PagerDuty Integration Setup

ScienceLogic Version 7.2.2.10

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™
- Dynamic Component Mapping™

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

Table of Contents

Chapter 1

Introduction

Overview

This document is designed to help administrators integrate ScienceLogic EM7 management system with the PagerDuty Incident Management SaaS service. This chapter will help prepare you for the integration tasks.

Who Should Read This Manual?

Any EM7 administrator who wants to integrate with PagerDuty should read this manual. This manual might also be helpful for EM7 users who want to understand how PagerDuty integration works.

Prerequisites

- Requires PagerDuty service account
- Requires ScienceLogic EM7 7.2.2.x or better
- Requires administrative accounts for both products

Integration Steps

To integrate PagerDuty with ScienceLogic the following steps will be required.

- Create PagerDuty API Service
- Import PagerDuty Power-Pack into ScienceLogic system
- Create credential for PagerDuty API
- Align ScienceLogic Run Book Automation policies
- Advanced Integration (optional)

It is recommended that you familiarize yourself with the ScienceLogic Run Book Automation (RBA) functionality before activating the PagerDuty Power-Pack. The default PagerDuty RBA policies are very broad and will create new PagerDuty incidents for every event in ScienceLogic that is of severity minor, major, and critical.

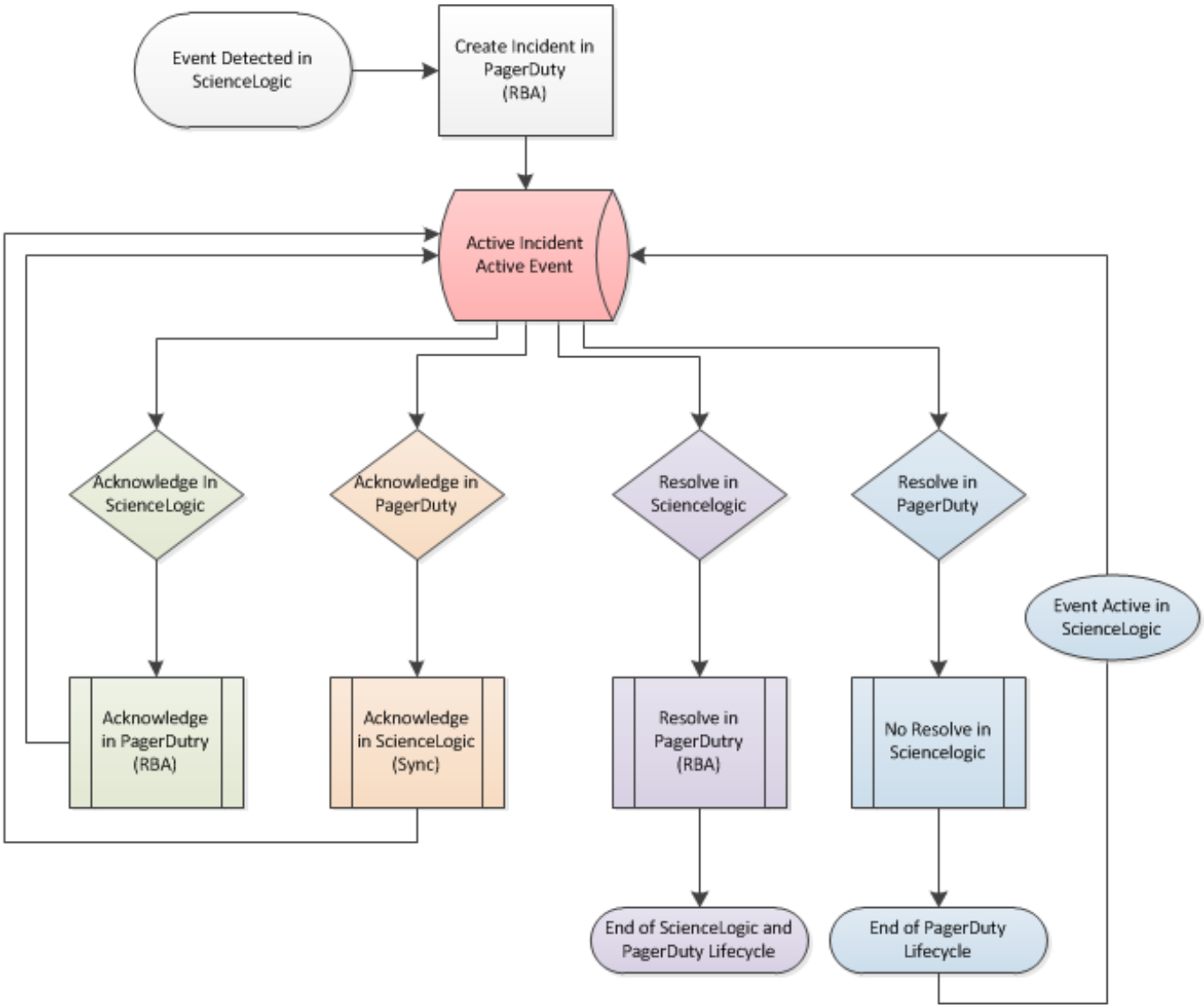
Understanding the ScienceLogic PagerDuty Integration

The ScienceLogic PagerDuty integration Power-Pack offers several key functions areas:

1. Run Book Automation policies to trigger, resolve, and acknowledge events from ScienceLogic to PagerDuty
2. Dynamic Application to collect PagerDuty performance metrics, and synchronize incidents acknowledged from PagerDuty.
3. PagerDuty performance KPI dashboard with historical dynamic trending.
4. PagerDuty example credentials for both Run Book Actions and Dynamic Applications
5. PagerDuty device classes and icons for both Pingable and Virtual devices.

The PagerDuty integration relies on Run Book Automation policies to “push” both events and related event actions to PagerDuty. Activities emanating from PagerDuty, for instance acknowledging an incident, are synchronized through a Dynamic Application. The below diagram shows the dataflow for how ScienceLogic events and PagerDuty incidents are synchronized.

3



Incidents resolved in the PagerDuty will not automatically resolve events in ScienceLogic. This is because most events in ScienceLogic will automatically resolve themselves if they are no longer active or detected. For instance, if a monitored device is detected as being unavailable, ScienceLogic will create an event, and then create an incident in PagerDuty. If the incident in PagerDuty is resolved but the device is still detected as being unavailable, ScienceLogic will automatically create another event and PagerDuty incident. However if the incident is resolved in PagerDuty, but the event still remains in ScienceLogic, duplicate events will be suppressed. Once the event is no longer valid, ScienceLogic will automatically resolve the event and update the incident in PagerDuty.

Chapter 2

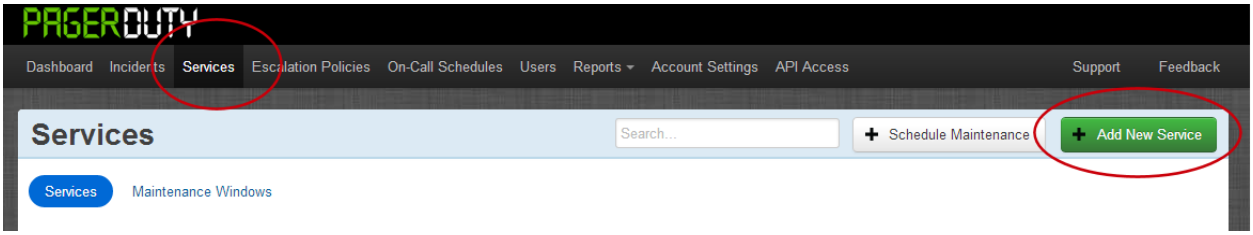
Configure PagerDuty

Overview

In this chapter we will create a PagerDuty "Generic API" service in the PagerDuty web portal for the ScienceLogic Run Book Automation integration. We will also add an API access key for ScienceLogic Dynamic Application performance and synchronization. Both steps will require you record the "key" to add to the respective ScienceLogic credential. You will need administrative access to your PagerDuty account.

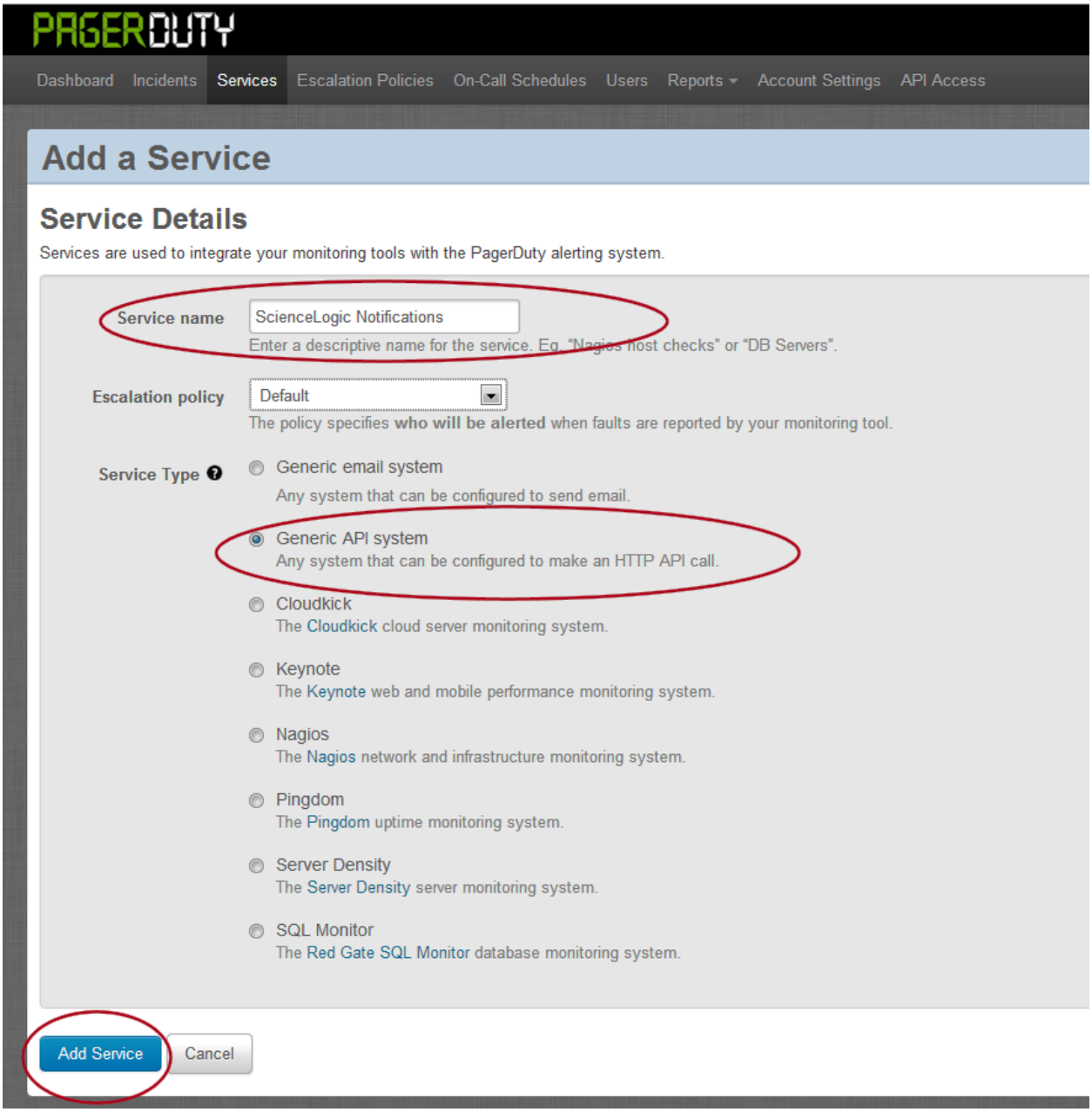
Add API Service (for Run Book Automation)

Login in to your PagerDuty portal using an administrator account. Click on the "Services" navigation menu at the top of the page, and then click on the "Add New Service" button.

