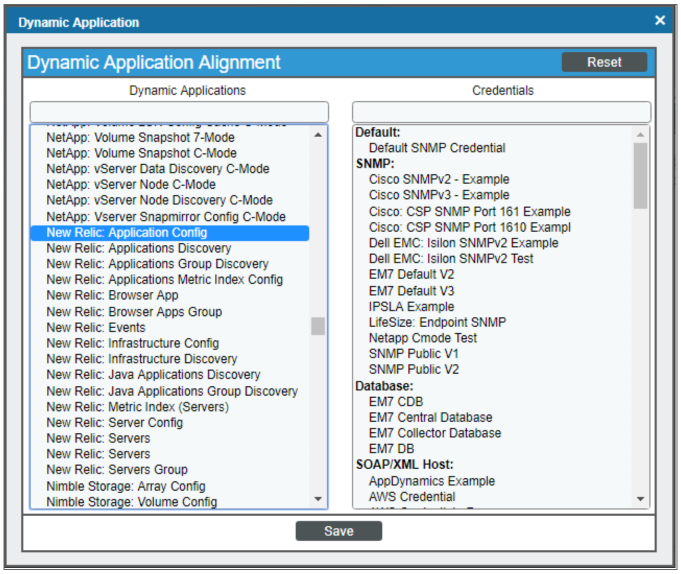
	Dynamic Application	ID	Poll Frequency	Type	Credential	Collector	☑
+	New Relic: APM Discovery & Collection Cache	2335	5 mins	Snippet Configuration	New Relic | Proxy Test	KNT-ISO1-CU1-53	□
+	New Relic: APM Events	2351	5 mins	Snippet Configuration	New Relic | Proxy Test	KNT-ISO1-CU1-53	□
+	New Relic: APM Infrastructure Group Discovery	2355	15 mins	Snippet Configuration	New Relic | Proxy Test	KNT-ISO1-CU1-53	□

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

If the listed Dynamic Applications have not been automatically aligned during discovery, or you want to align more Dynamic Applications, you can align them manually. To do so, perform the following steps:

1. Click the **[Action]** button, and then select *Add Dynamic Application*. The **Dynamic Application Alignment** page appears:


Dynamic Application
Dynamic Application Alignment
Reset
Dynamic Applications
Credentials
NetApp: Volume Snapshot 7-Mode
NetApp: Volume Snapshot C-Mode
NetApp: vServer Data Discovery C-Mode
NetApp: vServer Node C-Mode
NetApp: vServer Node Discovery C-Mode
NetApp: Vserver Snapmirror Config C-Mode
New Relic: Application Config
New Relic: Applications Discovery
New Relic: Applications Group Discovery
New Relic: Applications Metric Index Config
New Relic: Browser App
New Relic: Browser Apps Group
New Relic: Events
New Relic: Infrastructure Config
New Relic: Infrastructure Discovery
New Relic: Java Applications Discovery
New Relic: Java Applications Group Discovery
New Relic: Metric Index (Servers)
New Relic: Server Config
New Relic: Servers
New Relic: Servers
New Relic: Servers Group
Nimble Storage: Array Config
Nimble Storage: Volume Config
Default:
Default SNMP Credential
SNMP:
Cisco SNMPv2 - Example
Cisco SNMPv3 - Example
Cisco: CSP SNMP Port 161 Example
Cisco: CSP SNMP Port 1610 Exampl
Dell EMC: Isilon SNMPv2 Example
Dell EMC: Isilon SNMPv2 Test
EM7 Default V2
EM7 Default V3
IPSLA Example
LifeSize: Endpoint SNMP
Netapp Cmode Test
SNMP Public V1
SNMP Public V2
Database:
EM7 CDB
EM7 Central Database
EM7 Collector Database
EM7 DB
SOAP/XML Host:
AppDynamics Example
AWS Credential
Save

2. In the ***Dynamic Applications*** field, select the Dynamic Application you want to align.

3. In the ***Credentials*** field, select the credential specified in the table.

4. Click the **[Save]** button.

5. Repeat steps 1-4 for any other unaligned Dynamic Applications.

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:

