



CLOUDGUARD

14 April 2026

**CLOUDGUARD
CONTROLLER**

R81.20

Administration Guide



Check Point Copyright Notice

© 2022 - 2026 Check Point Software Technologies Ltd.

All rights reserved. This product and related documentation are protected by copyright and distributed under licensing restricting their use, copying, distribution, and decompilation. No part of this product or related documentation may be reproduced in any form or by any means without prior written authorization of Check Point. While every precaution has been taken in the preparation of this book, Check Point assumes no responsibility for errors or omissions. This publication and features described herein are subject to change without notice.

RESTRICTED RIGHTS LEGEND:

Use, duplication, or disclosure by the government is subject to restrictions as set forth in subparagraph (c)(1)(ii) of the Rights in Technical Data and Computer Software clause at DFARS 252.227-7013 and FAR 52.227-19.

TRADEMARKS:

Refer to the [Copyright page](#) for a list of our trademarks.

Refer to the [Third Party copyright notices](#) for a list of relevant copyrights and third-party licenses.

Important Information



Latest Software

We recommend that you install the most recent software release to stay up-to-date with the latest functional improvements, stability fixes, security enhancements and protection against new and evolving attacks.



Certifications

For third party independent certification of Check Point products, see the [Check Point Certifications page](#).



Check Point R81.20

For more about this release, see the R81.20 [home page](#).



Latest Version of this Document in English

Open the latest version of this [document in a Web browser](#).
Download the latest version of this [document in PDF format](#).



Feedback

Check Point is engaged in a continuous effort to improve its documentation. [Please help us by sending your comments](#).

Revision History

Date	Description
14 April 2026	Updated "Limitations" on page 97
20 November 2025	Updated "CloudGuard Controller for Cisco Identity Services Engine (ISE)" on page 40
21 August 2025	Updated "CloudGuard Controller Status" on page 83
11 June 2025	Added "Adding a user in Nutanix Prism Central with minimum permissions" on page 52
25 May 2025	Updated: "Data Center Query Objects" on page 76 "Configuration Parameters" on page 89
27 March 2025	Updated: <ul style="list-style-type: none"> ▪ "Configuration Parameters" on page 89 ▪ "Cisco ACI Objects and Properties" on page 38
21 January 2025	Updated "Azure Objects" on page 29
01 January 2025	Updated "Connecting to a Kubernetes Server" on page 45
12 December 2024	Added "Automatic Trust of Public Trusted Certificate Authorities" on page 71 Updated "Azure Objects and Properties" on page 29
01 July 2024	Updated "AWS Imported Objects" on page 21
01 May 2024	Updated "CloudGuard Controller for Cisco Application Centric Infrastructure (ACI)" on page 36
31 March 2024	Updated "Kubernetes Imported Objects" on page 47
21 February 2024	Updated "Configuring Data Center Query Objects in SmartConsole" on page 79
22 January 2024	Updated "Connecting to a Kubernetes Server" on page 45
01 January 2023	Removed CloudGuard Central Licensing

Date	Description
12 December 2023	Updated "VMware NSX-T Imported Objects" on page 66 Added "VMware NSX-T Policy mode APIs" on page 65
28 November 2023	Updated <ul style="list-style-type: none"> ▪ "CloudGuard Controller Logs and Events" on page 83 ▪ "Activating the Identity Awareness Software Blade" on page 17 ▪ "VMware NSX-T Imported Objects" on page 66 Added "Data Center Updates" on page 84
15 November 2023	Updated: <ul style="list-style-type: none"> ▪ "Connecting to a Kubernetes Server" on page 45 ▪ "Connecting to a Kubernetes Data Center Server with Management API" on page 48
13 November 2023	Updated "VMware NSX-T Imported Objects" on page 66
21 September 2023	Added "SmartTask" on page 87
07 September 2023	Updated "Connecting to a Kubernetes Server" on page 45
31 August 2023	Updated "Configuring Permissions for Amazon Web Services" on page 24
15 August 2023	Updated "Configuration Parameters" on page 89
03 August 2023	Updated "Data Center Query Objects" on page 76
18 July 2023	Updated "Connecting to a Kubernetes Server" on page 45
27 April 2023	Updated "VMware NSX-T Prerequisites" on page 65
19 April 2023	Updated: <ul style="list-style-type: none"> ▪ "Connecting to a Microsoft Azure Data Center Server from SmartConsole" on page 27 ▪ "CloudGuard Controller Monitoring" on page 83
29 March 2023	Updated "CloudGuard Controller for Cisco Identity Services Engine (ISE)" on page 40

Date	Description
05 March 2023	Updated <i>"CloudGuard Controller for VMware NSX-T Management Server"</i> on page 65
26 February 2023	Updated <i>"Azure Objects"</i> on page 29
27 November 2022	Updated: <i>"Cisco ACI Objects and Properties"</i> on page 38
20 November 2022	First release of this document

Table of Contents

Introduction to CloudGuard Controller	12
Use Case	13
What's New	15
New for AWS	15
New for Azure	15
Getting Started	16
Supported Security Gateways	16
Activating the Identity Awareness Software Blade	17
Supported Data Centers	18
CloudGuard Controller for Amazon Web Services (AWS)	19
Connecting to an Amazon Web Services Data Center Server from SmartConsole	19
Connecting to an Amazon Web Services Data Center Server with Management API	20
Connecting to an Amazon Web Services Data Center Server with Terraform	20
AWS Objects and Properties	21
AWS Imported Objects	21
AWS Import Options	22
AWS Object Names (Tags)	23
AWS Imported Properties	23
Configuring Permissions for Amazon Web Services	24
AWS STS Assume Role	25
Auto Scaling in Amazon Web Services	26
CloudGuard Controller for Microsoft Azure	27
Connecting to a Microsoft Azure Data Center Server from SmartConsole	27
Connecting to a Microsoft Azure Data Center Server with Management API	29
Connecting to a Microsoft Azure Data Center Server with Terraform	29
Azure Objects and Properties	29
Azure Objects	29

Azure Imported Properties	31
Auto Scaling in Microsoft Azure	31
CloudGuard Controller for Google Cloud Platform (GCP)	32
Configuring Permissions for Google Cloud Platform	32
Google Cloud Platform APIs	33
Connecting to a Google Cloud Platform Data Center with SmartConsole	33
Connecting to a Google Cloud Platform Data Center Server with Management API	33
Connecting to a Google Cloud Platform Data Center Server with Terraform	34
Google Cloud Platform Objects and Properties	34
GCP Imported Objects	34
GCP Import Options	34
GCP Object Names	34
GCP Imported Properties	35
CloudGuard Controller for Cisco Application Centric Infrastructure (ACI)	36
Prerequisites	36
Connecting to a Cisco ACI Data Center Server with SmartConsole	36
Connecting to a Cisco ACI Data Center Server with Management API	37
Connecting to a Cisco ACI Data Center Server with Terraform	37
Cisco ACI Objects and Properties	38
Cisco ACI Imported Objects	38
Limitations	39
CloudGuard Controller for Cisco Identity Services Engine (ISE)	40
Prerequisites	41
Connecting to a Cisco ISE Data Center with SmartConsole	42
Connecting to a Cisco ISE Data Center Server with Management API	42
Connecting to a Cisco ISE Data Center Server with Terraform	42
Cisco ISE Objects and Properties	43
Cisco ISE Imported Objects	43
Automatic Failover	43
Limitations	43

CloudGuard Controller for Kubernetes	44
Adding Kubernetes to CloudGuard Controller	44
Prerequisite	44
Connecting to a Kubernetes Server	45
Kubernetes Imported Objects	47
Connecting to a Kubernetes Data Center Server with Management API	48
Connecting to a Kubernetes Data Center Server with Terraform	48
CloudGuard Controller for Oracle Cloud Infrastructure (OCI)	49
Connecting to an OCI Data Center with SmartConsole	49
Connecting to an OCI Data Center Server with Management API	50
Connecting to an OCI Data Center Server with Terraform	50
OCI Objects and Properties	50
OCI Objects	50
OCI Imported Properties	51
CloudGuard Controller for Nutanix	52
Connecting to a Nutanix Prism Server in SmartConsole	52
Connecting to a Nutanix Data Center Server with Management API	52
Connecting to a Nutanix Data Center Server with Terraform	52
Adding a user in Nutanix Prism Central with minimum permissions	52
Nutanix Objects	55
Nutanix Imported Properties	55
CloudGuard Controller for Nuage Virtualized Services Platform (VSP)	56
Connecting to a Nuage Data Center with SmartConsole	56
Connecting to a Nuage Data Center Server with Management API	56
Connecting to a Nuage Data Center Server with Terraform	56
Nuage Objects and Properties	57
Nuage Imported Objects	57
Nuage Imported Properties	58
CloudGuard Controller for OpenStack	59
Prerequisites	59

Connecting to an OpenStack Server with SmartConsole	59
Connecting to an OpenStack Data Center Server with Management API	60
Connecting to an OpenStack Data Center Server with Terraform	60
OpenStack Objects and Properties	60
OpenStack Imported Objects	60
OpenStack Imported Properties	61
CloudGuard Controller for VMware Servers	62
Connecting to a VMware Server with SmartConsole	62
Connecting to a VMware Data Center Server with Management API	62
Connecting to a VMware Data Center Server with Terraform	62
CloudGuard Controller for VMware vCenter	63
VMware vCenter Prerequisites	63
VMware vCenter Objects and Properties	64
VMware vCenter Imported Objects	64
VMware vCenter Imported Properties	64
CloudGuard Controller for VMware NSX-T Management Server	65
VMware NSX-T Prerequisites	65
VMware NSX-T Policy mode APIs	65
VMware NSX-T Imported Objects	66
VMware NSX-T Imported Properties	66
VMware NSX-T Known Limitations	67
CloudGuard Controller for VMware NSX-V Manager Server	67
VMware NSX-V Objects and Properties	68
VMware NSX-V Imported Objects	68
VMware NSX-V Imported Properties	68
Limitations	69
Integrating with Data Center Servers	70
Connecting to a Data Center Server	70
Automatic Trust of Public Trusted Certificate Authorities	71
Using Data Center in Policy	74

Data Center Query Objects	76
Overview	76
Creating Rules with Data Center Query Objects	78
Configuring Data Center Query Objects in SmartConsole	79
Configuring Data Center Query Objects using management API	79
Configuring Data Center Query Objects using Terraform	79
Automation and Monitoring	81
CloudGuard Controller Command Line Interface	82
CloudGuard Controller Monitoring	83
CloudGuard Controller Logs and Events	83
CloudGuard Controller Status	83
Data Center Updates	84
SNMP Traps	84
Creating a User Defined Event and Sending Alerts	85
SmartTask	87
Configuration Parameters	89
Limitations	97
Glossary	99

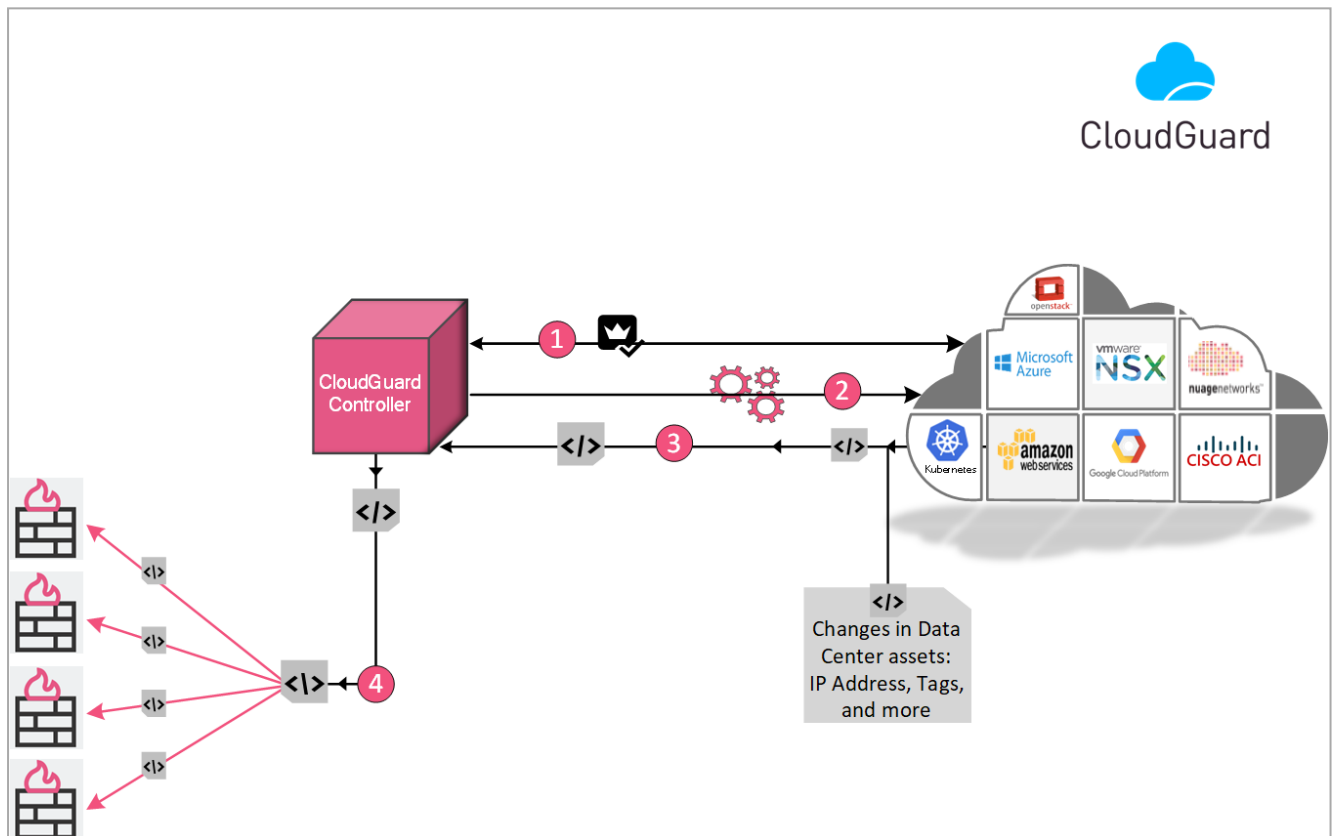
Introduction to CloudGuard Controller

A component of Check Point's Security Management Server, the CloudGuard Controller manages security in public and on-premises environments with one unified management solution.

The CloudGuard Controller dynamically learns about objects and attributes in data centers, such as changes in subnets, security groups, virtual machines, IP addresses and tags.

After using the vendor's API to establish a trust relationship with a data center, CloudGuard Controller regularly polls the connected environments for changes in objects and object attributes used in the Security Policy.

Changes are automatically pushed to the Security Gateway.



Item	Description
1	CloudGuard Controller establishes a trusted relationship with the cloud environment.
2	With the use of the vendor's APIs, the CloudGuard Controller connects to the cloud environment and regularly polls it for changes.

Item	Description
3	Changes in the cloud environment are sent to the CloudGuard Controller.
4	The CloudGuard Controller pushes updates to attributes and objects in the Security Policy rules to Check Point Security Gateways.

Use Case

Dynamic environments such as public and on-premises data centers and clouds present a large challenge to security professionals.

The number of subnets, machines, and IP addresses changes quickly.

The legacy model of manual updates to the security policy and Security Gateways every two or three days is too slow for such environments.

In most organizations, personnel from several different departments have permission to add or remove assets in data centers.

This kind of overlap creates a concern about the security and maintenance of assets in the data center.

The solution to manual updates is to protect the security and maintenance of the assets - automatically.

This is where the CloudGuard Controller comes in to assist.

With the CloudGuard Controller, the Security Operation Center (SOC) can configure the security policy to automatically detect changes in data centers, and push these changes directly to the Security Gateway.

For example, an R&D team needed to add a separate R&D server for production and a separate R&D server for staging.

This required constant emails and service tickets between the server team and SOC team.

To add or remove an IP address, the server team had to open a ticket with IT.

Then IT had to manually update the information.

For example:

Source	Destination	Action
IP1	Internet	Allow
IP2	Internet	Allow
IP3	Internet	Allow
IP4	Internet	Allow
IP5	Internet	Allow

The problem grows by each request from R&D to remove `IPxx` or add `IPyy`.

With the possibility of hundreds of IP addresses, the chance of error and frustration from the two teams is inevitable.

This is where the CloudGuard Controller comes in to help.

The CloudGuard Controller changes a static, manual process into a dynamic, automatic flow of data.

The two teams only have to use one tag.

This one tag is representative of changes in the data center.

Rather than the manual, meticulous IP table, and the constant emails between the teams, the CloudGuard Controller removes the dependency on a manual procedure.