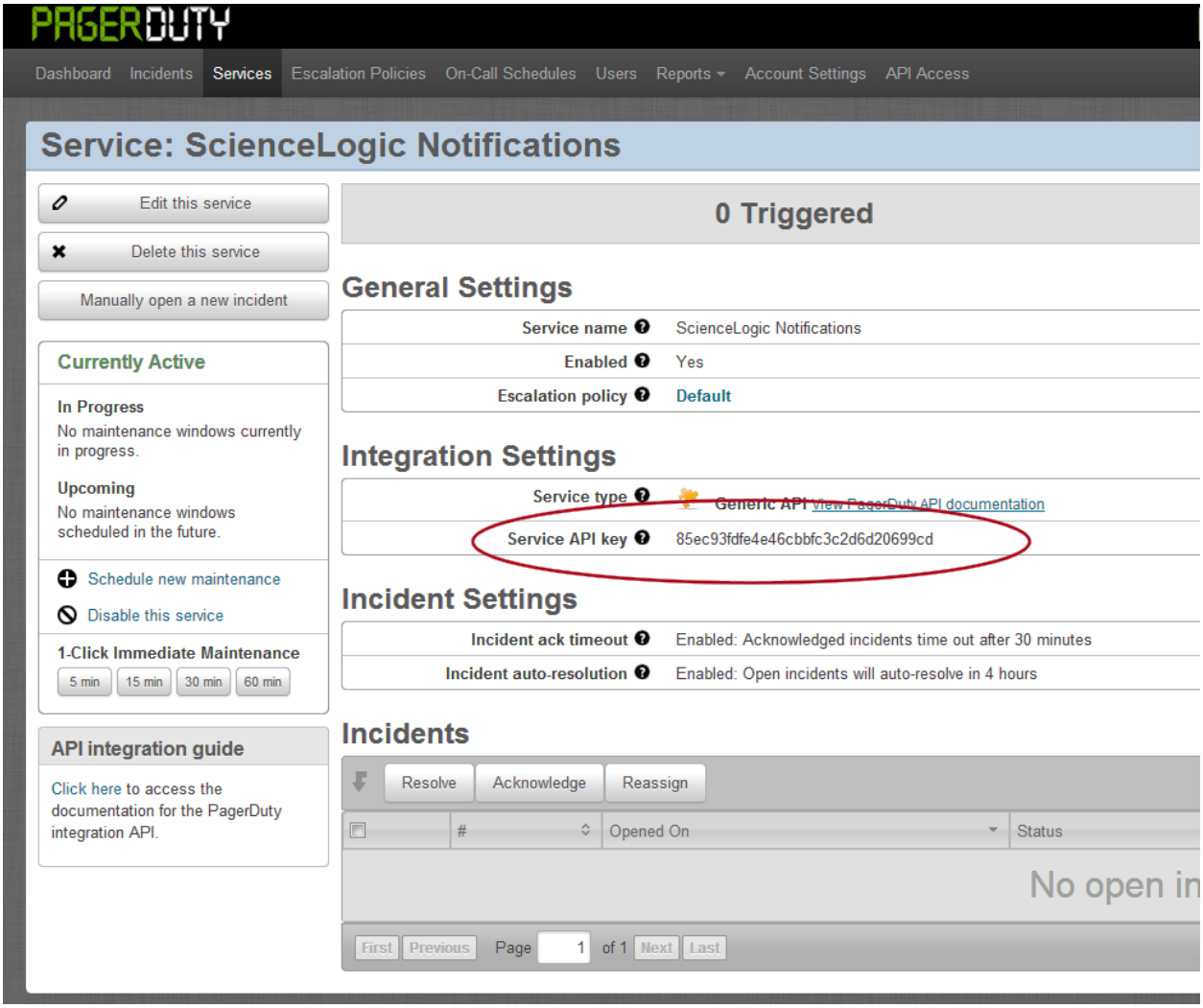


Enter a "service name" (in our example we used ScienceLogic Notifications), and then select "Generic API system". Once done, click the "Add Service" button.

3



Copy the "Service API Key", as this will be needed for the ScienceLogic Run Book Automation credential.

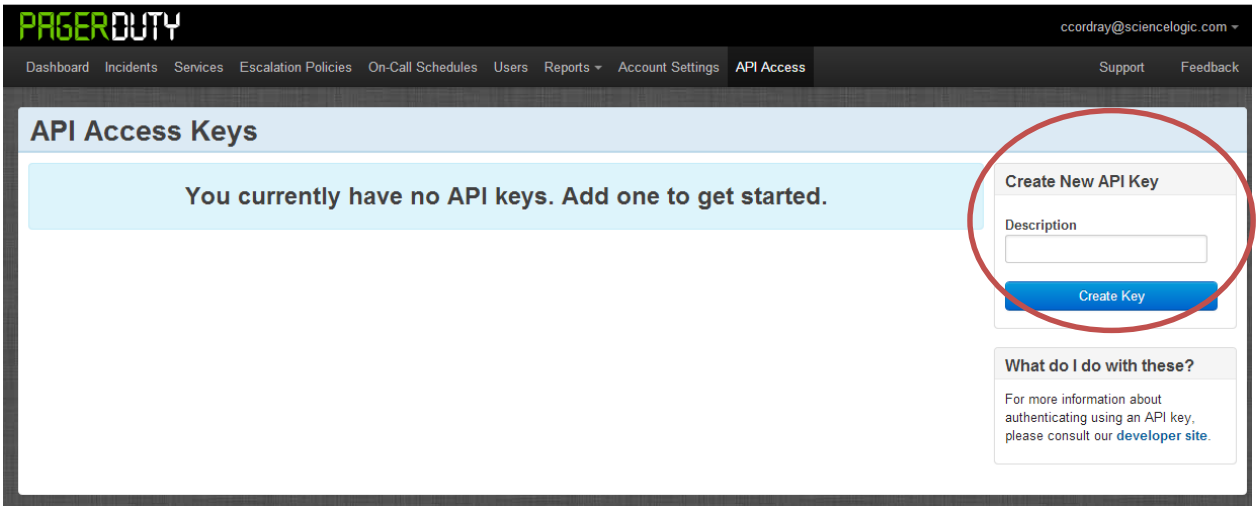


For your records, record the PagerDuty Service API key:

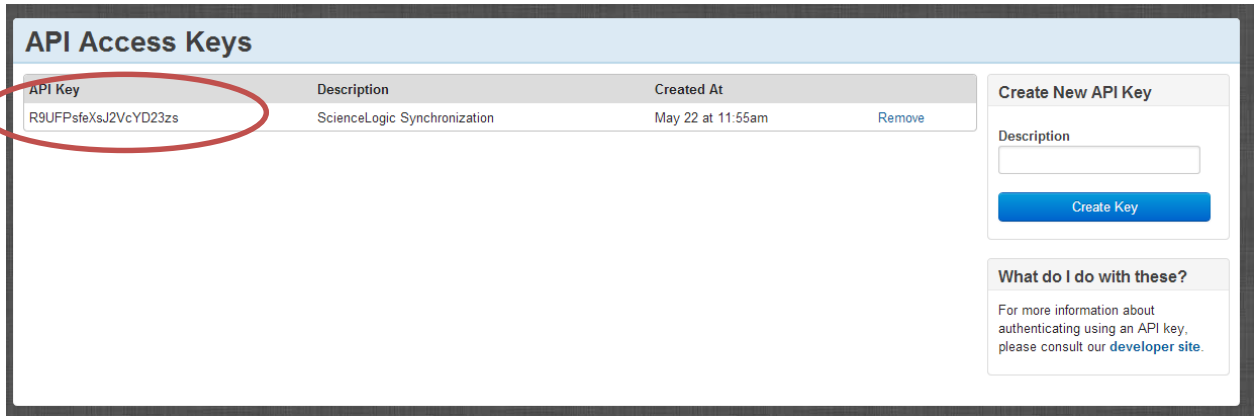
Service API Key: _____

Add API Access Key (for Dynamic Application)

Login in to your PagerDuty portal using an administrator account. Click on the "API Access" on the navigation menu at the top of the page. If there is no API Access Keys defined, create a new key. Add a description for the key, for instance ScienceLogic Synchronization, and then select the "Create Key" button.



When complete, copy the API key for use with the ScienceLogic Dynamic Application Credential.



For your records, record the PagerDuty API Access Key:

API Access Key: _____

Chapter 3

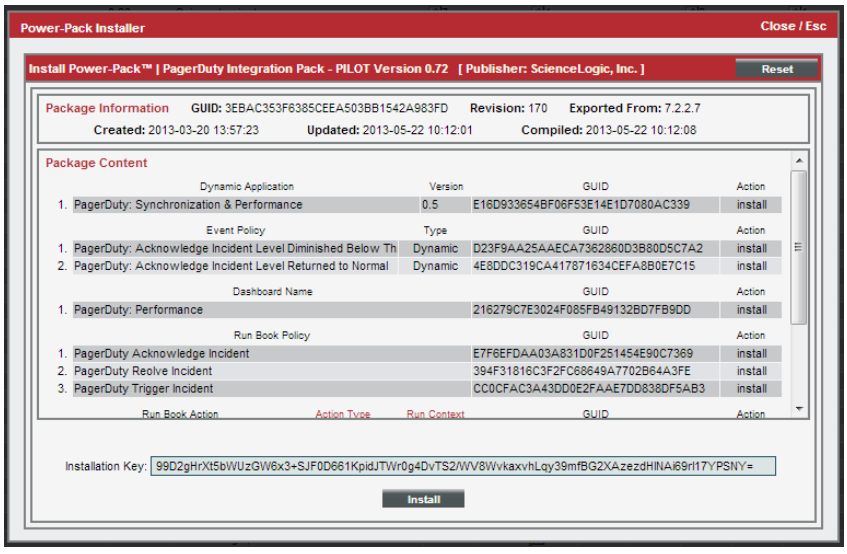
Importing the PagerDuty Power-Pack

Overview

In this chapter we will install the PagerDuty Power-Pack and then configure both the Run Book Automation credential and the Dynamic Application credential.

Installation

Obtain the latest copy of the "PagerDuty Integration" Power-Pack. In this document we will be using version 0.7.x of the Power-Pack.