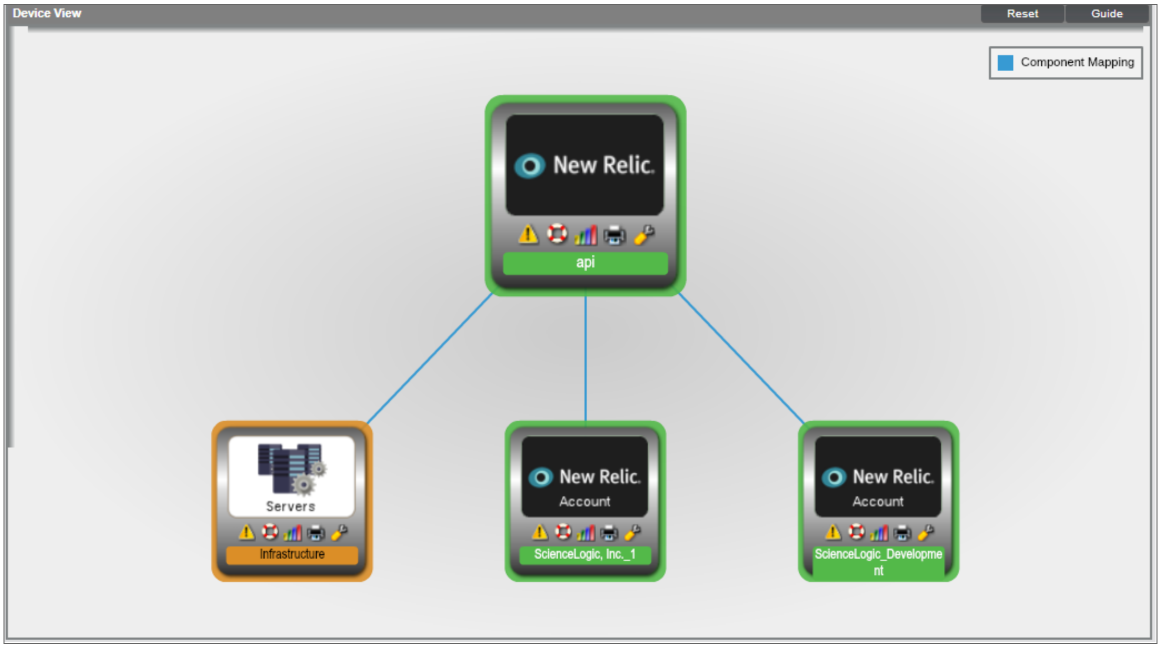
- The **Device Investigator** Map page (click **Map** in the **Device Investigator** page) displays a map of a particular device and all of the devices with which it has parent-child relationships. Double-clicking any of the listed devices reloads the page to make the selected device the primary device
- The **Device Components** page (Devices > Device Components) displays a list of all root devices and component devices discovered by 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 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

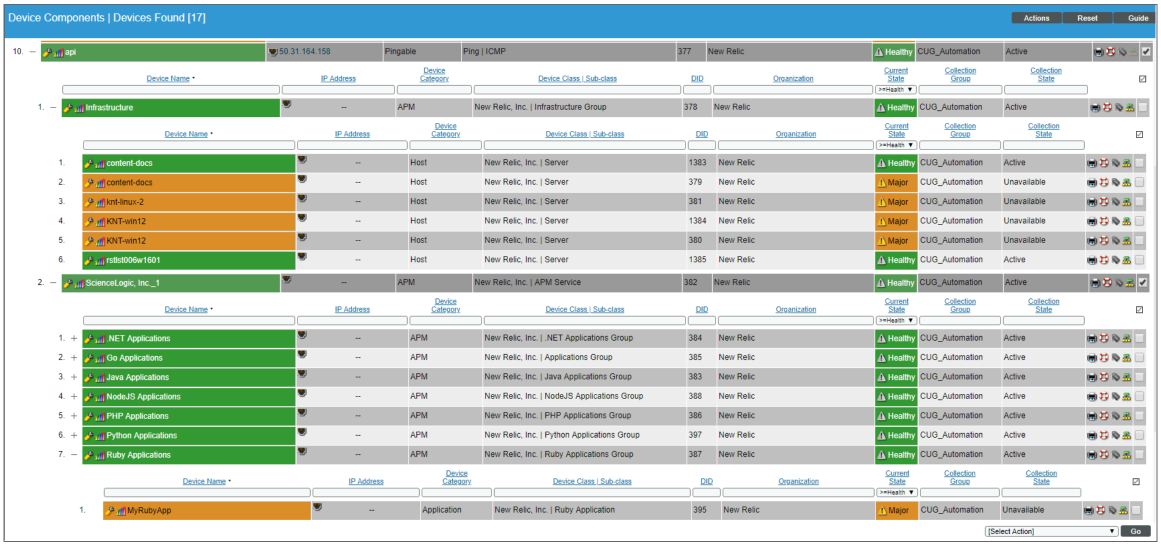
In addition to the **Device Manager** page (Registry > Devices > Device Manager), you can view the New Relic service and all associated component devices in the following places in the user interface:

