

Cisco DNA Center Alerts Integration Guide

First Published: 2022-08-04

PagerDuty and Cisco DNA Center Integration

Cisco Digital Network Architecture offers centralized, intuitive management that makes it fast and easy to design, provision, and apply policies across your network environment. The Cisco DNA Center GUI provides end-to-end network visibility and uses network insights to optimize network performance and deliver the best user and application experience. The Cisco DNA Center events framework provides reliable notifications to help detect and correct infrastructure problems.

PagerDuty is an incident management platform that provides reliable notifications to detect and correct infrastructure problems. For information about PagerDuty, see https://www.pagerduty.com/.

The integration between Cisco DNA Center and PagerDuty enables the delivery of event notifications to PagerDuty. The integration enables IT organizations to subscribe to network issues identified by Cisco DNA Center and send notifications to PagerDuty. Customers have a real-time network issues view on the PagerDuty platform, which improves issue resolution and increases network uptime.

Support

To submit a service request, visit Cisco Support.

How the Integration Works

PagerDuty integration with Cisco DNA Center is accomplished using the PagerDuty Events REST APIs and the Cisco DNA Center Events Framework.

For more information about the Cisco DNA Center Events Framework, see the *Cisco DNA Center Platform User Guide* for your Cisco DNA Center release.

For information about the PagerDuty Events APIs, see https://developer.pagerduty.com/docs/events-api-v2/ overview/.

Requirements

PagerDuty integrations require a Cisco DNA Center Admin base role for account authorization. If you do not have this role, contact an admin or account owner within your organization to configure the integration.

Integration Walkthrough

You can configure a Cisco DNA Center platform event notification to appear in PagerDuty as an alert. Complete the following steps to configure a Cisco DNA Center event notification so that it appears in PagerDuty.

Before you begin

Ensure that you have PagerDuty running on a system that you will integrate with Cisco DNA Center platform. Refer to your PagerDuty documentation for instructions on setting up PagerDuty.

You must have the appropriate permissions to perform the tasks as described in this procedure. For information about role-based access control for the Cisco DNA Center platform, see the *Cisco DNA Center Administrator Guide*.

Procedure

Step 1	In the Cisco DNA Center GUI, click the menu icon (\equiv) and choose Platform > Developer Toolkit > Events .									
Step 2	In the E	vents window, review the events table.								
	Note	You can adjust the events that are displayed in the GUI by entering a keyword in the Find field.								
Step 3	Review	the data on an individual event within the table.								
	The foll	owing Events data is provided:								
	• Eve	ent ID: Identification number for the event.								
	• Na	me: Name of the event (link).								
	If y Det	If you click this link, the Name slide-in pane opens for the event. The Name slide-in pane has Events Details and Active Subscriptions tabs.								
	• Description : Brief description of the event.									
	• Type: Network, App, System, Security, or Integrations type of event.									
	• Cat	Category: Error, Warn, Info, Alert, Task Progress, Task Complete.								
	• Sev	verity: 1 through 5.								
	Not	e Severity 1 is the most important or critical priority and should be assigned for this type of an event.								
	• Status : Subscription status (whether a user has subscribed to the event). If subscribed to an event, a line appears in this column to the Active Subscriptions tab.									
Step 4	Click a I	Name link to open an event subscription slide-in pane.								
Step 5	Review	the data displayed in the event subscription slide-in pane.								
	The foll	owing Event Details tab data is displayed:								
	• Des	scription: Brief description of the event and how it is triggered.								
	• Eve	ent ID: Identification number of the event.								
	• Ver	rsion: Version number of the event.								
	• Na	mespace: Namespace of the event.								
	The	e default value for all of the events is ASSURANCE.								
	• Do	main: REST API domain to which the event belongs.								

- Sub Domain: Subgroup under the REST API domain to which the event belongs.
- Type: Network, App, System, Security, or Integrations type of event.
- Category: Error, Warn, Info, Alert, Task Progress, Task Complete.
- Severity: 1 through 5.
- **Note** Severity 1 is the most important or critical priority and should be assigned for this type of an event.
- Cisco DNA Event Link: Event broadcast using REST URL.
- Note: Additional information about the event or to help understand the event.
- Tenant Aware: Whether the event is tenant aware or not.
- Tags: Tags indicate what Cisco DNA Center component is affected by the event. The default value for tags is ASSURANCE with more syntax for the specific Assurance issue.
- **Supported Endpoints**: What endpoint types are supported for the event notifications. The following endpoints are supported:
 - REST API
 - Syslog server
 - Email
 - SNMP trap

• Model Schema: Presents model schema about the event:

- Details: Example of model schema detail for the event.
- **REST Schema**: REST schema format for the event.
- **Step 6** Click the **Active Subscriptions** tab.

