

Prisma SD-WAN ServiceNow CloudBlade Integration Guide

Version 1.4.1

SD-WAN Events Overview	3
Alert and Alarm Attributes	4
Prisma SD-WAN ServiceNow CloudBlade	6
Configure ServiceNow	7
Configure ServiceNow CloudBlade in Prisma SD-WAN	7
Configure ServiceNow Parameters	8
Monitor ServiceNow Status in Prisma SD-WAN	11
ServiceNow CloudBlade Infrastructure	14
Querying for Events	14
Converting Prisma SD-WAN Events to ServiceNow Constructs	15
Incident Creation on ServiceNow	18
Incident Resolution in ServiceNow	19
Managing Incident Impact	19

SD-WAN Events Overview

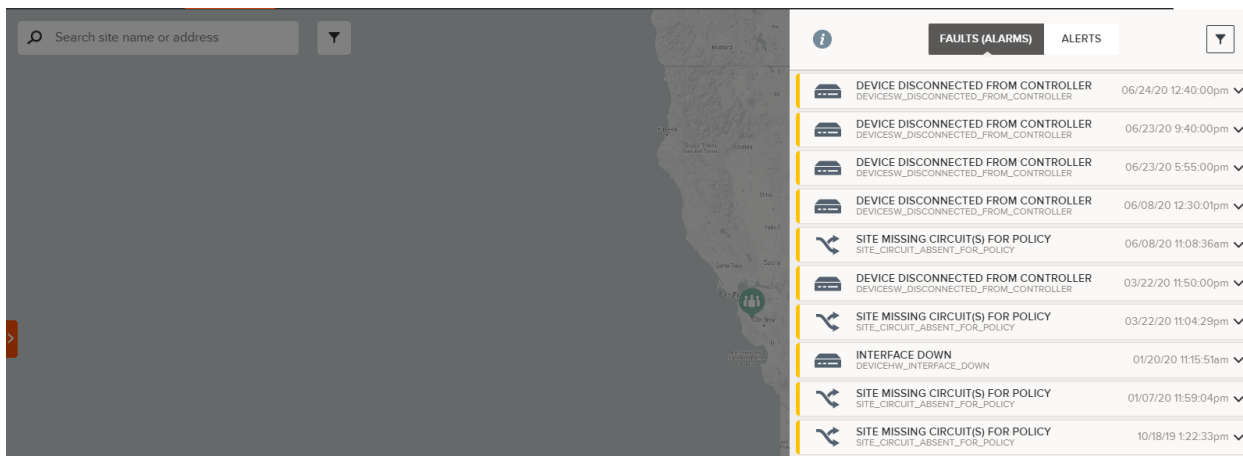
In day-to-day network functioning, many incidents occur that may be a cause for concern. Prisma SD-WAN identifies these incidents that occur in the network and classifies them into two types to determine the type of fault.

An **alarm** is an indication of a fault in the system. Alarms can be raised and cleared, and can be of the following severity:

- Critical – Whole or part of a network is down, and requires immediate action.
- Major – Network is impacted, and needs immediate attention.
- Minor – Network is degraded, and needs attention soon.

An **alert** may or may not be an indication of fault in the network. An alert is raised when system-defined or customer-defined thresholds are reached.

These alerts and alarms can be viewed on the top right corner of the Prisma SD-WAN portal.



Event Type	Event ID	Timestamp
DEVICE DISCONNECTED FROM CONTROLLER	DEVICESW_DISCONNECTED_FROM_CONTROLLER	06/24/20 12:40:00pm
DEVICE DISCONNECTED FROM CONTROLLER	DEVICESW_DISCONNECTED_FROM_CONTROLLER	06/23/20 9:40:00pm
DEVICE DISCONNECTED FROM CONTROLLER	DEVICESW_DISCONNECTED_FROM_CONTROLLER	06/23/20 5:55:00pm
DEVICE DISCONNECTED FROM CONTROLLER	DEVICESW_DISCONNECTED_FROM_CONTROLLER	06/08/20 12:30:01pm
SITE MISSING CIRCUIT(S) FOR POLICY	SITE_CIRCUIT_ABSENT_FOR_POLICY	06/08/20 11:08:36am
DEVICE DISCONNECTED FROM CONTROLLER	DEVICESW_DISCONNECTED_FROM_CONTROLLER	03/22/20 11:50:00pm
SITE MISSING CIRCUIT(S) FOR POLICY	SITE_CIRCUIT_ABSENT_FOR_POLICY	03/22/20 11:04:29pm
INTERFACE DOWN	DEVICEHW_INTERFACE_DOWN	01/20/20 11:15:51am
SITE MISSING CIRCUIT(S) FOR POLICY	SITE_CIRCUIT_ABSENT_FOR_POLICY	01/07/20 11:59:04pm
SITE MISSING CIRCUIT(S) FOR POLICY	SITE_CIRCUIT_ABSENT_FOR_POLICY	10/18/19 1:22:33pm