For example:

Source	Destination	Action
<code>department=rnd</code>	Internet	Allow

Note - "`department=rnd`" is the tag.

For more information, see ["Data Center Query Objects" on page 76](#).

Check Point's CloudGuard Controller integrates with multiple virtual cloud environments. See ["Supported Data Centers" on page 18](#).

What's New

- Rule base search in SmartConsole now also match Data Center Objects.
 - These objects now show the IP addresses of all included objects in SmartConsole:
 - AWS VPC and Availability Zone
 - Azure Virtual Network
 - GCP Network
 - Improve troubleshooting: Data Center name and scan duration now appear in SmartConsole logs.
 - Improved handling of Data Centers throttling or connectivity issues.
 - Improved monitoring by integration with SmartTask.
- See the [R81.20 Quantum Security Management Server Administration Guide](#).
- Support for the new Data Center:
 - Oracle Cloud Infrastructure (OCI).
 - Nutanix

New for AWS

- Added new object types:
 - Tags for Load Balancers
 - VPC Endpoint
 - VPN Gateways and Connections
- Added support for IMDSv2 authentication.

See "[CloudGuard Controller for Amazon Web Services \(AWS\)](#)" on page 19.

New for Azure

- Added new object types:
 - Application Security Groups
 - Private Endpoints

See "[CloudGuard Controller for Microsoft Azure](#)" on page 27.

Getting Started

CloudGuard Controller is a process that runs on the Check Point Security Management Server.

Important:

1. When you install R81.20 CloudGuard Controller, these files are overwritten with default values:
 - `$MDS_FWDIR/conf/tagger_db.C`
 - `$MDS_FWDIR/conf/AWS_regions.conf`
 - `$MDS_FWDIR/conf/Azure_environments.conf`
2. Before you start the upgrade, back up all files that you changed.

Notes:

- During the upgrade, CloudGuard Controller does not communicate with the Data Center. Therefore, Data Center objects are not updated on the CloudGuard Controller or the Security Gateways.
- When the CloudGuard Controller is enabled on the Security Management Server, it starts automatically. You can stop the CloudGuard Controller with the command: `vsec stop`, and start it with: `vsec start`.
- Starting [R81.20 Jumbo Hotfix Accumulator](#) Take 84, CloudGuard Controller updates are performed automatically. For more information, refer to [sk181842](#).

- ★ **Best Practice** Check Point recommends not to add sensitive information (for example, email address or employee name) to tags, VM names, or other objects.


Supported Security Gateways

R81.20 CloudGuard Controller can manage these Security Gateways:

See the [R81.20 Release Notes](#).

-  **Note** - Support for Data Center Query Objects is from R80.10 and above.

Activating the Identity Awareness Software Blade

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click Gateways & Servers .
3	Create a new Host object with these settings: <ul style="list-style-type: none"> ▪ Name: <code>LocalHost</code> ▪ IPv4 address: <code>127.0.0.1</code>
4	Open the applicable Security Gateway / Cluster object.
5	From the left tree, click the General Properties page.
6	On the Network Security tab, select the Identity Awareness Software Blade: <ol style="list-style-type: none"> a. The Identity Awareness Configuration wizard opens. b. In the Methods for Acquiring Identity window, clear the AD Query option, if you do not use it. c. Click Cancel.
7	From the left tree, click the Identity Awareness page.
8	Select Identity Web API and click Settings .
9	Configure the Identity Web API settings: <ol style="list-style-type: none"> a. In the section Authorized Clients, click [+] and select the Host object you created earlier (<code>LocalHost</code>). b. In the Selected Client Secret field, enter your secret word, or generate a random secret. c. Click OK. <p> Note - If you add more than one authorized client host, the host that represent <code>127.0.0.1</code> must be the first item in the Authorized Clients list of the Identity Web API.</p>
10	Click OK .
11	Install the Access Control Policy.

Supported Data Centers

There are multiple ways to configure Data Centers servers:

- SmartConsole.
- Check Point Management API. See [Management API Reference](#) > Data Center topic.
- Terraform through the Check Point Provider. See [Check Point Provider](#) and search for 'data_center'.

Check Point integrates the CloudGuard Controller with these Data Centers:

- ["CloudGuard Controller for Amazon Web Services \(AWS\)" on page 19](#)
- ["CloudGuard Controller for Microsoft Azure" on page 27](#)
- ["CloudGuard Controller for Google Cloud Platform \(GCP\)" on page 32](#)
- ["CloudGuard Controller for Cisco Application Centric Infrastructure \(ACI\)" on page 36](#)
- ["CloudGuard Controller for Cisco Identity Services Engine \(ISE\)" on page 40](#)
- ["CloudGuard Controller for Kubernetes" on page 44](#)
- ["CloudGuard Controller for Nuage Virtualized Services Platform \(VSP\)" on page 56](#)
- ["CloudGuard Controller for OpenStack" on page 59](#)
- ["CloudGuard Controller for VMware vCenter" on page 63](#)
- ["CloudGuard Controller for VMware NSX-T Management Server" on page 65](#)
- ["CloudGuard Controller for VMware NSX-V Manager Server" on page 67](#)
- ["CloudGuard Controller for Oracle Cloud Infrastructure \(OCI\)" on page 49](#)
- ["CloudGuard Controller for Nutanix" on page 52](#)

CloudGuard Controller for Amazon Web Services (AWS)

The CloudGuard Controller integrates the Amazon Web Services (AWS) cloud with Check Point security.

- i Important** - The CloudGuard Controller server clock must be synchronized with the current, local time. Use of a NTP server is recommended. Time synchronization issues can cause polling information from the cloud to fail.

Connecting to an Amazon Web Services Data Center Server from SmartConsole

Step	Instructions
1	In SmartConsole, create a new Data Center object in one of these ways: <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > New AWS. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > AWS.
2	In the Enter Object Name field, enter a name.
3	Select the applicable authentication method: <ul style="list-style-type: none"> ▪ User Authentication - Uses the Access keys to authenticate. ▪ Role Authentication - Uses the AWS IAM role to authenticate. This option requires the Security Management Server to be deployed in AWS, and have an IAM Role.
4	If you choose User Authentication , enter your Access key ID and Secret access key .
5	In the Region field, select the AWS region to which you want to connect.
6	Click Test Connection .
7	Click OK .
8	Publish the SmartConsole session.
9	Install the Access Control policy on the Security Gateway object.

Connecting to an Amazon Web Services Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **AWS**.


Connecting to an Amazon Web Services Data Center Server with Terraform

See [checkpoint_management_aws_data_center_server](#).

AWS Objects and Properties

AWS Imported Objects

Object	Description
VPC	Amazon Virtual Private Cloud enables you to launch resources into your Virtual Network.
Availability Zone	A separate geographic area of a region. There are multiple locations with regions and availability zones worldwide.
Subnet	All the IP addresses from the Network Interfaces related to this subnet.
Instance	Virtual computing environments.
Tags	Groups all the instances that have the same Tag Key and Tag Value.
Security Group	Groups all the IP addresses and Security Groups from all objects associated with this Security Group.
Load Balancers	Load Balancer distributes incoming traffic across multiple targets such as EC2 Instances and IP addresses. Only Application and Network Load Balancers are supported.
VPC Endpoint	A VPC endpoint enables connections between a VPC and supported services, without requiring that you use an internet gateway, NAT device, VPN connection, or AWS Direct Connect connection.
VPN Gateways VPN Connections Customer Gateway	For VPN site-to-site connections.

Object	Description
ENI	<p>Elastic Network Interface. Supported starting R81.20 Jumbo Hotfix Accumulator Take 70.</p> <p> Note - This object is disabled by default. To enable it:</p> <ol style="list-style-type: none"> Edit the <code>vsec.conf</code> file on the Management Server (<code>\$FWDIR/conf/</code> on Security Management Server, <code>\$MDSDIR/conf/</code> on Multi-Domain Management Server) and add the line: <pre>aws.enableShowAwsENIs=true</pre> Restart the CloudGuard Controller with the command: <code>vsec stop;vsec start</code>

AWS Import Options

Use one of these options to import AWS objects to your policy:

Option	Description
Regions	Import AWS VPCs, Load Balancers, Subnets, or Instances from a certain region to your Security Policy.
Security Groups	Import all IP addresses that belong to a specific Security Group. The Security Group is used only as a container for the list of all IP addresses of Instances that are attached to this group.
Tags	Import all instances and Security Groups that have a specific Tag Key or Tag Value.

Notes:

- CloudGuard Controller saves the Tags with Key and no Value as: "Tag key="
- CloudGuard Controller truncates leading and trailing spaces in Tag Keys and Tag Values.
- All changes in AWS are updated automatically with the Check Point Security Policy. Users with permissions to change resource tags in AWS can change their access permissions.

AWS Object Names (Tags)

Object names are the same as those in the AWS console.

VPC, Subnet, Instance, and Security Group use these names:

Tag Name	Object Name
Tag Name exists	"<Object ID> (<Value of the Tag Name>)"
Tag Name does not exist	"<Object ID>"
Tag Name is empty	"<Object ID>"

AWS Imported Properties

Property	Description
Name	Resource name as shown in the AWS console. User can edit the name after importing the object.
Name in Server	Resource name as shown in the AWS console
Type in Server	Resource type
IP	Associated private and public IP addresses
Note	CIDR for subnets and VPC objects
URI	Object path
Tags	Tags (Keys and Values) that are attached to the object

Configuring Permissions for Amazon Web Services

Minimal permissions for the User or Role

Item	Value
Effect	Allow
Actions	<ul style="list-style-type: none"> ▪ ec2:DescribeInstances ▪ ec2:DescribeNetworkInterfaces ▪ ec2:DescribeSubnets ▪ ec2:DescribeVpcs ▪ ec2:DescribeSecurityGroups
Resource	All ("*")

Additional optional permissions for the User or Role

Item	Value	Used for
Effect	Allow	
Actions	"elasticloadbalancing:DescribeLoadBalancers", "elasticloadbalancing:DescribeTags"	Using Load Balancers tags and using them in the policy.
Actions	"ec2:DescribeVpnGateways", "ec2:DescribeVpnConnections", "ec2:DescribeCustomerGateways"	Automatic configuration of Site-to-site VPN.
Actions	"ec2:DescribeVpcEndpoints"	Describes VPC endpoints.

For more information about Roles and the IAM policy, see [Amazon Web Services documentation](#).

AWS STS Assume Role

AWS's Security Token Service (STS) Assume Role allows administrators to give access to AWS resources across different AWS user accounts.

Use Case

This feature is especially helpful for CloudGuard Controller administrators who manage multiple data centers.

Instead of the need for administrators to create multiple AWS user accounts and configure access permissions to AWS resources for each account, the STS Assume Role, allows them to create the necessary permissions once for use across multiple AWS accounts. For the CloudGuard Controller, this means that it connects to a specific AWS account from a different AWS user account, which has the correct credentials configured.

For more information, see [Amazon's IAM documentation](#) or watch a short video [here](#).

Configuring the STS Assume Role

The CloudGuard Controller AWS Data Center authentication supports STS Assume Role, in addition to user and IAM authentication.

In R81 and lower, the only options for authentication were the Access key and Secret access key or Role Authentication.

In R81.10 and higher, authentication includes the addition of the **STS Assume Role** checkbox, which allows these:

- Access key and Secret access key with or without STS Assume Role.
- Role Authentication with or without STS Assume Role.

To use the STS Assume Role in SmartConsole:

1. Create a new AWS Data Center object.
2. Select the authentication type (**User or Role**).

3. Select the checkbox **STS Assume Role**.
4. Enter the Role and ID as you configured during the creation of the STS Assume Role.

Auto Scaling in Amazon Web Services

The AWS Auto Scaling service with the Check Point Auto Scaling group can increase or decrease the number of CloudGuard Gateways according to the current load.


The CloudGuard Controller for AWS works with the Check Point Auto Scaling Group.

The Check Point Security Management Server updates Data Center objects automatically on the Check Point Auto Scaling group.

CloudGuard CME for Amazon Web Services automatically configures CloudGuard Gateways in Auto Scaling group to support updates of Data Center Objects from the CloudGuard Controller.


CloudGuard Controller for Microsoft Azure

CloudGuard Controller integrates the Microsoft Azure cloud with Check Point security.

-  **Important** - The CloudGuard Controller server clock must be synchronized with the current, local time. Use of a NTP server is recommended. Time synchronization issues can cause polling information from the cloud to fail.

Connecting to a Microsoft Azure Data Center Server from SmartConsole

To connect to a Microsoft Data Center Server:



-  **Best Practice** - In Microsoft Azure create a service principal (see this [article](#) for details) and assign relevant rights.

The minimum recommended permission is **Reader**.

You can assign the **Reader** permission in one of these ways:

- Assign to all Resource Groups, from which you want to pull an item
- Add the permission on a subscription level

Step	Instructions
1	In SmartConsole, create a new Data Center object in one of these ways: <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > Cloud > Data Center > New Microsoft Azure. ▪ In the top right corner, click Objects Pane > New > Cloud > Data Center > Microsoft Azure.
2	In the Enter Object Name field, enter a name.
3	Select the applicable authentication method: <ul style="list-style-type: none"> ▪ Service Principal - Uses the Service Principal to authenticate. ▪ Microsoft Entra ID User Authentication - Uses the Microsoft Entra ID User to authenticate.

Step	Instructions
4	<p>If you selected Service Principal Authentication (default):</p> <ul style="list-style-type: none"> ▪ Enter your Application ID, Application Key, and Directory ID. You can create the Service Principal in the Azure Portal, with the Azure PowerShell, or with the Azure CLI. <p>If you selected Azure AD User Authentication:</p> <ul style="list-style-type: none"> ▪ Enter your Username and Password. <p>The minimum recommended permission is Reader. You can assign the Reader permission in one of these ways:</p> <ul style="list-style-type: none"> ▪ Assign to all Resource Groups, from which you want to pull an item ▪ Add the permission on a subscription level <p> Important - If you do not have the necessary permissions, some of the functionality might not work.</p>
5	Click Test Connection .
6	Click OK .
7	<p>Import objects from your Microsoft Azure server to your policy (for more about these objects, see the next sections).</p> <ul style="list-style-type: none"> ▪ Network by Subscriptions - Import VNETS, subnets, Virtual Machines, or VMSS. ▪ Network Security Groups (NSG) - Import all IP addresses that belong to a specific NSG. The NSG is used only as a container for the list of all IP addresses (assigned to NICs and subnets) that are attached to this group. ▪ Tags - Imports all the IP addresses of Virtual Machines and VMSS that have specific tags and values. <p> Note - All changes in Microsoft Azure are updated automatically with the Check Point Security Policy. Users with permissions to change Resource Tags in Microsoft Azure can change their access permissions.</p>
8	Publish the SmartConsole session.
9	Install the Access Control policy on the Security Gateway object.

Connecting to a Microsoft Azure Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **Microsoft Azure**.

Connecting to a Microsoft Azure Data Center Server with Terraform

See [checkpoint_management_azure_data_center_server](#).

Azure Objects and Properties

Azure Objects

Object	Description
Subscription	Helps you organize access to your cloud components.
Virtual Network	Represents your Microsoft Azure Virtual Network (VNET) in the cloud.
Subnet	A range of IP addresses in a VNET. A VNET can be divided into many subnets.
Virtual Machine (VM)	Virtual computing environment.
Virtual Machine Scale Set (VMSS)	Manages sets of Virtual Machines.
Network Security Group (NSG)	NSGs contain a list of Access Control List (ACL) rules that allow or deny network traffic to the Virtual Machines instances in a Virtual Network. NSGs can be associated with either subnets or individual Virtual Machine instances in that subnet.
Load Balancer	Load Balancer distributes incoming traffic that arrives into the Load Balancer's frontend to backend pool instances, according to rules and health probes.
Tags	Keys and values attached to the object.
Application Security Group	ASGs enable you to configure network security as a natural extension of an application's structure, allowing you to group virtual machines and define network security policies based on those groups.