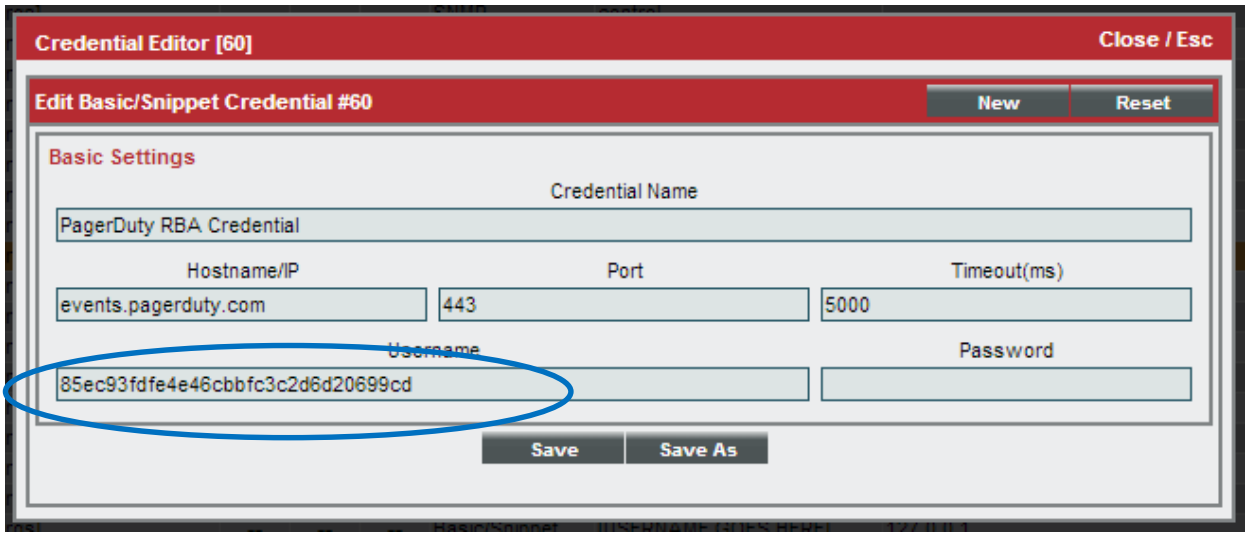
Using normal Power-Pack installation procedures, got the System tab, select Manage\Power-Packs, and then select the Action button, and select "Import Power-Pack" Locate the Power-Pack file, and then select the Import button.

Click install to begin the import process. Once the Power-Pack is installed, proceed to the next section to configure the credential.

3

Configure RBA Credential

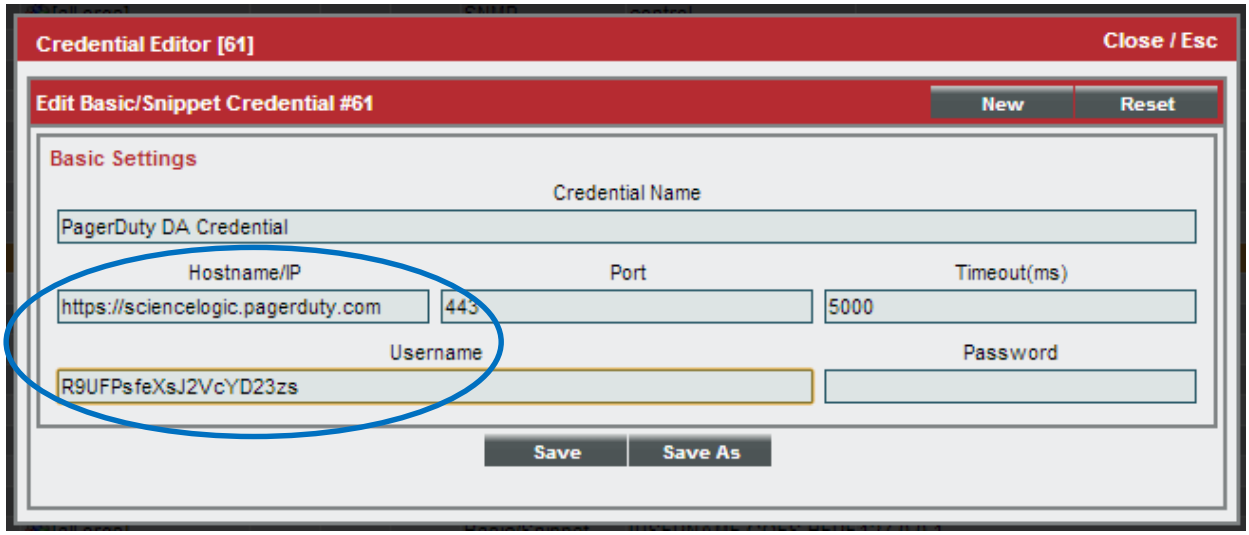
With the Power-Pack installed, we can now configure our Run Book Automation credential. Navigate to the System tab, select Manage\Credentials. Locate the "PagerDuty RBA Credential" credential and then check on the wrench to edit it. In the "Username" field, enter the PagerDuty "Service API Key" you copied from the previous chapter. Click the Save button to update the credential, or use the Save As button to create a new credential.



Configure Dynamic Application Credential

The Dynamic Application credential is needed if you wish to synchronize incident changes from PagerDuty to ScienceLogic. Navigate to the System tab and select Manage\Credentials. Locate the "PagerDuty DA Credential" credential and then check on the wrench to edit it.

In the "Username" field, enter the PagerDuty "API Access Key" you copied from the previous chapter. In the Hostname field, add the URL of our PagerDuty account, for instance: http://mycompany.pagerduty.com. This should be the same account that you use to access your PagerDuty administration interface. Click the Save button to update the credential, or use the Save As button to create a new credential.


Credential Editor [61]
Close / Esc
Edit Basic/Snippet Credential #61
New
Reset
Basic Settings
Credential Name
PagerDuty DA Credential
Hostname/IP
Port
Timeout(ms)
https://sciencelogic.pagerduty.com
443
5000
Username
Password
R9UFPsfeXsJ2VcYD23zs
Save
Save As

Chapter 4

Configure Run Book Automation Policies

Overview

In this chapter we will configure the PagerDuty Run Book Automation Policy, aligning the credential, and begin sending events to PagerDuty. The Run Book Automation policies provided by ScienceLogic will create outbound incidents in PagerDuty.

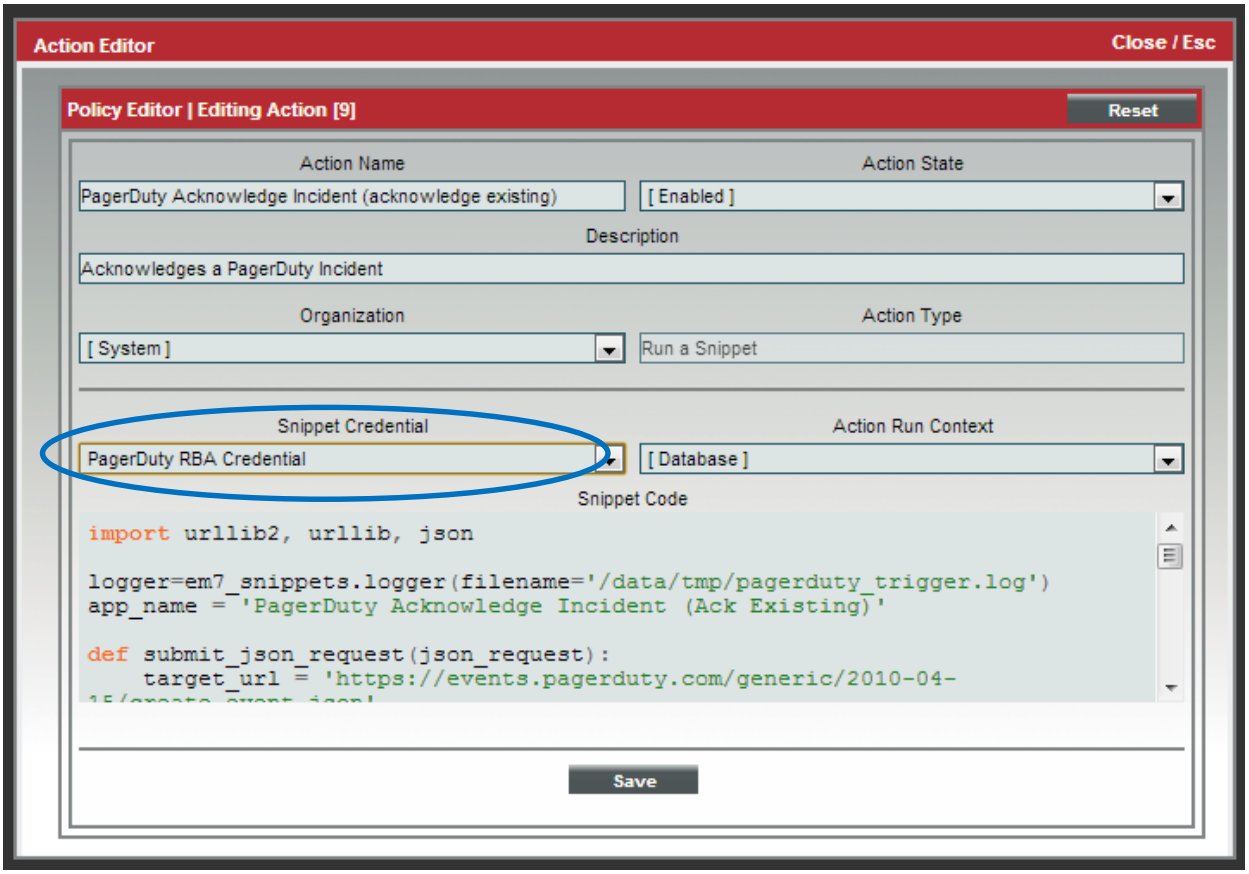
Run Book Actions

Navigate to the Run Book Actions page by clicking on Registry tab, then Run Book, and then Actions. You will notice three PagerDuty actions.

1. PagerDuty Trigger Incident
2. PagerDuty Acknowledge Incident
3. PagerDuty Resolve Incident

Each of these actions performs a different function and allows you to align different Automation policies based on your business needs. To configure these actions, we muct manually edit each and align the proper PagerDuty credential that contains the PagerDuty API key.

Edit each Action by clicking on the yellow wrench, then select the PagerDuty Credential, then select Save.



Note: PagerDuty Actions must run on the ScienceLogic Database, double check that the Action Run Context is set to Database.