The following Active Subscriptions tab data is displayed:

- Broadcast Methods: Email, REST API, or SNMP trap.
- Count and Instances: Number of instances of notifications for emails, REST APIs, or SNMP traps.
- **Note** After subscribing to an event, click the subscription count under **Count and Instances** to edit or unsubscribe from the active subscription. After clicking the individual subscription count, click **Unsubscribe** to unsubscribe or **Edit** to further edit it. For multiple subscriptions, you must unsubscribe from each subscription one at time. The ability for multiple subscribing or unsubscribing is not supported using the GUI.
- Actions: Either unsubscribe or edit the active subscription.
- **Note** After subscribing to an event, a **Try It** button appears in the **Active Subscriptions** tab. Click this button to run an event simulation.

- **Step 7** Click the **Subscribe** button to add this event to your active subscription of events. For a *PagerDuty subscription*, configure the following fields:
 - Name: Name of the event.
 - Subscription Type: PagerDuty.
 - Select an existing endpoint: Select the subscription endpoint.
 - Create a new endpoint: Enter a new Endpoint Name and Endpoint Description.

Enter values for the following fields:

- PagerDuty Events API URL
- PagerDuty Integration Key
- PagerDuty Events API Version

Click Subscribe to save and enable the subscription.

Step 8 Review your subscriptions in the **Active Subscriptions** tab.

The following information is provided for a subscription:

- Broadcast Method: Email, REST API, or SNMP trap notification.
- Counts and Instances: Number of instances of notification.

Click the Unsubscribe and Edit links to unsubscribe or edit the subscription.

- Actions: Actions taken for the events.
- **Note** You can adjust the subscriptions that are displayed in the GUI by clicking the **Filter** icon and using the filter, or entering a keyword in the **Find** field.

What to do next

Access PagerDuty to review the events.

The Cisco DNA Center events will appear in PagerDuty as alerts within the PagerDuty **INCIDENTS** window. You can review and mark the alert as **Resolved** in this window.

Integration Workflow Test

Figure 1: Cisco DNA Center-to-PagerDuty Integration



Figure 2: Create a PagerDuty Integration





Figure 3: Create a New PagerDuty Service (1 of 6)

Figure 4: Create a New PagerDuty Service (2 of 6)

agerDuty	Incidents Services	People Automatio	n Analytics	Integrations	Status	Q Search		0	e	1	
Service D A service in Page Usually it's some Services Mainte	Service Directory Service in PagerDuty represents a component, microservice or piece of infrastructure a team operates, manages, and monitors. Usually it's something you'd go on call for. Learn more about the service directory.										
Q Search for a	Q. Search for a service by name or description										
TEAM All Teams 1 total services	BUSINESS SERVICE Any business s	ervices -	ENT SC	↓ Service name	ə (A − Z) ▼		1. Add New Serv	vice			
Webb Servic	nook_Integration se for Webhook Receiver to se	and alerts	TEAM No team is a the <mark>Basic Es</mark> Policy escal	assigned to scalation lation policy.	ON CALL NOW Gabriel Zapodeanu	LAST INCIDENT Oct 5 at 5:53 PM	OPEN INCIDENTS O triggered O acknowledged	More *			

Figure 5: Create a New PagerDuty Service (3 of 6)

PagerDuty	/ Incidents	Services	People	Automation	Analytics	Integrations	Status		۹ ۵	Search			0	ŧ	Ą
	Create a S	Service													
	1 Name —	2 Ass	ign ——	3 Reduce	Noise —	- 4 Integra	ations								
	Name and Description														
	A technical service reflects a discrete piece of functionality that is wholly owned by one team. One more technical services combine to deliver customer-facing or business capabilities.												_		
	Example names of technical services									1. Name	e the new se	ervice	9		
	 Payment Proces Checkout App S Inventory Datab 	ssing • Cre Server • Acc base • Sea	ate Account ount Authen	tication						2. Desci 3. Next	ription				
	Name*											-	-		
	DNAC_Notification	s						1							
	Tip: Avoid using Pager	Duty or Alerts in the	service name a	as this will appear in	the notification										
	Description														
	This Service will be	used for the Cisco	DNA Center n	otifications channe	əl			2							
3	Next Can	cel													

Figure 6: Create a New PagerDuty Service (4 of 6)