Alerts and alarms generated in the system are triggered by different types of events, categorized broadly as hardware issues, software issues, device interface issues, device registration issues, peering issues, sitelevel issues, tunnel issues, and application performance issues. These issues, based on the type of event, may originate from the ION device or the controller.

Alert and Alarm Attributes

Each event contains a bunch of attributes that can be used to gain more information on the condition. Depending on the type of event, the attributes that constitute the event differ.

An alarm typically consists of the following attributes:

```
{
  "_created_on_utc": "2021-07-15T05:48:39.121000Z",
  "_etag": 1,
  "_updated_on_utc": "2021-07-15T05:48:39.121000Z",
  "acknowledged": false,
  "acknowledgement_info": null,
  "cleared": false,
  "code": "SITE_CONNECTIVITY_DEGRADED",
  "correlation_id": "6Qeqj3iD",
  "element_id": null,
  "entity_ref": "tenants/1092/sites/16015589439620037",
  "id": "60efcc376534671b7600e09f",
  "info": null,
  "notes": null,
  "policy_info": {
    "policy_applied_time": "2021-07-15T05:48:39.121000Z",
    "policyrule_id": null,
    "policyset_id": "16226851857240070"
  },
  "priority": "p3",
  "severity": "major",
  "site_id": "16015589439620037",
  "suppressed": false,
  "suppressed_info": {
    "event_ids": null,
    "other_reasons": null,
    "summary_event_ids": null,
    "suppressed_time": null
  },
  "time": "2021-07-15T05:10:00.098000Z",
  "type": "alarm"
}
```

ID

A unique ID used to identify an event.

Code

An event code which describes the event.

Correlation ID*

Correlation ID is a system-generated ID for a raised alarm. An Alarm is associated with two states – **raise** and **clear**. At any given time, there can be multiple alarms with the same event code in either a raised or cleared state. Using the Correlation ID, you may distinguish among alarms with the same event code.

When an alarm is cleared, the Correlation ID will indicate that the specific alarm is cleared. This ID will continue to be associated with an alarm, even if the alarm is cleared or resolved.

Time

The time at which this condition was seen or the event was raised/cleared.

Element ID

ID of the device on which this condition was seen.

Site ID

If the device is associated with a site, **site_id** will also be packaged in the event. If not, this attribute is not present.

Type

This field indicates the event type i.e. alert or alarm.

Severity

Severity for alarms are based on the following categories:

- Critical - Whole or part of a network is down, and requires immediate action.
- Major - Network is impacted, and needs immediate attention.
- Minor - Network is degraded, and needs attention soon.

Entity Reference

Entity reference refers to the specific entity where the alarming condition is seen. This string can be used as an API URI to query the entity using the Prisma SD-WAN SDK. In the example above, the **entity_ref** attribute contains information about the element that is disconnected from the controller.

Info

Info sheds more lights on the entity that is causing the alarming condition. It can contain information regarding interfaces, or IP addresses if there is a collision. The value in this field changes depending on the event code.

Notes

The Notes field is used to add remarks/comments to events. You can edit notes for active alarms only.

Priority

This attribute indicates the priority of the event/alarm.

Suppressed

Suppressed is a boolean attribute that indicates if the event is suppressed by the Prisma SDWAN's Event Correlation & Suppression engine.

Suppressed Info

If the event is suppressed, `suppressed_info` contains details about the suppression time and correlated event IDs.

Policy Info

If the event was updated using an event policy rule, the `policy_info` attribute contains details this action through details about the event policy set, event policy rule, and rule application time.