Object	Description
Private Endpoint	<p>A private endpoint is a network interface that uses a private IP address from your virtual network.</p> <p>This network interface connects you privately and securely to a service powered by Azure Private Link.</p> <p>By enabling a private endpoint, you're bringing the service into your virtual network.</p>
Virtual network Gateway (VNET GW)	<p>A virtual network gateway is composed of two or more VMs that are automatically configured and deployed to a specific subnet you create called the <i>gateway subnet</i>.</p> <p>The gateway VMs contain routing tables and run specific gateway services.</p>
VPN Gateway	<p>The gateway type 'VPN' specifies that the type of virtual network gateway created is a 'VPN gateway'.</p> <p>This distinguishes it from an ExpressRoute gateway, which uses a different gateway type.</p> <p>A virtual network can have two virtual network gateways - one VPN gateway and one ExpressRoute gateway.</p> <p>This object is also supported by vWAN.</p>
Application Gateway	<p>Application Gateway is supported starting R81.20 CloudGuard Controller self-updatable package Take 15.</p> <p>Note: This object is disabled by default. To enable it:</p> <ol style="list-style-type: none"> 1. Edit the <i>vsec.conf</i> file on the Management Server (<i>\$FWDIR/conf/</i> on Security Management Server, <i>\$MDSDIR/conf/</i> on a Multi-Domain Security Management Server.) 2. Add the line: <code>azure.enableApplicationGateways=true</code> 3. Restart the CloudGuard Controller with the command: <code>vsec stop;vsec start</code>
API Management service	<p>API Management service is supported starting R81.20 CloudGuard Controller self-updatable package Take 16.</p> <p>Note: This object is disabled by default. To enable it:</p> <ol style="list-style-type: none"> 1. Edit the <i>vsec.conf</i> file on the Management Server (<i>\$FWDIR/conf/</i> on Security Management Server, <i>\$MDSDIR/conf/</i> on a Multi-Domain Security Management Server.) 2. Add the line: <code>azure.enableApiManagementServices=true</code> 3. Restart the CloudGuard Controller with the command: <code>vsec stop;vsec start</code>

Azure Imported Properties

Imported Property	Description
Name	Name of the object and the object's Resource Group Format is: <code>obj_name (obj_resource_group_name)</code> The user can edit the name after importing the object.
Name in server	Name of the object and the object's Resource Group Format is: <code>obj_name (obj_resource_group_name)</code>
Type in server	Object type
IP address	<ul style="list-style-type: none"> ▪ Virtual Machines and VMSS: Public and Private IP addresses ▪ Load Balancers: Frontend IP addresses ▪ Subnets: VMs, VMSSs, and Internal Load Balancers Frontend IPs ▪ NSGs: VMSSs and Subnets IP addresses associated with this NSG ▪ Tags: VNETS, VMs, VMSSs and Load Balancers IP addresses associated with this specific Tag Key or Tag Value
Note	Contains the address prefixes for VNETs and subnets
URI	Object path
Tags	Keys and Values attached to the Object
Location	Physical location in Microsoft Azure

Auto Scaling in Microsoft Azure

The Microsoft Azure Auto Scaling service with the Check Point Auto Scaling group can increase or decrease the number of CloudGuard Gateways according to the current load.

The CloudGuard Controller for Microsoft Azure can work with the Check Point Auto Scaling Group.

The Check Point Security Management Server can update Data Center objects automatically on the Check Point Auto Scaling group.

CloudGuard CME for Microsoft Azure automatically configures CloudGuard Gateways in Auto Scaling group to support updates of Data Center Objects from the CloudGuard Controller.

CloudGuard Controller for Google Cloud Platform (GCP)

The CloudGuard Controller integrates the Google Cloud Platform (GCP) with Check Point security.

Important - The CloudGuard Controller server clock must be synchronized with the current, local time. Use of a NTP server is recommended. Time synchronization issues can cause polling information from the cloud to fail.

Configuring Permissions for Google Cloud Platform

You must authenticate and connect to your Google Cloud Platform account to retrieve objects.

Authentication is done by GCP Service Account credentials.

The CloudGuard Controller retrieves objects from all projects, to which the Service Account has access.

You can use these authentication methods:

Authentication Method	Description
Service Account VM Instance Authentication	Uses the Service Account VM Instance to authenticate. This option requires the Security Management Server to be deployed in a GCP, and run as a Service Account with the required permissions.
Service Account Key Authentication	Uses the Service Account private key file to authenticate. Use the GCP web console to create a Service Account Key JSON file.

Minimum permissions for the service account

The service account must have read permissions for all the relevant resources (example: viewer role).

- Networks
- Instances
- Subnetworks

Google Cloud Platform APIs

You must enable the Cloud Resource Manager API for the project to which the service account belongs.

The Compute Engine API must be enabled for all the projects to which the Service Account has access.

This is made from the GCP API Library.

Connecting to a Google Cloud Platform Data Center with SmartConsole

Step	Instructions
1	In SmartConsole, create a new Data Center object in one of these ways: <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > New Google Cloud Platform. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > Google Cloud Platform.
2	In the Enter Object Name field, enter the applicable name.
3	Select the applicable authentication method: <ul style="list-style-type: none"> ▪ Service Account Key Authentication ▪ Service Account VM Instance Authentication
4	If you choose Service Account Key Authentication , import the Service Account JSON file.
5	Click Test Connection .
6	Click OK .
7	Publish the SmartConsole session.
8	Install the Access Control policy on the Security Gateway object.

Connecting to a Google Cloud Platform Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **Google Cloud Platform**.

Connecting to a Google Cloud Platform Data Center Server with Terraform

See [checkpoint_management_gcp_data_center_server](#).

Google Cloud Platform Objects and Properties

GCP Imported Objects

Object	Description
VPC Networks	Your GCP VPC networks in the cloud
Subnet	All the IP addresses from the network interfaces related to this subnet
Instance	Virtual Machines instances
Tags	Groups all the instances that have the same network tag

GCP Import Options

Use **Projects** or **Tags** to import GCP objects to your policy:

Option	Description
Projects	Import VPC networks, subnets or instances from another project to your Security Policy
Tags	Import all instances that have a specific network tag

Note - All changes in GCP are automatically updated with the Check Point Security Policy. Users with permissions to change network tags in GCP can change their access permissions.

GCP Object Names

Object names are the same as those in the GCP console.

Instance and Subnet use the following names:

Object	Object Name
Instance	"<Instance Name> (<Zone Name>)"
Subnet	"<Subnet Name> (<Region Name>)"

GCP Imported Properties

Property	Description
Name	Resource name as shown in the GCP console. User can edit the name after importing the object.
Name in server	Resource name as shown in the GCP console
Type in server	Resource type
IP	Associated private and public IP addresses
Note	For instances, the list of VPC networks to which the instance belongs
URI	Object path
Tags	Network tags attached to the object

CloudGuard Controller for Cisco Application Centric Infrastructure (ACI)

CloudGuard Controller integrates the Cisco ACI fabric with Check Point security.

Prerequisites

- Cisco ACI version 6.0 or lower.
- You must have a Cisco ACI user role with at least read permissions for Tenant EPG.

Note - This role is sufficient for CloudGuard Controller functionality.

More permissions may be required for device package installation (CloudGuard for ACI).

- Enable Bridge Domain unicast routing to allow IP address learning for EPGs on the Cisco ACI.
- Define a subnet on the Bridge Domain to help the fabric maintain IP address learning tables.

This prevents time-outs on silent hosts that respond to periodic ARP requests.

- Before you upgrade the Management Server, if you have a Cisco APIC server, keep only one URL. After the upgrade, add the other URLs.

Connecting to a Cisco ACI Data Center Server with SmartConsole

Step	Instructions
1	<p>In SmartConsole, create a new Data Center object in one of these ways:</p> <ul style="list-style-type: none"> ▪ In the top left corner, click the Objects menu > More object types > Server > Data Center > New Cisco ACI. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > Cisco ACI.
2	<p>In the Enter Object Name field, enter the applicable name.</p>
3	<p>In the URLs field, enter the IP addresses of Cisco ACI Cluster Members. Multiple URLs allow support for APIC cluster for redundancy.</p> <p>Important - These IP addresses can be either HTTP or HTTPS, but not both. You must add <code>http://</code> or <code>https://</code> before the IP address.</p> <p>Important - When using multiple cluster members with HTTPS, all members must have the same HTTPS Certificate.</p>

Step	Instructions
4	In the Username field, enter your Cisco APIC server User ID. When using Login Domains, use the following syntax: <pre>apic:<domain>\<username></pre>
5	In the Password field, enter the Cisco APIC server password.
6	Click Test Connection .
7	Click OK .
8	Publish the SmartConsole session.
9	Install the Access Control Policy on the Security Gateway object.

Connecting to a Cisco ACI Data Center Server with Management API

Go to [Management API Reference](#) > Click on see arguments per Data Center Server type and select Cisco ACI.

Connecting to a Cisco ACI Data Center Server with Terraform

See [checkpoint_management_aci_data_center_server](#).

Cisco ACI Objects and Properties

Cisco ACI Imported Objects

Object	Description
Tenant	A logical separator for customers, BU, groups, traffic, administrators, visibility, and more.
Application Profile	A container of logically related EPGs, their connections, and the policies that define those connections.
End-Point Group (EPG)	A container for objects that require the same policy treatment. EPG examples : app tiers or services (usually, VLAN)
End-point Security Group (ESG)	A logical entity that contains a collection of physical or virtual network endpoints.
L2 Out	A bridged external network.
L2 External EPG	An EPG that represents external bridged network endpoints.



Note - Name Alias, A cosmetic substitute for a GUI entity, is also imported.

Limitations

- Supported fabric size: The total amount of all the following objects must not exceed 100,000:
 - Tenants
 - Application Profiles
 - EPGs
 - IP addresses

For information regarding Cisco guidelines and limitations, refer to [Guidelines and Limitations for Using the REST API](#).

- APIC HTTP URLs, which redirect to HTTPS, are not supported. Use either HTTPS URLs directly, or HTTP without redirection.
- When multiple APIC URLs are specified, the connectivity test will succeed, as long as one of the URLs connects. There is no requirement for initial verification for all the URLs.
- On failure to connect to all the given APIC URLs, the returned error message is for the first unsuccessful URL.
- If an object imported from Cisco APIC is deleted on the APIC, and created again, the object must be re-imported into Check Point Policy. Enforcement will work correctly once the object is recreated in APIC, but the re-import is required to maintain updates for the object in the Management Server.
- Changes to privileges of the APIC user that was used to create the Data Center Object, are not reflected during an active login session.

For example, if a new security domain is added to the user, which allows him to see a new tenant, this is not visible to the APIC scanner.

- To resolve: Run the `vsec_controller_stop` command on the CloudGuard Controller to restart the CloudGuard Controller services and force a new log in.

CloudGuard Controller for Cisco Identity Services Engine (ISE)

The CloudGuard Controller integrates Cisco ISE with Check Point security. It allows the use of TrustSec Security Groups in the Security Policy according to the static IP-to-SGT mappings in ISE. The ISE server is represented as the Data Center server in Check Point. It connects to the ISE administration nodes and automatically retrieves object data. For redundancy, it is possible to provide both primary and secondary ISE administration nodes.

The ISE External RESTful Services (ERS) API enables communication with ISE.

Prerequisites

- Cisco ISE version 3.2
- An ISE administrator with the ERS-Operator or ERS-Admin group assignment
- ERS enabled on the ISE administration nodes

Enable ERS (port 9060)

ERS uses HTTPS port 9060, which is closed by default. Clients attempting to access this port without first enabling ERS will face a timeout from the server. Therefore, the first requirement is to enable ERS from the Cisco ISE admin UI.

Go to **Administration > Settings > API Settings** and enable the **ERS (Read/Write)** toggle button.

API Settings

Overview **API Service Settings** API Gateway Settings

✓ API Service Settings for Administration Node

ERS (Read/Write)

Open API (Read/Write)

✓ CSRF Check (only for ERS Settings)

Enable CSRF Check for Enhanced Security (Not compatible with pre ISE 2.3 Clients)

Disable CSRF For ERS Request (compatible with ERS clients older than ISE 2.3)

Connecting to a Cisco ISE Data Center with SmartConsole

Step	Instructions
1	In SmartConsole, create a new Data Center object in one of these ways: <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > New Cisco ISE. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > Cisco ISE.
2	In the Enter Object Name field, enter a name.
3	In the Hostname(s) field, add the ISE administration Node(s) IP address or hostname.
4	In the Username field, enter the ISE administrator username.
5	In the Password field, enter the ISE administrator password.
6	Click Test Connection .
7	Click OK .
8	Publish the SmartConsole session.
9	Install the Access Control Policy on the Security Gateway object.

Connecting to a Cisco ISE Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **Cisco ISE**.

Connecting to a Cisco ISE Data Center Server with Terraform

See [checkpoint_management_ise_data_center_server](#).


Cisco ISE Objects and Properties

Cisco ISE Imported Objects

Object	Description
Security Groups	Groups of users, endpoints, and resources that share Access Control policies. You define the Security Groups in Cisco ISE.

Automatic Failover

If there is a failure to communicate with the provided ISE administration nodes, CloudGuard Controller enters a recovery mode. In recovery mode, it automatically attempts to establish the connection again with the administration nodes. Connection is attempted with the nodes based on the order they were entered.

-  **Important** - Make sure that the secondary node is correctly synchronized with the primary node. If not, the IP-to-SGT data may not be up to date.

Limitations

- Filtering IP-to-SGT mappings by Security Gateway name uses a wildcard ('SG_NAME') search, so incorrect IPs may be returned, in case two Security Gateway's have overlapping names (one is contained in the other).

CloudGuard Controller for Kubernetes

Adding Kubernetes to CloudGuard Controller

Check Point CloudGuard Controller now protects North-South inspection for increased Kubernetes security.

The new Container security component is available in native Kubernetes and managed Kubernetes services such as Azure Kubernetes Service (AKS), Amazon EKS, Google Kubernetes Engine, and others.

Prerequisite

- Kubernetes version 1.12 and higher.

Note - Island Mode (NATed IP address for Nodes) is not supported.

Connecting to a Kubernetes Server

1. Configure the settings in Kubernetes

- a. Create a service account for CloudGuard Controller that includes access to: endpoints, pods, services, and nodes.

Example:

Run these "kubectl create" commands in the order listed below:

```
kubectl create serviceaccount cloudguard-controller
```

```
kubectl create clusterrole endpoint-reader --  
verb=get,list --resource=endpoints
```

```
kubectl create clusterrolebinding allow-cloudguard-  
access-endpoints --clusterrole=endpoint-reader --  
serviceaccount=default:cloudguard-controller
```

```
kubectl create clusterrole pod-reader --verb=get,list --  
resource=pods
```

```
kubectl create clusterrolebinding allow-cloudguard-  
access-pods --clusterrole=pod-reader --  
serviceaccount=default:cloudguard-controller
```

```
kubectl create clusterrole service-reader --  
verb=get,list --resource=services
```

```
kubectl create clusterrolebinding allow-cloudguard-  
access-services --clusterrole=service-reader --  
serviceaccount=default:cloudguard-controller
```

```
kubectl create clusterrole node-reader --verb=get,list -  
-resource=nodes
```

```
kubectl create clusterrolebinding allow-cloudguard-  
access-nodes --clusterrole=node-reader --  
serviceaccount=default:cloudguard-controller
```

- b. Get the Kubernetes URL:

```
kubectl cluster-info
```

- c. It is necessary to have a service account token for the connection. Refer to the Kubernetes documentation for your version. For example:
- For Kubernetes version 1.24 and higher, generate and export a token for the service account to a file. The token you create must not expire. If the token expires, the Data Center loses connectivity. To create a token that does not expire:

```
kubectl apply -f - <<EOF
apiVersion: v1
kind: Secret
metadata:
  name: cloudguard-controller-secret
  annotations:
    kubernetes.io/service-account.name: cloudguard-
controller
type: kubernetes.io/service-account-token
EOF
```


```
kubectl create token cloudguard-controller > token_
file
```

Note: To add the data center in SmartConsole, the token must be Base64 decoded.

- For Kubernetes version 1.23 and lower, export the service account token to a Base64 encoded file.


```
kubectl get secret $(kubectl get serviceaccount
cloudguard-controller -o jsonpath="{.secrets
[0].name}") -o jsonpath="{.data.token}" | base64 --
decode -w 0 > token_file
```

2. Configure the settings in SmartConsole

Step	Instructions
1	In SmartConsole, create a new Data Center object in one of these ways: <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > Kubernetes ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > Kubernetes.
2	Enter a name for the Data Center object.
3	Enter the Kubernetes URL (from Step 1-b).
4	Import the service account token file (from Step 1-c).
5	Import CA certificate: connect to your Kubernetes Data Center and access kube/config. In the config, copy the *certificate-authority-data* of the relevant Data Center into a .txt file and use it as the CA certificate. <p> Note - The CA Certificate needs to be double Base64 encoded (encoded once more on top of how you receive it from Kubernetes).</p>
6	Click Test Connections and make sure that the connection works.
7	Click OK .
8	Publish the SmartConsole session.
9	Install the Access Control Policy on the Security Gateway object.

Kubernetes Imported Objects

Object	Description
Namespace	Group of resources in a single cluster.
Node	A virtual or physical machine, depending on the Cluster.
Pod	The smallest deployable units of computing that you can create and manage in Kubernetes. A group of one or more containers, with shared storage and network resources, and a specification for how to run the containers.
Service	A method for exposing a network application that runs as one or more Pods in your Cluster.