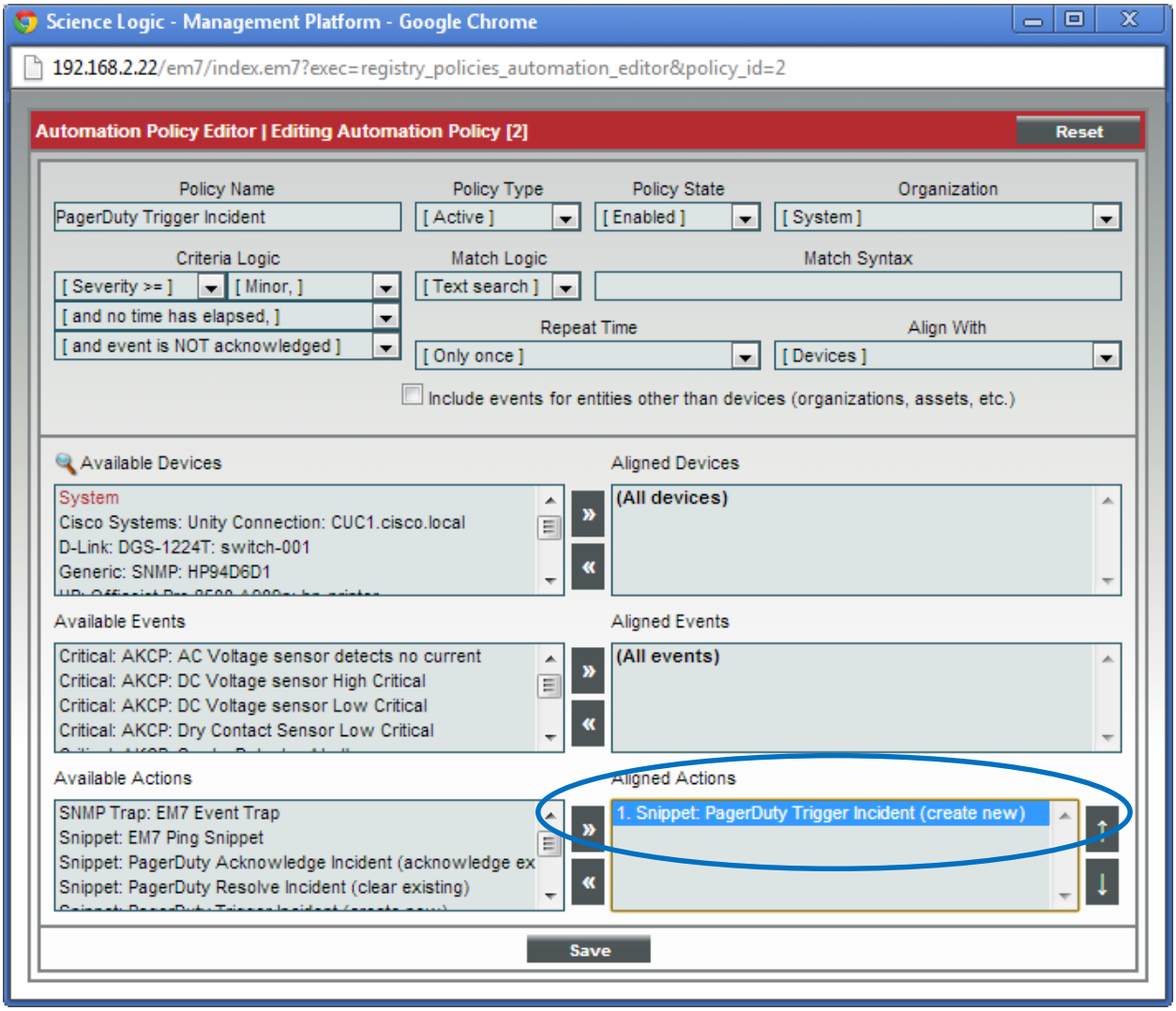
Once complete, lets double check the PagerDuty Automation Policies.

Automation Policies

Like the PagerDuty Run Book Actions, there are three Automation Policies. Each Automation Policy performs a different task based on criteria established in the Policy. By default the PagerDuty Automation Policies are very broad, allowing every ScienceLogic event that has a severity higher than or equal to "minor" to trigger a PagerDuty incident. Although this may be good to begin testing your PagerDuty integration, it is advised to adjust each PagerDuty Automation policy to meet the needs of your business.

Navigate to the Run Book Automation page by clicking on Registry tab, then Run Book, and then Automation. You will notice three PagerDuty actions.

Click the yellow wrench for each policy to edit it. Note that the default policies work against all devices, in all organizations. Make sure the matching RBA Action is aligned. When complete making changes, click the Save button. With all Automation Policies validated, we can now proceed to the next chapter.



Chapter 5

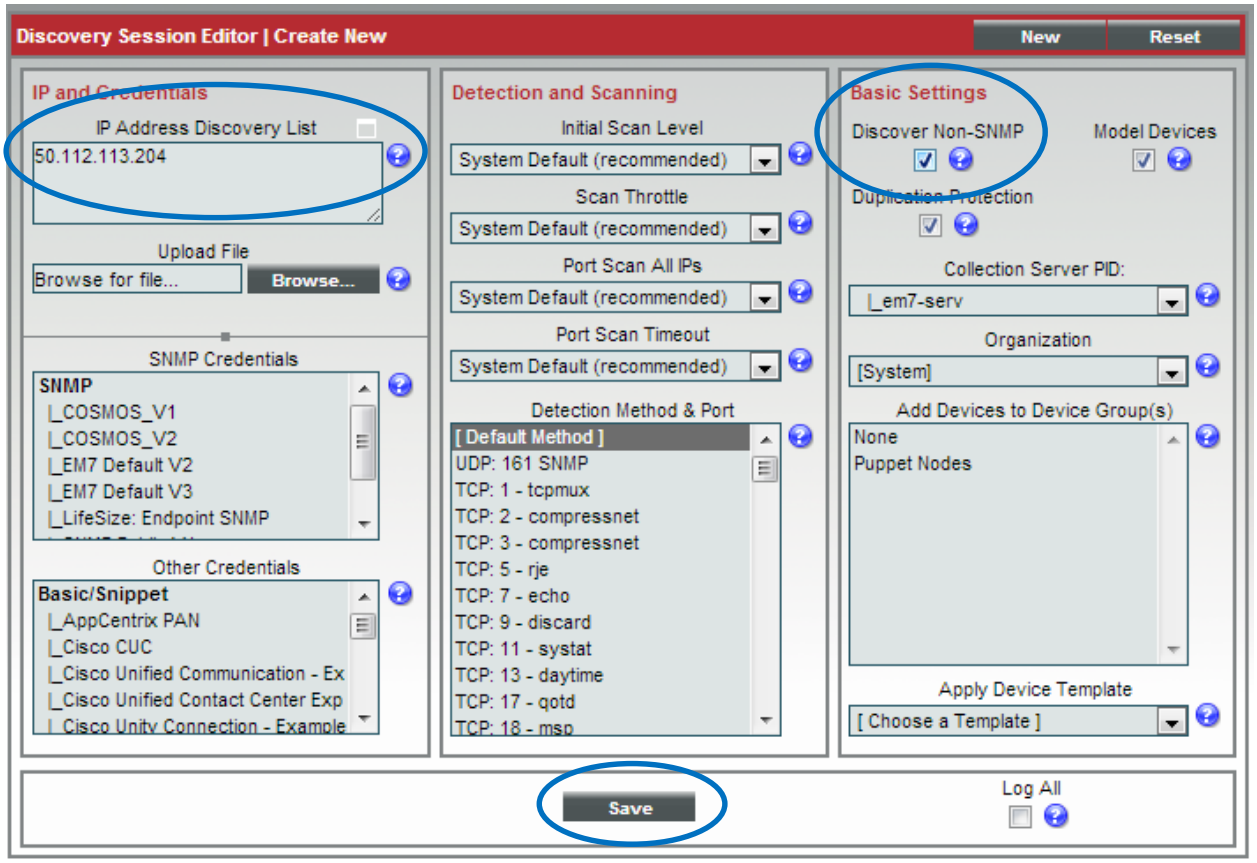
Configure PagerDuty Device and Dynamic Application

Overview

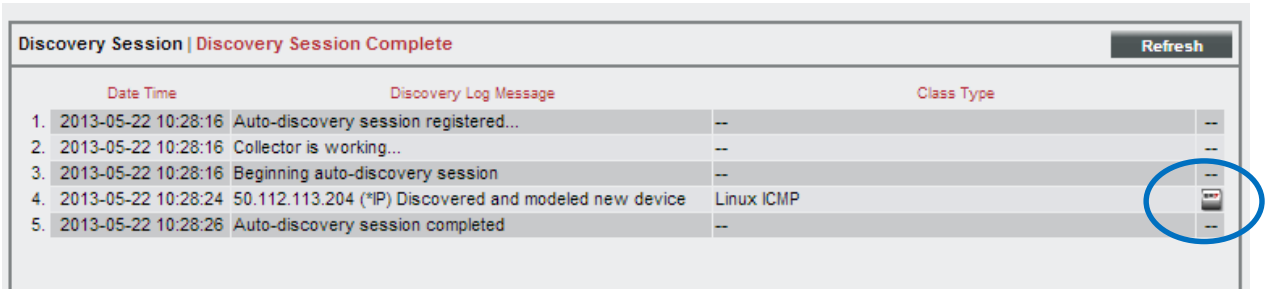
In this chapter we will create a PagerDuty device, and manually align the PagerDuty Synchronization and Performance Dynamic Application. The Synchronization and Performance Dynamic Application provided by ScienceLogic will provide near-real time performance data regarding your PagerDuty service, as well as synchronize changes emanating from PagerDuty.

Create PagerDuty Device

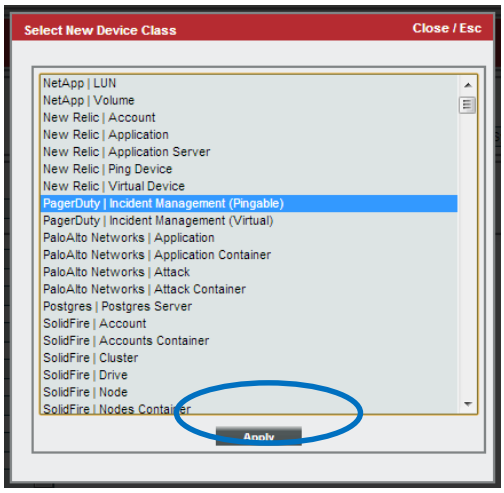
Although the PagerDuty Dynamic Application may be aligned to any ScienceLogic device, we this section will walkthrough creating a dedicated PagerDuty device. Navigate to the Discovery Console Panel by clicking on System > Manage > Discovery. Create a new discovery session to discover a pingable device, setting the IP address to the desired location. Next select "Discover Non-SNMP" devices, and when complete select Save.

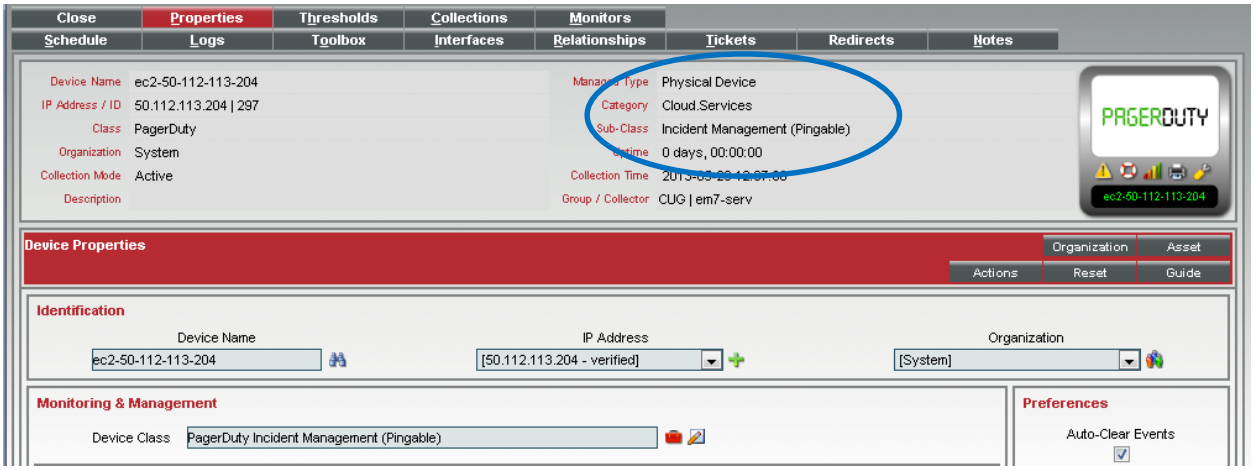


Run the discover session by clicking on the lightning bolt icon. In the Discover Session modal, the device will be modeled as a standard Linux device.