- 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 (Registry > 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 (+):



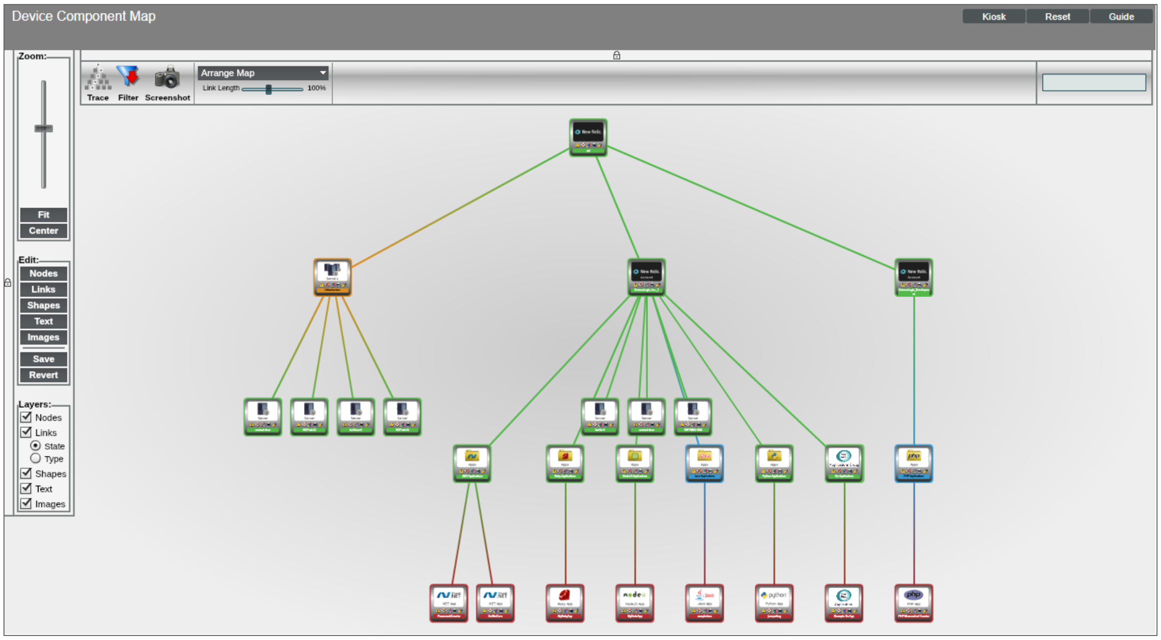
Device Components | Devices Found [17]

Actions | Reset | Guide

	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	☑
	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State (>=Health)	Collection Group	Collection State	☑
1. –	Infrastructure	--	APM	New Relic, Inc. | Infrastructure Group	378	New Relic	Healthy	CUG_Automation	Active	□
	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State (>=Health)	Collection Group	Collection State	☑
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	☑
	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State (>=Health)	Collection Group	Collection State	☑
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	□
	Device Name	IP Address	Device Category	Device Class | Sub-class	DID	Organization	Current State (>=Health)	Collection Group	Collection State	☑
1.	MyRubyApp	--	Application	New Relic, Inc. | Ruby Application	395	New Relic	Major	CUG_Automation	Unavailable	□

[Select Action] ▼ Go

- 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.



