

# **INSTALLATION AND CONFIGURATION GUIDE**

Check Point CloudGuard Dome9 Application for ServiceNow  
(1.3.0)

**VERSION CONTROL**

#	Document Version	Date	Owner	Document Status	Comments
1	1.0.0	09th September, 2019	Arpit Shah	Completed	Added details about 1.0.0 version
2	1.1.0	08th January, 2021	Ketul Patel	Completed	Added details about 1.1.0 version
3	1.3.0	13th Jan, 2022	Dhaval Bhimani	Completed	Added details about 1.3.0, Rome version support

## Contents

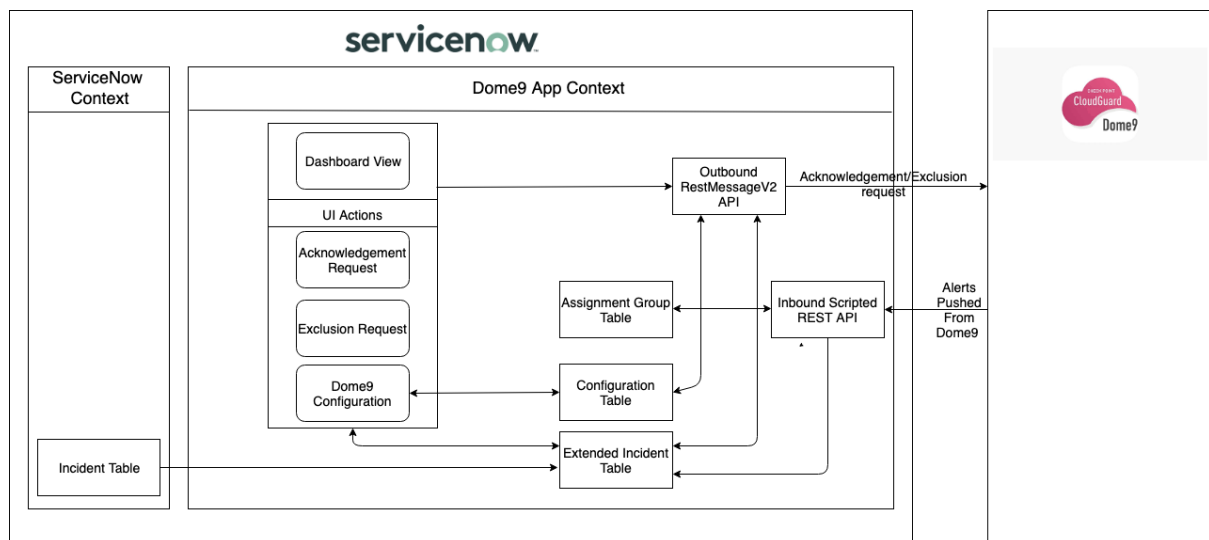
Overview	<b>5</b>
Application features	5
Compatibility	6
Installation	<b>7</b>
Pre-Requisites	7
ServiceNow Plugins	7
Permissions and Roles	7
Application Download and Installation	8
Data Migration	9
Configuration	<b>11</b>
Configure User Roles	11
Create Users	12
API Configuration (optional)	15
Configure Compliance Incidents (optional)	16
Configure Related List in incident table	18
Dome9 Notification Configuration	19
Use Cases	<b>22</b>
Alert mapping to the fields of incident	22
View Incidents	22
Acknowledge Dome9 Incidents	24
Create Dome9 Exclusions	25
View linked information on Dome9 from incidents in ServiceNow	26
Copy to Clipboard	26
Configure assignment criteria to auto-assign new Dome9 incidents to a ServiceNow group	27
Ability to set the resolve States from available Incident states	29
Incident state update automatically when alert is resolved on Dome9	29
Reopen Incident if same alert generated again	30
Set a condition to create child incident when parent incident reopens	31
Customize Mandatory Fields While Closing Incidents	32
Create incident if not present in SNOW when alert received with status “Passed”	34
View the Dashboard	34

Uninstallation	36
Support, Troubleshooting, and Known Limitations	37
Support	37
Troubleshooting	37
Application Logs	37
Unable to install Dome9 application from ServiceNow Store	37
Unable to find Dome9 custom roles	38
Unable to create new user Dome9 custom roles	38
Unable to install/activate plugin in ServiceNow instance	38
Unable to get Dome9 findings and alerts	38
Unable to perform UI Actions	39
Child Incident Creation Condition shows the fields which are not related to Dome9	39
All Child Incidents getting reopened when parent reopens	39
Widget not visible on Dashboard	39
Known Limitations	39

## 1. Overview

Check Point CloudGuard Dome9 (from now – “Dome9”) is a Security and a Compliance solution for the Public Cloud. When granted access to a user’s cloud environment, Dome9 will continually run assessments for compliance to a number of best-practice standards (and user custom-designed policies as well) and generate findings in real-time for issues that need to be rectified. A well-requested integration is with ServiceNow, a platform for managing tickets/incidents and organizational flows. Findings generated by the Dome9 Compliance Engine are sent to ServiceNow and recorded as a new ServiceNow incident. These can be managed as tickets in ServiceNow and, once resolved, will be cleared from Dome9 in a subsequent assessment.

This document describes how to configure ServiceNow to receive findings from Dome9. This is done using a purpose-built ServiceNow application. Dome9 sends findings to this application, using the ServiceNow REST API. The application creates ServiceNow incidents from these findings, which can then be viewed on the ServiceNow Dashboard. The application can also configure the user’s Dome9 account, using the Dome9 REST API, to set up exclusions, and to acknowledge findings.



### 1.1. Application features

The main features of the application are:

1. Create incidents attach it to respective records in ServiceNow from Dome9 Compliance Findings/Alerts.
2. Acknowledge Alert on Dome9 from ServiceNow.
3. Create exclusions, to exclude specific types of findings from being sent from Dome9 to ServiceNow.
4. View details about entities related to findings, in the Dome9 web application, directly from links in the incidents on ServiceNow.
5. Reopen closed incidents if that appear for updates received from Dome9.
6. Mandatory values must have values assigned while closing incidents.

## 1.2. Compatibility

The Dome9 application in ServiceNow is compatible with these versions of ServiceNow:

**ServiceNow Version:** Orlando, Paris, Quebec, and Rome

## 2. Installation

This section describes how to download and install the ServiceNow Dome9 application from the store.

### 2.1. Pre-Requisites

These are the prerequisites required to install the ServiceNow Dome9 application.

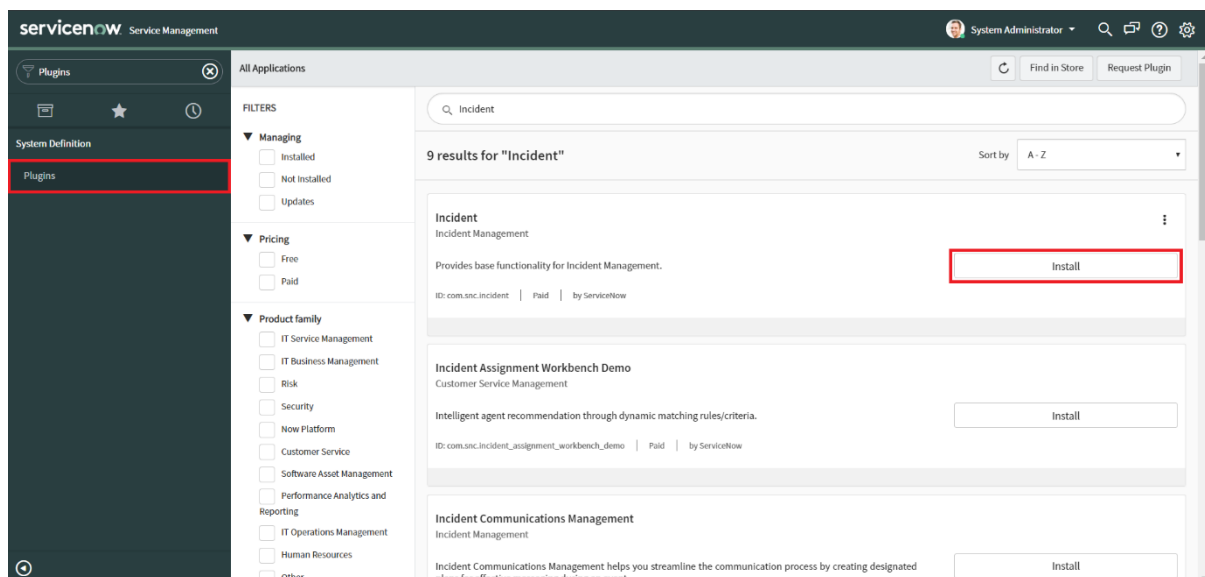
#### ServiceNow Plugins

These ServiceNow plugins must be activated:

- Scripted REST APIs (com.glide.scripted\_rest\_services)
- Incident (com.snc.incident)

To install these plugins:

1. Login to your instance with your user credentials.
2. Verify you have the system administrator (admin) role.
3. Navigate to “System Definition” “Plugins” in your instance.
4. Search and install above plugins.



### 2.2. Permissions and Roles

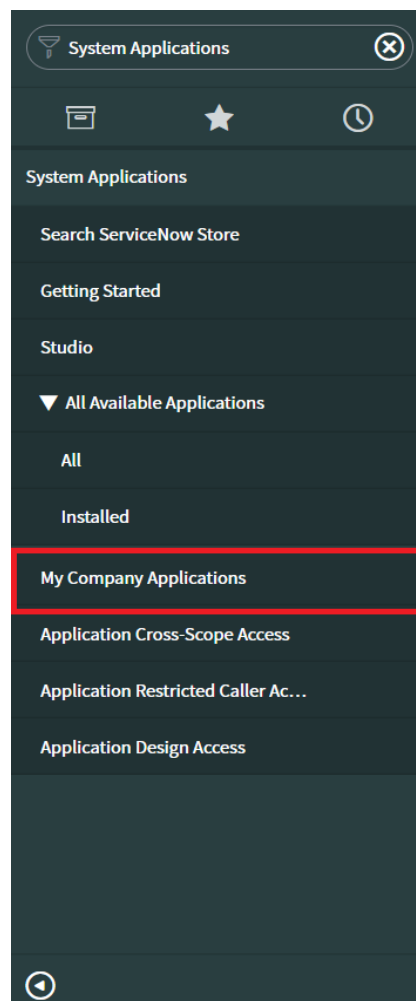
These are the ServiceNow roles and the permissions that are needed to install the application, and to use it to view and manage Dome9 incidents on ServiceNow.