Object	Description
Labels	Key-value pairs attached to Services and Nodes within a Kubernetes cluster.
Service Endpoint	Each Service object defines a logical set of endpoints (usually, these endpoints are Pods) along with a policy about how to make those pods accessible.
Tags	<p>Keys and Values attached to the Object.</p> <p> Note - PODs get an implicit '__namespace' tag with the value of their namespace. You can use it, for example, when creating a Data Center Query to filter PODs by their namespace:</p> <ul style="list-style-type: none"> ▪ Type in data center: pod ▪ Tag key=__namespace and Tag value=<the relevant namespace> <p>The __namespace tag is supported starting R81.20 Jumbo HFA Take 43.</p>

Connecting to a Kubernetes Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **Kubernetes**.

Notes:

- The token needs to be Base64 encoded (as you receive it from Kubernetes).
- The CA Certificate needs to be double Base64 encoded (encoded once more on top of how you receive it from Kubernetes).

Connecting to a Kubernetes Data Center Server with Terraform

See [checkpoint_management_kubernetes_data_center_server](#).

CloudGuard Controller for Oracle Cloud Infrastructure (OCI)

Important - The CloudGuard Controller server clock must be synchronized with the current, local time. Use of a NTP server is recommended. Time synchronization issues can cause polling information from the cloud to fail.

Connecting to an OCI Data Center with SmartConsole

Step	Instructions
1	<p>In SmartConsole, create a new Data Center object in one of these ways:</p> <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > New Oracle Cloud. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > Oracle Cloud.
2	In the Enter Object Name field, enter a name.
3	<p>Select the applicable authentication method:</p> <ul style="list-style-type: none"> ▪ API Key Authentication A user generated API key will be uploaded to the Management machine to authenticate with OCI. This API key must be configured with read permissions for all resources in the tenancy. <ul style="list-style-type: none"> • User id: The id of the user the key belongs to • Tenancy id: The tenancy the key belongs to • Region id: The region to scan • API key: Secret key ▪ VM Instance Authentication Tells the Management Server it is a VM in OCI with inspect permissions. It requires that the Management Server be installed in OCI and is part of a dynamic group with a policy that provides read permissions for all resources in the tenancy.
4	Click Test Connection .
5	Click OK .
6	Publish the SmartConsole session.
7	Install the Access Control policy on the Security Gateway object.

Connecting to an OCI Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **Oracle Cloud**.

Connecting to an OCI Data Center Server with Terraform

See <https://registry.terraform.io/providers/CheckPointSW/checkpoint/latest>.

OCI Objects and Properties

OCI Objects

Object	Description
VPC	Oracle Cloud Infrastructure enables you to launch resources into your Virtual Network.
Subnet	All the IP addresses from the Network Interfaces related to this subnet.
Instance	Virtual computing environments.
Tags	Groups all the objects that have the same Tag Key and Tag Value.

Notes:

- CloudGuard Controller truncates leading and trailing spaces in Tag Keys and Tag Values.
- All changes in OCI are updated automatically with the Check Point Security Policy.
Users with permissions to change resource tags in OCI can change their access permissions.

OCI Imported Properties

Property	Description
Name	Resource name as shown in the OCI console. User can edit the name after importing the object.
Name in Server	Resource name as shown in the OCI console.
Type in Server	Resource type.
IP	Associated private and public IP addresses.
Note	CIDR for subnets and VPC objects.
URI	Object path.
Tags	Tags (Keys and Values) that are attached to the object.

CloudGuard Controller for Nutanix

Connecting to a Nutanix Prism Server in SmartConsole

Step	Instructions
1	In SmartConsole, create a new Data Center object in one of these ways: <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > New Nutanix. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > Nutanix.
2	In the Enter Object Name field, enter the applicable name.
3	In the Hostname field, enter the IP address or hostname of your Nutanix Prism Server.
4	In the Username field, enter your Nutanix Prism Central administrator username.
5	In the Password field, enter your Nutanix Prism Central administrator password
6	Click Test Connection .
7	Click OK .
8	Publish the SmartConsole session.
9	Install the Access Control policy on the Security Gateway object.

Connecting to a Nutanix Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **Nutanix**.

Connecting to a Nutanix Data Center Server with Terraform

See <https://registry.terraform.io/providers/CheckPointSW/checkpoint/latest>.

Adding a user in Nutanix Prism Central with minimum permissions

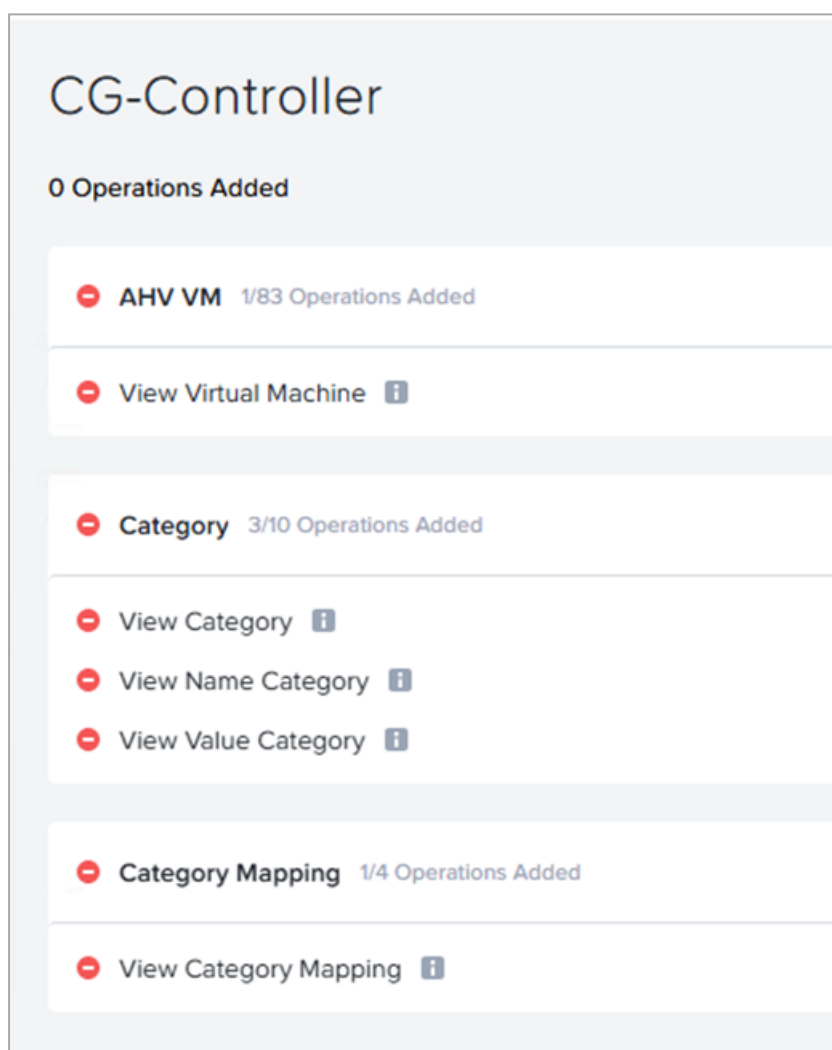


Note - These instructions are supported starting from Nutanix Prism Central Version pc.2024.2

To add a user with minimum permissions, follow these steps:

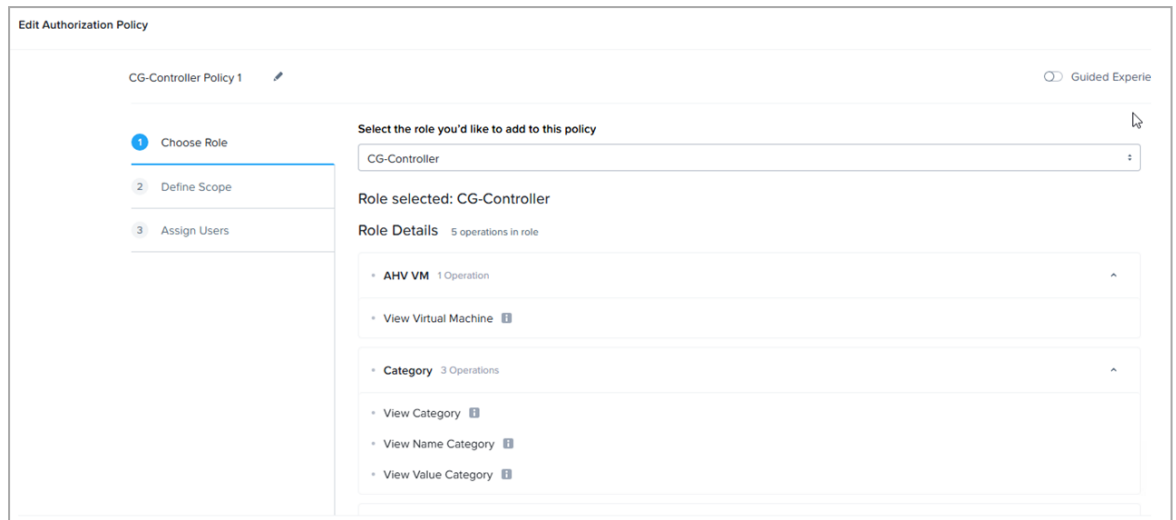
1. Add a new local user.
2. Create a new **Role** with these **Operations**:
 - a. In **AHV VM**:
 - View virtual machine
 - b. In **Category**:
 - View Category
 - View Name Category
 - View Value Category
 - c. In **Category Mapping**:
 - View Category Mapping

For example:



3. Create an Authorization Policy:

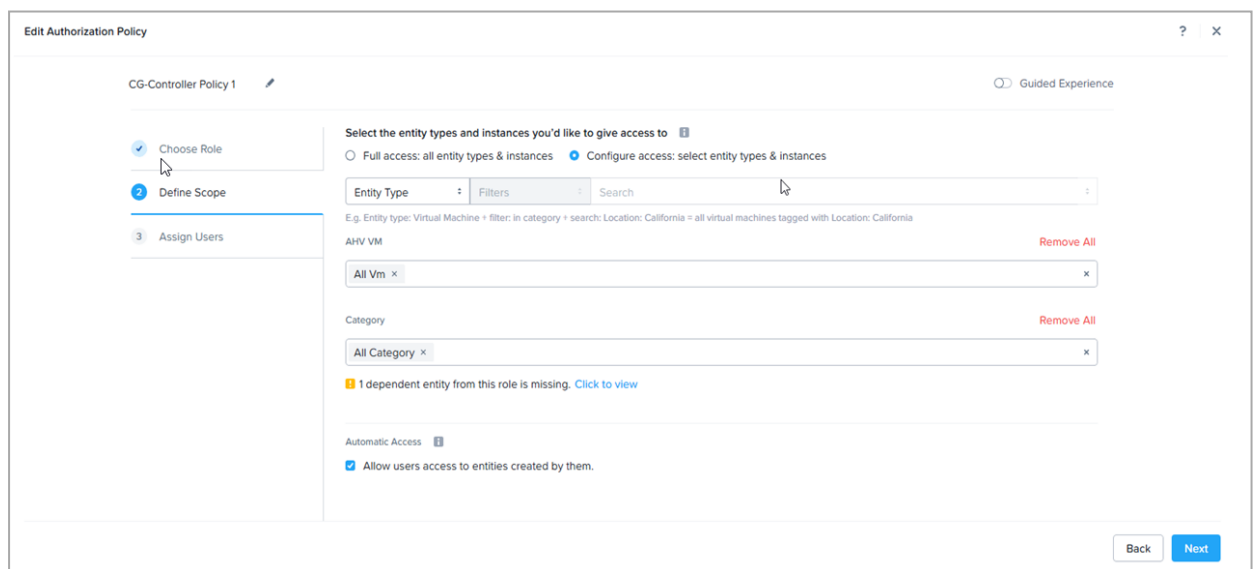
- a. In **Choose Role** tab, select the role you created before, for example:



4. In the **Define Scope** tab:

- a. Check the **Configure access: select entry types & instances** check box.
- b. In the **AHV VM** field, enter **All VM**.
- c. In the **Category** field enter **All Category**.
- d. Check the **Allow users access to entities created by them**.

For example:



5. In the **Assign Users** tab, add the local user you created in step 1.

For example:



6. Click **Save**.

Nutanix Objects

Object	Description
VM	Represents an entity of type 'VM' in Nutanix Prism
Category	A category in Nutanix Prism contains values, and a VM can be assigned with values. In SmartConsole, a category contains all the VMs that are assigned with any of the values of that category.

The entities (objects) that are imported from the data center, whether a VM or a category, have the following properties:

Nutanix Imported Properties

Imported Property	Description
Name	Name of the entity
Name in data center	Name of the entity in Nutanix Prism data center:
Type in data center	Type of the entity in Nutanix Prism data center (e.g. VM, category)
IP	All the VM's IP addresses
Note	Description of the entity
URI	Object path

CloudGuard Controller for Nuage Virtualized Services Platform (VSP)

The CloudGuard Controller integrates the Nuage cloud with Check Point security.

Connecting to a Nuage Data Center with SmartConsole

Step	Instructions
1	In SmartConsole, create a new Data Center object in one of these ways: <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > New Nuage. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > Nuage.
2	In the Enter Object Name field, enter the applicable name.
3	In the Hostname field, enter the IP address or hostname of the Nuage server. Important - The addresses can be either HTTP or HTTPS, but not both. The Nuage version is set by default to 4.0 and the port to 8443.
4	In the Username field, enter your Nuage administrator username.
5	In the Organization field, enter your organization name or enterprise.
6	In the Password field, enter your Nuage administrator password.
7	Click Test Connection .
8	Click OK .
9	Publish the SmartConsole session.
10	Install the Access Control policy on the Security Gateway object.

Connecting to a Nuage Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **Nuage**.

Connecting to a Nuage Data Center Server with Terraform

See [checkpoint_management_nuage_data_center_server](#).

Nuage Objects and Properties

Nuage Imported Objects

Object	Description
Enterprise	A logical separator for customers, BU, groups, traffic, administrators, visibility, and more.
Domain	A logical network that enables L2 and L3 communication among a set of Virtual Machines.
Security Zone	A set of network endpoints that have to agree with the same Security Policies.
Policy Group	<p>Collections of vPorts and/or IP addresses that are used as building blocks for Security Policies that include multiple endpoints.</p> <p>Add one or more vPorts to a policy group using this interface.</p> <p>A policy group can also represent one or more IP/MAC addresses that it learned from external systems from BGP route advertisements based on origin.</p>
Subnet	<p>Subnets are defined under a zone.</p> <p>It is equivalent to an L2 broadcast Domain, which enables its endpoints to communicate as if they were part of the same LAN.</p>
Instance	Virtual Machine.
vPort	<p>It is attached to a Virtual Machine or to a host and bridge interface.</p> <p>It provides connectivity to BMS and VLANs.</p> <p>It can be created or auto-discovered.</p>
L2Domain	<p>An L2 Domain is a distributed logical switch that enables L2 communication.</p> <p>An L2 Domain template can be started as often as required.</p> <p>This creates functioning L2 Domains.</p>
Network Macro	<p>Organization-wide defined macros that can be used as a destination of a policy rule.</p> <p>For example, you can create a network that represents your internal Internet access.</p> <p>You can then use it as a destination of a policy rule to drop any packet that arrives from a particular port.</p>
Network Macro Group	<p>A collection of existing Network Macros.</p> <p>These groups can be used in Security Policies to create rules that match multiple Network Macros.</p>

Nuage Imported Properties

Property	Description
Name	Resource name as shown in the Nuage console User can edit the name after importing the object.
Name in Data Center	Resource name as shown in the Nuage console
Type in Data Center	Resource type
IP	Associated IP address
Note	<ul style="list-style-type: none">▪ Instances - "Auto generated" description▪ Domain - Comment on domain object inserted in VSD▪ Subnet - Subnet IP address in CIDR format▪ Zone - Comment on zone object inserted in VSD▪ vPort - Auto-generated description
URI	Object path

CloudGuard Controller for OpenStack

The CloudGuard Controller integrates the Check Point Security Management Server with OpenStack Keystone. Authentication is done through OpenStack Keystone and network objects are updated from OpenStack Neutron.

Prerequisites

Version "Ussuri" or lower.