Chapter 3

Dashboards

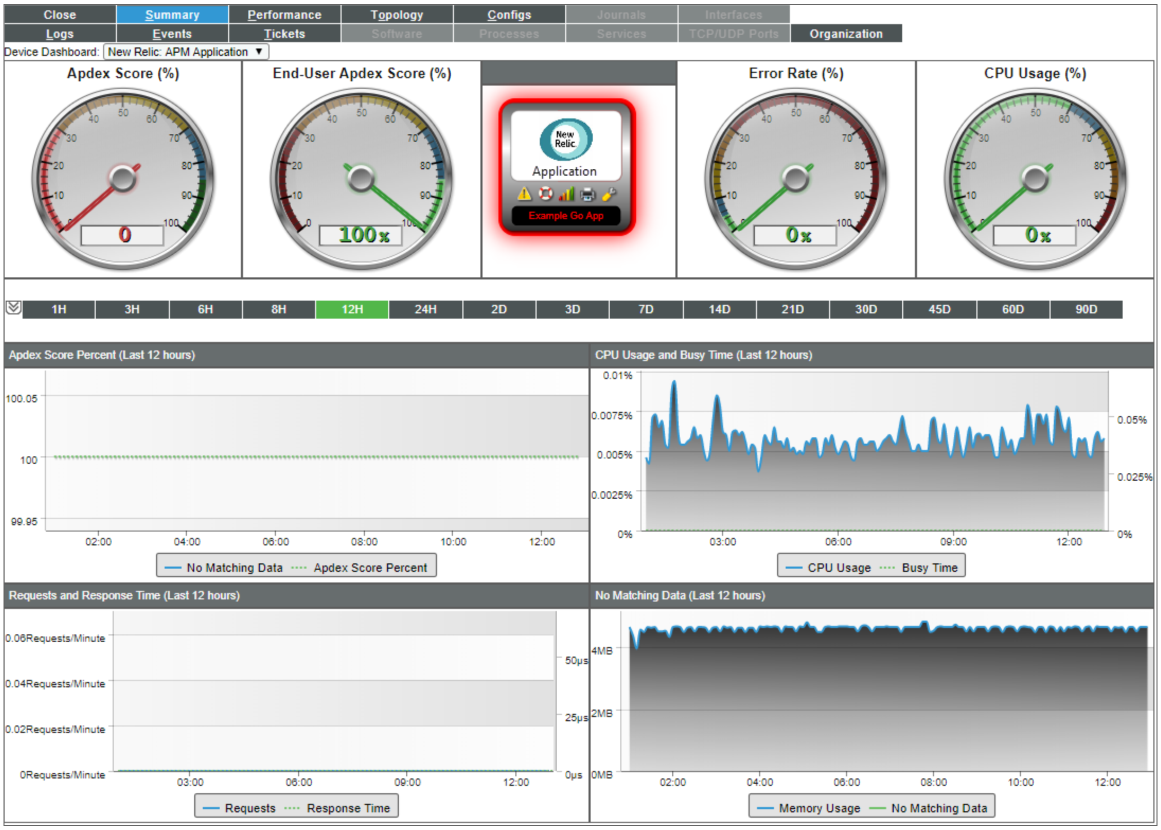
Overview

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

Device Dashboards

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

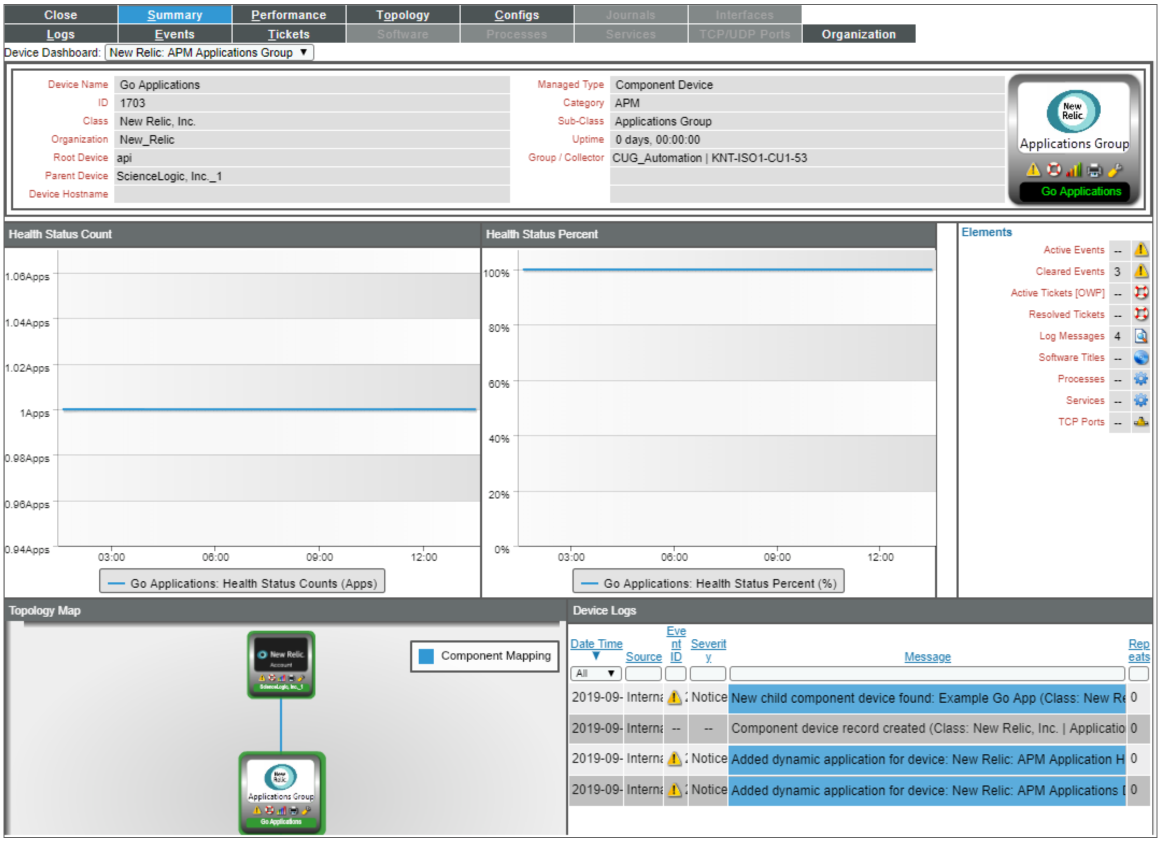
New Relic: APM Application



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	Managed Type	Component Device
ID	1703	Category	APM
Class	New Relic, Inc.	Sub-Class	Applications Group
Organization	New_Relic	Uptime	0 days, 00:00:00