Role	Permissions
System administrator (admin)	<ul style="list-style-type: none"> <li>• Installation of the integration application plugins</li> <li>• View Application Logs</li> <li>• Edit Dashboard</li> </ul>

Dome9 Admin	<ul style="list-style-type: none"> <li>• Configure “API Configuration” and “Compliance Incident Configuration”.</li> <li>• Perform “Acknowledge on Dome9” and “Create Dome9 Exclusion” UI Actions on Compliance Incidents.</li> <li>• View “Dashboard” and apply filters.</li> <li>• View “Support Contact” module.</li> </ul>
Dome9 User	<ul style="list-style-type: none"> <li>• Perform “Acknowledge on Dome9” and “Create Dome9 Exclusion” UI Actions on Compliance Incidents.</li> <li>• View “Dashboard” and apply filters.</li> <li>• View “Support Contact” module.</li> </ul>

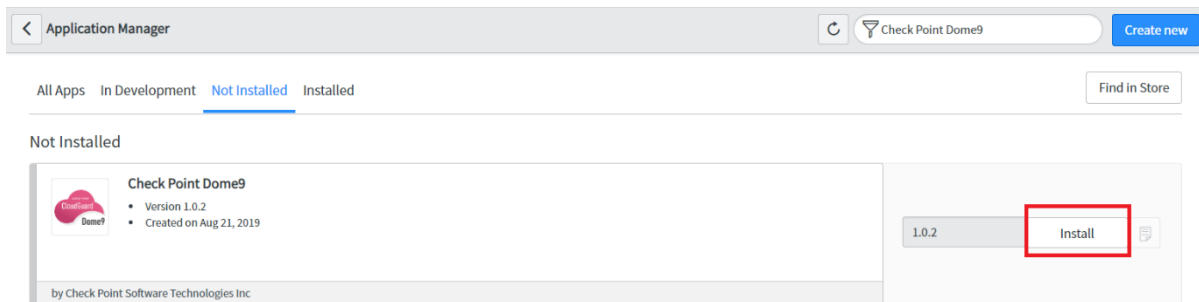
### 2.3. Application Download and Installation

- Get the Dome9 App from the ServiceNow Store for the ServiceNow instance by clicking on “Get” and entering your user credentials.
- Login to the instance on which you want to install the application.
- Navigate to “System Applications” “My Company Application” .

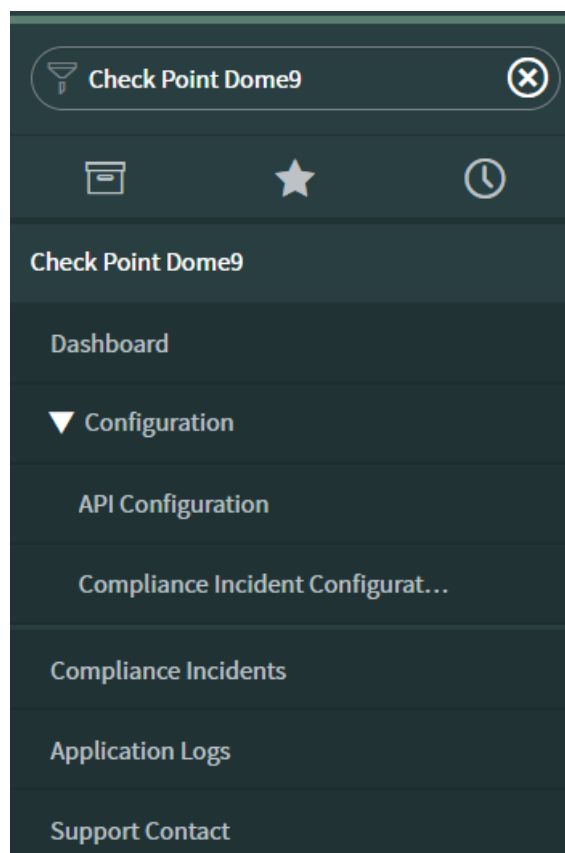


- Click the “Not Installed” tab. A list of applications available for installation is displayed.
- Locate the Dome9 application, select it, and click “Install”.





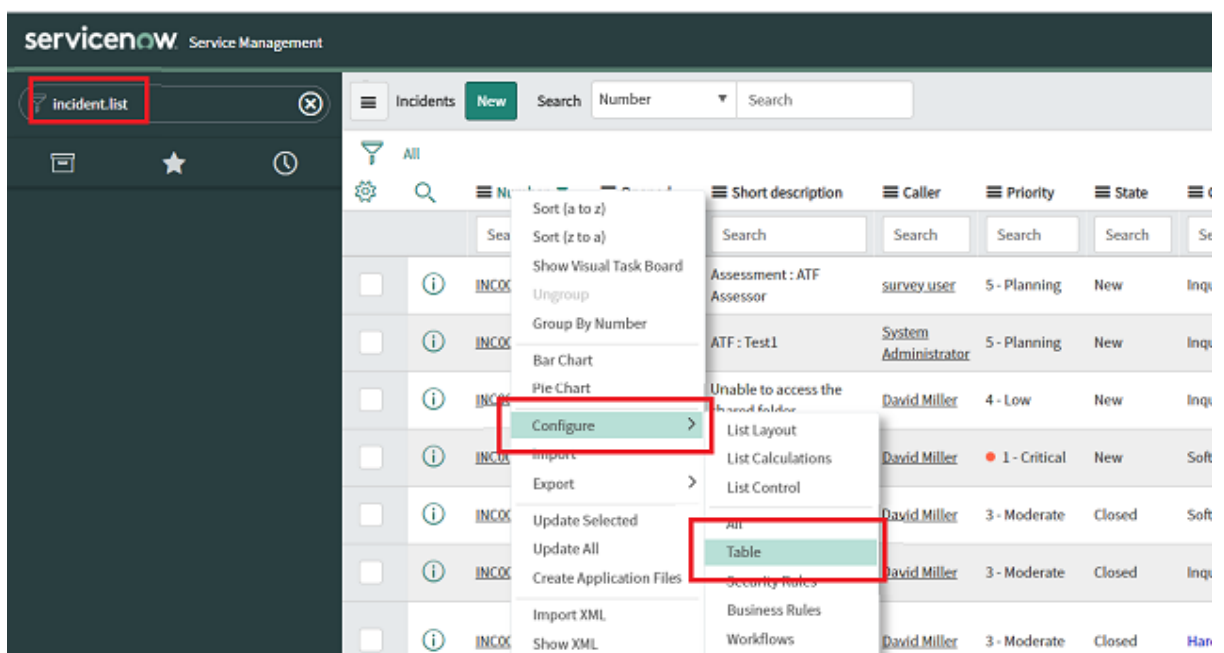
- The application will be installed into your instance.
- **Note:** When User Install or upgrade the App, Compliance incident Configuration will be set to default configuration.
- Navigate to the application by searching “Check Point Dome9” in the navigation bar:



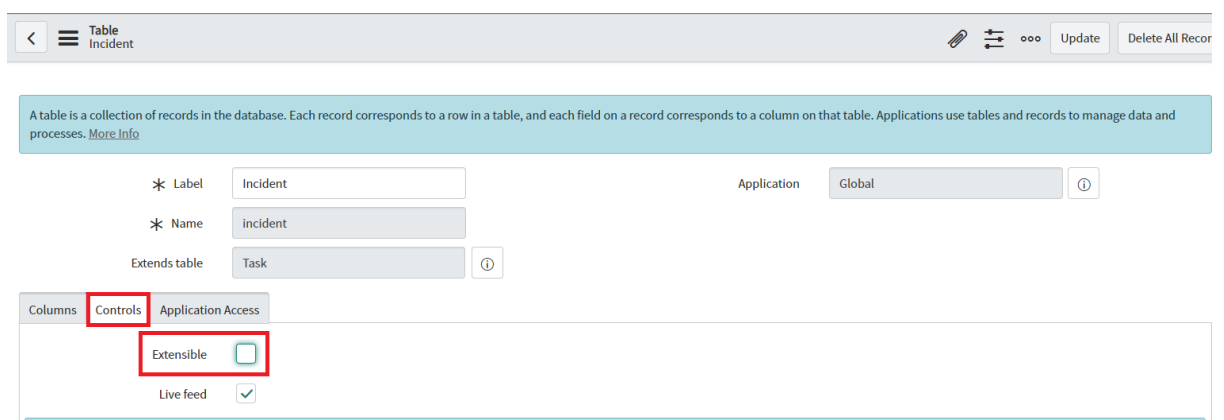
### 2.3.1. Data Migration

- As part of this release, an alert will be stored in the custom table “Dome9 Compliance Incident” and the incident related to it will be stored in the system table “Incident”.
- Alert in the custom table will have a reference to the related incident.
- To make the previous app version compatible with the new release, a Fix script “Data Migration” will be executed automatically when the application is installed or updated.
- After this script execution, all the alerts from the older deprecated table will be migrated to the newer implementation approach.

- New records will be created in the new Dome9 Compliance Incident Table for each record which is available in the Old table.
- Information related to alert from the old Dome9 Compliance Incident will be migrated to the newer Dome9 Compliance Incident table
- New Dome9 Compliance Incident table has the reference field for the incident. So the record from the older table is linked to the newer table via this field in order to maintain the histories of old data.
- New alert from the dome9 will create the record in the new Dome9 Compliance Incident table as well as Incident table.
- **Note:** For the existing users it is recommended to uncheck extensible checkbox from the Incident table. To do this follow below steps:
  - Type incident.list in application navigator and hit Enter.
  - Right click on the header part and go to Configure->Table.



- Select the Controls section and uncheck Extensible checkbox.



### 3. Configuration

This section describes how to configure ServiceNow and Dome9 to use the application.

#### 3.1. Configure User Roles

The application comes with two custom roles out of the box. System roles must be added to these custom roles.