Clear*

This attribute is Boolean and indicates if the event condition still exists or is cleared. A value of True indicates that the condition no longer exists. When an alarm is raised, it is raised with Clear set to False.

Acknowledged*

This attribute is Boolean and indicates if an event has been acknowledged by a user. If acknowledged, the `acknowledgement_info` field contains the time and the user who acknowledged the event.

Note: (*) indicates it is not part of the Prisma SD-WAN alert.

A Prisma SD-WAN alert contains most of these attributes **except** cleared, acknowledged and `correlation_id` as alerts are not standing conditions. Here's a sample alert:

```
{
  "info": {
    "name": "internet 1",
    "circuit_labels": "Budapest-INET-VZ"
  },
  "code": "DEVICEHW_INTERFACE_ERRORS",
  "severity": "major",
  "_updated_on_utc": "2019-12-23T14:04:34.736000Z",
  "site_id": "15282991838450011",
  "id": "5e00c972d7b0fa2f8cb418ce",
  "entity_ref":
"tenants/1083/sites/15282991838450011/elements/15230097588400085/interfaces/15230098062640233"
,
  "correlation_id": null,
  "time": "2019-12-23T14:04:31.395000Z",
  "element_id": "15230097588400085",
  "_created_on_utc": "2019-12-23T14:04:34.736000Z",
  "type": "alert",
  "_etag": 1
}
```

Prisma SD-WAN ServiceNow CloudBlade

The ServiceNow CloudBlade is used to translate events raised on Prisma SD-WAN into incident tickets on ServiceNow. Once a ticket is created in ServiceNow, the IT Operations team can be alerted to check the network condition and take immediate action for remediation, thus making

sure that network SLAs and thereby application SLAs are met. See the following sections to complete the integration between Prisma SD-WAN and ServiceNow.

Configure ServiceNow

Before you configure the ServiceNow CloudBlade, your ServiceNow instance should be configured and ready for integration.

As part of your design, consider the following key design points on making the integration seamless:

- Build the ServiceNow Table and allocate columns to map mandatory fields such as **event code**, **correlation ID**, **severity**, and **incident state**.
- For more meaningful information in the tickets, you can create columns to store fields from the Prisma SD-WAN events such as **entity_ref**, **info**, **site name**, **element name**, **type** – if opting to create tickets for both alerts and alarms, cleared, acknowledged.
- ServiceNow CloudBlade communicates with the ServiceNow instance using REST based Table APIs.
- Create a user that will be used by Prisma SD-WAN to perform CRUD operations on the ServiceNow instance table using the table APIs. Make sure this user has the following privileges: **web_service_admin**, **rest_api_explorer**, or **admin**.

Configure ServiceNow CloudBlade in Prisma SD-WAN

Configure the Prisma SD-WAN CloudBlade to prepare the Prisma SD-WAN controller for integration as follows:

1. From the Prisma SD-WAN portal, click the **CloudBlades** tab.

ServiceNow

Integration with ServiceNow to automatically create tickets to handle incid...

Installed Version: 1.4.1

Vendor: ServiceNow

enabled

Monitor Messages Audit Log Configure

2. In **CloudBlades**, locate the **ServiceNow** CloudBlade. If this CloudBlade does not appear, contact Palo Alto Networks Support.

Configure ServiceNow Parameters

On the **ServiceNow** CloudBlade, click **Configure** to configure ServiceNow parameters.

The core configuration parameters of the Prisma SD-WAN ServiceNow CloudBlade are defined as follows.

Note:

Some of the ServiceNow parameters display the column name and not the label, which is typically displayed on the UI as the column header.