PagerDuty	Incidents	Services	People	Automation	Analytics	Integrations	Status		C	& Search	0	ť	0
	Create a S	ervice	ian	3 Deduce	Noise	A Integr	ations						
	Assign an Escalation Policy Generate or assign an Escalation Policy to this service. Escalation Policies connect services to individual users and/or schedules and they ensure the right people are notified at the right time.												
	 Generate a new Escalation Policy Create a new Escalation Policy for this service where you will be the default on-call. The Escalation Policy can be updated at any time after you create the service. 						1. Select the escalation policy 2. Next	2					
	Select an existence of the second	sting Escalatio	n Policy				×	1					
2	Next Cano	cel											

Figure 7: Create a New PagerDuty Service (5 of 6)

Ale	rt Grouping		
Com	bine similar alerts into a single incident to reduce not	ification noise and provide	
	latellizent a sta	_	
۲	Intelligent Recommended Intelligently based on alert content and past groups.	1	1 Alert grouping selection
0	Content-Based When contents of specified alert fields match.		2. Next
0	Time-Based For a selected duration.	2 minutes 💌	
0	Turn Off Alert Grouping		

Figure 8: Create a New PagerDuty Service (6 of 6)

learch for an integra	ation(s)			~		
ur selections (1)					
☑ _						
P						
Events API V2						
ost popular int	egrations					
0	aws	splunk>	Nagios	ZABBIX		
Prometheus	Amazon CloudWatch	Splunk	Nagios	Zabbix		
					1.	Select Events API v
					2.	Create Service
DATADOG	solarwinds	New Relic	System Center Operations Manager	Microsoft Azure		
Datadog	SolarWinds Orion	New Relic	Microsoft SCOM - Email	Microsoft Azure		
AlertSite UXM	pingdom	fx	<u>×</u>			
	Disadam	SignalEx	Empil			

Figure 9: Save the Integration Key and URL

ş

gerDuty	Incidents Services People Autom	nation Analytics Integ	rations Status		Q Search	0	ff
SERVICE DIRECTOR	W > DNAC_NOTIFICATIONS > INTEGRATIONS						
DNAC_No	otifications 🖌 Edit					+ New Incident	More -
This Service will b	be used for the Cisco DNA Center notifications cha	annel					
STATUS	ON CALL NOW	ESC	ALATION POLICY	TEAM	Save the		
No open incidents Cabriel Zapodeanu Basic Escalation Policy				No team is assigned to the Basic Escalation Policy escalation policy.	1. Integration key		
Activity Integr	ations Settings Service Dependencies	d an integration					
€ Events AP	IV2	d un integration.			No Test Alert Received		
Events A	API v2 Overview			Integration Name			
The Events API	v2 is a highly reliable, highly available asynchrono	ous API that ingests machin	e events from monitoring tools and	Events API V2	1		
other systems systems. Event	like code repositories, observability platforms, aut is sent to this API are ultimately routed to a Pager	omated workflow tools, and Duty service and processed	configuration manage	Integration Key 参示序成本印刷研	0		
Event Type	es			Integration LIDI (Change Events			
The Events API	v2 can ingest multiple types of events. Each even	t type is described below.		https://events.pagerduty.com/v2/cha	ange/enqueue		
Event Type	Description	Example Events	Notifications can be sent?	Integration URL (Alert Events)			
	A problem in a machine monitored system.	High error rate		nups//www.s.pagerouty.com/v2/end	fonce		

Figure 10: PagerDuty Integration Details

PagerDuty DEVELOPER PLATFORM		Search Q	API References	Documentation	Community	GET STARTED
Introduction Tools & Libraries ~ API Client Libraries API Tools & Code Samples	Send an A	Alert Ev	ent :	PagerDuty Commo messages Timestamp format Use Integration Ke Notifications sent t	n Event Format (l ted ISO 8601 y in API request p to events queue /	PD-CEF) Dayload API endpoint:
PagerDuty On-Prem Agent Retrieving Incident Details Build Apps & Integrations ~	https://events.pr	agerduty.com/v	2/enqueue	nttps://events.pag	EYENT Acti Event Acti Example R Response:	inqueue on Behavior tequest Payloa s and Limits
App Overview Developer Account FAQ	Parameters				Context Pr Try it Out	roperties
Register an App App Functionality Overview API Pickers Events Integration Functionality	PARAMETERS routing_key Required	TYPE	DESCRIPTION This is the 32 chara an integration on a ruleset.	acter Integration Key for service or on a global		
Writing App Event Transformers OAuth 2.0 Functionality	event_action Required	String	The type of event. acknowledge or r	Can be trigger , resolve .		
OAuth 2.0 Authorization Code Grant Flow OAuth 2.0 PKCE Flow Publish an App	dedup_key	String	Deduplication key f and resolves. The r length of this prope	for correlating triggers naximum permitted erty is 255 characters.		