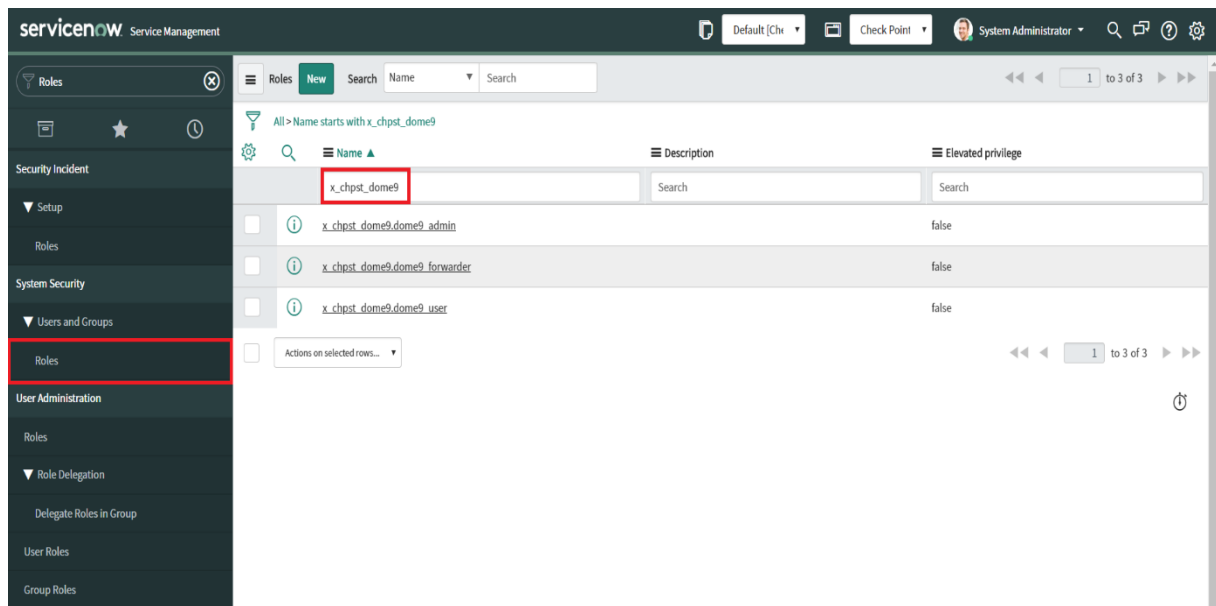
**Role Required:** System Administrator (admin)

Add these System roles to the Custom roles:

Custom Role	System Roles to be added
Dome9 Admin (x_chpst_dome9.dome9_admin)	x_chpst_dome9.dome9_user, personalize_dictionary, itil
Dome9 User (x_chpst_dome9.dome9_user)	personalize_dictionary, itil
Dome9 Forwarder (x_chpst_dome9.dome9_forwarder)	None

**Procedure:**

1. Navigate to “System roles”, and filter for custom roles.



2. Select the custom role to which the system roles are to be added.



- Tab.



### 3.2. Create Users

The ServiceNow platform admin creates the various Dome9 users.

Username (for example)	Role to be assigned
Dome9 Admin	x_chpst_dome9.dome9_admin

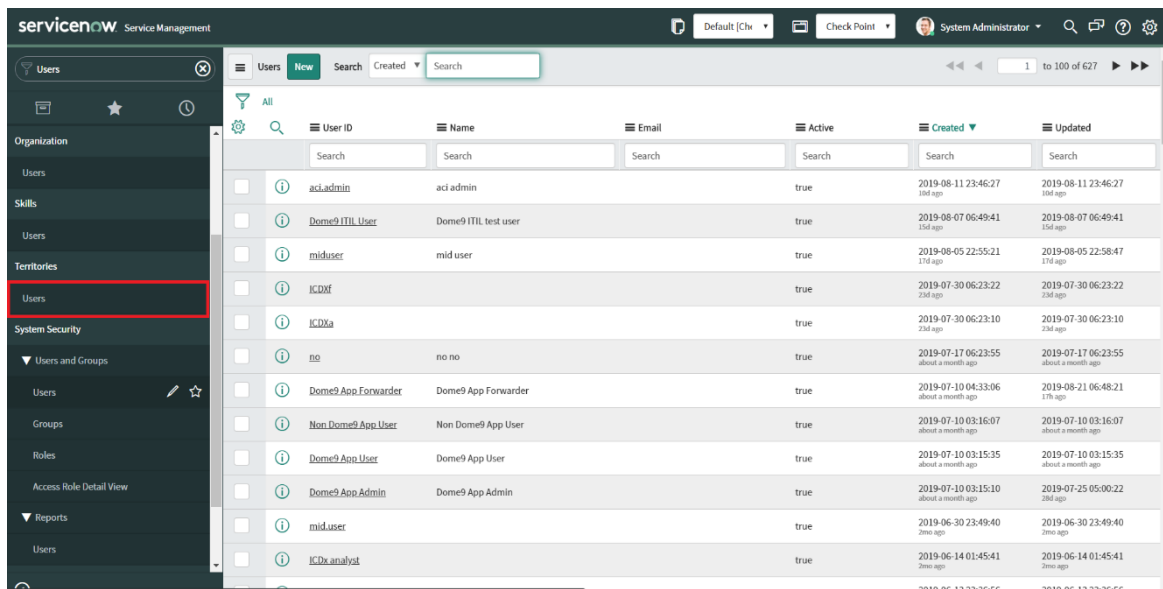
Dome9 User	x_chpst_dome9.dome9_user
Dome9 Forwarder	x_chpst_dome9.dome9_forwarder

Below is the example showing how to create a Dome9 Admin user and assign the x\_chpst\_dome9.dome9\_admin role to it. Other users can be created in a similar manner by assigning the corresponding role to him/her.

**Role Required:** System Administrator (admin)

#### Procedure:

1. Navigate to “Organization” “Users”.
2. Click the “Users” module.



3. On the Users list that is displayed, click “New”. A new user form is displayed.



8. Once the record is open, go to the Roles section, and click “Edit”.
9. On the Edit Members form that is displayed, enter x\_chpst\_dome9.dome9\_admin in the Collection field.
10. In the Collection column, select and move x\_chpst\_dome9.dome9\_admin to the Roles List.

11. Click “Save”.

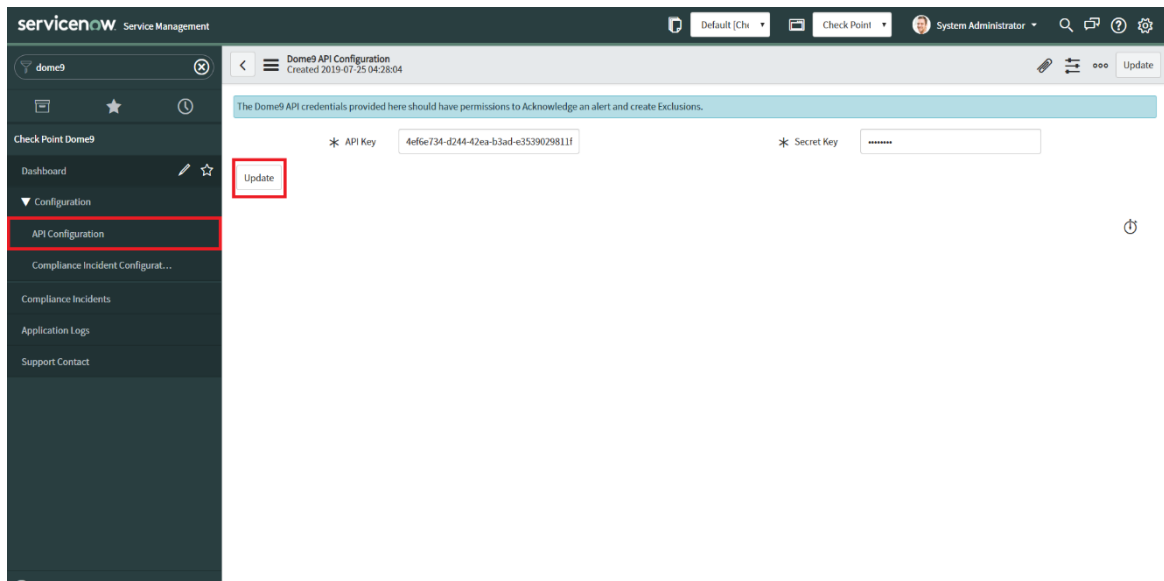
### 3.3. API Configuration (optional)

This section describes how to configure the “API Configuration”, which is used to perform the “Acknowledge on Dome9” and “Create Dome9 Exclusion” actions on Dome9.

**Role Required:** x\_chpst\_dome9.dome9\_admin

**Procedure:**

1. Login to the ServiceNow instance.
2. In the top left- corner, in the search menu enter “Check Point Dome9”. This will open the Dome9 application menu. (As shown in the snapshot below).
3. Click “Configuration” “API Configuration”.
4. Enter the API key and Secret Key of Dome9 Instance, and then click “Update”.



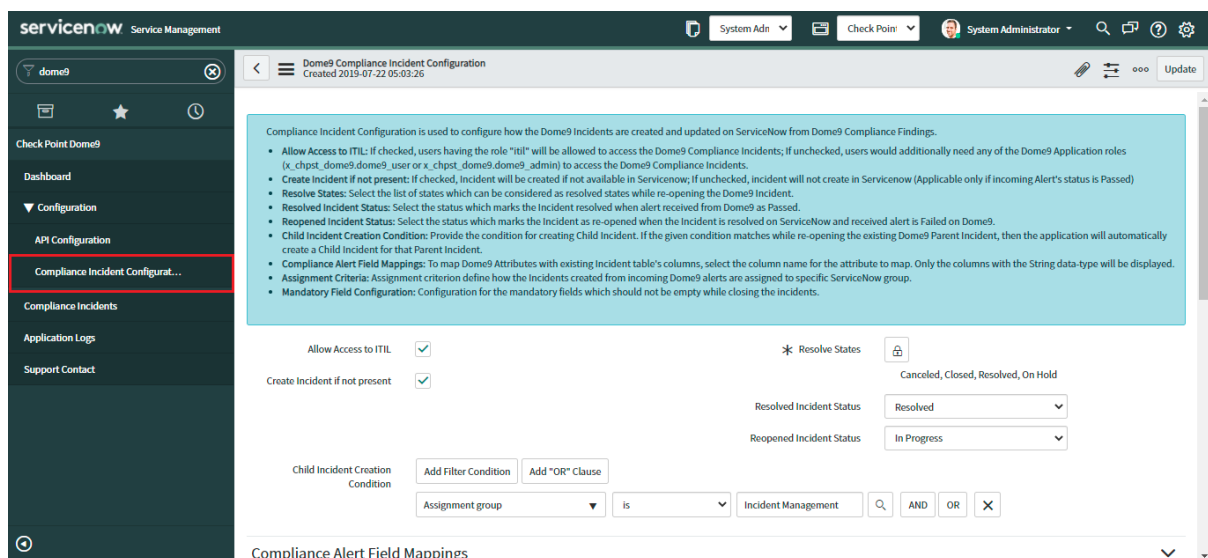
### 3.4. Configure Compliance Incidents (optional)

This section describes how to set up the “Compliance Incident Configuration” which determines how the Dome9 incidents are created from Dome9 Compliance findings, and how they appear as ServiceNow incidents. This includes mappings from Dome9 values (such as severity) to ServiceNow values. If these are not configured, default mappings will be applied.