Click the device icon to edit the device properties. On the device properties page, click the red toolbox icon to change the device class. Select “PagerDuty | Incident Management (Pingable)” device class, then select Apply.

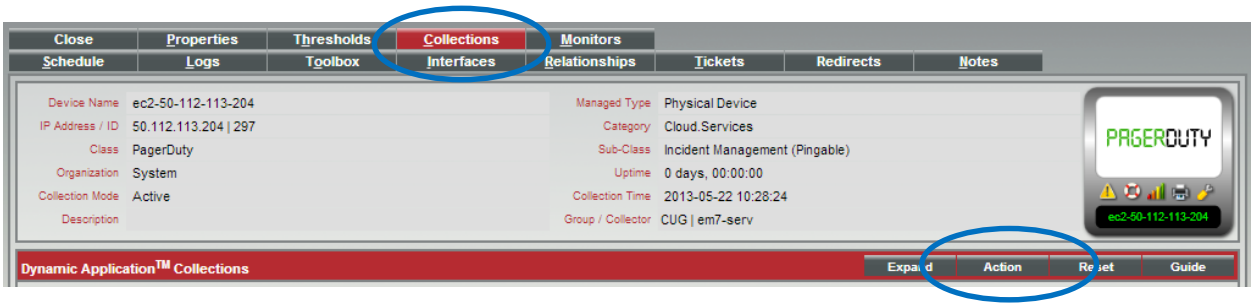




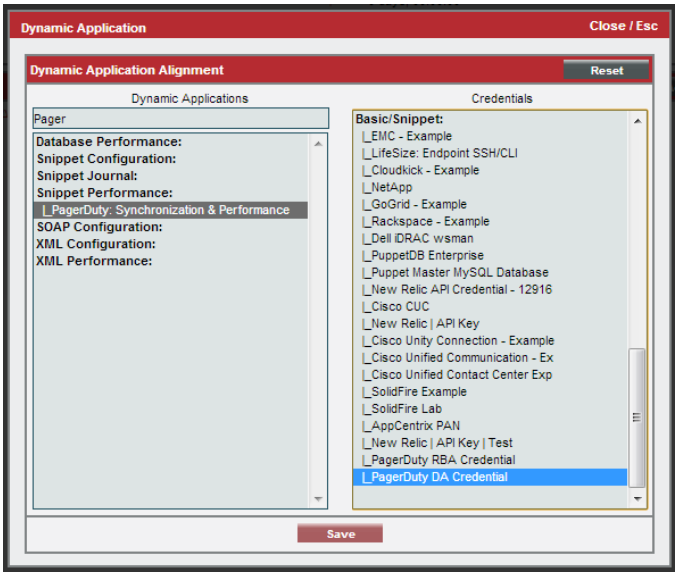
When complete the device icon and device class information will be aligned to PagerDuty.

Align Dynamic Application

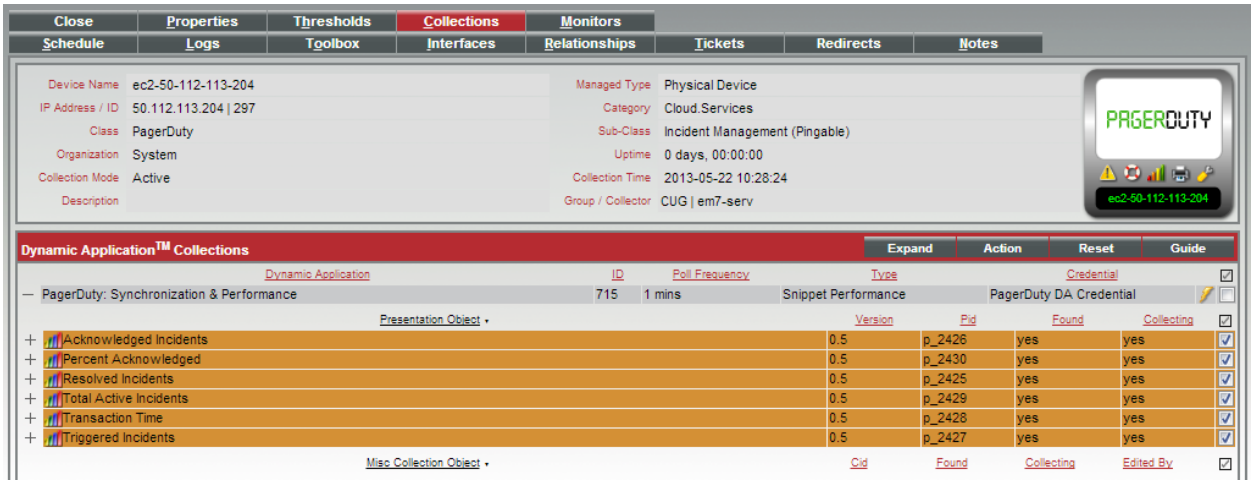
To align the Pager Duty Synchronization and Performance Dynamic Application, click on the Collection tab while in the Device Properties panel.



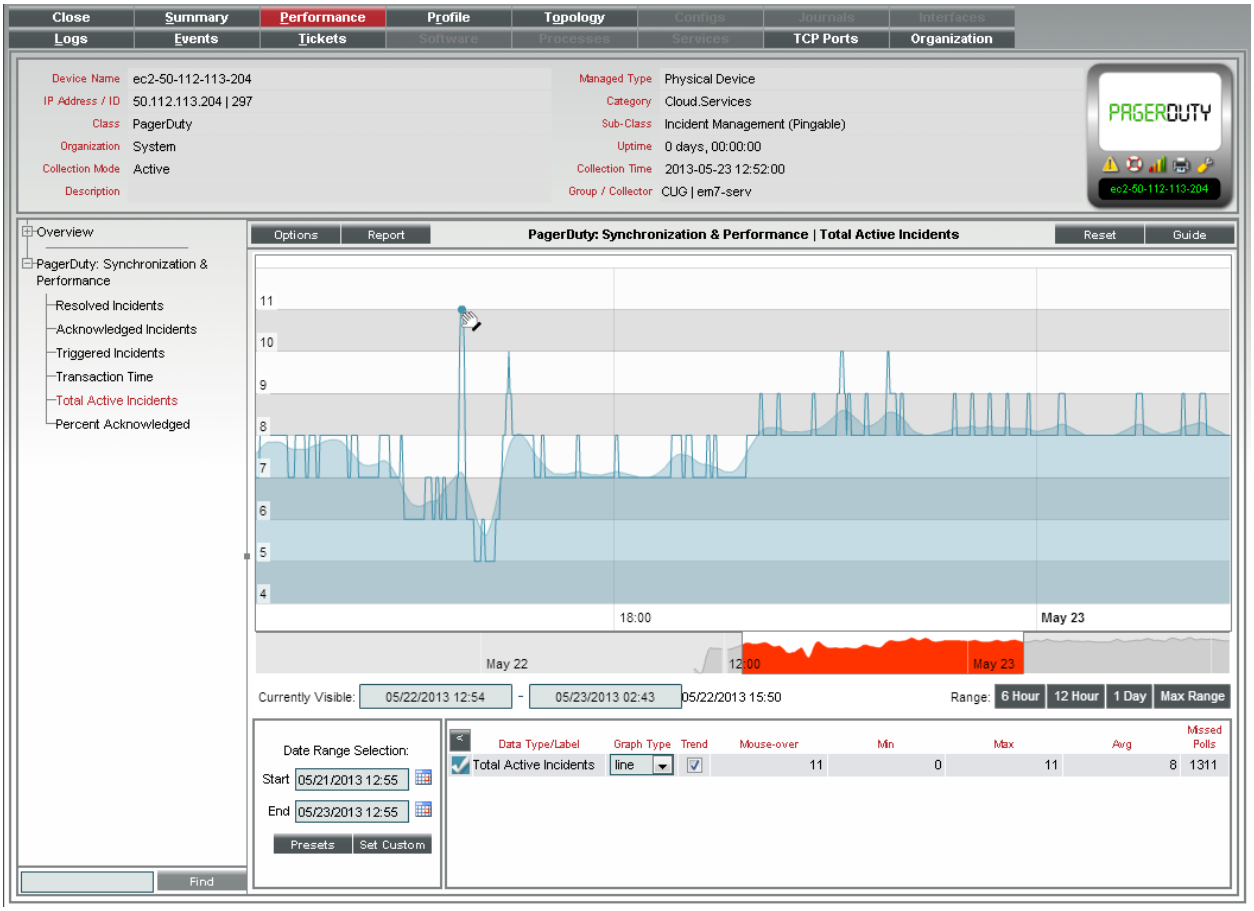
Next, select Action, then Add Dynamic Application. Type "Pager" in the search box, then Select the "PagerDuty" Synchronization & Performance" application. Select the "PagerDuty DA Credential" with the "API Access Key" you created in Chapter 3. Select the Save button to save changes.



Once aligned, the application will take about 60 seconds to populate. By default the application runs every 60 seconds looking for updates to existing ScienceLogic events and updating performance and status data.



The application performance metrics will begin collecting every 60 seconds.



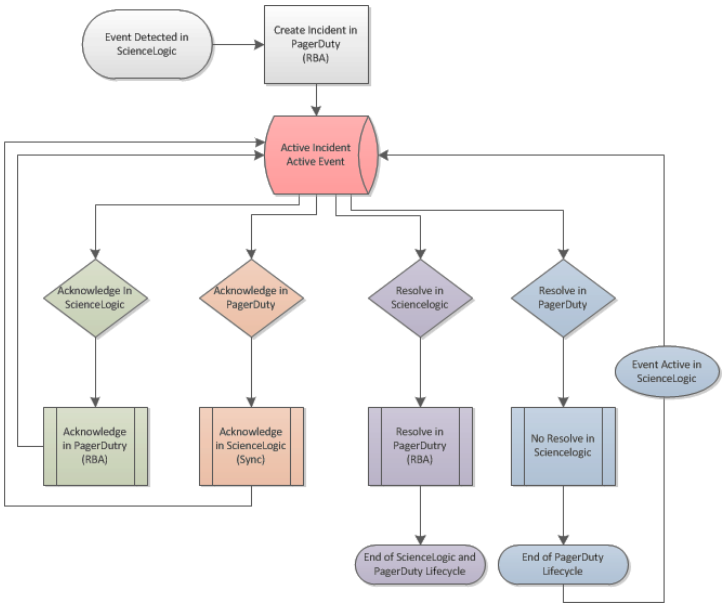
Chapter 6

Using PagerDuty Integration

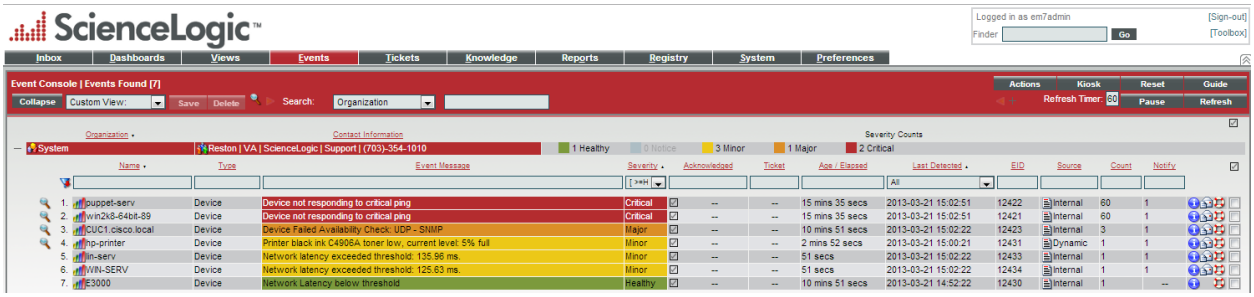
Run Book (Forward Synchronization)

Every ScienceLogic event that matches the PagerDuty Run Book Automation policy will create a new PagerDuty incident. Once an incident is created, notification and escalation policies on the Pager Duty system will go into effect.