gerDuty Incidents Services People Automation Analytics Integrations Status	Q Search	
Gabriel Zapodeanu		View Audit Trail Reporting
Contact Information Notification Rules User Settings Permissions & Teams On-Call Shifts Subscriptions		You're always on-call
When someone invites me to respond to an incident Notify me according to my high urgency notification rules. To learn more about being added to an incident as a responder, read our guide.		You are always on-call for ∞ All Engineers Esca L1
When a high-urgency incident is assigned to me	යි එ x	Teams Gabriel Zapodeanu is not a member of any teams
Solution So	ය පැ * රේ එ ¥ රේ එ ¥	Resources Why isn't my phone being recognized under Contact Methods?
When a high-urgency incident assigned to me changes Add Notification Rule teams, on-call sched	, the PagerDuty configuratio Jules, notification, and escala	n of people, ation rules.
When a low-urgency incident is assigned to me		1899
] Immediately after it's assigned to me, push notify me on Gabi's iPhone	<i>ලි සි</i> ≭	
Immediately after it's assigned to me, sms me at +1 503-309- (Other)	C 4 ×	

Figure 11: Notifications and Escalation Rules

Figure 12: Subscribe to Events (1 of 2)

≡ Cisco	DNA Center Step 1 - Select Site and Events Pick the site and events for your notification Select a site Gobal/CO × Global/NY × Global/OR ×	Create a New Notification 1. Select the sites 2. Select the events 3. Next	Q (O) (O) (Q)
	Q Search Table		∇
	1 Selected		
	Event Name *	Channels Supported	
	High input/output Utilization on Switch Interfaces	REST SYSLOG EMAIL WEBEX PAGERDUTY	
	High input/output utilization on Switch WAN interfaces	REST SYSLOG EMAIL WEBEX PAGERDUTY	
2	Interface Connecting Network Devices is Down	REST SYSLOG EMAIL WEBEX PAGERDUTY	
	Interface Flapping On Network Device	REST SYSLOG EMAIL WEBEX PAGERDUTY	
	ISE AAA trust establishment failure	REST SNMP SYSLOG EMAIL WEBEX PAG	BERDUTY
		Showing 200 of 200	
Exit		3	Next

Figure 13: Subscribe to Events (2 of 2)

≡ Cisco DNA Center		Create a New Notification		Q @ @ 4
Step 2 - Select Cha Choose the notification channels	nnels			
	P •			• W
EMAIL Send an Email notification Supported Events (1/1)	PAGERDUTY POST Cisco DNA Center Event Notifications to Pagerduty Supported Events (1/1)	REST Send the data via HTTP push API Supported Events (1/1)	SYSLOG Send data to a Syslog server Supported Events (1/1)	WEBEX POST Clisco DNA Center Event Notifications to WEBEX Supported Events (1/1)
	1. 2.	Select PAGERDUTY noti Next	ification channel	
Exit				Back Next

Figure 14: Configure PagerDuty Destination (1 of 2)

≡ Cisco DNA Center	Create a New Notification	Q @ @ 4
Step 3 - PAGERDUTY Settings Configure the PAGERDUTY channel settings for this notification SERVICE CONFIGURATION C Select Existing Instance PagerOury_DNAC_Notifications PagerOury_DNAC_Notifications PagerOury Events API URL* https://events.pagerduty.com/v2/engueue 2 PagerOury Events API URL* Lacov	 Create new instance Instance name PagerDuty Integration Key Next 	
Exit	Bac	k 4 Next

	Create a New Notification	Q @ @ A
Step 4 - Name and Description Provide a name and short description for your notification Name* PagerDuty Interface Down Description* Lib PagerDuty Notification 2	 Notification name Notification description Next 	
Exit	Back	3 Next

Figure 16: Review the New PagerDuty Event Notification

=	Cisco DNA Center	Create a New Notification	Q (Ø . (@ .). -
	Summary		
	Review your notification and make	any changes. If you are satisfied, select $\ensuremath{^*}\xspace$ Finish $\ensuremath{^*}\xspace$ to complete this workflow	
	v Name and Description Edit	t	
	Name	PagerDuty Interface Down	
	Description	Lab PagerDuty Notification	
	 Site and Events Edit Sites (3) 	Global/OO Global/NY Global/R	
	Events (1)	Interface Connecting Network Devices is Down	
	V PAGERDUTY Settings Edit		
	PagerDuty Events API URL	https://events.pagerduty.com/v2/enqueue	
	PagerDuty Integration Key	***********	

Figure 17: PagerDuty Notification Channel



Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL: https://www.cisco.com/c/en/us/about/legal/trademarks.html. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)

© 2022 Cisco Systems, Inc. All rights reserved.