Connecting to an OpenStack Server with SmartConsole

Step	Instructions
1	<p>In SmartConsole, create a new Data Center object in one of these ways:</p> <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > New OpenStack. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > OpenStack.
2	In the Enter Object Name field, enter the applicable name.
3	<p>In the Hostname field, enter the URL of your OpenStack server in this format (HTTP or HTTPS):</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <pre>http://1.2.3.4:5000/<keystone_version></pre> </div> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <pre>https://1.2.3.4:5000/<keystone_version></pre> </div> <p>Example:</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <pre>https://1.2.3.4:5000/v3</pre> </div> <p>Note - If you do not know your keystone URL, run this command on the OpenStack server to find it:</p> <div style="border: 1px solid #ccc; padding: 5px; margin-bottom: 5px;"> <pre>openstack endpoint show keystone grep publicurl</pre> </div>
4	In the Username field, enter your username for the OpenStack server.
5	In the Password field, enter your password for the OpenStack server.
6	<p>Click Test Connection.</p> <p>If the certificate window opens, confirm the certificate and click Trust.</p>
7	<p>When the connection status changes to Connected, Click OK.</p> <p>If the status is not Connected, troubleshoot the issue before you continue.</p>

Step	Instructions
8	Click OK.
9	Publish the SmartConsole session.
10	Install the Access Control policy on the Security Gateway object.

Connecting to an OpenStack Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **OpenStack**.

Connecting to an OpenStack Data Center Server with Terraform

See [checkpoint_management_openstack_data_center_server](#).

i Important - If it is necessary to log into an OpenStackDomain that is not your default Domain, use this format:

```
<OpenStack_domain_name>/<user_name>
```

OpenStack Objects and Properties

OpenStack Imported Objects

Object	Description
Instances	Virtual Machines inside the cloud.
Security Groups	Sets of IP address filter rules for networking access. They are applied to all instances within a project.
Subnet	A block of IP addresses and associated configuration states. Subnets are used to allocate IP addresses when new ports are created on a network.

OpenStack Imported Properties

Property	Description
IP	<ul style="list-style-type: none">▪ VM - Virtual Machine's IP address▪ Security Group - IP addresses of the Virtual Machines inside the group▪ Subnets - IP addresses of the Virtual Machines inside the subnet
Note	<ul style="list-style-type: none">▪ Instances - Empty▪ Security Group - Description of the group▪ Subnet - IP address and mask of the subnet
URI	Object path

CloudGuard Controller for VMware Servers

Connecting to a VMware Server with SmartConsole

Step	Instructions
1	In SmartConsole, create a new Data Center object in one of these ways: <ul style="list-style-type: none"> ▪ In the top left corner, click Objects menu > More object types > Server > Data Center > New VMware vCenter, or New VMware NSX-V, or the new VMware NSX-T. ▪ In the top right corner, click Objects Pane > New > More > Server > Data Center > VMware vCenter, or VMware NSX-V, or VMware NSX-T.
2	In the Enter Object Name field, enter the applicable name.
3	In the Hostname field, enter the IP address or hostname of your vCenter or NSX Manager server.
4	In the Username field, enter your VMware administrator username.
5	In the Password field, enter your VMware administrator password.
6	Click Test Connection .
7	Click OK .
8	Publish the SmartConsole session.
9	Install the Access Control policy on the Security Gateway object.

Connecting to a VMware Data Center Server with Management API

Go to [Management API Reference](#) > Click on **see arguments per Data Center Server type** and select **VMWare vCenter** or **VMWare NSX** or **VMWare NSX-T**.

Connecting to a VMware Data Center Server with Terraform

See [checkpoint_management_vmware_data_center_server](#).

CloudGuard Controller for VMware vCenter

VMware vCenter Prerequisites

- VMware vCenter versions 5.x, 6.x, 7.x, 8.0.
- You must have a VMware NSX-V user with Auditor (or higher) permission to access the CloudGuard Controller.

For NSX operations, it is necessary to have at minimum read-only permissions.

- The CloudGuard Controller integrates the VMware NSX Manager Server with Check Point security.

VMware vCenter Objects and Properties

VMware vCenter Imported Objects

Object	Description
Cluster	A collection of ESXi hosts and associated Virtual Machines configured to work as a unit.
Datacenter	An aggregation of many object types required to work in a virtual infrastructure. These include hosts, Virtual Machines, networks, and datastores.
Folder	Lets you group similar objects.
Host	The physical computer where you install ESXi. All Virtual Machines run on a host.
Resource pool	Compartmentalizes the host or cluster CPU and memory resources.
Virtual machine	A virtual computer environment where a guest operating system and associated application software runs.
vSphere vApp	A packaging and managing application format. A vSphere vApp can contain multiple Virtual Machines.
Tags	All the Virtual Machines tagged with the vCenter tag. Note - This is supported with vCenter 6.5 and above.

VMware vCenter Imported Properties


Imported Property	Description
IP	IP address or Hostname of vCenter Server. You must install VMware Tools on each Virtual Machine to retrieve the IP addresses for each computer.
Note	VMware vCenter object notes.
URI	Object path.

CloudGuard Controller for VMware NSX-T Management Server

The CloudGuard Controller integrates the VMware NSX-T Management Server with Check Point security.

VMware NSX-T Prerequisites

- NSX-T versions 2.5, 3.0, 3.1.x, 3.2.1.

 **Note** - NSX-T 4.0.0.x and higher versions are supported in R81.20 with Jumbo HFA Take 8 and higher versions.


- You must have a VMware NSX-T username with the minimal permission of an *Auditor* (or higher) to access the CloudGuard Controller.

Note - This role is sufficient for CloudGuard Controller functionality. More permissions may be required for service registration (CloudGuard Gateway for NSX-T).

VMware NSX-T Policy mode APIs

Starting from R81.20 with Jumbo HFA Take 26:

- In NSX-T 4.0.0.x and higher versions, Manager Mode APIs are deprecated. The use of Policy Mode is recommended.
- Import NSX-T Tags (NSgroups and VMs) is supported.
- Import NSX-T Virtual Machine objects is supported.

 **Note** - You can enable Virtual Machines Import only with Policy Mode APIs. When enabled, the number of API requests to the NSX-T Manager increases.

Migration from Manager Mode to Policy Mode:

1. Use VMware Promotion Process: [Promote Manager Objects to Policy Objects](#)
2. Change NSX-T DC property to Policy Mode.

To use Policy Mode:

- For new NSX-T DC objects: Select the **Policy Mode (Recommended)** field.
- For all old NSX-T DC objects: Use the `usePolicyModeApis` parameter in the `vsec.conf` file.

For more information refer to "[Configuration Parameters](#)" on page 89.

VMware NSX-T Imported Objects

Object	Description
Ns Group	Enables a static or dynamic grouping based on objects such as Virtual Machines, vNICs, vSphere clusters, logical switches, and so on.
Virtual Machine (VM)	Starting from R81.20 with Jumbo HFA Take 26. A virtual computer environment that runs a guest operating system and applications software. You can import a VM only with Policy Mode API's.
Tag	Starting from R81.20 with Jumbo HFA Take 26 all the NS Groups and Virtual Machines tagged with the NSX-T tag.


To import Virtual Machines:

- For new NSX-T DC objects: Select the **Import Virtual Machines** field.
- For all old NSX-T DC objects: Use the **importVms** parameter in the *vsec.conf* file.

For more information refer to ["Configuration Parameters" on page 89](#)

VMware NSX-T object import supports IPv4/IPv6 IP sets with ranges or CIDR block notations. Each object can be up to 1000 IP addresses.

Supported IP Ranges are in the format: a.b.c.x - a.b.c.y.

 **Important** - Starting from R81.20 with JHF Take 41, this feature is disabled by default. To enable the import of IPv4/IPv6 IP sets with ranges or CIDR block notations, add this parameter to the *vsec.conf* file in the NSX-T section:

```
nsxt.ipRangeEnable=true
```

 **Note** - IPv4 IP sets with ranges or CIDR block notations import many IP Addresses, which can affect the CloudGuard Controller's performance.

The default number of IP addresses an object can hold is 1000 and you can not increase it.

To decrease the range value, add this parameter to the *vsec.conf* file in the NSX-T section:

```
nsxt.ipRangeLimit = <max amount of IPs to import in a single range>
```

VMware NSX-T Imported Properties

Imported Property	Description
IP	All the Ns Group IP addresses
Note	Description value of a Ns Group
URI	Object path

VMware NSX-T Known Limitations

- Logs for rules with VMware NSX-T Ns Groups will contain only the IP address. The logs will not contain the instance name.
- Because of an API change on VMware side in NSX-T Manager 3.2, the creation of NSX-T 3.2 Data Center in the Security Management fails. VMware made a fix in version 3.2.1.
- It is recommended to install official VMware Tools on a Virtual Machine for the VMware NSX-T Controller to pool IP addresses successfully. Install the VMware Tools for your specific version. You can find alternatives for IP discovery without VMware Tools in the [VMware NSX Administration Guide](#).
- For information regarding VMware Deprecation announcement for NSX-T Manager API's, refer to [sk180244](#).

CloudGuard Controller for VMware NSX-V Manager Server

- The Check Point Data Center Server connects to the VMware NSX Manager Server and retrieves object data.
- The CloudGuard Controller updates IP addresses and other object properties in the **Data Center Objects** group.
- You must have a VMware NSX user with permission of an Auditor (or higher) to access the CloudGuard Controller.

All NSX permissions allow users to see everything, but allowed operations depend on the NSX permission profile.

- 📘 **Important** - This role is sufficient for CloudGuard Controller functionality. More permissions can be required for service registration (CloudGuard Gateway for NSX).

VMware NSX-V Objects and Properties

VMware NSX-V Imported Objects

Object	Description
Security Group	Enables a static or dynamic grouping, based on objects such as Virtual Machines, vNICs, vSphere clusters, logical switches, and so on.
Universal Security Group	Enables defining a Security Group across VMware NSX managers. Note - Import these objects separately for each VMware NSX manager.

VMware NSX-V Imported Properties

Imported Property	Description
IP	All the Security Group IP addresses
Note	Description value of a Security Group
URI	Object path

Limitations

- Official VMware Tools must be installed on a VM for the CloudGuard Controller to pool IP addresses successfully.

Integrating with Data Center Servers

Connecting to a Data Center Server

The Management Server connects to the Software-defined data center (SDDC) through the Data Center server object you create in SmartConsole. In addition you can connect to the Data Center with management APIs and Terraform. See [Management API Reference](#) and the `data_center_server` Terraform such as [checkpoint management azure data center server](#).

To create a connection to the Data Center:

1. In SmartConsole, create a new Data Center object in one of these ways:
 - In the top left corner, click **Objects** menu > **More object types** > **Cloud** > **Data Center** > applicable Data Center.
 - In the top right corner, click **Objects Pane** > **New** > **More** > **Cloud** > **Data Center** > applicable Data Center.
2. In the **Enter Object Name** field, enter a name.
3. Enter the connection and credentials information.
4. To establish a secure connection, click **Test Connection**.
If the certificate window opens, verify the certificate and click **Trust**.
5. Click **OK** when the **Connection Status** changes to **Connected**.
If the status is not **Connected**, troubleshoot the issues before you continue.
6. Click **OK**.
7. Publish the SmartConsole session.



Notes:

- If the connection properties of a Data Center server change (for example, the credentials or the URL), **make sure to reinstall the policy on all the security gateways which have objects from that Data Center in their policy**.
- If the Data Center Server's certificate was changed, then communication with the Data Center Server fails.

To repair:

1. Open the Data Center Server object in SmartConsole.
2. Click **Test Connection** again.
3. Accept the new certificate.

Automatic Trust of Public Trusted Certificate Authorities

You can configure CloudGuard Controller to automatically trust Data Center certificates that are issued by trusted Certificate Authorities.

Automatic Trust is supported starting [R81.20 CloudGuard Controller self-updatable package Take 15](#).

This feature is off by default. To turn the feature on, add this parameter to the *vsec.conf* file (see "[Configuration Parameters](#)" on page 89 for more information):

```
useCAValidation=true
```

The CloudGuard Controller fetches and validates the certificate against the Trusted Root Certificate Authorities list in the *\$CPDIR/conf/ca-bundle-public-cloud.crt* file.

Example of the Root Certificate Authorities list:

```
GlobalSign Root CA
Entrust.net Premium 2048 Secure Server CA
Entrust Root Certification Authority
Comodo AAA Services root
Go Daddy Class 2 CA
DigiCert Assured ID Root CA
DigiCert Global Root CA
DigiCert High Assurance EV Root CA
COMODO Certification Authority
COMODO ECC Certification Authority
GlobalSign Root CA - R3
Go Daddy Root Certificate Authority - G2
DigiCert Assured ID Root G2
DigiCert Assured ID Root G3
DigiCert Global Root G2
DigiCert Global Root G3
DigiCert Trusted Root G4
COMODO RSA Certification Authority
USERTrust RSA Certification Authority
USERTrust ECC Certification Authority
GlobalSign ECC Root CA - R4
GlobalSign ECC Root CA - R5
IdenTrust Commercial Root CA 1
IdenTrust Public Sector Root CA 1
Entrust Root Certification Authority - G2
Entrust Root Certification Authority - EC1
ISRG Root X1
Amazon Root CA 1
Amazon Root CA 2
Amazon Root CA 3
Amazon Root CA 4
GlobalSign Root CA - R6
Entrust Root Certification Authority - G4
GlobalSign Root R46
GlobalSign Root E46
GlobalSign Root CA
GlobalSign Root CA - R2
Verisign Class 3 Public Primary Certification Authority - G3
Entrust.net Premium 2048 Secure Server CA
Baltimore CyberTrust Root
Entrust Root Certification Authority
Comodo AAA Services root
Comodo Secure Services root
Comodo Trusted Services root
```

```

Go Daddy Class 2 CA
StartCom Certification Authority
VeriSign Class 3 Public Primary Certification Authority - G5
COMODO Certification Authority
COMODO ECC Certification Authority
VeriSign Universal Root Certification Authority
VeriSign Class 3 Public Primary Certification Authority - G4
GlobalSign Root CA - R3
Go Daddy Root Certificate Authority - G2
StartCom Certification Authority
StartCom Certification Authority G2
COMODO RSA Certification Authority
GlobalSign ECC Root CA - R4
GlobalSign ECC Root CA - R5
Entrust Root Certification Authority - G2
Entrust Root Certification Authority - EC1
DST Root CA X3
Verisign Class 3 Public Primary Certification Authority
DigiCert Global Root CA

```

The advantages of using the automatic trust:

- **Automated Data Center Addition:** You can now add Private Cloud Data Centers without manually validating the fingerprint.
- **API Integration:** You can add Private Cloud Data Centers through API without manual fingerprint validation (The same API command, without providing certificate-fingerprint and unsafe-auto-accept).

For example, to add Nutanix Data Center with Management API, run:

```

mgmt_cli -r true add data-center-server name "myNutanix" type
"nutanix" hostname "1.1.1.1" username "admin" password "*****" 30
10

```

- **Certificate Changes Handling:** If the certificate changes, the connection with the Data Center persists.

Using Data Center in Policy

You can use Data Center objects and Data Center Query objects in Access Control, Threat Prevention, and HTTPS Inspection rules. In addition, you can use Data Center objects (but not Data Center Queries) in NAT rules in the Original Source and Original Destination columns.

To add Data Center objects to the policy:

1. In the applicable rule, click **+** to add new items.
2. Click **Import**.
3. Do one of these:
 - Select an existing Data Center object.
 - Create a new Data Center object - click **Data Centers** > **New Data Center** > select the applicable Data Center type.
4. Install the Access Control Policy.

Data Center Query Objects

Overview

Note - Support for Data Center Query Objects on Security Gateways is for versions R81 and higher.

With Data Center Query Objects, administrators can now create one **Query Object** based on attributes across multiple data centers. This simplifies the work when administrators create policies for multiple rules, because they only need to **use one query object for data center objects from multiple data centers**. Furthermore, admins can create the policy even before they configure a data center in SmartConsole. This makes it easier to separate responsibilities between security admins and other teams that possibly need to create data centers in SmartConsole.

The Query object is used in the same way as Data Center objects. As with Data Center Objects, when the Data Center Query is added to the Rule base the CloudGuard Controller pulls the assets from all the Data Centers in the query object and updates the Security Gateway accordingly.

Without Data Center Query	With Data Center Query
<ol style="list-style-type: none"> 1. Create the Data Center account (s). 2. Import objects from each Data Center to the Rule base. 3. No choice for complex logic inside the rules. 	<ul style="list-style-type: none"> ■ Create Data Center Query objects and add them to the rule base before or after you create Data Center account(s). Create Data Center Query object with the All Data Centers option. The advantage is that if new Data Center Servers are added later on, then rules in the rule base with such Data Center Query object (with the 'All Data Centers' option) are automatically applied to assets in the new Data Centers. Note - After adding a new Data Center, you must install the policy on all the Security Gateways that have this Data Center Query in their policy. ■ One Data Center Query Object can use assets (objects) from more than one, or all, Data Centers. This results in simpler security rules. ■ The Query is more complex and larger than what is possible in the security rule's logic. <ul style="list-style-type: none"> ○ OR logic inside each query rule, use " ; " between items ○ AND logic between query rules

Example 1: Data Center Query Object

Applies to all current and future data centers.