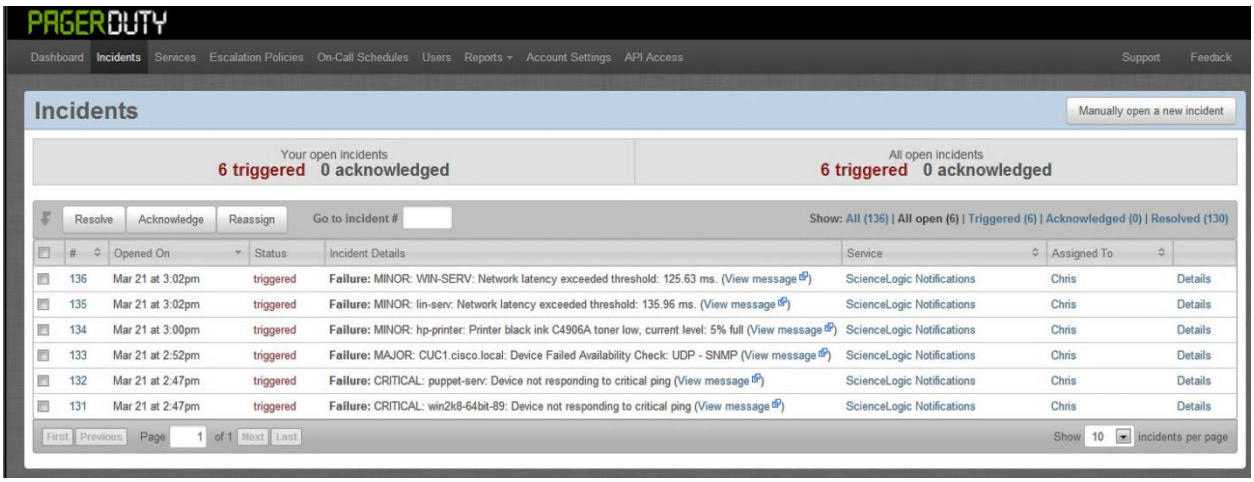
ScienceLogic's Run Book Automation integration is a forward synchronization process, meaning that events and activities emanate from the ScienceLogic system to the PagerDuty service system. Just as new ScienceLogic events will create new PagerDuty incidents, acknowledging or clearing events from within ScienceLogic's event monitor will perform the same function via the PagerDuty API.



Acknowledging incidents from the PagerDuty service portal will only update events in ScienceLogic if the PagerDuty Synchronization and Performance Dynamic Application is configured. If events are auto cleared by ScienceLogic, because either the event has timed-out or the system no-longer detects there's still a problem, events will also be automatically resolved in PagerDuty. The below example shows a ScienceLogic Event Console with several different active events:

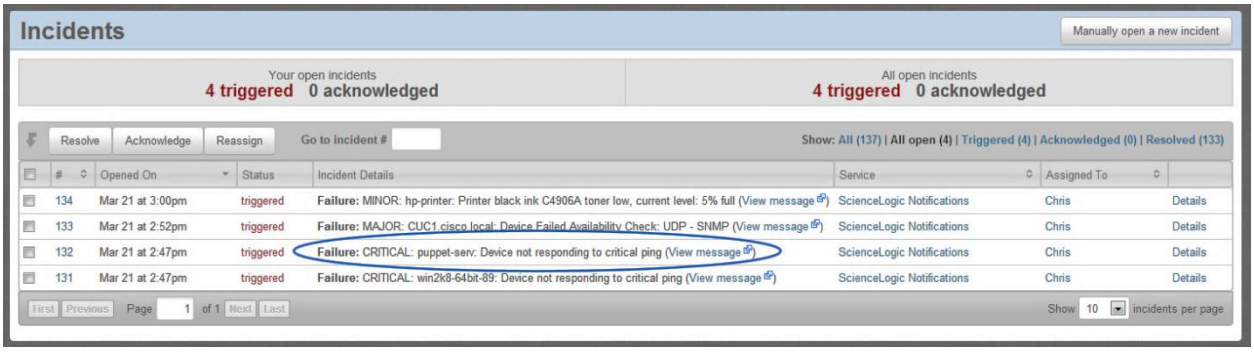


The same events are synchronized in PagerDuty as triggered incidents:

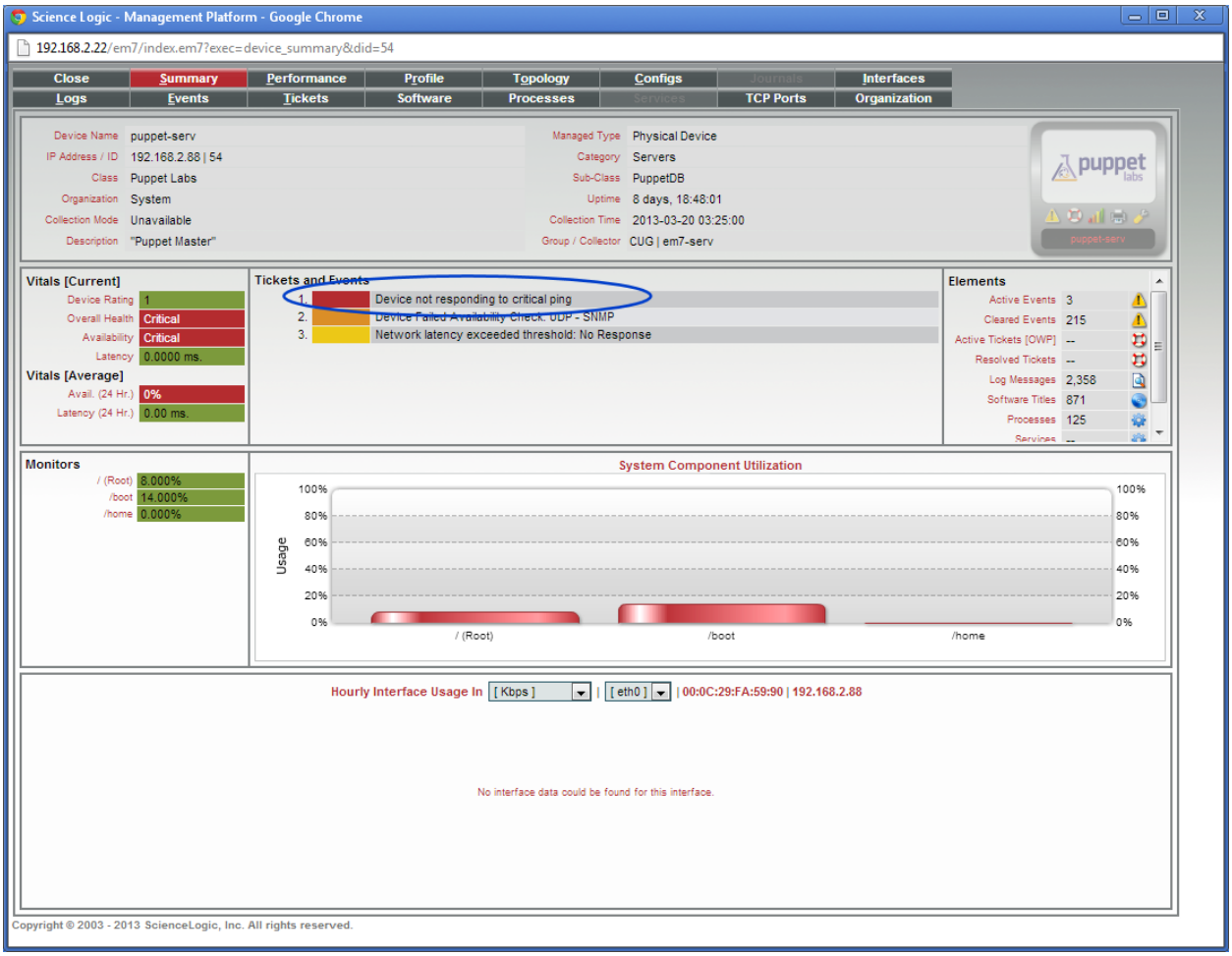


Note: For this example all events are creating incidents in PagerDuty, which is a function of the ScienceLogic Run Book Automation policy and can be adjusted to meet the needs of your business.