Root Device	api	Group / Collector	CUG_Automation | KNT-ISO1-CU1-53
Parent Device	ScienceLogic, Inc._1		
Device Hostname			

Elements

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

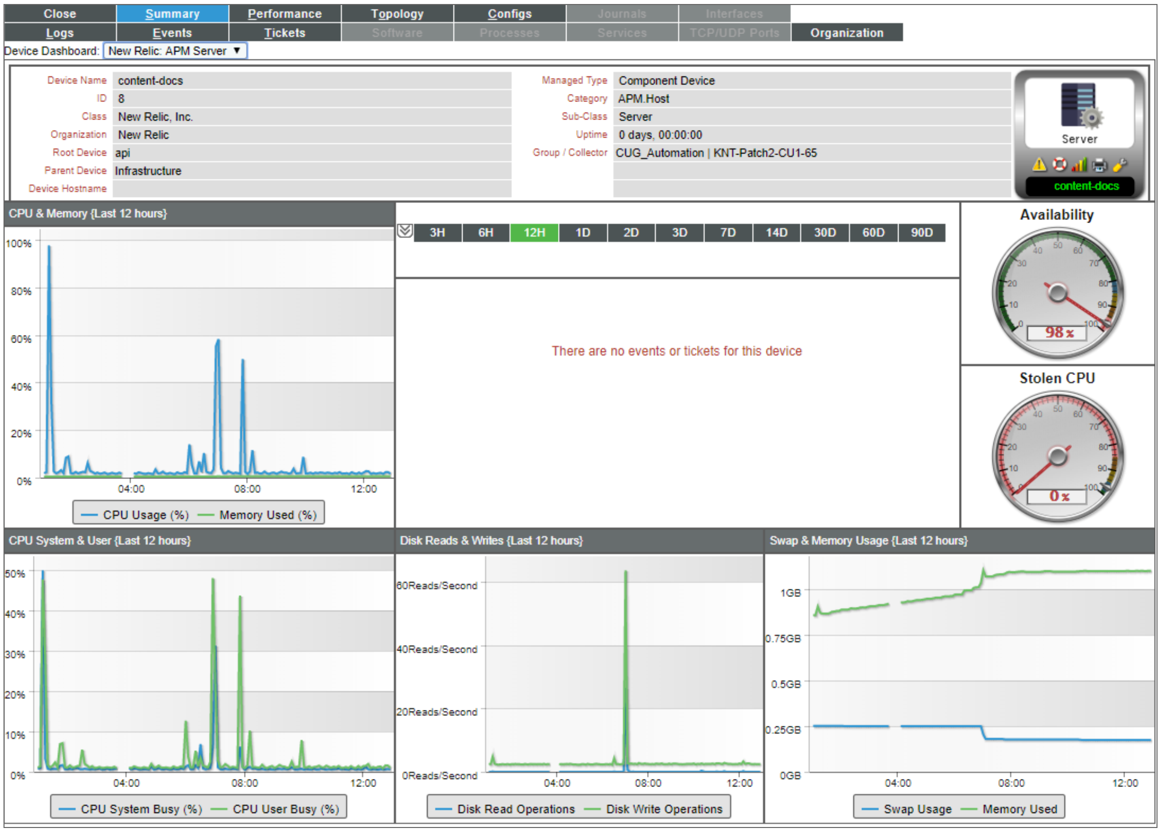
Device Logs

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
- Topology Map
- 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

ScienceLogic

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

International: +1-703-354-1010