**Role Required:** x\_chpst\_dome9.dome9\_admin

#### Procedure:

1. Login to the ServiceNow instance.
2. In the top left-hand corner, in the search menu enter “Check Point Dome9”. This will open the Dome9 application menu. (As shown in the snapshot below).
3. Click “Configuration” “Compliance Incident Configuration”.




4. Fill in the form with the following details, and then click “Update”.

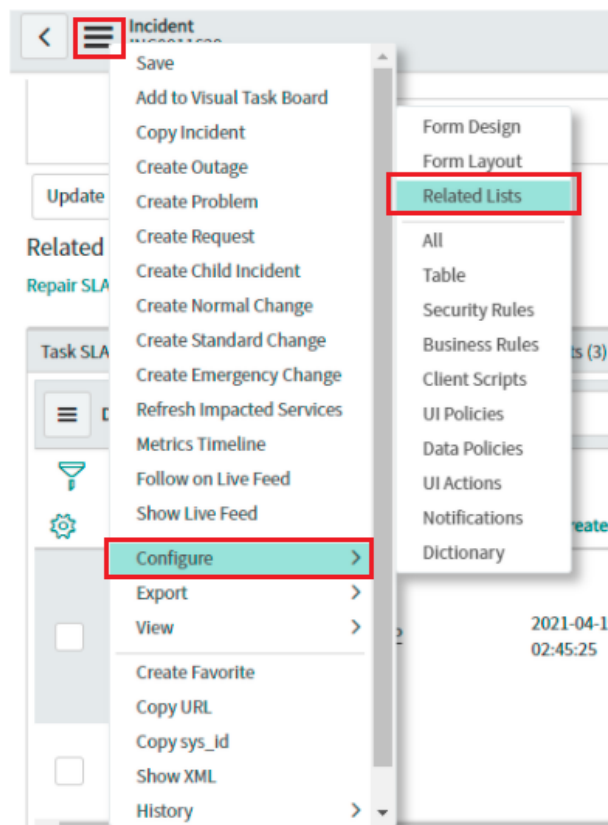


Field	Description	Default Value
Allow Access to ITIL	If checked, users having the role "itil" will be allowed to access the Dome9 Compliance Incidents; if unchecked, users would additionally need any of the Dome9 Application roles (x_chpst_dome9.dome9_user or x_chpst_dome9.dome9_admin) to access the Dome9 Compliance Incidents.	Checked
Resolve States	List of incident state, User can select multiple state in Resolve States and selected states will be considered as resolved and populated in dropdown of Resolved Incident Status, remaining states will be populated in Repened Incident Status	Canceled, Closed, Resolved
Resolved Incident Status	Select the status which marks the Incident resolved when alert received from Dome9 as Passed.	None
Reopened Incident Status	Select the status which marks the Incident as re-opened when the Incident is resolved on ServiceNow and received alert is Failed on Dome9.	New
Child Incident Creation Condition	Provide the condition for creating a Child Incident. If the given condition matches while re-opening the existing Dome9 Parent Incident, then the application will automatically create a Child Incident for that Parent Incident. If the condition is not given then the child incident will not be created.	
Compliance Alert Field Mappings	To map Dome9 Attributes with existing Incident table's columns, select the column name for the attribute to map. Only the columns with the String data type will be displayed.	<ul style="list-style-type: none"> <li>Compliance Rule Short description</li> <li>Compliance Rule Description Description</li> </ul>
Assignment Criteria	Assignment criteria define how the Incidents created from incoming	Empty list

	Dome9 alerts are assigned to specific ServiceNow groups.	
Mandatory field configuration	It defines the fields which should not be empty while closing incidents	

### 3.5. Configure Related List in incident table

1. To configure the related list to see the related Dome9 alert, click on the “additional actions” button  located at top left of the incident table form view.
2. Hover the cursor over the “Configure” menu item and click on the “Related Lists” in the sub menu.



3. Select the “Dome9 Compliance Incident” relationship from the list, click on the add button and then click on the save button.

- The related list for the related Dome9 alert can be seen at the bottom of the form.

Incident	Cloud Platform	Created	Short description	Cloud Account	Entity	Entity Type	Assignment group
INC0011629	GCP	2021-04-19 02:45:25	VMInstance with service SQL Server Analysis Service browser(TCP:2382) is exposed to a wide network scope	GCP (fullenv-149408)	gke-your-first-cluster-1-pool-1-c325781a...	iamUser	(empty)

### 3.6. Dome9 Notification Configuration

This section describes how to configure a Notifications Policy on Dome9, which is used to send alerts to ServiceNow using the Dome9 application on ServiceNow.

**Role Required:** Dome9 Application Role

**Procedure:**

- Login to the Dome9 web application (<https://secure.dome9.com>).
- Navigate to "Compliance & Governance" "Notifications".
- Click "Add Notification".

4. One pop-up will appear for creating a new Notification. Fill in the form with the following details.

Field	Description
Name	Name of Notification
Immediate Notification	Select "Send to HTTP Endpoint" option.
Endpoint URL	https://<instance-name>. service-now.com/api/x_chpst_dome9/alerts.
Authentication Type	Select "Basic".
Username and Password	<ul style="list-style-type: none"> <li>• Create a User on ServiceNow instance with "x_chpst_dome9.dome9_forwarder" application role. (see <a href="#">Create Users</a>).</li> <li>• Enter the Username and Password of that User here.</li> </ul>

5. Click "Test" to check the connectivity with ServiceNow. If successful, "Webhook test succeeded" will be displayed.

**Create New Notification**

**Name**  
ServiceNow Instance

**Description**

**Alerts Console**  
☒ Include in the alerts console

**Scheduled Report**  
☐ Email scheduled report

**Immediate Notification**  
☐ Email report with changes from previous assessment  
☐ Send a separate message for each finding  
☐ SNS notification for each new finding as soon as it is discovered  
☒ Send to HTTP Endpoint  
 Endpoint URL: https://INSTANCE-NAME.service-now.com/api/x\_chpst\_dome9/alerts **Test**

**Authentication Type**  
Basic

**Username**  
dome9.forwarder

**Password**  
\*\*\*\*\*

**Security Management Systems**  
☐ Send findings to AWS Security Hub

**Issue Management Systems**  
☐ PagerDuty

**CANCEL** **SAVE**

6. Click "Save".

## 4. Use Cases

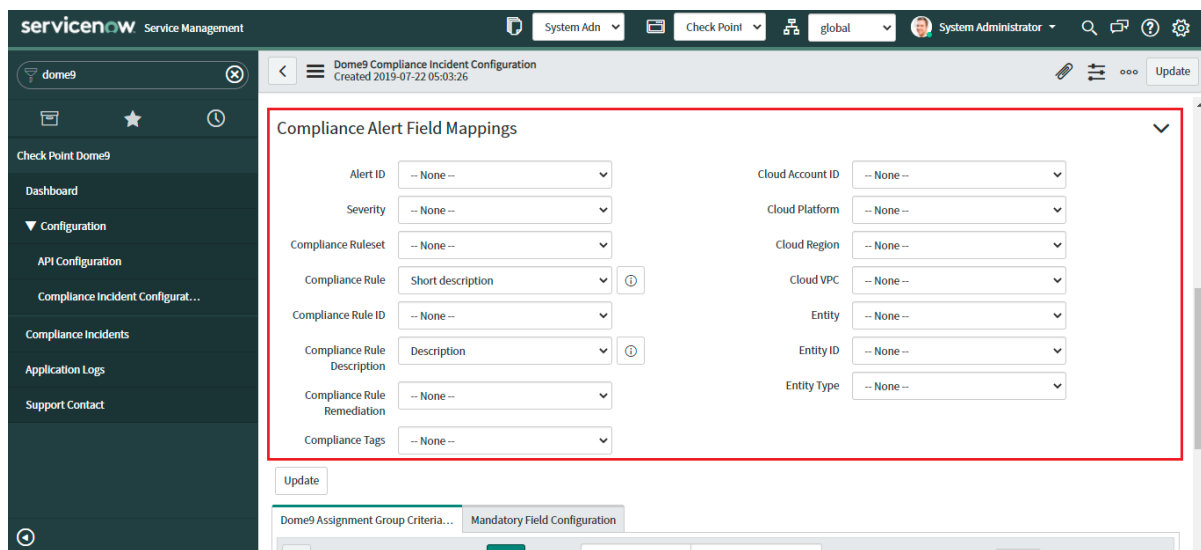
This section describes some use-cases for the ServiceNow-Dome9 integration, to view and manage Dome9 incidents on ServiceNow.

### 4.1. Alert mapping to the fields of incident

**Role Required:** x\_chpst\_dome9.dome9\_admin

**Procedure:**

1. Login to the ServiceNow instance.
2. Navigate to the 'Compliance Incident Configuration'.
3. Users can see the section 'Compliance Alert Field Mapping'.



4. Users can set any Dome9 alert attributes to the string field of the incident.
5. By default 'Compliance Rule' is mapped to the 'Short Description' field of incident and 'Compliance Rule Description' is mapped to the 'Description' field of incident.
6. When a new alert is forwarded to the ServiceNow at that time the fields of incident will be populated based on the mapping given by the user.