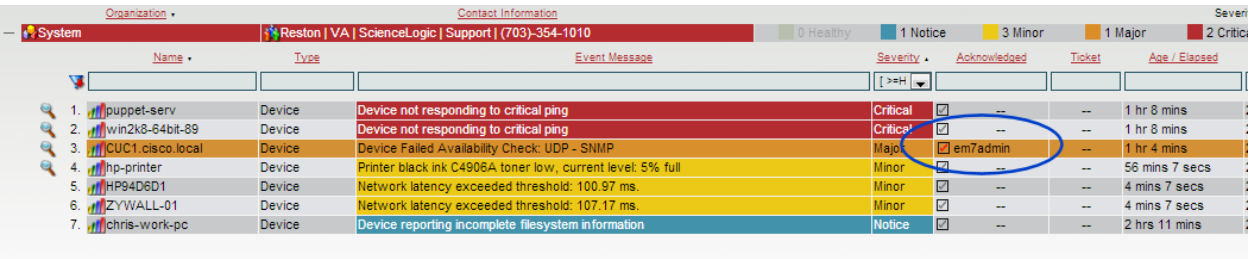
Since PagerDuty requires a unique incident ID to de-duplicate events, ScienceLogic uses the device ID, called the DID, to help eliminate duplicate event storms for a single device. If a device has multiple events, the parent event (usually the highest severity event) will be used for the PagerDuty incident. If subsequent events appear after the initial event correlation process by ScienceLogic (usually time based), the new event will update the PagerDuty incident with the new description. In PagerDuty we can see the primary "critical" event for device "puppet-serv":



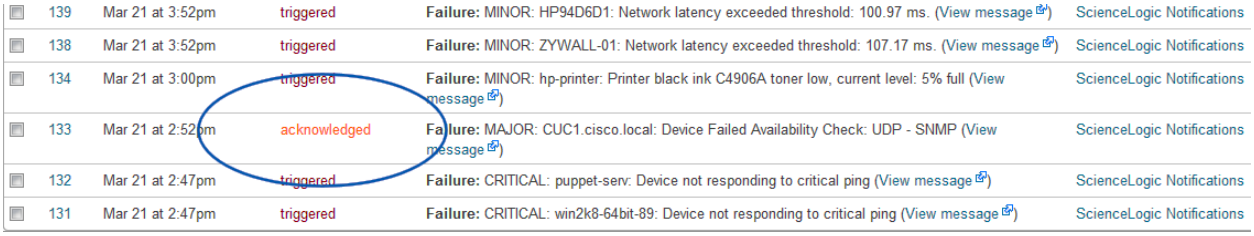
In ScienceLogic we can see several events for device “puppet-serv”:



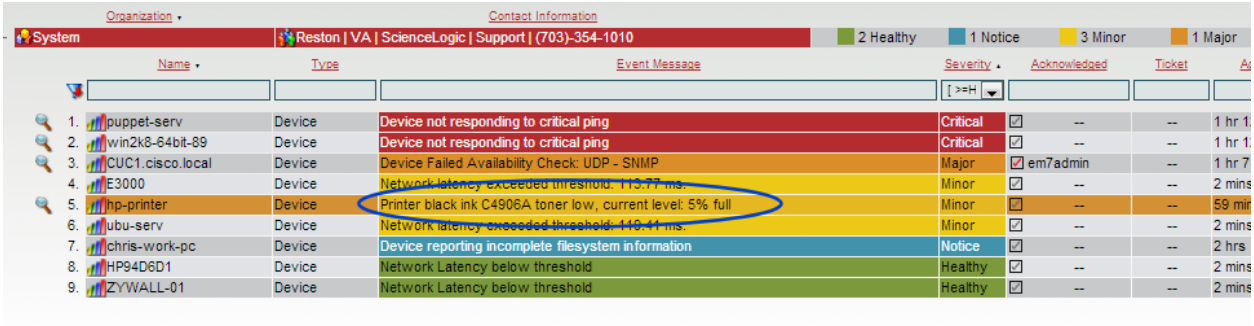
When events are acknowledged in ScienceLogic, the acknowledged status will be synchronized to PagerDuty. This process can take up to 60 seconds.



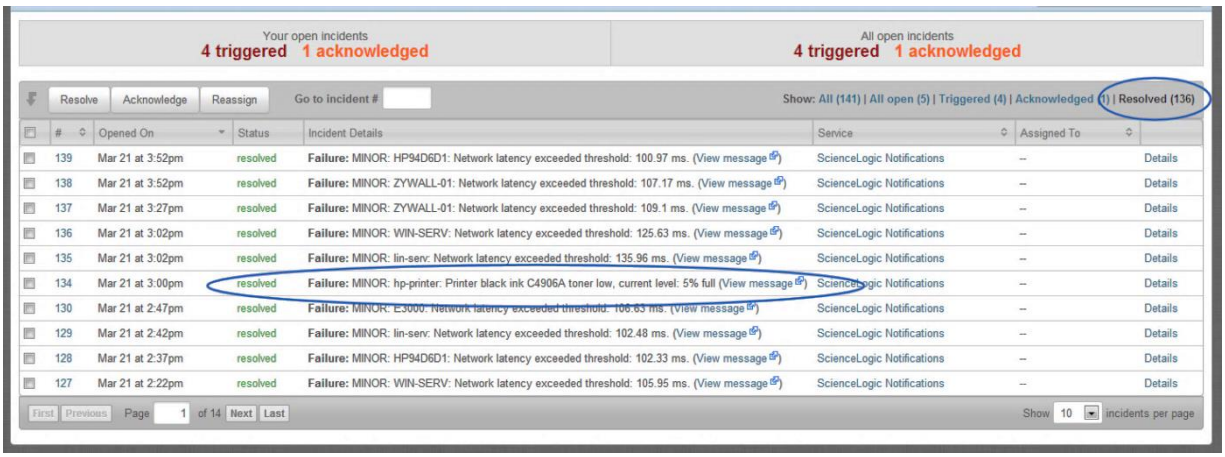
Once synchronized the status of the PagerDuty incident is updated. Resolving an event in the ScienceLogic event monitor also updates the status of the Incident in PagerDuty.



Note the below event which once resolved is also cleared in PagerDuty.

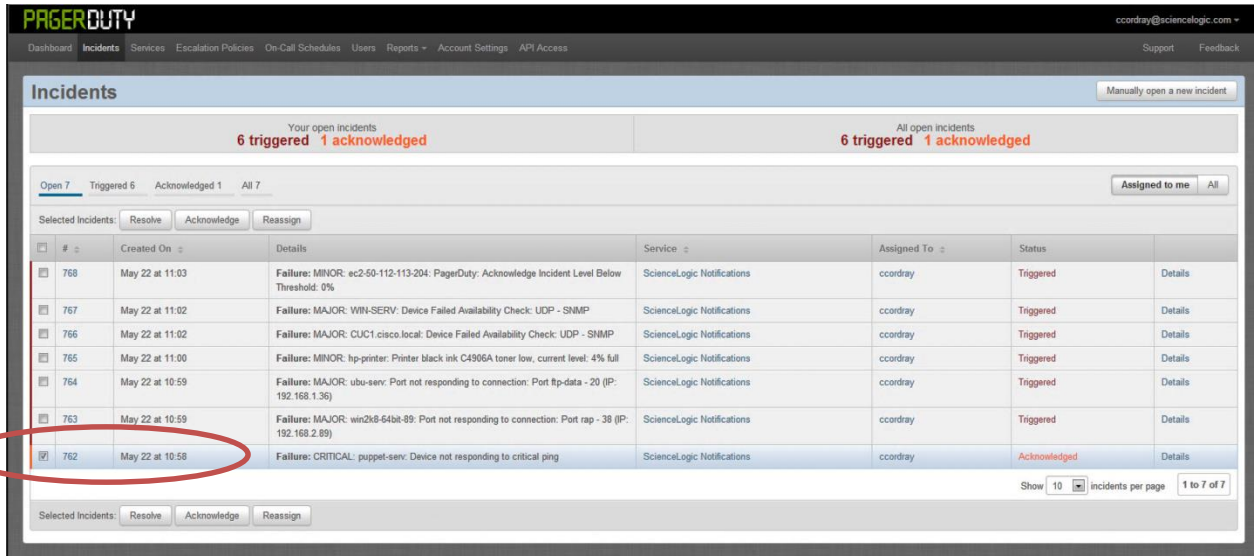


In PagerDuty, the incident is removed, but can be found by clicking the “Resolved” link.



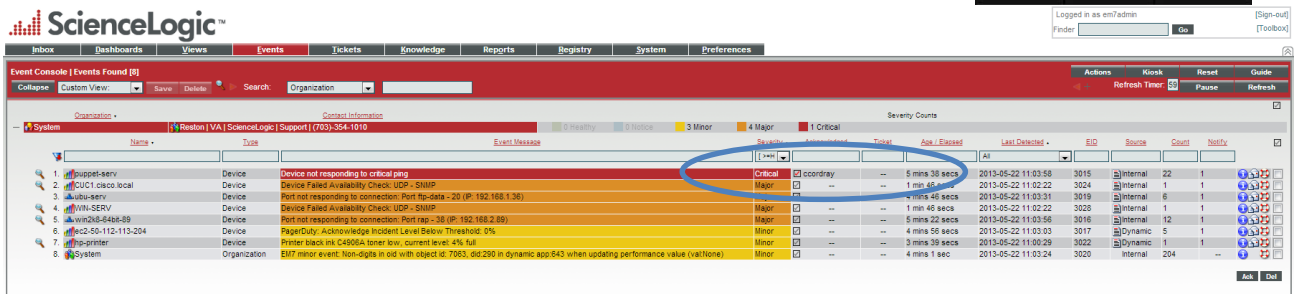
Acknowledging in PagerDuty (Reverse Synchronization)

Incidents that are acknowledged in the PagerDuty portal or Smart Phone applications will synchronize back to ScienceLogic if the PagerDuty Dynamic Application has been installed.



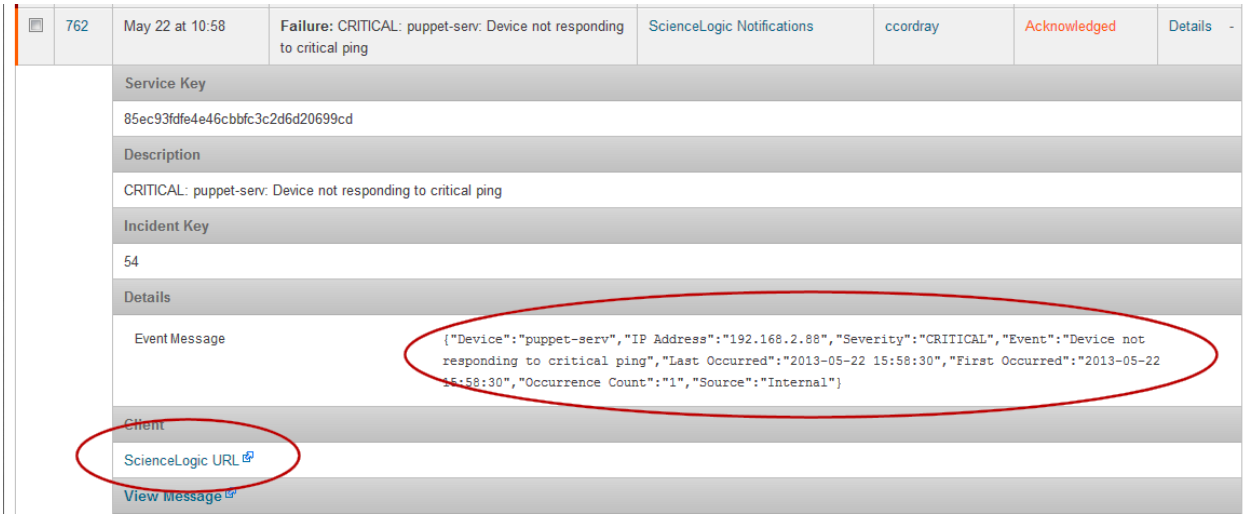
By default, synchronization can take up to 60 seconds, however users can change the frequency be editing the Dynamic Application properties. In order to maintain continuity of user assignment, ScienceLogic matches the PagerDuty assigned username to the ScienceLogic username. If there is a match ScienceLogic events will be updated to matching PagerDuty incidents. If no username can be found, no updates will be made.

For instance, if the username in ScienceLogic is "jdoe", the same username must exist in PagerDuty for the reverse synchronization process to update events in ScienceLogic. The primary reason for this is because of ScienceLogic uses advanced auditing and change control process that must know which user account is acknowledging events.