ServiceNow Parameters	Description
ServiceNow URL	<p>This field contains the URL that will be used to connect to the ServiceNow instance via the ServiceNow Table APIs. The URI must include the entire domain name and the table name.</p> <p>The URI follows the following template: <code>https://<domain name>/api/now/table/myTable</code></p> <p>where myTable is the name of the Table on ServiceNow where tickets will be created.</p>
ServiceNow Username	Incident tickets on ServiceNow will be

	<p>created using this User. Make sure that the User has the right set of privileges, especially to make changes to the table via APIs. The ServiceNow Developers document lists the following roles to be assigned to a user:</p> <p>Role required: web_service_admin, rest_api_explorer, or admin</p>
ServiceNow Password	<p>Password for the above user. These credentials will be used by the CloudBlade to create/edit tickets on the ServiceNow instance using the ServiceNow Table APIs.</p>
Poll Interval	<p>Poll Interval is the interval time in seconds. After you install, the CloudBlade will query the controller for any standing alarms based on the set poll interval.</p>
Retry Attempts	<p>Retry attempts indicate the number of attempts that happen when a ticket could not be created for an event. Retry attempts can be anywhere between 0 and 5. The default value is 3.</p>
Exclude Events Raised and Cleared during Poll Interval	<p>When this option is checked, the events which are created and cleared (resolved) during the poll interval will not be ticketed in ServiceNow.</p>
Event Codes	<p>These are event codes used in monitoring and which need incident tickets to be created in ServiceNow. These event codes need to match the Prisma SD-WAN event codes. You can select one or multiple event codes from the drop-down, for example:</p> <p>NETWORK_VPNLINK_DOWN, NETWORK_DIRECTINTERNET_DOWN,NETW ORK_DIRECTPRIVATEWAN_DOWN.</p>
ServiceNow Table Column to Store: EventCode	<p>Column name on the Incident table to store Prisma SD-WAN event code.</p>

ServiceNow Table Column to Store: CorrelationID	Column name on the Incident table to store Prisma SD-WAN event correlation_id .
ServiceNow Table Column to Store: Severity	Column name on the Incident table to store Prisma SD-WAN event severity .
ServiceNow Table Column to Store: EventID	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN Event ID .
ServiceNow Table Column to Store: Time	This is an optional field. This is a Column name on the Incident table to store the Prisma SD-WAN event time .
ServiceNow Table Column to Store: Site_ID	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event site_id , which is translated to its site name .
ServiceNow Table Column to Store: Element_ID	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event element_id , which is translated to its device name.
ServiceNow Table Column to Store: Entity_Ref	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event entity_ref , after a name-ID translation.
ServiceNow Table Column to Store: Info	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event info , after a name-ID translation.
ServiceNow Table Column to Store: Acknowledged	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event acknowledged attribute.

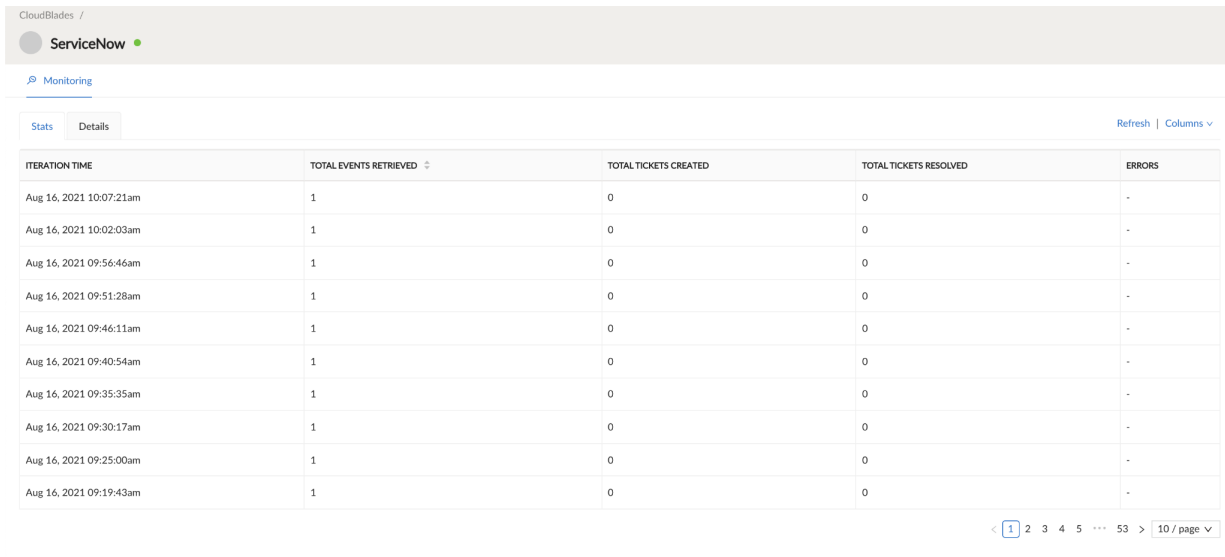
ServiceNow Table Column to Store: Cleared	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event cleared attribute.
ServiceNow Table Column to Store: Type	This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event type .
ServiceNow Table Column to Store: Suppressed	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event suppressed state.
ServiceNow Table Column to Store: Suppressed_Info	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event suppressed info .
ServiceNow Table Column to Store: Policy_Info	This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event policy info .
ServiceNow Table Column to Store: Notes	This is an optional field. This is a Column name on the Incident table to store the Prisma SD-WAN event notes .
ServiceNow Table Column to store Incident State	This is a mandatory field. This is a Column name to store the state of an incident . This column will be set to Resolved, once the event condition for which the ticket was created is resolved.
ServiceNow Table: Custom	This is an optional field. This field is for any custom value that you intend to include for every incident ticket. This is typically used by IT organizations to include details about an environment or to include caller information. Enter a value in JSON format for this field i.e. key-value pairs For example:

“caller”: “CloudGenix Auto Ticketing”,
“environment”: “Production”

Monitor ServiceNow Status in Prisma SD-WAN

To monitor the status of the events, go to **Prisma SD-WAN > CloudBlades > ServiceNow > Monitoring**.

The **Stats** view in the **Monitoring** tab provides information on events created / retrieved, tickets resolved, and lists any errors during each CloudBlade iteration. This view is only updated when at least one event is retrieved. CloudBlade status can only be monitored for up to 7 days.



CloudBlades / ServiceNow

Monitoring

Stats Details Refresh | Columns

ITERATION TIME	TOTAL EVENTS RETRIEVED	TOTAL TICKETS CREATED	TOTAL TICKETS RESOLVED	ERRORS
Aug 16, 2021 10:07:21am	1	0	0	-
Aug 16, 2021 10:02:03am	1	0	0	-
Aug 16, 2021 09:56:46am	1	0	0	-
Aug 16, 2021 09:51:28am	1	0	0	-
Aug 16, 2021 09:46:11am	1	0	0	-
Aug 16, 2021 09:40:54am	1	0	0	-
Aug 16, 2021 09:35:35am	1	0	0	-
Aug 16, 2021 09:30:17am	1	0	0	-
Aug 16, 2021 09:25:00am	1	0	0	-
Aug 16, 2021 09:19:43am	1	0	0	-

1 2 3 4 5 ... 53 > 10 / page

Field	Description
Iteration Time	CloudBlade iteration time.
Total Events Retrieved	Total number of events retrieved from Prisma SD-WAN Controller.
Total Tickets Created	Total number of tickets created on ServiceNow Incident Management Table.
Total Tickets Resolved	Total number of tickets resolved.

Errors

Error messages displayed whenever the CloudBlade encounters an error during the app run.

The **Details** view provides information on all the tickets that are created. The CloudBlade status can only be monitored for up to 7 days.