This is the query logic:

- All assets from type instances OR Load Balancers

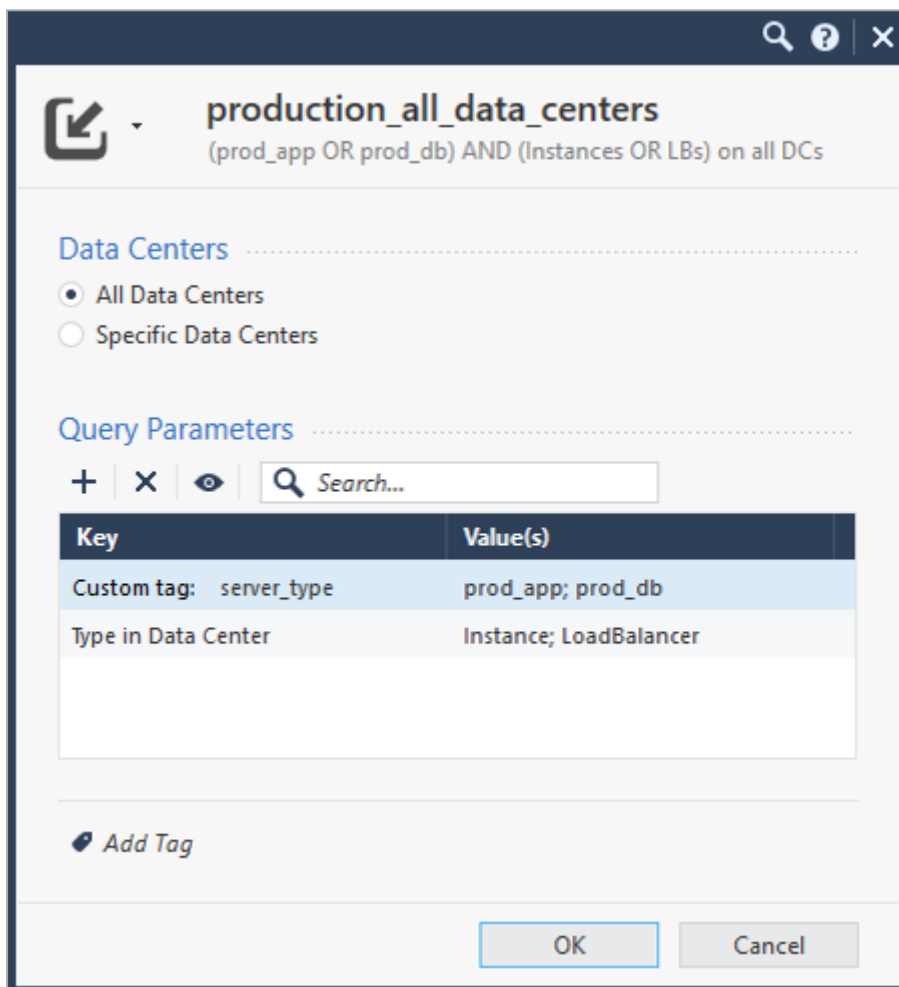
AND

- Tagged with:

"server_type=prod_app"

OR

"server_type=prod_db"








**Example 2: Rule Base**

Earlier versions require you to use multiple tag objects for multiple accounts.

- Rules must be updated for every data center added.
- Rules cannot have the logic for only Instances or Load Balancers.

With uses Data Center Query objects:

- No need to update the rule when new data center(s) is added.
- Rule can include complex OR and AND operations to better the policy.

No.	Name	Comments	Source	Destination
1		prod_app or prod_db from all AWS accounts. NOTES: 1. Must update rule for new new accounts. 2. Cannot include only Instances or LBs	* Any	 server_type=prod_app  server_type=prod_db  server_type=prod_app  server_type=prod_db  server_type=prod_app  server_type=prod_db
2		Only Instances and LBs tagged with prod_app or prod_db from all AWS accounts. No need to update rule when adding new accounts	* Any	 production_all_data_centers

Note - Rule No. 1 is without Data Center Query, and Rule No 2 is with Data Center Query.

Creating Rules with Data Center Query Objects

To add Data Center Query to a rule:

You can add a Data Center Query in the same way you can add Data Center Object to a rule.

Configuring Data Center Query Objects in SmartConsole

Step 1: Create a Data Center Query Object.

- a. Go to SmartConsole > Cloud > Data Center Queries > New.
- b. Add the applicable Data Center(s).
- c. Configure the **Query Rules** to match the value used for **Type**, **Name**, and **IP** in the **Import Data Center** window.

Type in Data Center	<i>Type</i> in Data Center, such as Instance, Virtual Machine, Load Balancer, Subnet, Availability Zone, and more. Note: You cannot query Tag, Tag Value, or Tag Key with Type in data center .
Name in Data Center	The asset's name (Not the Tag's name).
IP address	The asset's IP address.
Customer tag	Free text key and value. If you have only Tags with keys without values, you can set the Tag with key only and keep the value empty and the CloudGuard Controller enforce all the assets which have this Tag key. The Tags evaluation is case insensitive. For example, if the Tag configured on the Cloud is KEY=VALUE, and the Data Center Query Tag is key=value, there is a match.

Note - All object IP addresses that match the query are updated on the Security Gateway.

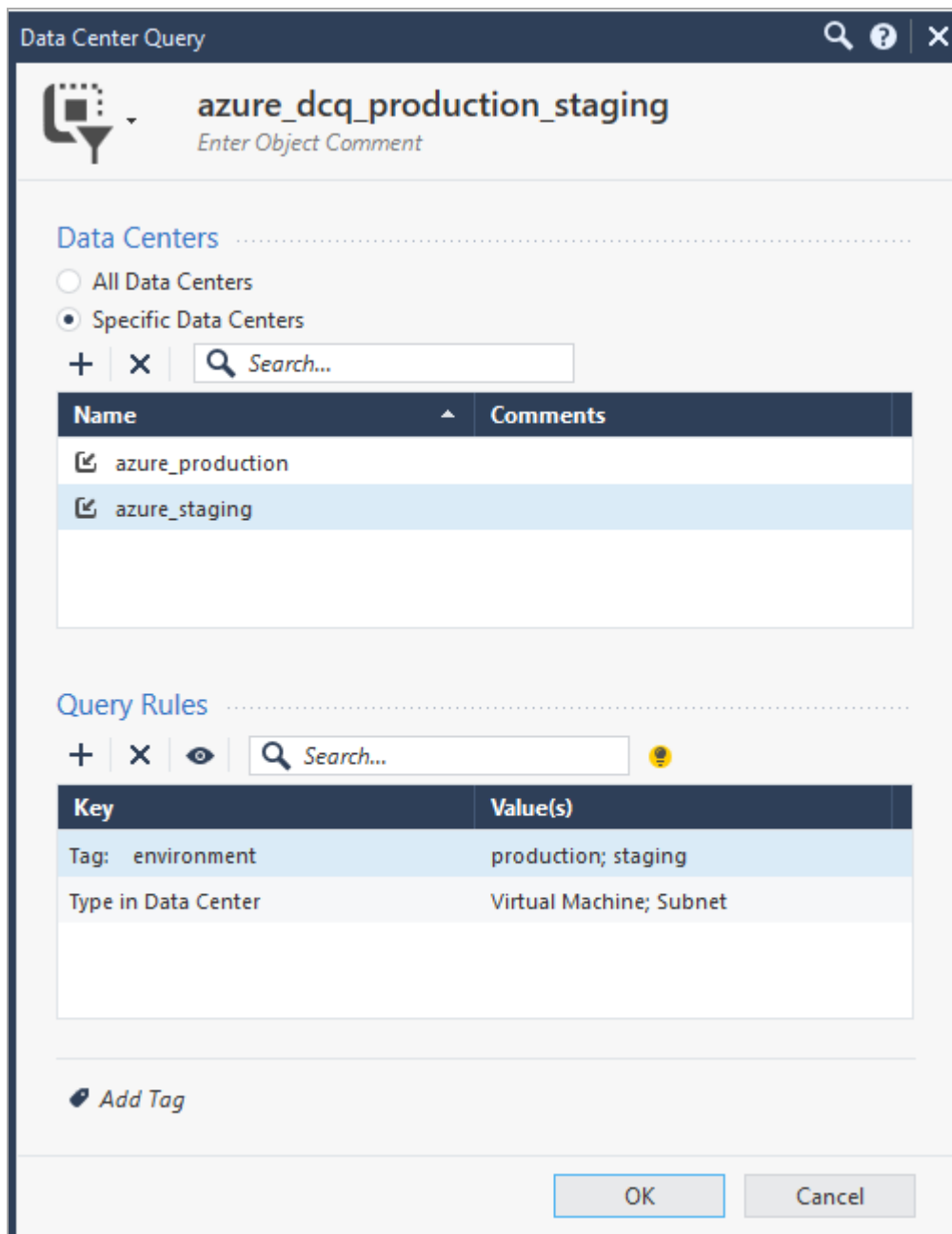
- d. **Optional:** To preview the query:
 - i. Publish the changes.
 - ii. Reopen the **Query Rules** section.
 - iii. Click the eye icon on **Data Center Query**.
- e. Click OK.

Configuring Data Center Query Objects using management API

See [Management API Reference](#).

Configuring Data Center Query Objects using Terraform

See [checkpoint_management_data_center_query](#).



Step 2: Add the Data Center Query object from Step 1 to the Rule base.

Step 3: Install the policy on the Security Gateway.

Automation and Monitoring


Check Point Management API and Terraform are available to add, delete, set, and show Data Center Servers and their contents, and to show, delete, and import Data Center objects and Data Center Query objects.

Use the API and resources to automate Data Center security management and monitoring.

See [Check Point Management API Reference](#) (at the top, select the correct version) .

See <https://registry.terraform.io/providers/CheckPointSW/checkpoint/latest/docs> and search for 'data_center'.

CloudGuard Controller Command Line Interface

 **Note** - For other commands, see the [R81.20 CLI Reference Guide](#).

The "vsec_controller_cli" command allows resending enforcement data to a Security Gateway when the Security Gateway is not synchronized by the CloudGuard Controller.

Reset the CloudGuard Controller state on the Security Gateway

Step	Instructions
1	Connect to the command line on the Management Server.
	Log in to the Gaia Clish, or Expert mode.
2	Run: <code>vsec_controller_cli</code>
3	Select: Resend enforcement data to gateway.
4	Select the Security Gateway to reset.

Note - If data is not synchronized after reset, contact your Check Point partner, or Check Point Support.

CloudGuard Controller Monitoring

CloudGuard Controller Logs and Events


To monitor the CloudGuard Controller, use any of these options:

- Filter the logs in SmartConsole with this query syntax:

```
blade:"CloudGuard IaaS" AND severity:Critical
```

- Create a User Defined Event based on logs and severity, see "[Creating a User Defined Event and Sending Alerts](#)" on page 85.
 - Connect the Event to an Automatic Reaction such as emails or scripts.

See the [R81.20 Logging and Monitoring Administration Guide](#) > Section *Automatic Reactions*.

-  **Note** - As the CloudGuard Controller uses Identity Awareness on the Security Gateway, the Security Gateway's kernel table limit can be reached in a scenario when there is a large number of IP addresses. You can monitor and get a notification for this issue in SmartLog. For details, refer to [sk113833](#).

CloudGuard Controller Status

Options for checking the CloudGuard Controller status

Option	Description
On the Management Server	Follow these steps: <ol style="list-style-type: none"> 1. Connect to the command line. 2. Run: <code>cpstat vsec</code>
In SmartConsole	Follow these steps: <ol style="list-style-type: none"> 1. From the left navigation panel, click Gateways & Servers.. 2. Select your Management Server object. 3. At the bottom, from the Summary tab, click Device & License Information > Device Status.

Output table columns:

- **Imported objects** - Shows objects that are updated in the CPM process or in SmartConsole.
- **Controller Updates** -Shows the number of updates sent about imported objects since the last CloudGuard Controller restart.

Note: The `cpstat -vsec` tool does not monitor ["Data Center Query Objects" on page 76](#).

Data Center Updates

CloudGuard Controller requires reliable connectivity to the Security Gateways to continuously update the Security Gateways with changes to the Data Center objects.

The updates of Data Center objects include:

- Adding new IP addresses to the rule base.
- Removing redundant IP addresses from the rule base.
- Extending the expiration time on existing objects in the rule base so they do not expire and automatically erase.

If the Security Gateway stops receiving updates for a Data Center Object, the Gateway has no way to verify that the object is still a valid object on the Data Center.

To create a balance between security and connectivity, each IP address of a Data Center object has a built-in expiration timer (aka Time To Live - TTL).

The CloudGuard Controller updates the IP addresses of the Data Center objects TTL on the Security Gateway to avoid TTL expiration.

However, if the Security Gateway(s) update fails continuously (for example, because of lack of connectivity between the Management and the Security Gateway), the TTL of the IP address is not updated.

When the full TTL of the IP address is reached, the IP address expires, and security policy rules that use this IP of that Data Center object are no longer enforceable.

Due to the critical nature of Data Center Objects, it is highly recommended to monitor CloudGuard Controller status.

You can configure the TTL from 5 minutes to 30 days.

For more information see the `enforcementSessionTimeoutInMinutes` parameter in the ["Configuration Parameters" on page 89](#) section.

SNMP Traps

To configure custom SNMP traps, refer to [sk124532](#).

Creating a User Defined Event and Sending Alerts

The CloudGuard Controller is very critical component for the security of an organization.

If the CloudGuard Controller loses connection with a data center, for some reason, then there are no updates to the Gateways.

This is a serious situation for any security administrator.

While administrators can monitor the SmartConsole logs in the office, there is also option to send critical CloudGuard Controller Events to an administrator's smartphone or email.

To create a User Defined Event

1. Enable the **SmartEvent** Software Blade on the Management Server.

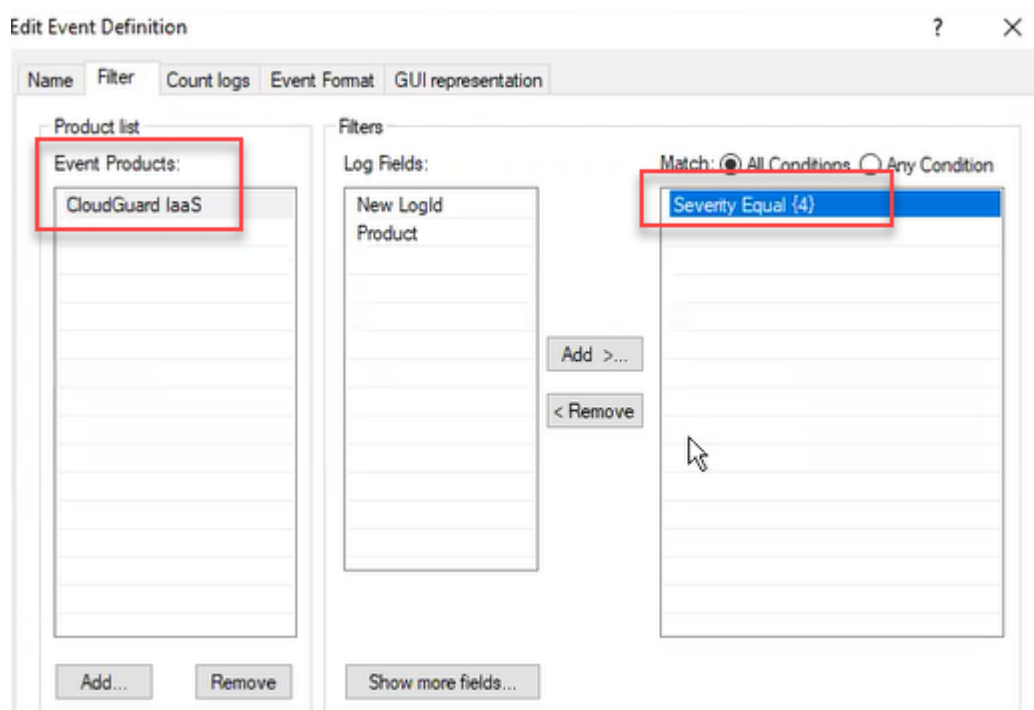
See the [R81.20 Logging and Monitoring Administration Guide](#) > Section *Deploying SmartEvent*.

2. Open the Legacy SmartEvent GUI client:
 - a. From the left navigation panel, click **Logs & Monitor**.
 - b. At the top, click the **+** tab.
 - c. At the bottom, in the section **External Apps**, click **SmartEvent Settings & Policy**.
3. In the **SmartEvent Policy** tree, right-click **Event policy**.