PagerDuty Interface

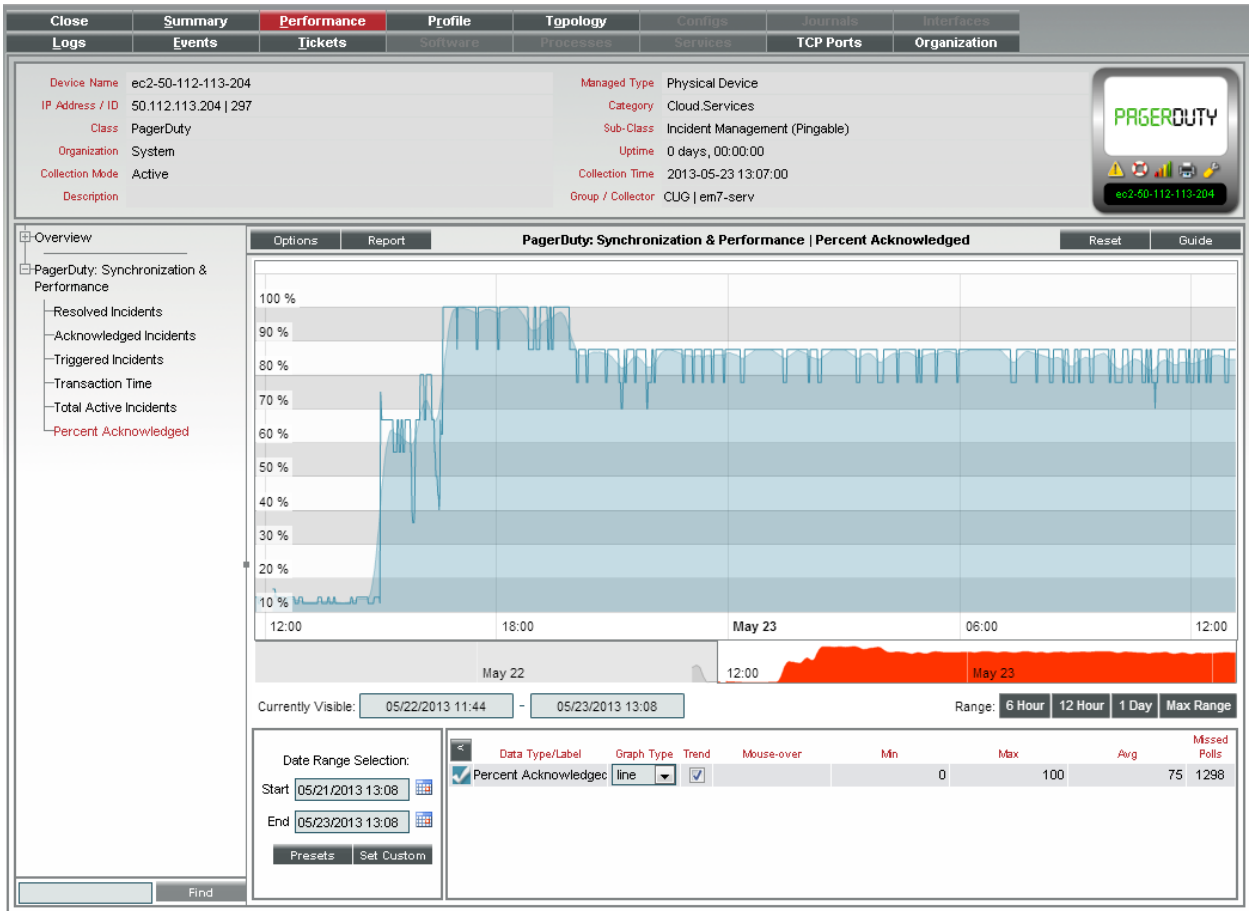
In PagerDuty, any ScienceLogic created incident will have additional notes and details about the event. The details include information about the device, including the last occurrence, severity, and IP address. Users can also navigate from PagerDuty to ScienceLogic by clicking the Client URL link.



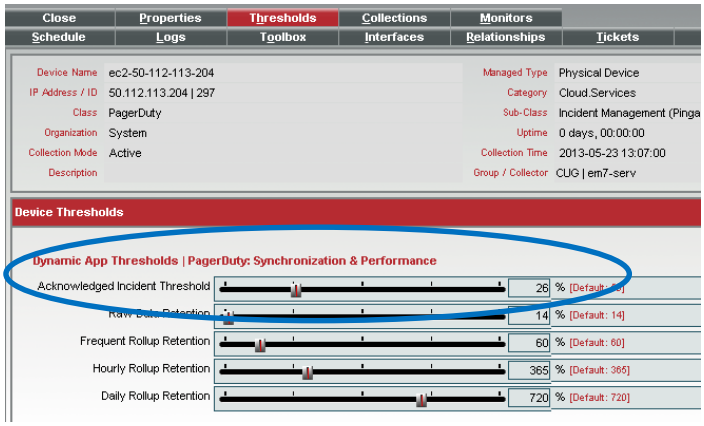
Performance Metrics and Dashboard

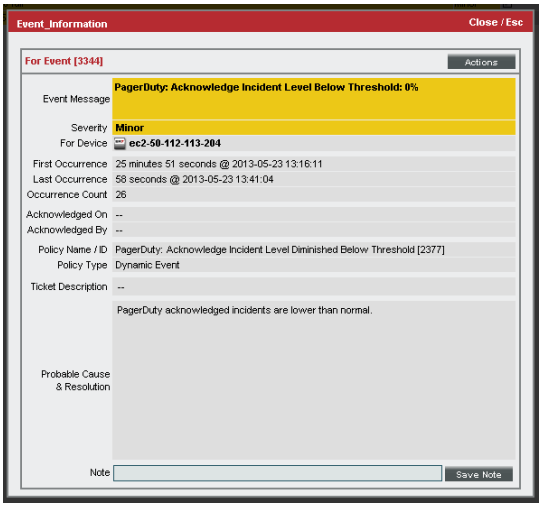
If the "PagerDuty Synchronization & Performance" Dynamic Application is installed, users can see several different performance metrics. Those include:

- Number of Resolved Incidents
- Number of Acknowledged Incidents
- Number of Triggered Incidents
- Transaction Time of PagerDuty API Requests
- Number of Active Incidents (Acknowledged + Triggered)
- Percentage of Acknowledged Incidents



In addition to the above performance metrics, the "Percentage of Acknowledged" metric also has an alarm threshold that can be adjusted to meet the needs of your environment. The threshold value can be set on the Device Properties > Thresholds tab.





In addition to performance metrics and alerts, the

ScienceLogic PagerDuty solution provides an interactive performance dashboard. In the event customers have multiple PagerDuty accounts the dashboard will support multi-tenancy allowing a consolidated view of all PagerDuty performance metrics.

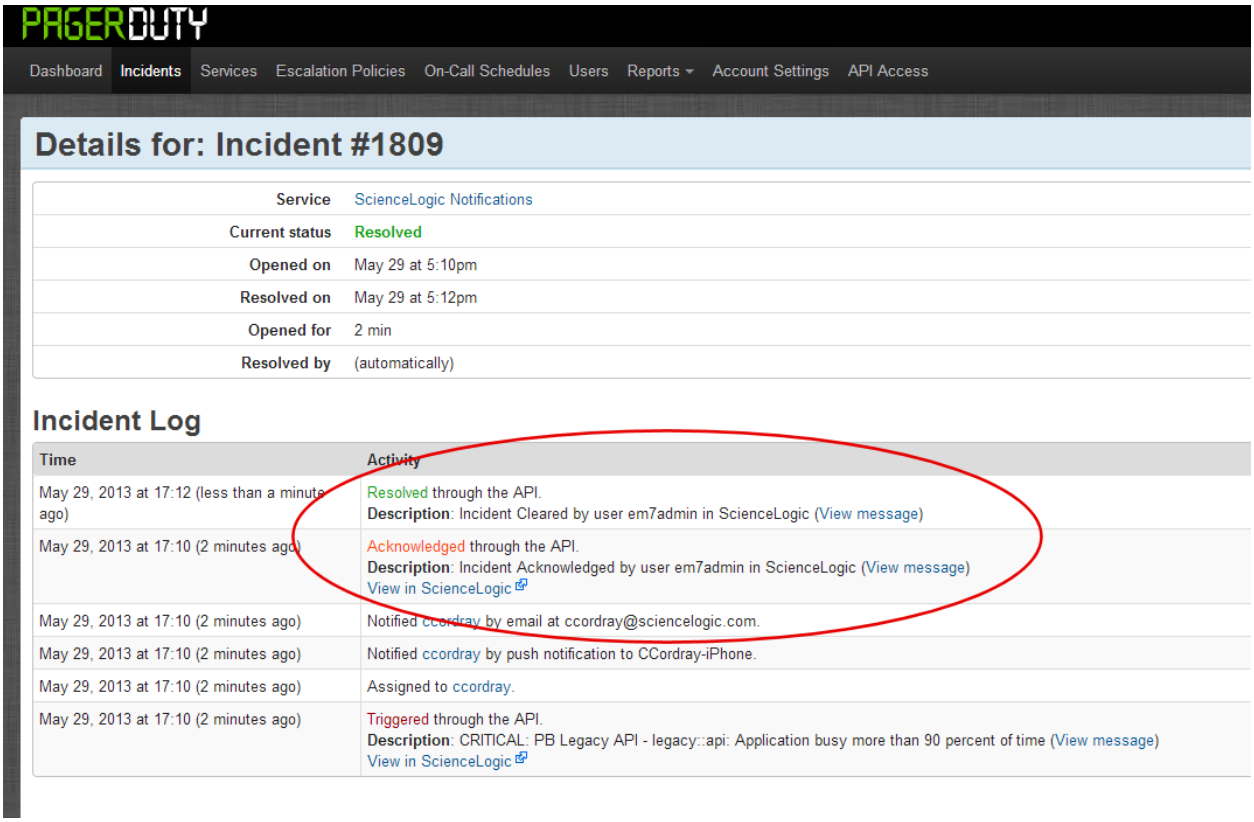
Chapter 7

Advanced Configuration and Troubleshooting

Audit Logging

When an event is acknowledged or resolved in ScienceLogic (event monitor or auto-clear), it runs the matching RBA policy and tells the PagerDuty API to acknowledge/resolve the matching incident. The PagerDuty API does not support any fields to indicate who acknowledged the incident; as a result API acknowledged incidents show up as “Through the API".

Although this is normal behavior, ScienceLogic also provides audit logging of who on the ScienceLogic system acknowledges or resolves an incident. This is available by navigating to the Incident Log of any incident.



Incident Suppression by Device

Incidents in PagerDuty are created (triggered) using a unique ID. This ID is set by ScienceLogic when the Run Book Automation policy creates a new PagerDuty Incident. To help eliminate spurious events, ScienceLogic uses the DID of the device as this ID. The result is that only one PagerDuty incident per ScienceLogic device is created. If there are multiple ScienceLogic events per device, the highest severity event will be used to trigger the RBA policy.

ScienceLogic Only Incidents

Only incidents created by ScienceLogic Run Book Automation policies will be acknowledged and resolved by ScienceLogic. Other incidents in PagerDuty will not be impacted.

The Synchronization & Performance Dynamic Application does report on the total number of incidents (triggered/acknowledged/resolved) across all types of incidents for a given account. In other words, if an incident was not created by ScienceLogic, it will still be represented in the performance metrics.

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

International: +1-703-354-1010