CloudBlades / ServiceNow

Monitoring

Stats Details Refresh Columns

TIME	EVENT ID	EVENT CODE	CREATED	SERVICENOW SYS ID	CORRELATION ID	RESOLVED STATUS	TICKET RESOLUTION TIME	EVENT TYPE	RETRY ATTEMPTS	STATUS CODE
2021 02:55:43am	6109b433b464be000722f0de	DEVICESW_DISCONNECTED_FROM_CONTROLLER	False	-	TTf5Ymow	NOT RESOLVED	N/A	ALARM	3	200
2021 02:50:40am	6109b2b4b464be000722db91	DEVICESW_DISCONNECTED_FROM_CONTROLLER	False	-	B70Nw8	NOT RESOLVED	N/A	ALARM	3	200
2021 02:50:38am	6109b2b4b464be000722db8f	DEVICESW_DISCONNECTED_FROM_CONTROLLER	False	-	TTf5Ymow	NOT RESOLVED	N/A	ALARM	3	200
2021 03:27:52pm	6109129a10f68d00070ed8c7	DEVICESW_GENERAL_PROCESSRESTART	True	01c464b887f13010bd5c8517cebb3598	N/A	N/A	N/A	ALERT	0	201
2021 03:27:52pm	6109129a10f68d00070ed8c6	DEVICEHW_INTERFACE_DOWN	True	f8c464f487f13010bd5c8517cebb3532	LIMCf7DZ	RESOLVED	Aug 3, 2021 03:32:56pm	ALARM	0	201
2021 03:27:51pm	6109129a10f68d00070ed8c5	SITE_CONNECTIVITY_DEGRADED	True	f8c4a83887f13010bd5c8517cebb3536	enXc0nkE	RESOLVED	Aug 3, 2021 03:32:55pm	ALARM	0	201
2021 10:41:34am	6108cf1010f68d00070af971	DEVICESW_GENERAL_PROCESSRESTART	True	4b334fa887313010bd5c8517cebb3590	N/A	N/A	N/A	ALERT	0	201
2021 10:41:34am	6108cf1010f68d00070af972	DEVICESW_GENERAL_PROCESSRESTART	True	8b332b2c87313010bd5c8517cebb3514	N/A	N/A	N/A	ALERT	0	201
2021 10:41:33am	6108cf6110f68d00070afe55	DEVICESW_GENERAL_PROCESSRESTART	True	03334fa887313010bd5c8517cebb358f	N/A	N/A	N/A	ALERT	0	201
2021 10:41:33am	6108cf6110f68d00070afe56	DEVICESW_GENERAL_PROCESSRESTART	True	72332b2c87313010bd5c8517cebb3513	N/A	N/A	N/A	ALERT	0	201

< 1 2 3 4 5 >

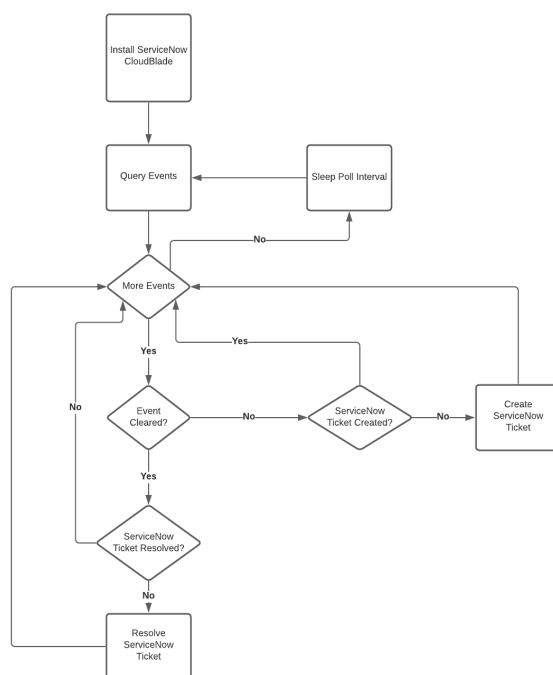
Field	Description
Event Time	Time of the event.
Event ID	Unique ID of the event.
Event Code	Code of the event.
Created	Status of event creation (True / False).
ServiceNow Sys ID	ServiceNow ID of the event.
Correlation ID	Correlation ID of the event.
Resolved Status	Status of the ticket (Resolved/Not Resolved/NA).
Ticket Resolution Time	Time when the ticket was resolved.

Event Type	Type of Event (Alarm/Alert).
Retry Attempts	The number of attempts made to create/resolve the ticket. Retry attempts can be anywhere between 0 and 5. The default value is 3.
Status Code	Status Code returned by ServiceNow Incident Management Table API endpoint for ticket creation/resolution.

ServiceNow CloudBlade Infrastructure

Once the CloudBlade configuration parameters are set up and the CloudBlade is installed, the CloudBlade infrastructure will perform the following tasks:

- Extract configuration parameters received from the CloudBlade
- Query for events based on the event codes provided
- Create or resolve existing tickets
- Wait until poll_interval for next iteration



Querying for Events

Once the ServiceNow configuration is extracted, the CloudBlade queries for events using the following API query:

```
events_query_payload = {
  "limit": {
    "count": 100,
    "sort_on": "time",
    "sort_order": "descending"
  },
  "query": {
    "code": event_codes
  },
  "severity": [],
  "start_time": start_time
}
```

Here, the **event_codes** is a list of event codes configured on the UI. Once the events are retrieved, they are mapped against an internal database to check if a ticket is already created in ServiceNow. If the event is cleared and a ticket exists, the ticket is set to **Resolved** in ServiceNow. If the ticket does not exist on ServiceNow, the event is ignored. If the clear is set to False, a new ticket is created in ServiceNow.