The **Event Definition** wizard opens.

- a. Step 1/6: In the Event Definition wizard window, below **Create an event**, select **that is completely new** > click **Next**.
- b. Step 2/6: In the **Name** field, enter a name for the Event.
From the **Severity** list, select a severity for the event > click **Next**.
- c. Step 3/6: Select **a single log** > click **Next**.
- d. Step 4/6: Click **Add product** > select the checkbox for **CloudGuard IaaS** > click **Next**.

- e. Step 5/6: Below the **Define the condition that specifies which {your event name} logs are appropriate for this event:**
 - i. Select **Show more fields > Existing field.**
The **Select Log Fields** window opens.
 - ii. Below **Log Fields**, select **Severity >** click **OK.**
 - iii. Below Available Log Fields, select **Severity**, click **Add.**
The Severity Filter window opens.
 - iv. Click **Add**, in the **Value** field enter the number '4' for the value (four is the highest, referred to as "critical") > click **OK.**
 - v. Make sure that In the **Event Definition** wizard window, the right-side box now shows **Severity Equal {x}** > click **Next.**



- vi. Click **Finish.**
- vii. To install the policy, click **Yes.**

Note - In the SmartEvent window that opens, click **Yes** to install the policy.

There is now a User Defined Event, in this example "CloudGuard IaaS Critical", that you can connect to Automatic Reaction which you create.

(Optional) To create an Automatic Reaction Alert

Use SmartEvent to send push notifications to your mobile device or email account.

This allows you to get notification even when your not in front of SmartConsole, and even when your are not in the office.

In SmartEvent, this is called "Automatic Reaction."

CloudGuard IaaS Critical

Detect the event when at least connections were detected over a period of seconds.

Severity:

Automatic Reactions: Send automatic reactions but don't generate an event

For more information about how to edit an event, see the [R81.20 Logging and Monitoring Administration Guide](#)

1. In the SmartEvent tree, right-click **User Defined Events** select the event.
2. In the top field, enter the parameters for detecting an Event.

Example, "Detect the event when at least **2** connections where detected over a period of **120** seconds".

3. Select the button to the right of the **Automatic Reactions** tab.
4. Select **Add new** > select **Mail** or **External Script**.

The Add Automatic Reaction window opens.

For more information about External scripts, see the [R81.20 Logging and Monitoring Administration Guide](#) > Section *Creating an External Script Automatic Reaction*.

5. In the **Name** field, delete the default name and enter a different name. For example, "CloudGuard Network alert email".
6. In the **Command line** field, enter the path and the name of the script. For example, `"/var/log/myscript.sh"`.
7. Click **Save**.
8. In the **Automatic Reactions** window, click **OK**.
9. From the **SmartEvent** toolbar, click the save icon > click **Yes**.

SmartTask

Starting in R81.20, there is a new SmartTask in SmartConsole for monitoring CloudGuard Controller.

SmartTasks let you configure automatic actions according to different triggers in the system. A SmartTask is a combination of trigger and action.

The trigger is a CloudGuard Controller Event that is activated when a new log is generated that matches this query in SmartConsole > **Logging & Monitoring** view > **Logs** tab:

```
blade:"CloudGuard IaaS" AND severity:Critical
```

For the action you can select: Run script, execute a Web request, or send mail.

Example:

The screenshot shows the 'New SmartTask' configuration window for 'Alert on CloudGuard Controller failure'. The window has a dark blue header with the title and a search icon. Below the header, there is a sidebar with 'General' and 'Advanced' tabs. The 'General' tab is selected, and a toggle switch is set to 'ON'. The 'Description' field is empty. The 'Trigger and Action' section is highlighted with a red box and contains two dropdown menus: 'CloudGuard Controller Event' and 'Run Script'. Below this, there is a 'Select script from repository:' dropdown menu with the text 'No item selected.'. The 'Custom Data' field is empty. At the bottom, there is an 'Add Tag' button and 'OK' and 'Cancel' buttons.

For more information on SmartTasks refer to [Quantum Security Management R81.20 Administration Guide](#).

Configuration Parameters

The CloudGuard Controller uses configuration parameters that can be adjusted to your specific needs.

This section provides a list of the configuration parameters including their description, minimum and maximum value, and the command to force the parameter's update.

CloudGuard Controller can be configured through various parameters in the `vsec.conf` file. See the `vsec.conf` file for more information.


Locations of the `vsec.conf` file:


- On a Security Management Server:

```
$FWDIR/conf/vsec.conf
```

- On a Multi-Domain Server:

```
$MDSDIR/conf/vsec.conf
```

 **Note** - In a Multi-Domain Security Management High-Availability environment, the configuration file is synchronized from the Multi-Domain Management Server member who's its Global domain is active, to the other members. Restart the CloudGuard Controller service on the other member for the changes to take effect.

-  **Important** - All configuration values are read from the `vsec.conf` file only when CloudGuard Controller is loaded. If you change one of the parameters, you must restart the CloudGuard Controller with the `"vsec stop ; vsec start"` commands.

```
# ports for mgmt<-->Controller communications
# Do not change
wsPort=999
wsTaggerPort=1004

# delay time (secs) between GW policy update cycles
# Default value: 10
enforcementUpdateIntervalTime=10

# TTL (mins) for objects expiration on GW in case there are no updates
# from the Controller
# min value=5
# max value=43200
# Default value: 10080
enforcementSessionTimeoutInMinutes=10080
```

```
# Update interval on changes of properties of imported data center in
# the mgmt/SmartConsole
# This value is used by the mgmt to pull changes from Controller
# When changing this value, mgmt need to restart
# Default value: 30
autoUpdateIntervalInSeconds=30

# Number of GWs to update policy concurrently. Increasing to too high
# value will increase load on the server
# Default value: 5
enforcementThreadPool=5

# If to use the system (Gaia) proxy when connecting to Data Centers.
# !! Enabling this will affect all Data Centers and can cause
# connectivity issues !!
# This setting is not relevant to Azure+AWS+GCP, which uses the system
# (Gaia) proxy automatically.
useSystemProxy=false

# Interval (secs) for fetching the Gaia proxy settings for connections
# to data centers when 'useSystemProxy' is set to true
# Default value: 60
systemProxyUpdateIntervalSeconds=60

# Number of retries and delay (secs) between retries when sending
# policy updates to the GW
# Default value: 3, 3
sendAndRunScriptRetryTimes=3
sendAndRunScriptRetrySleep=3

# Number of retries and delay (milliseconds) between retries when
# doing
# API calls to NSXT data center
# Default value: 5, 1000
failAPIRetryNumber=5
failAPIRetrySleepInMilliseconds=1000

# Controll Data Center scanning on Standby domain in mgmt-ha
# environment.
# In mgmt-ha only the Controller on the Active domain is pushing
# policy
```

```
# updates to the GWs so there is no real need for the Controller on
the
# Standby domain to scan the data centers consume system resources.
# When the Standby domain will be promoted to Active, the Controller
on
# that new-Active domain will automatically start pushing policy
updates
# to the GWs
# Default value: false
scanStandbyManagement=false

# Delay time (secs) between successful Data Center scan intervals.
# This is a global setting that will be applied only to Data Centers
# without this setting
# Default value: 30
global.scannerInterval=30

# Upper limit value (secs) for delay between failed Data Center scan
# intervals. When Data Center scan fails, the delay between further
# scans will grow gradually up to this value.
# Default value: 300
global.scanSleepUpperLimitInSeconds=300

# Maximum timeout (milliseconds) for establishing a connection with a
# Data Center.
# This is a global setting that will be applied only to data centers
# without this setting
# Default value: 5000000
global.connectTimeoutInMilliseconds=5000000

# Maximum timeout (milliseconds) when reading data from Data Center
APIs
# This is a global setting that will be applied only to data centers
# without this setting
# Default value: 120000
global.readTimeoutInMilliseconds=120000

# ACI Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# global.readTimeoutInMilliseconds
# Default value: 30, 300, 5000000, 120000
apic.scannerInterval=30
```

```
apic.scanSleepUpperLimitInSeconds=300
apic.connectTimeoutInMilliseconds=5000000
apic.readTimeoutInMilliseconds=120000

# NSX-V Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# global.readTimeoutInMilliseconds
# Default value: 30, 300, 5000000, 120000
nsx.scannerInterval=30
nsx.scanSleepUpperLimitInSeconds=300
nsx.connectTimeoutInMilliseconds=5000000
nsx.readTimeoutInMilliseconds=120000

# NSX-T Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# global.readTimeoutInMilliseconds
# Default value: 30, 300, 5000000, 120000
nsxt.scannerInterval=30
nsxt.scanSleepUpperLimitInSeconds=300
nsxt.connectTimeoutInMilliseconds=5000000
nsxt.readTimeoutInMilliseconds=120000

# Nutanix Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# global.readTimeoutInMilliseconds
# Default value: 30, 300, 5000000, 120000
nutanix.scannerInterval=30
nutanix.scanSleepUpperLimitInSeconds=300
nutanix.connectTimeoutInMilliseconds=5000000
nutanix.readTimeoutInMilliseconds=120000

# OpenStack Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# global.readTimeoutInMilliseconds
```

```
# Default value: 30, 300, 5000000, 120000
openstack.scannerInterval=30
openstack.scanSleepUpperLimitInSeconds=300
openstack.connectTimeoutInMilliseconds=5000000
openstack.readTimeoutInMilliseconds=120000

# vCenter Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# global.readTimeoutInMilliseconds
# Default value: 30, 300, 5000000, 120000
vcenter.scannerInterval=30
vcenter.scanSleepUpperLimitInSeconds=300
vcenter.connectTimeoutInMilliseconds=5000000
vcenter.readTimeoutInMilliseconds=120000

# AWS Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# Default value: 30, 300, 5000000
aws.scannerInterval=30
aws.scanSleepUpperLimitInSeconds=300
aws.connectTimeoutInMilliseconds=5000000

# Azure Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# Default value: 30, 300, 5000000
azure.scannerInterval=30
azure.scanSleepUpperLimitInSeconds=300
azure.connectTimeoutInMilliseconds=5000000

# AzureAD Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# Default value: 30, 300, 5000000
azure_ad.scannerInterval=30
azure_ad.scanSleepUpperLimitInSeconds=300
```

```
azure_ad.connectTimeoutInMilliseconds=5000000

# Updatable Objects Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# Default value: 300, 300
onlineservices.scannerInterval=300
onlineservices.scanSleepUpperLimitInSeconds=300

# Google Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# Default value: 30, 300, 5000000
google.scannerInterval=30
google.scanSleepUpperLimitInSeconds=300
google.connectTimeoutInMilliseconds=5000000

# oracle (OCI) Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# Default value: 30, 300, 5000000
oracle.scannerInterval=30
oracle.scanSleepUpperLimitInSeconds=300
oracle.connectTimeoutInMilliseconds=5000000

# Kubernetes Data Center configuration values.
# Overrides:
# global.scannerInterval
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# global.readTimeoutInMilliseconds
# Default value: 30, 300, 5000000, 120000
kubernetes.scannerInterval=30
kubernetes.scanSleepUpperLimitInSeconds=300
kubernetes.connectTimeoutInMilliseconds=5000000
kubernetes.readTimeoutInMilliseconds=120000
# show or hide specific Kubernetes types of assets
kubernetes.displayServiceLabels=true
kubernetes.displayServices=true
kubernetes.displayNodes=true
kubernetes.displayNodeLabels=true
```

```
kubernetes.displayPods=true
```

```
# ISE Data Center configuration values.
```

```
# Overrides:
```

```
# global.scannerInterval
```

```
# global.scanSleepUpperLimitInSeconds
```

```
# global.connectTimeoutInMilliseconds
```

```
# global.readTimeoutInMilliseconds
```

```
# Default value: 30, 300, 5000000, 120000
```

```
ise.scannerInterval=30
```

```
ise.scanSleepUpperLimitInSeconds=300
```

```
ise.connectTimeoutInMilliseconds=5000000
```

```
ise.readTimeoutInMilliseconds=120000
```

```
# number of concurrent worker threads that poll data from the ISE server
```

```
ise.threadPoolSize=2
```

```
# the page size argument when calling ISE /sgt API
```

```
ise.maxPageSize=100
```

```
# Nuage Data Center configuration values.
```

```
# Overrides:
```

```
# global.scannerInterval
```

```
# global.scanSleepUpperLimitInSeconds
```

```
# global.connectTimeoutInMilliseconds
```

```
# global.readTimeoutInMilliseconds
```

```
# Default value: 30, 300, 60000, 120000
```

```
nuage.scannerInterval=30
```

```
nuage.scanSleepUpperLimitInSeconds=300
```

```
nuage.connectTimeoutInMilliseconds=5000000
```

```
nuage.readTimeoutInMilliseconds=120000
```

```
# IoTDiscovery scanner config
```

```
iotdiscovery.handleFirstPolicyRequestOnly=false
```

```
iotdiscovery.applyAccountingToRules=true
```

```
iotdiscovery.validPolicyPorts=["any", "ssh", "ftp", "telnet", "http", "https"]
```

```
iotdiscovery.validPolicyProtocols=["any", "tcp", "udp", "icmp", "igmp"]
```

```
iotdiscovery.validPolicyProperties=["src", "dst", "name", "action", "service", "port", "protocol", "application"]
```

```
# policySource options: VISIBILITY_RULES, VENDOR, CHECKPOINT_BASELINE
```

```
iotdiscovery.policySource=VENDOR
```

```
# Check Point Data Center configuration values.
```

```
# Overrides:
```

```
# global.scannerInterval
```

```
# global.scanSleepUpperLimitInSeconds
# global.connectTimeoutInMilliseconds
# global.readTimeoutInMilliseconds
# Default value: 30, 300, 60000, 120000
checkpoint.scannerInterval=30
checkpoint.scanSleepUpperLimitInSeconds=300
checkpoint.connectTimeoutInMilliseconds=60000
checkpoint.readTimeoutInMilliseconds=120000

# Generic Data Center scanner config
genericdatacenter.scannerInterval=60
genericdatacenter.deleteTemporaryFiles=true
genericdatacenter.ignoreInvalidContent=false
genericdatacenter.scanningLogsOn=false
genericdatacenter.scanFlatListFiles=false
```

In version R81.20 with Jumbo HFA Take 26 and higher:

Added support for sending Data Center updates from the CloudGuard Controller to the main IP address of Active member on the Management Plane instead of the cluster VIP address on the Data Plane (PRJ-43926, PRHF-27357.)

This feature enables Data Center updates to clusters with MDPS-enabled where cluster members primary IP addresses are on Management Plane and VIP address is on the Data Plane.

```
# In version R81.20 with Jumbo HFA Take 26 and higher:
# Send Data Center updates from the CloudGuard Controller to the main
IP address of Active member
# on the Management Plane instead of the cluster VIP address on the
Data Plane
updateClusterMemberAndNotVip=true
```

Limitations

- Changes in connection properties (such as credentials or URL) of existing Data Center Servers will take effect (for example importing objects, updating objects updates, and so on) only after policy installation on all the Security Gateways that have Data Center Objects from this Data Center Server (**VSECC-589**).
- In a High-Availability deployment, the Standby server does not have complete Data Center information. The message "Standby machine (partial data)" appears in SmartView or when you run "cpstat vsec" from the CLI (**VSECC-311**).
- For Multi-Domain Management Server HA managing a VSX gateway, a domain server must be deployed on all MDS servers that manage the VSX gateway installed with imported Data Center Objects.

Note: This instruction applies to the VSX object. This is not mandatory for the virtual systems (**VSECC-1069**).

- IPv6 information is not imported for Data Center Objects in Public Cloud (**VSECC-1097**).
- VS Cluster's first policy installation should not include Data Center Objects (**VSECC-1070**).

Note: If this cannot be achieved, a full-sync must be run on the cluster. Run these commands on the Standby member:

1. `fw ctl setsync off`
2. `fw ctl setsync start`

- Non-ASCII characters (non-English languages) in 'Data Center Server' properties (i.e., user, password and shared secret fields) are not supported. If an object name contains one of the above characters, enforcement will not work (**VSECC-1064**).
- If Data Center Object's name includes Non-ASCII characters (non-English languages), enforcement will work, but its name might not be displayed properly in Security Logs and Events (**VSECC-1064**).
- After executing the commands: reboot, cprestart, and cloudguard off, Data Centers that have no imported objects, are not automatically shown in the Data Center table. To see the Data Centers in the table, open each Data Center individually in SmartConsole (**VSECC-422**).
- CloudGuard Objects (Data Center Servers and Data Center Objects) are not supported in Global Domain (**VSECC-1063**).
- Cluster objects (ClusterXL and 3rd party Cluster with the exception of CloudGuard for NSX) must be configured with reachable VIP as the main Cluster IP address to receive updates on Data Center imported objects (**VSECC-1059**).