### 4.2. View Incidents

**Role Required:** x\_chpst\_dome9.dome9\_admin or x\_chpst\_dome9.dome9\_user

**Procedure:**

1. Login to the ServiceNow instance.
2. Navigate to "Compliance Incidents", to see the list of Incidents.

Incident	Cloud Platform	Created	Short description	Cloud Account	Entity	Entity Type	Assignment group
INC0012871	GCP	2023-04-14 02:16:09	VMInstance with service SQL Server Analysis Service browser(TCP:2382) is exposed to a wide network scope	GCP (fullenv-149408)	gke-your-first-cluster-1-pool-1-c325781a	VMInstance	AdminTeam
INC0012870	GCP	2023-04-14 00:09:51	VMInstance with service SQL Server Analysis Service browser(TCP:2382) is exposed to a wide network scope	GCP (fullenv-149408)	gke-your-first-cluster-1-pool-1-c325781a	VMInstance	AdminTeam
INC0012222	AWS	2023-04-13 06:10:57	Instances without Inspector runs in the last 30 days	AWS	scheduler-VMSSafe-qa (i-01314ba17030978d8f)	Instance	(empty)
INC0012221	AWS	2023-04-13 06:10:57	Instances without Inspector runs in the last 30 days	AWS	scheduler-NetSec3-qa (i-00af60c0eccc0d04f)	Instance	(empty)
INC0012241	AWS	2023-04-13 06:10:57	Instances without Inspector runs in the last 30 days	AWS	mongo-qa (i-0c53127f1338c705a)	Instance	(empty)
INC0012231	AWS	2023-04-13 06:10:57	Instances without Inspector runs in the last 30 days	AWS	scheduler-Misc-qa (i-0215a4e908418af52)	Instance	(empty)
INC0011119	AWS	2023-04-13 06:10:57	Ensure first access key is rotated every 90 days or less	AWS	yogev-jNDASSYOLWSF5BPMYU2	lambdaUser	(empty)
INC0012244	AWS	2023-04-13 06:10:57	Ensure multi factor authentication (MFA) is enabled for all IAM users that have a console password	AWS	hj box app poc (AIDAXSFJBDGPKAV7NMVB)	lambdaUser	(empty)
INC0012231	AWS	2023-04-13 06:10:57	Instances without Inspector runs in the last 30 days	AWS	bastion-qa (i-0f8bd481944286c75)	Instance	(empty)
INC0012225	AWS	2023-04-13 06:10:57	Instances without Inspector runs in the last 30 days	AWS	scheduler-NetSec3-qa (i-0f8bd481944286c75)	Instance	(empty)
INC0011193	AWS	2023-04-13 06:10:57	Instances without Inspector runs in the last 30 days	AWS	mongo-qa (i-0c53127f1338c705a)	Instance	(empty)
INC0012066	AWS	2023-04-13 06:10:57	Ensure multi factor authentication (MFA) is enabled for all IAM users that have a console password	AWS	hj box app poc (AIDAXSFJBDGPKAV7NMVB)	lambdaUser	(empty)
INC0012220	AWS	2023-04-13 06:10:57	Instances without Inspector runs in the last 30 days	AWS	scheduler-NetSec3-qa (i-0f8bd481944286c75)	Instance	(empty)

- Click on any Compliance Incident record to open the form view and view the fields related to the Dome9 alert. Form view also contains the attached incidents as related lists, and the user can navigate to the linked incident by clicking on it.

Alert ID: asdfghyrewazcgh

Compliance Ruleset: GCP Dome9 Best Practices

Rule ID: D9.GCP.NET.AG3.VMInstance.2382.TCP

Entity: gke-your-first-cluster-1-pool-1-c325781a-e657

Entity Type: VMInstance

Assignment group: AdminTeam

Compliance Rule Remediation: Configure your database to only allow access from internal networks and limited access scope. If public interface exists, remove it and limit the access scope within the network only to applications or instances that requires access. See <https://cloud.google.com/compute/docs/networking> for further reading about GCP networking and Firewall rules.

Raw JSON Alert:

```

{
  "status": "Failed",
  "policy": {
    "object": "policy: Object"
  },
  "findingKey": "asdfghyrewazcgh",
  "bundle": {
    "object": "bundle: Object"
  },
  "reportTime": "2019-08-19T11:15:05.662",
  "rule": {
    "object": "rule: Object"
  },
  "account": {
    "object": "account: Object"
  },
  "region": "us-central1",
  "entity": {
    "object": "entity: Object"
  },
  "remediationActions": [
    "Array(0)"
  ]
}

```

Update Acknowledge on Dome9 Create Dome9 Exclusion Delete

Parent Incident (1) Child Incidents

- Users can see the related parent incident as well as child incidents in the related list given below the form. Detailed information about the child incident will be found in section 4.10.

Update Acknowledge on Dome9 Create Dome9 Exclusion Delete

Parent Incident (1) Child Incidents (1)

Incidents

Number	Opened	Short description	Caller	Priority	State	Category	Assignment group	Assigned to	Updated	Updated by
INC0010764	2021-04-20 04:04:06	VMInstance with service SQL Server Analysis Service browser(TCP:2382) is exposed to a wide network scope	Dome9 Forwarder	5 - Planning	In Progress	Inquiry / Help	Incident Management	(empty)	2021-04-20 04:06:47	Dome9 Forwarder

- Users can directly open the incident from list view by clicking on the incident number in the incident column.

### 4.3. Acknowledge Dome9 Incidents

**Role Required:** x\_chpst\_dome9.dome9\_admin or x\_chpst\_dome9.dome9\_user

**Procedure:**

- Login to the ServiceNow instance.
- Navigate to "Compliance Incidents".
- Click on any compliance incident to open the form view and click "Acknowledge on Dome9". (Note: the API configuration must be configured; see [API Configuration \(optional\)](#)).

System Admin Check Point System Administrator

Update Acknowledge on Dome9 Create Dome9 Exclusion Delete

Alert ID asdfghytrewazxcfgh Incident INC0012870

Compliance Ruleset GCP Dome9 Best Practices Short description VMInstance with service SQL Server Anal

Rule ID D9.GCP.NET.AG9.VMInstance.2382.TCP Dome9 Severity Medium

Entity gke-your-first-cluster-1-pool-1-c325781e Compliance Tags Network Ports Security

Entity Type VMInstance Cloud Account GCP (fullenv-149408)

Entity Tags Cloud Region us-central1

Assignment group AdminTeam Cloud VPC

Compliance Rule Remediation Configure your database to only allow access from internal networks and limited access scope. If public interface exists, remove it and limit the access scope within the network only to applications or instances that requires access. See <https://cloud.google.com/compute/docs/networking> for further reading about GCP networking and Firewall rules.

Raw JSON Alert

```

status: Failed
policy: Object
findingKey: asdfghytrewazxcfgh
bundle: Object
reportTime: 2019-08-19T11:15:05.66Z
  
```

- One pop-up will open, enter a comment (maximum 200 characters) for the acknowledgement, and then click "Acknowledge".



#### 4.4. Create Dome9 Exclusions

**Role Required:** x\_chpst\_dome9.dome9\_admin or x\_chpst\_dome9.dome9\_user

**Procedure:**

1. Login to the ServiceNow instance.
2. Navigate to “Compliance Incidents”.
3. Click on any compliance incident to open the form view and click “Create Dome9 Exclusion”. (Note: the API configuration must be configured; see [API Configuration \(optional\)](#)).

4. One pop-up will open, check the appropriate criteria for creating the exclusion, and enter a comment (maximum 200 characters). Click “OK” to create the exclusion on Dome9.

**Create New Exclusion**

Exclusions are filters on compliance findings. For more information [click here](#).

Ruleset  
AWS PCI-DSS 3.2

☒ Exclude by Rule  
Restrict outbound traffic to that which is necessary, and specifically deny all other

☒ Exclude by Cloud Account  
AWS (520045580702)

☐ Exclude by Entity ID

Comment (34/200)  
Exclusion created from ServiceNow.

Cancel OK

#### 4.5. View linked information on Dome9 from incidents in ServiceNow

**Role Required:** x\_chpst\_dome9.dome9\_admin or x\_chpst\_dome9.dome9\_user

**Procedure:**

1. Login to the ServiceNow instance.
2. Navigate to "Compliance Incidents".
3. Click on any compliance incident to open the form view, and then click "Open on Dome9" opposite corresponding to fields, to open a page in the Dome9 web application showing information for the selected field.

**ServiceNow Service Management**

**Dome9 Compliance Incident**  
Created 2021-04-14 00:09:51

Alert ID: asdfghytrewazxcfgh [Open on Dome9](#)

Compliance Ruleset: GCP Dome9 Best Practices

Rule ID: D9.GCP.NET.AG9.VMInstance.2382.TCP [Open on Dome9](#)

Entity: gke-your-first-cluster-1-pool-1-c325781s [Open on Dome9](#)

Entity Type: VMInstance

Entity Tags:

Assignment group: AdminTeam

Compliance Rule Remediation: Configure your database to only allow access from internal networks and limited access scope. If public interface exists, remove it and limit the access scope within the network only to applications or instances that requires access. See <https://cloud.google.com/compute/docs/networking> for further reading about GCP networking and Firewall rules.

Raw JSON Alert: 

```
{
  "status": "Failed",
  "policy": "Object",
  "findingKey": "asdfghytrewazxcfgh",
  "bundle": "Object",
  "reportTime": "2019-08-19T11:15:05.66Z",
  "rule": "Object"
}
```

Incident: INC0012870

Short description: VMInstance with service SQL Server Anal

Dome9 Severity: Medium

Compliance Tags: Network Ports Security

Cloud Account: GCP (fullenv-149408)

Cloud Region: us-central1

Cloud VPC:

**Note:** Users may have to navigate to other time slots or change the default filtering criteria on Dome9 web application to view the information for the selected field.

#### 4.6. Copy to Clipboard

**Role Required:** x\_chpst\_dome9.dome9\_admin or x\_chpst\_dome9.dome9\_user

**Procedure:**

1. Login to the ServiceNow instance.
2. Navigate to “Compliance Incidents”.
3. Click on any compliance incident to open the form view, and then click “Copy to Clipboard” next to the Raw JSON Alert field to copy the alert JSON to the clipboard.