Converting Prisma SD-WAN Events to ServiceNow Constructs

Before a ticket is created on ServiceNow, the Prisma SD-WAN event JSON is converted to a data structure understood by the ServiceNow instance. This mapping is dependent on the parameters configured on the CloudBlade. For example, the CloudBlade configuration below is translated in the following manner:

The screenshot displays the configuration interface for the ServiceNow integration. At the top, it shows the Name (ServiceNow), Vendor (ServiceNow), and Installed Version (1.4.1). Below this, there are tabs for VERSION (1.4.1), STATUS (beta), PERMISSIONS (View), and ADMIN STATE (Enabled). The main configuration area includes several fields:

- SERVICENOW URL:** https://dev57534.service-now.com/api/now/table/u_end_to_end_regression_s...
- SERVICENOW USERNAME:** admin
- SERVICENOW PASSWORD:** masked with dots, with an 'unmask' link.
- POLL INTERVAL (SECONDS) (optional):** 300
- RETRY ATTEMPTS (optional):** 3
- EXCLUDE EVENTS RAISED AND CLEARED DURING POLL INTERVAL:** unchecked checkbox.
- EVENT CODES:** 57 selected.
- SERVICENOW TABLE COLUMN TO STORE: EVENTCODE:** u_eventcode
- SERVICENOW TABLE COLUMN TO STORE: CORRELATIONID:** u_correlationid
- SERVICENOW TABLE COLUMN TO STORE: SEVERITY:** u_severity
- SERVICENOW TABLE COLUMN TO STORE: PRIORITY (optional):** (empty field)

 On the right side, there are links for 'View Audit Log' and 'View Messages'.

Prisma SD-WAN Event Attributes	ServiceNow Construct
code	u_code
correlation_id	u_correlation_id
severity	u_urgency
id	u_event_id
time	u_time

site_id	u_site
element_id	u_element
entity_ref	u_entity_ref
info	u_info
acknowledged	u_acknowledged
cleared	u_cleared
type	u_type
severity	impact

The following Prisma SD-WAN attributes are translated before converting to the ServiceNow construct:

Entity_Ref

The IDs in the entity_ref are translated to their respective names and a meaningful string is generated that provides the user information about the entity of the alarm.

For example, the entity_ref below:

`"tenants/1083/sites/15282991838450011/elements/15230097588400085/interfaces/15230098062640233"`

is translated to the string:

Site: Portland Office

Element: Portland3K-A

Interface: internet1

Note:

The ServiceNow CloudBlade does a topology mapping once a week. If new VPN links are created since the last topology mapping, then it may result in certain VPN link IDs not being translated to names.

Info

Similar to entity_ref, the IDs in the info are also translated to their respective names.

Site ID

If a `site_id` exists in the Prisma SD-WAN event, it is translated to its name before populating the ServiceNow construct with the value.

Element ID

If an `element_id` exists in the Prisma SD-WAN event, it is also translated to its name before populating the ServiceNow construct with the value.

Severity

In the above example, the Prisma SD-WAN **severity** is directly mapped to **u_urgency**. However, this field is also mapped to another attribute named **impact**. The following translation takes place before the ServiceNow construct is populated.

Prisma SD-WAN Severity	ServiceNow Impact
critical	1 - High
major	2 - Medium
minor	3 - Low

The impact value may change depending on the tags configured at the site and/or element level. More about this feature is discussed in length under the section **Managing Incident Impact**.

Along with the attributes above, the CloudBlade also populates the tenant name in an attribute called **company**.

Incident Creation on ServiceNow

Once all the Prisma SD-WAN attributes are translated and populated into the ServiceNow construct, a session is established with the ServiceNow instance configured in the CloudBlade using Basic HTTP Authentication. An incident ticket is created where the Prisma SD-WAN Event attributes are mapped to ServiceNow table columns. Upon successful ticket creation, ServiceNow returns HTTP code 201 – Created and the response package contains the incident ticket number.

