<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>SD-WAN Events Overview</td>
<td>3</td>
</tr>
<tr>
<td>Alert and Alarm Attributes</td>
<td>4</td>
</tr>
<tr>
<td><strong>Prisma SD-WAN ServiceNow CloudBlade</strong></td>
<td>6</td>
</tr>
<tr>
<td>Configure ServiceNow</td>
<td>7</td>
</tr>
<tr>
<td>Configure ServiceNow CloudBlade in Prisma SD-WAN</td>
<td>7</td>
</tr>
<tr>
<td>Configure ServiceNow Parameters</td>
<td>8</td>
</tr>
<tr>
<td>Monitor ServiceNow Status in Prisma SD-WAN</td>
<td>11</td>
</tr>
<tr>
<td><strong>ServiceNow CloudBlade Infrastructure</strong></td>
<td>14</td>
</tr>
<tr>
<td>Querying for Events</td>
<td>14</td>
</tr>
<tr>
<td>Converting Prisma SD-WAN Events to ServiceNow Constructs</td>
<td>15</td>
</tr>
<tr>
<td>Incident Creation on ServiceNow</td>
<td>18</td>
</tr>
<tr>
<td>Incident Resolution in ServiceNow</td>
<td>19</td>
</tr>
<tr>
<td>Managing Incident Impact</td>
<td>19</td>
</tr>
</tbody>
</table>
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.

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:

```json
{
  "_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/160155894396200037",
  "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": "160155894396200037",
  "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.
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.

<table>
<thead>
<tr>
<th>ServiceNow Parameters</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>ServiceNow URL</strong></td>
<td>This field contains the <strong>URL</strong> 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. The <strong>URI</strong> follows the following template: https://&lt;domain name&gt;/api/now/table/myTable where <strong>myTable</strong> is the name of the Table on ServiceNow where tickets will be created.</td>
</tr>
<tr>
<td><strong>ServiceNow Username</strong></td>
<td>Incident tickets on ServiceNow will be</td>
</tr>
</tbody>
</table>
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:

Role required: **web_service_admin, rest_api_explorer, or admin**

<table>
<thead>
<tr>
<th>ServiceNow Password</th>
<th>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.</th>
</tr>
</thead>
<tbody>
<tr>
<td>Poll Interval</td>
<td>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.</td>
</tr>
<tr>
<td>Retry Attempts</td>
<td>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.</td>
</tr>
<tr>
<td>Exclude Events Raised and Cleared during Poll Interval</td>
<td>When this option is checked, the events which are created and cleared (resolved) during the poll interval will not be ticketed in ServiceNow.</td>
</tr>
<tr>
<td>Event Codes</td>
<td>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: NETWORK_VPNLINK_DOWN, NETWORK_DIRECTINTERNET_DOWN, NETWORK_DIRECTPRIVATEWAN_DOWN.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: EventCode</td>
<td>Column name on the Incident table to store Prisma SD-WAN event code.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: CorrelationID</td>
<td>Column name on the Incident table to store Prisma SD-WAN event <code>correlation_id</code>.</td>
</tr>
<tr>
<td>-----------------------------------------------</td>
<td>----------------------------------------------------------------------------------</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: Severity</td>
<td>Column name on the Incident table to store Prisma SD-WAN event <code>severity</code>.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: EventID</td>
<td>This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN Event ID.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: Time</td>
<td>This is an optional field. This is a Column name on the Incident table to store the Prisma SD-WAN event <code>time</code>.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: Site_ID</td>
<td>This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event <code>site_id</code>, which is translated to its site name.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: Element_ID</td>
<td>This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event <code>element_id</code>, which is translated to its device name.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: Entity_Ref</td>
<td>This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event <code>entity_ref</code>, after a name-ID translation.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: Info</td>
<td>This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event <code>info</code>, after a name-ID translation.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store: Acknowledged</td>
<td>This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event <code>acknowledged</code> attribute.</td>
</tr>
<tr>
<td>ServiceNow Table Column to Store</td>
<td>Description</td>
</tr>
<tr>
<td>----------------------------------</td>
<td>-------------</td>
</tr>
<tr>
<td><strong>Cleared</strong></td>
<td>This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event <strong>cleared</strong> attribute.</td>
</tr>
<tr>
<td><strong>Type</strong></td>
<td>This is an optional field. This is a Column name on the Incident table to store Prisma SD-WAN event <strong>type</strong>.</td>
</tr>
<tr>
<td><strong>Suppressed</strong></td>
<td>This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event <strong>suppressed</strong> state.</td>
</tr>
<tr>
<td><strong>Suppressed_Info</strong></td>
<td>This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event <strong>suppressed info</strong>.</td>
</tr>
<tr>
<td><strong>Policy_Info</strong></td>
<td>This is an optional field. This is a Column name on the Incident table to store a Prisma SD-WAN event <strong>policy info</strong>.</td>
</tr>
<tr>
<td><strong>Notes</strong></td>
<td>This is an optional field. This is a Column name on the Incident table to store the Prisma SD-WAN event <strong>notes</strong>.</td>
</tr>
<tr>
<td><strong>Incident State</strong></td>
<td>This is a mandatory field. This is a Column name to store the state of an <strong>incident</strong>. This column will be set to Resolved, once the event condition for which the ticket was created is resolved.</td>
</tr>
<tr>
<td><strong>Custom</strong></td>
<td>This is a mandatory 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:</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>Iteration Time</strong></td>
<td>CloudBlade iteration time.</td>
</tr>
<tr>
<td><strong>Total Events Retrieved</strong></td>
<td>Total number of events retrieved from Prisma SD-WAN Controller.</td>
</tr>
<tr>
<td><strong>Total Tickets Created</strong></td>
<td>Total number of tickets created on ServiceNow Incident Management Table.</td>
</tr>
<tr>
<td><strong>Total Tickets Resolved</strong></td>
<td>Total number of tickets resolved.</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Field</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Event Time</td>
<td>Time of the event.</td>
</tr>
<tr>
<td>Event ID</td>
<td>Unique ID of the event.</td>
</tr>
<tr>
<td>Event Code</td>
<td>Code of the event.</td>
</tr>
<tr>
<td>Created</td>
<td>Status of event creation (True / False).</td>
</tr>
<tr>
<td>ServiceNow Sys ID</td>
<td>ServiceNow ID of the event.</td>
</tr>
<tr>
<td>Correlation ID</td>
<td>Correlation ID of the event.</td>
</tr>
<tr>
<td>Resolved Status</td>
<td>Status of the ticket (Resolved/Not Resolved/NA).</td>
</tr>
<tr>
<td>Ticket Resolution Time</td>
<td>Time when the ticket was resolved.</td>
</tr>
</tbody>
</table>
### 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:

```json
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:
<table>
<thead>
<tr>
<th>Prisma SD-WAN Event Attributes</th>
<th>ServiceNow Construct</th>
</tr>
</thead>
<tbody>
<tr>
<td>code</td>
<td>u_code</td>
</tr>
<tr>
<td>correlation_id</td>
<td>u_correlation_id</td>
</tr>
<tr>
<td>severity</td>
<td>u_urgency</td>
</tr>
<tr>
<td>id</td>
<td>u_event_id</td>
</tr>
<tr>
<td>time</td>
<td>u_time</td>
</tr>
</tbody>
</table>
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.

<table>
<thead>
<tr>
<th>Prisma SD-WAN Severity</th>
<th>ServiceNow Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical</td>
<td>1 - High</td>
</tr>
<tr>
<td>major</td>
<td>2 - Medium</td>
</tr>
<tr>
<td>minor</td>
<td>3 - Low</td>
</tr>
</tbody>
</table>

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.
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.

<table>
<thead>
<tr>
<th>Alarm Severity</th>
<th>Site/Element Tag</th>
<th>Modified Impact</th>
</tr>
</thead>
<tbody>
<tr>
<td>critical, major, minor</td>
<td>snow-high</td>
<td>1 - High</td>
</tr>
<tr>
<td>critical, major, minor</td>
<td>snow-med</td>
<td>2 - Medium</td>
</tr>
<tr>
<td>critical, major, minor</td>
<td>snow-low</td>
<td>3 - Low</td>
</tr>
</tbody>
</table>