The screenshot shows the ServiceNow interface for a Dome9 Compliance Incident. The left sidebar contains navigation links for Check Point Dome9, Dashboard, Configuration, API Configuration, Compliance Incident Configuration, Compliance Incidents, Application Logs, and Support Contact. The main form displays the following fields:

- Alert ID: asdfghytrewazxcfgh
- Incident: INC0012870
- Compliance Ruleset: GCP Dome9 Best Practices
- Short description: VMInstance with service SQL Server Anal
- Rule ID: D9.GCP.NET.AG9.VMInstance.2382.TCP
- Dome9 Severity: Medium
- Entity: gke-your-first-cluster-1-pool-1-c325781e
- Compliance Tags: Network Ports Security
- Entity Type: VMInstance
- Cloud Account: GCP (fullenv-149408)
- Entity Tags:
- Cloud Region: us-central1
- Assignment group: AdminTeam
- Cloud VPC:
- Compliance Rule Remediation: Configure your database to only allow access from internal networks and limited access scope. If public interface exists, remove it and limit the access scope within the network only to applications or instances that requires access. See <https://cloud.google.com/compute/docs/networking> for further reading about GCP networking and Firewall rules.
- Raw JSON Alert: status: Failed, policy: Object, findingKey: asdfghytrewazxcfgh, bundle: Object, reportTime: 2019-08-19T11:15:05.66Z, rule: Object

#### 4.7. Configure assignment criteria to auto-assign new Dome9 incidents to a ServiceNow group

**Role Required:** x\_chpst\_dome9.dome9\_admin

**Procedure:**

1. Login to ServiceNow Instance.
2. Navigate to the “Compliance Incident Configuration”.
3. Go to “Dome9 Assignment Group Criteria” Related List.
4. Click on the “New” button.

The screenshot shows the ServiceNow interface for a Dome9 Compliance Incident Configuration. The form displays the following fields:

- Alert ID: -- None --
- Severity: -- None --
- Compliance Ruleset: -- None --
- Compliance Rule: Short description
- Compliance Rule ID: -- None --
- Compliance Rule Description: Description
- Compliance Rule Remediation: -- None --
- Compliance Tags: -- None --
- Cloud Account ID: -- None --
- Cloud Platform: -- None --
- Cloud Region: -- None --
- Cloud VPC: -- None --
- Entity: -- None --
- Entity ID: -- None --
- Entity Type: -- None --

The 'New' button is highlighted with a red box, indicating where to click to create a new assignment group criteria.

5. It will open below screen
6. Fill in the form with the following details and then click “Submit”.
7. Select the group and condition on Dome9 Compliance Incidents fields for which incident should be assigned to that group.

8. If a child incident is created then the assignment group will be assigned to the child incident.

**Dome9 Assignment Group Criteria**  
New record

\* Assignment Group: Capacity Mgmt

\* Order: 100

\* Condition: All of these conditions must be met

Impact is 1 - High

Compliance Rule starts with Rule

OR AND

OR AND

or

New Criteria

\* Table: Dome9 Compliance Incident [x\_chpst\_dome9\_dome9\_incident]

Submit

Field	Description
Assignment Group	Select the User Group to which Incidents are to be assigned.
Order	If more than one criterion can be applied on an incident the order of criteria will be used for application.
Condition	Create a condition which determines on which incidents the criterion will be applied.  The fields are related to Dome9 Compliance Incident [x_chpst_dome9_compliance_incident] table.

To update an existing criterion, click on the record from list view, do the required changes, and then click "Update". To delete a criterion, open the record and click "Delete".

**Dome9 Assignment Group Criteria**  
Created 2019-08-21 23:39:34

\* Assignment Group: ATF\_TestGroup\_ServiceDesk

\* Order: -10

\* Condition: All of these conditions must be met

Cloud Platform is GCP

OR AND

or

All of these conditions must be met

Dome9 Severity is Low

OR AND

or

New Criteria

\* Table: Dome9 Compliance Incident [x\_chpst\_dome9\_dome9\_incident]

Update Delete

## 4.8. Ability to set the resolve States from available Incident states

**Role Required:** x\_chpst\_dome9.dome9\_admin

**Procedure:**

1. Login to the ServiceNow Instance.
2. Navigate to the "Compliance Incident Configuration".
3. Click on Resolve States.
4. List of incident state should be there in dropdown
5. Users can select multiple states in the resolve states field.
6. Selected Resolve States will be added as an option in the Resolve Incident Status field.
7. The remaining states from Resolve States will be added as an option in the Reopened Incident State.

The screenshot displays the 'Compliance Incident Configuration' page in ServiceNow. The page includes a sidebar with navigation links like 'Dashboard', 'Configuration', 'API Configuration', 'Compliance Incident Configur...', 'Compliance Incidents', 'Application Logs', and 'Support Contact'. The main content area shows configuration details for Dome9 incidents, including sections for 'Allow Access to ITIL', 'Create Incident if not present', 'Child Incident Condition', and 'Resolve States'. A red box highlights the 'Resolve States' dropdown menu, which is open and shows a list of incident states: None, New, In Progress, On Hold, Resolved, Closed, and Cancelled. The 'Resolved' state is currently selected.

## 4.9. Incident state update automatically when alert is resolved on Dome9

**Role Required:** x\_chpst\_dome9.dome9\_admin

**Procedure:**

1. Login to the ServiceNow Instance.
2. Navigate to the "Compliance Incident Configuration".
3. User can select Resolved Incident State from dropdown
4. If the incident is resolved on dome9 and return status as "Passed", then in ServiceNow, incident state will be updated as per selection in dropdown
  - a. If None is selected, then App will not update the incident.

Dome9 Compliance Incident Configuration  
Created 2019-07-22 05:03:26

Compliance Incident Configuration is used to configure how the Dome9 Incidents are created and updated on ServiceNow from Dome9 Compliance Findings.

- Allow Access to ITIL:** If checked, users having the role "itil" will be allowed to access the Dome9 Compliance Incidents; If unchecked, users would additionally need any of the Dome9 Application roles (x\_chpst\_dome9\_dome9\_user or x\_chpst\_dome9\_dome9\_admin) to access the Dome9 Compliance Incidents.
- Create Incident if not present:** If checked, Incident will be created if not available in ServiceNow; If unchecked, incident will not create in ServiceNow (Applicable only if incoming Alert's status is Passed)
- Resolve States:** Selected states will be considered as resolved states for incident in ServiceNow.
- Resolved Incident Status:** The status to which the incident will transition, once the alert associated with it is resolved on Dome9.
- Reopened Incident Status:** The status to which the incident will transition, once the alert associated with it is reopened after resolved on Dome9.
- Child Incident Condition:** Provide the condition for creating Child Incident. If the given condition matches while re-opening the existing Dome9 Parent Incident, then the application will automatically create a Child Incident for that Parent Incident.
- Compliance Alert Field Mappings:** To map Dome9 Attributes with existing Incident table's columns, select the column name for the attribute to map. Only the columns with the String data-type will be displayed.
- Assignment Criteria:** Assignment criterion define how the Incidents created from incoming Dome9 alerts are assigned to specific ServiceNow group.
- Mandatory Field Configuration:** Configuration for the mandatory fields which should not be empty while closing the incidents.

Allow Access to ITIL ☒

Create Incident if not present ☒

Child Incident Condition

Add Filter Condition
Add "OR" Clause

\* Resolve States

Canceled, Closed, Resolved

Resolved Incident Status

Resolved

Reopened Incident Status

-- None --
Canceled
Closed
Resolved

5. If any option selected other than 'None' then worknote as well as Application Logs will be added. For ex - "Close" is selected in Resolved Incident Status
  - a. In work Notes - State changed to "Closed" automatically as the finding is resolved on Dome9.
  - b. In Application logs - [resolveIncident] Changing the state of the incident with number <INCIDENT NUMBER>to Closed(7)
6. If any fields of the Incident table are populated with default values then it will be mentioned in Work Notes as well as Application Logs.
  - a. Populating default values for the fields : category, subcategory
7. Proper Application logs are added for better User Experience.  
**Note:** we are just updating status while closing/resolving incidents. Other fields will not be updated.

#### 4.10. Reopen Incident if same alert generated again

**Role Required:** x\_chpst\_dome9.dome9\_admin

**Procedure:**

1. Login to ServiceNow Instance.
2. Navigate to "Compliance Incident Status".
3. The user can select Reopened Incident State from dropdown. The default value for this field will be "New".
4. If the incident's state is in list of resolve states on ServiceNow and if the same alert is generated again on Dome9 then the app will reopen the incident as per selection in dropdown. otherwise it will create a new incident.
  - a. If None is selected, then App will not change the state of incident
5. **Note:** If Any incident is Created and resolved in SNOW and after that deleted from SNOW and again the same alert is received from SNOW then it will be considered as a new Incident.

Date: 13 Jan 2022

Page 30 of 40

Compliance Incident Configuration is used to configure how the Dome9 Incidents are created and updated on ServiceNow from Dome9 Compliance Findings.

- Allow Access to ITIL:** If checked, users having the role "itil" will be allowed to access the Dome9 Compliance Incidents; If unchecked, users would additionally need any of the Dome9 Application roles (x\_chpst\_dome9.dome9\_user or x\_chpst\_dome9.dome9\_admin) to access the Dome9 Compliance Incidents.
- Create Incident if not present:** If checked, Incident will be created if not available in ServiceNow; If unchecked, incident will not create in ServiceNow (Applicable only if incoming Alert's status is Passed)
- Resolve States:** Selected states will be considered as resolved states for incident in ServiceNow.
- Resolved Incident Status:** The status to which the incident will transition, once the alert associated with it is resolved on Dome9.
- Reopened Incident Status:** The status to which the incident will transition, once the alert associated with it is reopened after resolved on Dome9.
- Child Incident Condition:** Provide the condition for creating Child Incident. If the given condition matches while re-opening the existing Dome9 Parent Incident, then the application will automatically create a Child Incident for that Parent Incident.
- Compliance Alert Field Mappings:** To map Dome9 Attributes with existing Incident table's columns, select the column name for the attribute to map. Only the columns with the String data-type will be displayed.
- Assignment Criteria:** Assignment criterion define how the Incidents created from incoming Dome9 alerts are assigned to specific ServiceNow group.
- Mandatory Field Configuration:** Configuration for the mandatory fields which should not be empty while closing the incidents.