This incident ticket number is stored locally in a database and mapped to the Prisma SD-WAN **event_id**.

		acknowledged	cleared	code	correlation_id	element	entry_ref	event_id	incident_state	info	site	urgency	type
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	DEVICEHW_INTERFACE_DOWN	8dMervYM	NJ-3K-1	Site: New Jersey Branch 1 Element: NJ-3K...	5e015fb686115c07ac9ae914	Resolved	[circuit_labels~, name~sl-azure-15011179...	New Jersey Branch 1	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	NETWORK_VPNLINK_DOWN	VTZcMBe1	MAD-7K-1	Site: Madrid DC Site	5e0152b686115c07ac9ae6ed	Resolved	Could not query anymet link 1501116987121...	Madrid DC Site	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	DEVICEHW_INTERFACE_DOWN	liijDWG4	NJ-3K-1	Site: New Jersey Branch 1 Element: NJ-3K...	Sdf44486115c099d9ae5a	Resolved	[circuit_labels~, name~sl-azure-15011179...	New Jersey Branch 1	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	NETWORK_VPNLINK_DOWN	xIhtZiCG	MAN-3K-1	Site: Manchester Branch 3	Sdf45b6c86115c73d39ae597	Resolved	Could not query anymet link 150112796781...	Manchester Branch 3	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	DEVICEHW_INTERFACE_DOWN	EvziQTkx	NJ-3K-1	Site: New Jersey Branch 1 Element: NJ-3K...	Sdfc91d86115c17fd9ae823	Resolved	[circuit_labels~, name~sl-azure-15011179...	New Jersey Branch 1	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	NETWORK_VPNLINK_DOWN	UGUGRPrY	MAN-3K-1	Site: Manchester Branch 3	Sdf452286115c73d39ae821	Resolved	Could not query anymet link 150112729193...	Manchester Branch 3	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	NETWORK_VPNLINK_DOWN	LJn5DKNE	MAN-3K-1	Site: Manchester Branch 3	Sdfb83986115c60429ae994	Resolved	Could not query anymet link 150112796781...	Manchester Branch 3	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	NETWORK_VPNLINK_DOWN	sxQIPa5	DAL-7K-1	Site: Dallas Data Center	Sdfcdc9b86115c17fd9ae502	Resolved	Could not query anymet link 150112729193...	Dallas Data Center	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	NETWORK_VPNLINK_DOWN	GzeBUdxv	MIL-3K-1	Site: Milan Branch 2	Sdfcd9e086115c17fd9ae40a	Resolved	Could not query anymet link 150112800790...	Milan Branch 2	2 - Medium	alarm
<input type="checkbox"/>	<input checked="" type="radio"/>	false	true	DEVICEHW_INTERFACE_DOWN	ddNjKscv	NJ-3K-1	Site: New Jersey Branch 1 Element: NJ-3K...	Sdfbf0ae86115c60429ae6e1	Resolved	[circuit_labels~, name~sl-azure-15011179...	New Jersey Branch 1	2 - Medium	alarm

Incident Resolution in ServiceNow


When an event clears on Prisma SD-WAN, the CloudBlade retrieves the incident ticket number from the local database and sets the ticket as **Resolved**. In the above example, the column **u_incident_state** is configured to store the incident state and will be set to the value **Resolved**. IT Operators managing ServiceNow tickets use this column as a filtering mechanism and can choose to ignore tickets marked as **Resolved**.

Managing Incident Impact

All Prisma SD-WAN events have a severity associated with them. Information on event severity can be found in the **Alerts and Alarms** section in the *Prisma SD-WAN Administrator's Guide*. However, incidents generated from certain sites or devices may have a higher or lower impact than the Prisma SD-WAN event severity. To handle such scenarios, the ServiceNow CloudBlade makes use of tags that can be configured at the site and device level to adjust the impact mapping in ServiceNow.

The tags **snow-high**, **snow-med**, and **snow-low** can be used to adjust impact of events generated from sites and/or elements. If any of these tags are configured at the site or device, all events generated from that particular site or device will have the corresponding impact.

Alarm Severity	Site/Element Tag	Modified Impact
critical, major, minor	snow-high	1 - High
critical, major, minor	snow-med	2 - Medium



critical, major, minor	snow-low	3 - Low
-----------------------------------	----------	---------