Allow Access to ITIL ☒

Create Incident if not present ☒

Child Incident Condition

Resolved Incident Status

Resolved Incident Status

Reopened Incident Status

Created

#### 4.11. Set a condition to create child incident when parent incident reopens

**Role Required:** x\_chpst\_dome9.dome9\_admin

**Procedure:**

1. Login to ServiceNow Instance.
2. Navigate to "Compliance Incident Configuration".
3. A User can set a condition in "Child Incident Creation Condition".
4. If the incident is resolved and received Dome9 alert with status 'Failed' then:
  - a. If no conditions are provided, then the application will work the same as before i.e. the child incident will not be created.
  - b. If the condition is provided and matched with the parent incident then the parent incident will be reopened and a new child incident will be created and will have the same state as parent incident.
  - c. If the condition is not matched then the parent incident will be reopened and the child incident will not be created.
  - d. If the child incident is created, then data will be updated to child incident only. So in future if the same alert is generated again with status 'Failed' it will update the child incident.
  - e. If the child incident is resolved and again the same alert with status 'Failed' is forwarded to ServiceNow then again we will create a new child incident if condition is matched in configuration, and if condition doesn't match then it will reopen the parent incident.
  - f. If the same alert with status 'Passed' is forwarded to ServiceNow then it will close all the child as well as the parent.

**5. Note:**

- a. If Any incident is Created and resolved in SNOW and after that deleted from SNOW and again the same alert is received from SNOW then it will be considered as a new Incident.

- b. If the state of the parent incident is manually changed by the user, then the state of all the children will be synchronized with parent incident as per the default behaviour of servicenow.
- c. Even if the user uses any custom state or selects “New” in resolved incident state and “In Progress” in reopen incident state, then while reopening the incident all the children and parent incident will get reopened as per the default behaviour of servicenow. The parent-child synchronization is explained in the URL given below.

<https://docs.servicenow.com/bundle/quebec-it-service-management/page/product/incident-management/concept/parent-child-state-sync.html>

The screenshot displays the 'Dome9 Compliance Incident Configuration' page in ServiceNow. The left sidebar shows the navigation menu with options like 'Check Point Dome9', 'Dashboard', 'Configuration', 'API Configuration', 'Compliance Incident Configurat...', 'Compliance Incidents', 'Application Logs', and 'Support Contact'. The main content area has a title bar 'Dome9 Compliance Incident Configuration' and a subtitle 'Created 2019-07-22 05:03:26'. A blue information box at the top explains the purpose of the configuration. Below this, there are several configuration sections: 'Allow Access to ITIL' (checked), 'Create Incident if not present' (checked), 'Resolve States' (set to 'Canceled, Closed, Resolved'), 'Resolved Incident Status' (set to 'Resolved'), and 'Reopened Incident Status' (set to 'In Progress'). The 'Child Incident Condition' section is highlighted with a red box, showing a filter condition: 'Resolved' before 'Last 30 days'. Below this is the 'Compliance Alert Field Mappings' section with dropdowns for Alert ID, Severity, Compliance Ruleset, Cloud Account ID, Cloud Platform, Cloud Region, and Cloud MDR.

## 4.12. Customize Mandatory Fields While Closing Incidents

**Role Required:** admin

**Procedure:**

1. Login to the ServiceNow instance.
2. Navigate to “Compliance Incident Configuration”.
3. Go to “Mandatory Field Configuration” related list.
4. Click on the “New” button.



**Dome9 Compliance Incident Configuration**  
Created 2019-07-22 05:03:26

Update

Alert ID	-- None --	Cloud Account ID	-- None --
Severity	-- None --	Cloud Platform	-- None --
Compliance Ruleset	-- None --	Cloud Region	-- None --
Compliance Rule	Short description	Cloud VPC	-- None --
Compliance Rule ID	-- None --	Entity	-- None --
Compliance Rule Description	Description	Entity ID	-- None --
Compliance Rule Remediation	-- None --	Entity Type	-- None --
Compliance Tags	-- None --		

Update

Dome9 Assignment Group Criteria Mandatory Field Configuration (4)

Mandatory Field Configuration New Search Mandatory Field while closing incident Search

1 to 4 of 4

Dome9 Mandatory Field Configurations

Mandatory Field while closing incident Default Value

5. It will open below the screen.

**Dome9 Mandatory Field Configuration**  
New record

Submit

This configuration give flexibility to customize the mandatory fields which should not be empty while closing the incidents.

- Mandatory Field while closing incident:** Select name of the field which should not be empty while closing incident.
- Default Value:** The selected field will be populated with default value, if selected field found empty while closing the incident.

If the default value field is not defined then the selected field will be populated with preformatted string(Dome9 URL\_Alert ID\_Updated Date).

**Note:** Please enter the value from the available choice list if the selected field in the incident table has a dropdown

\* Mandatory Field while closing incident -- None --

Default Value

Submit

6. Select any field from the dropdown list, to make it mandatory while closing the incident.
7. Provide default value for the selected field in "Default Value" field.
8. If the user didn't provide any value in the field then the selected field will be populated with "<Dome9 URL>\_<Alert\_ID>\_<Updated Date>" if found empty while closing the incident.

**Note:** To open existing records, users have to click on the Default value field. Clicking on the first column will redirect the user to the parent table(As per ServiceNow out of the box feature).

**Note:** It would be good to provide default value from choices available in the incident table in case the selected field has choices. ex - if the selected field is Category then provide the default value as software or hardware.

**Note:** Mandatory field while closing Incident will be visible to the user who has an admin role, As this field shows the option from the system table.

#### 4.13. Create incident if not present in SNOW when alert received with status “Passed”

**Role Required:** x\_chpst\_dome9.dome9\_admin

**Procedure:**

1. Login to the ServiceNow instance.
2. Navigate to “Compliance Incident Configuration”.
3. Checkbox for ‘Create Incident if not present’ is given.
4. By default this checkbox will be checked.
5. If the checkbox is checked then if any alert received with status ‘Passed’ in servicenow, but incident or dome9 compliance incident record for the same alert is not found in servicenow then it will create the incident and mark it as closed/resolved as per the selection in Resolved Incident status. and return status 201 to Dome9.
6. If the checkbox is not checked and the alert received with the status 'Passed' in SNOW, but the incident is not present for the same alert then it will not create an incident as per configuration and the 200 status code will be returned.

Dome9 Compliance Incident Configuration  
Created 2019-07-22 05:03:26

Compliance Incident Configuration is used to configure how the Dome9 Incidents are created and updated on ServiceNow from Dome9 Compliance Findings.

- **Allow Access to ITIL:** If checked, users having the role "ITIL" will be allowed to access the Dome9 Compliance Incidents; if unchecked, users would additionally need any of the Dome9 Application roles (x\_chpst\_dome9.dome9\_user or x\_chpst\_dome9.dome9\_admin) to access the Dome9 Compliance Incidents.
- **Create Incident if not present:** If checked, Incident will be created if not available in ServiceNow; if unchecked, Incident will not create in ServiceNow (Applicable only if Incoming Alert's status is Passed)
- **Resolved Incident Status:** The status to which the incident will transition, once the alert associated with it is resolved on Dome9.
- **Reopened Incident Status:** The status to which the incident will transition, once the alert associated with it is reopened after resolved on Dome9.
- **Compliance Alert Field Mappings:** To map Dome9 Attributes with existing Incident table's columns, select the column name for the attribute to map. Only the columns with the String data-type will be displayed.
- **Assignment Criteria:** Assignment criterion define how the Incidents created from Incoming Dome9 alerts are assigned to specific ServiceNow group.
- **Mandatory Field Configuration:** Configuration for the mandatory fields which should not be empty while closing the incidents.

Allow Access to ITIL ☒

Create Incident if not present ☒

Resolved Incident Status

Reopened Incident Status

Compliance Alert Field Mappings

#### 4.14. View the Dashboard

**Role Required:** x\_chpst\_dome9.dome9\_admin or x\_chpst\_dome9.dome9\_user

**Procedure:**

1. Login to the ServiceNow instance.
2. Navigate to “Dashboard” from the Navigation Menu.
3. Apply filters as necessary to view the displayed information.
4. If any filter shows option (empty) then also the user can select the filter of (empty) and clicking on “Apply Filter” will populate the dashboard accordingly.
5. Dashboard will show the counts based on Dome9 Compliance Incidents record.

**Note:** Created Incident and Active incident will show the counts of the parent incident which are directly associated with the Dome9 Compliance Incident

## Dome9 Compliance Incidents Dashboard



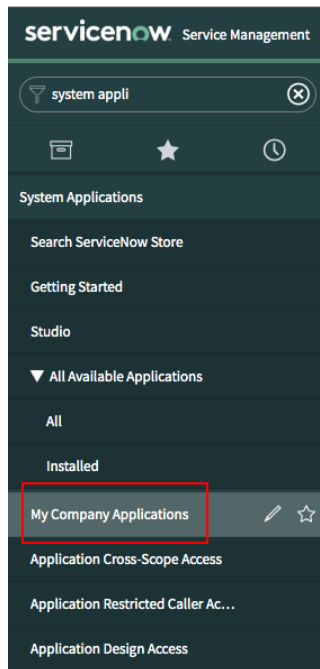
## 5. Uninstallation

This section describes how to uninstall the Dome9 application from a ServiceNow instance.

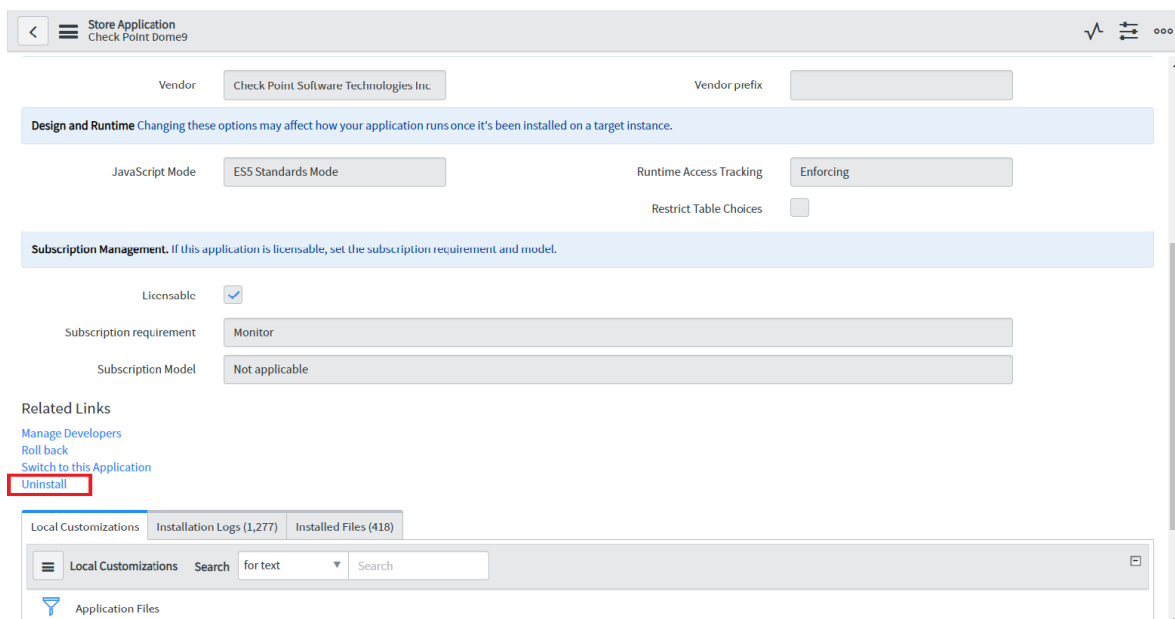
**Role Required:** System Administrator (admin)

Following steps will guide you how to uninstall the Check Point Dome9 App from the ServiceNow UI.

1. Search for “Applications” under “System Applications” from the left navigation menu.



2. From the Application Manager, select “Check Point Dome9” application.
3. Click “Uninstall” to remove the application.

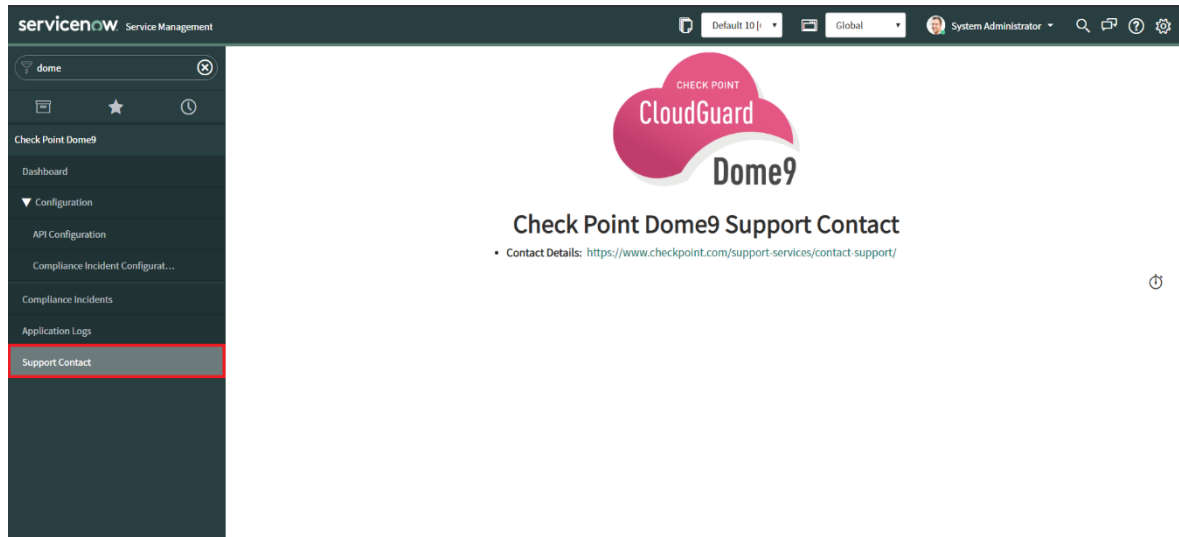


## 6. Support, Troubleshooting, and Known Limitations

### 6.1. Support

**Role Required:** x\_chpst\_dome9.dome9\_admin or x\_chpst\_dome9.dome9\_user

Support Contact Details: <https://www.checkpoint.com/support-services/contact-support/>

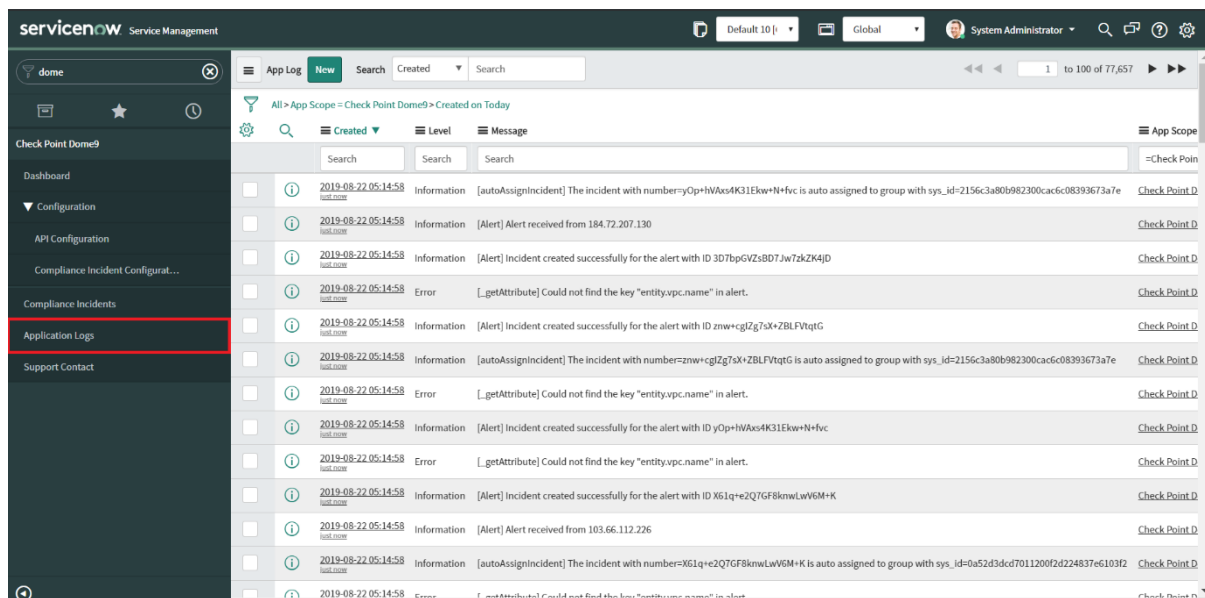


### 6.2. Troubleshooting

#### 6.2.1. Application Logs

**Role Required:** System Administrator (admin)

1. The user should check the application logs whenever it experiences any errors.



#### 6.2.2. Unable to install Dome9 application from ServiceNow Store

**Problem Statement:** Unable to install the application from ServiceNow Store.

1. Verify you have the system administrator (admin) role.
2. Navigate to “System Definition” “Plugins” in your instance.
3. Verify the following plugins are in active state. If not then first [install and activate these plugins](#).
  - a. Scripted REST APIs (com.glide.scripted\_rest\_services)
  - b. Content Management (com.glide.cms)
  - c. Incident (com.snc.incident)

### 6.2.3. Unable to find Dome9 custom roles

**Problem Statement:** Unable to find Dome9 custom roles.

1. Login to the ServiceNow instance with System Administrator.
2. Navigate to “System Application” “Applications”.
3. Verify the Check Point Dome9 application installed properly.
4. If the error persists, then the user should reinstall the application.

### 6.2.4. Unable to create new user Dome9 custom roles

**Problem Statement:** Unable to create a new user for Dome9.

1. Review the following link and execute the steps.

[https://docs.servicenow.com/bundle/quebec-platform-administration/page/administer/users-and-groups/task/t\\_CreateAUser.html](https://docs.servicenow.com/bundle/quebec-platform-administration/page/administer/users-and-groups/task/t_CreateAUser.html)

### 6.2.5. Unable to install/activate plugin in ServiceNow instance

**Problem Statement:** Unable to install/activate plugin in ServiceNow instance.

1. Review the following link and execute the steps.

[https://docs.servicenow.com/bundle/quebec-platform-administration/page/administer/plugins/task/t\\_ActivateAPlugin.html](https://docs.servicenow.com/bundle/quebec-platform-administration/page/administer/plugins/task/t_ActivateAPlugin.html)

### 6.2.6. Unable to get Dome9 findings and alerts

**Problem Statement:** Unable to get alerts from Dome9 as incidents on ServiceNow.

1. Login to the Dome9 instance.
2. Navigate to “Compliance & Governance” “Notifications”.
3. Open the notification and click “Test” to check the connectivity between Dome9 and ServiceNow.
4. If the error message is displayed, check the endpoint URL. It should be of the form *https://<instance-name>.service-now.com/api/x\_chpst\_dome9/alerts*.

5. Check the Username and Password of ServiceNow Dome9 forwarder user and confirm whether the `x_chpst_dome9.dome9_forwarder` application role is assigned to the user.

#### 6.2.7. Unable to perform UI Actions

**Problem Statement:** Unable to perform UI Actions “Acknowledge on Dome9” or “Create Dome9 Exclusion”.

1. Login to the ServiceNow instance with Dome9 Admin user.
2. Check whether the “API Configuration” is configured (see [API Configuration \(optional\)](#)).
3. Also check whether the API Key and Secret Key are not deleted from Dome9 application.

#### 6.2.8. Child Incident Creation Condition shows the fields which are not related to Dome9

**Description:** In Compliance Incident Configuration, Child Incident Condition field will show the fields of the table which are extended from incident.

#### 6.2.9. All Child Incidents getting reopened when parent reopens

**Problem Statement:** All Child Incidents getting reopened when parent reopens

In the incident record, If the state of the parent incident is manually changed, then the state of all the children will be synchronized with parent incident as per the default behaviour of servicenow.

Even if the user uses any custom state or selects “New” in resolved incident state and “In Progress” in reopen incident state, then while reopening the incident all the child and parent incident will get reopened as per the default behaviour of servicenow. The parent-child synchronization is explained in the URL given below.

<https://docs.servicenow.com/bundle/quebec-it-service-management/page/product/incident-management/concept/parent-child-state-sync.html>

#### 6.2.10. Widget not visible on Dashboard

**Problem Statement:** Widget not visible because it exceeded the load time.

1. Login to the ServiceNow instance.
2. Move the mouse pointer over the widget which is not visible.
3. In the top- right corner of the widget, click “refresh” icon.

### 6.3. Known Limitations

- The dashboard view may be disoriented when the screen width is minimized less than 1366px.
- Currently “Compliance Alert Field Mappings” shows fields of Incident and Task table with fields type “String”, because payload get from dome9 is in String. And we have used the same String Fields in Mandatory Fields Configuration. As of now it is not

technically possible to provide static value to all the data types or get the values from the User in different formats.