- Policy Verification for overlapping, hiding, or contradicting rules that include Data Center Objects is not supported (**VSECC-1066**).
- If a Security Gateway works with CloudGuard Controller and other Identity Sources, there must not be IP addresses belonging to Data Center Objects also associated with Machines in other Identity Sources. Such overlapping can result in disassociation of the IP addresses from either the Data Center Object, or Access Roles with such Machines, and improper Security Policy enforcement (**VSECC-1071**).
- If a Data Center Object name contains these characters in its name (**VSECC-1065**):
 - "{" - opening curly bracket
 - "}" - closing curly bracket
 - "[" - opening square bracket
 - "]" - closing square bracket
 - "<" - less than
 - ">" - greater than

Then, the Data Center Object name will appear in SmartLog with double quotes "" without a content, instead of each of the above characters.

For example: "{Name1}" will appear as "Name1_".

- Logs for rules with Subnets, AWS Security Groups, Microsoft Azure Network Security Groups or VMware NSX Security Groups will contain only the IP address, and will not contain the instance name (**VSECC-1096**).
- Data Center Tags (**VSECC-1098**):
 - Tags keys and values longer than 100 characters will be truncated to the first 100 characters, and "..." will be padded to the end of the tag.
 - In Microsoft Azure, Tag keys are case-insensitive, whereas Tag values are case-sensitive. In CloudGuard Controller, both Tag key and Tag value will be treated as case-sensitive. Meaning, the same key/value in different cases will be shown on 2 different lines in SmartConsole.
- The IP addresses of Data Center objects which were deleted from the Data Center while CloudGuard Controller was stopped are not removed from the Security Gateway when CloudGuard Controller starts and scans the Data Center again (**VSECC-1580**).
- CloudGuard Controller is not supported with Maestro Dual-Site in VSLs mode.

Glossary

A

Anti-Bot

Check Point Software Blade on a Security Gateway that blocks botnet behavior and communication to Command and Control (C&C) centers. Acronyms: AB, ABOT.

Anti-Spam

Check Point Software Blade on a Security Gateway that provides comprehensive protection for email inspection. Synonym: Anti-Spam & Email Security. Acronyms: AS, ASPAM.

Anti-Virus

Check Point Software Blade on a Security Gateway that uses real-time virus signatures and anomaly-based protections from ThreatCloud to detect and block malware at the Security Gateway before users are affected. Acronym: AV.

Application Control

Check Point Software Blade on a Security Gateway that allows granular control over specific web-enabled applications by using deep packet inspection. Acronym: APPI.

ARM

Microsoft® Azure Resource Manager. Technology to administer assets using Resource Group.

ASN

Autonomous System Number.

Audit Log

Log that contains administrator actions on a Management Server (login and logout, creation or modification of an object, installation of a policy, and so on).

Available Quota

The available license pool quota is the number of unallocated cores.

AWS

Amazon® Web Services. Public cloud platform that offers global compute, storage, database, application and other cloud services.

AWS Region

In AWS, a geographic area to place resources. Each region has multiple, isolated locations known as Availability Zones.

AWS VPC

AWS Virtual Private Cloud. A private cloud that exists in the public cloud of Amazon. It is isolated from other Virtual Networks in the AWS cloud.

B

Bridge Mode

Security Gateway or Virtual System that works as a Layer 2 bridge device for easy deployment in an existing topology.

C

Central License

A Central License is a CloudGuard Security Gateway license. It is deployed and managed on the Security Management Server or Multi-Domain Server and distributed from a license pool to all CloudGuard Security Gateways connected to corresponding Management Servers.

Cisco ACI

Cisco® Application Centric Infrastructure. Comprehensive SDN architecture, policy-based automation solution for increased scalability through a distributed enforcement system with greater network visibility. Trademark of Cisco.

Cisco APIC

Cisco® Application Policy Infrastructure Controller. Automation and management point for the Cisco ACI fabric. It centralizes access to fabric information, optimizes the application lifecycle for scale and performance, and supports flexible application provisioning across physical and virtual resources.

Cisco Contract

In Cisco ACI SDN, a policy between Endpoint Groups (EPGs), with one EPG providing and one EPG consuming, to virtualize a physical network cable connection.

Cisco ISE

Cisco® Identity Services Engine. Provides highly secure network access to users and devices to streamline security policy management and reduce operating costs. Trademark of Cisco.

CK

Certificate Keys (CKs) of Central Licenses in the License Pool.

CloudGuard Controller

Provisions SDDC services as Virtual Data Centers that provide virtualized computer networking, storage, and security.

CloudGuard Gateway

Check Point Virtual Security Gateway that protects dynamic virtual environments with policy enforcement. CloudGuard Gateway inspects traffic between Virtual Machines to enforce security, without changing the Virtual Network topology.

Cluster

Two or more Security Gateways that work together in a redundant configuration - High Availability, or Load Sharing.

Cluster Member

Security Gateway that is part of a cluster.

Compliance

Check Point Software Blade on a Management Server to view and apply the Security Best Practices to the managed Security Gateways. This Software Blade includes a library of Check Point-defined Security Best Practices to use as a baseline for good Security Gateway and Policy configuration.

Content Awareness

Check Point Software Blade on a Security Gateway that provides data visibility and enforcement. Acronym: CTNT.

Cores Quota

The Central License Cores Quota is the number of virtual cores the license covers. This number is specified when the license is purchased. The Central License can be used on multiple Security Gateways up to the cores quota. The number of cores in a Security Gateway determines how many cores that Security Gateway uses from the Central License cores quota.

CoreXL

Performance-enhancing technology for Security Gateways on multi-core processing platforms. Multiple Check Point Firewall instances are running in parallel on multiple CPU cores.

CoreXL Firewall Instance

On a Security Gateway with CoreXL enabled, the Firewall kernel is copied multiple times. Each replicated copy, or firewall instance, runs on one processing CPU core. These firewall instances handle traffic at the same time, and each firewall instance is a complete and independent firewall inspection kernel. Synonym: CoreXL FW Instance.

CoreXL SND

Secure Network Distributer. Part of CoreXL that is responsible for: Processing incoming traffic from the network interfaces; Securely accelerating authorized packets (if SecureXL is enabled); Distributing non-accelerated packets between Firewall kernel instances (SND maintains global dispatching table, which maps connections that were assigned to CoreXL Firewall instances). Traffic distribution between CoreXL Firewall instances is statically based on Source IP addresses, Destination IP addresses, and the IP 'Protocol' type. The CoreXL SND does not really "touch" packets. The decision to stick to a particular FWK daemon is done at the first packet of connection on a very high level, before anything else. Depending on the SecureXL settings, and in most of the cases, the SecureXL can be offloading decryption calculations. However, in some other cases, such as with Route-Based VPN, it is done by FWK daemon.

CPUSE

Check Point Upgrade Service Engine for Gaia Operating System. With CPUSE, you can automatically update Check Point products for the Gaia OS, and the Gaia OS itself.

D

DAIP Gateway

Dynamically Assigned IP (DAIP) Security Gateway is a Security Gateway, on which the IP address of the external interface is assigned dynamically by the ISP.

Data Center

Virtual centralized repository, or a group of physical networked hosts, Virtual Machines, and datastores. They are collected in a group for secured remote storage, management, and distribution of data.

Data Loss Prevention

Check Point Software Blade on a Security Gateway that detects and prevents the unauthorized transmission of confidential information outside the organization. Acronym: DLP.

Data Type

Classification of data in a Check Point Security Policy for the Content Awareness Software Blade.

Default Pool

A pool created by the first Central License that is added with the Central License tool. The pool type is defined based on the blades package of the first added Central License. CloudGuard Security Gateways automatically receive licenses from that pool. When all licenses in the Default License Pool are removed, a random pool is set as a default. When there are multiple pools, the user can select the default license pool.

Distributed Deployment

Configuration in which the Check Point Security Gateway and the Security Management Server products are installed on different computers.

Dynamic Object

Special object type, whose IP address is not known in advance. The Security Gateway resolves the IP address of this object in real time.

E

Endpoint Policy Management

Check Point Software Blade on a Management Server to manage an on-premises Harmony Endpoint Security environment.

Expert Mode

The name of the elevated command line shell that gives full system root permissions in the Check Point Gaia operating system.

G

Gaia

Check Point security operating system that combines the strengths of both SecurePlatform and IPSO operating systems.

Gaia Clish

The name of the default command line shell in Check Point Gaia operating system. This is a restricted shell (role-based administration controls the number of commands available in the shell).

Gaia Portal

Web interface for the Check Point Gaia operating system.

GCP

See 'Google Cloud Platform'.

GCP Project

GCP Projects form the basis for creating, enabling, and using all Cloud Platform services. This includes managing APIs, enabling billing, adding and removing collaborators, and managing permissions for Cloud Platform resources.

GCP Regions and Zones

A region is a specific geographical location where you can run resources. Each region has one or more zones.

GCP VPC Network

A Virtual Private Cloud is a global private isolated Virtual Network partition that provides managed networking functionality for your GCP resources.

Generic Data Center

The Generic Data Center is an object that points to a JSON file on an external server that contains the IP addresses that you want to access. This way, when the Generic Data Center object is used in a policy, SmartConsole can retrieve the IP information from the JSON file as necessary.

Google Cloud Platform

Google® Cloud Platform is a suite of products and services that includes hosting, cloud computing, database services and more. Acronym: GCP.

H

Hotfix

Software package installed on top of the current software version to fix a wrong or undesired behavior, and to add a new behavior.

HTTPS Inspection

Feature on a Security Gateway that inspects traffic encrypted by the Secure Sockets Layer (SSL) protocol for malware or suspicious patterns. Synonym: SSL Inspection. Acronyms: HTTPSI, HTTPSi.

I

ICA

Internal Certificate Authority. A component on Check Point Management Server that issues certificates for authentication.

Identity Awareness

Check Point Software Blade on a Security Gateway that enforces network access and audits data based on network location, the identity of the user, and the identity of the computer. Acronym: IDA.

Identity Logging

Check Point Software Blade on a Management Server to view Identity Logs from the managed Security Gateways with enabled Identity Awareness Software Blade.

ILB

Internal Load Balancer, used to load balance traffic in a virtual network

Internal Network

Computers and resources protected by the Firewall and accessed by authenticated users.

IoT Cloud Adapter

IoT Cloud Adapters are connectors between IoT devices and cloud platforms. IoT adapters deliver data from the device to the cloud platform that stores it.

IPS

Check Point Software Blade on a Security Gateway that inspects and analyzes packets and data for numerous types of risks (Intrusion Prevention System).

IPsec VPN

Check Point Software Blade on a Security Gateway that provides a Site to Site VPN and Remote Access VPN access.

J

Jumbo Hotfix Accumulator

Collection of hotfixes combined into a single package. Acronyms: JHA, JHF, JHFA.

K

Kerberos

An authentication server for Microsoft Windows Active Directory Federation Services (ADFS).

Kubernetes

Kubernetes is a portable, extensible, open-source platform for managing containerized workloads and services that facilitates both declarative configuration and automation.

L

License Pool

A License Pool is a group of CloudGuard Central Licenses with the same blades and valid contracts. A Security Management Server or Multi-Domain Server can have multiple license pools. Each pool is defined by: - Pool Type - Total Quota - Available Quota - Certificate Keys - Subscribed Security Gateways

Log Server

Dedicated Check Point server that runs Check Point software to store and process logs.

Logging & Status

Check Point Software Blade on a Management Server to view Security Logs from the managed Security Gateways.

M

Management Interface

(1) Interface on a Gaia Security Gateway or Cluster member, through which Management Server connects to the Security Gateway or Cluster member. (2) Interface on Gaia computer, through which users connect to Gaia Portal or CLI.

Management Server

Check Point Single-Domain Security Management Server or a Multi-Domain Security Management Server.

Manual NAT Rules

Manual configuration of NAT rules by the administrator of the Check Point Management Server.

Microsoft Azure

Collection of integrated cloud services that developers and IT professionals use to build, deploy, and manage applications through a global network of data centers managed by Microsoft®.

Mobile Access

Check Point Software Blade on a Security Gateway that provides a Remote Access VPN access for managed and unmanaged clients. Acronym: MAB.

Multi-Domain Log Server

Dedicated Check Point server that runs Check Point software to store and process logs in a Multi-Domain Security Management environment. The Multi-Domain Log Server consists of Domain Log Servers that store and process logs from Security Gateways that are managed by the corresponding Domain Management Servers. Acronym: MDLS.

Multi-Domain Server

Dedicated Check Point server that runs Check Point software to host virtual Security Management Servers called Domain Management Servers. Synonym: Multi-Domain Security Management Server. Acronym: MDS.

N

Network Object

Logical object that represents different parts of corporate topology - computers, IP addresses, traffic protocols, and so on. Administrators use these objects in Security Policies.

Network Policy Management

Check Point Software Blade on a Management Server to manage an on-premises environment with an Access Control and Threat Prevention policies.

Nuage

The Nuage Networks Virtualized Services Platform (VSP) is the industry-leading network automation platform, enabling a complete range of SDN, SD-WAN, and cloud solutions.

Nutanix

Nutanix is a private and hybrid cloud software provider that offers software for virtualization, Kubernetes, database-as-a-service, software-defined networking, security, as well as software-defined storage for file, object, and block storage.

NVA

Network Virtual Appliance - A resource deployed in Azure's Virtual Hub that includes Security Gateways and other networking infrastructure.

O

Open Server

Physical computer manufactured and distributed by a company, other than Check Point.

OpenStack

An open source cloud-computing infrastructure for service providers and enterprises. It includes modules for administration, storage, networking and Virtual Machine deployment and control.

Oracle Cloud

Oracle Cloud is a cloud computing service offered by Oracle Corporation. It provides servers, storage, networks, applications, and services through a global network of Oracle Corporation-managed data centers.

P

Private Network (L3)

A Layer 3 network that separates routing instances, and can be used as an administrator separation.

Provisioning

Check Point Software Blade on a Management Server that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: SmartProvisioning, SmartLSM, Large-Scale Management, LSM.

Proxmox VE

Proxmox Virtual Environment - complete, open-source server management platform for enterprise virtualization. It integrates the KVM hypervisor and Linux Containers (LXC), software-defined storage and networking functionality, on a single platform.

Q

QoS

Check Point Software Blade on a Security Gateway that provides policy-based traffic bandwidth management to prioritize business-critical traffic and guarantee bandwidth and control latency.

R

Resource Group for Microsoft Azure

Object used in ARM to monitor, control access, provision and manage billing for collections of assets that are required to run an application, or used by a client or company department.

Rule

Set of traffic parameters and other conditions in a Rule Base (Security Policy) that cause specified actions to be taken for a communication session.

Rule Base

All rules configured in a given Security Policy. Synonym: Rulebase.

S

SD-WAN

Software Defined - Wide Area Network (WAN), more information on this solution:
<https://www.checkpoint.com/cyber-hub/network-security/what-is-sd-wan/>

SDDC

Software-Defined Data Center. Data Center infrastructure components that can be provisioned, operated, and managed through an API for full automation.

SDN

Software-Defined Network. Virtualization of topology, traffic, and functionality.

SecureXL

Check Point product on a Security Gateway that accelerates IPv4 and IPv6 traffic that passes through a Security Gateway.

Security Gateway

Dedicated Check Point server that runs Check Point software to inspect traffic and enforce Security Policies for connected network resources.

Security Group for AWS

Acts as a virtual firewall that controls the traffic for one or more instances in AWS. Security Groups are associated with network interfaces.

Security Group for VMware NSX

A collection of virtual objects that defines the Distributed Firewall protection policy in VMware NSX.

Security Management Server

Dedicated Check Point server that runs Check Point software to manage the objects and policies in a Check Point environment within a single management Domain. Synonym: Single-Domain Security Management Server.

Security Policy

Collection of rules that control network traffic and enforce organization guidelines for data protection and access to resources with packet inspection.

Service Graph

Ordered set of function nodes between terminals, which identifies network service functions required by an application. Required for CloudGuard integration.

Service Manager

Component that manages the communication between Check Point products, CloudGuard Controller and the VMware NSX, through the VMware REST API.

SIC

Secure Internal Communication. The Check Point proprietary mechanism with which Check Point computers that run Check Point software authenticate each other over SSL, for secure communication. This authentication is based on the certificates issued by the ICA on a Check Point Management Server.

SLB

Software Load Balancer, used to distribute tenant and tenant customer network traffic to virtual network resources. SLB enables multiple servers to host the same workload, providing high availability and scalability

SmartConsole

Check Point GUI application used to manage a Check Point environment - configure Security Policies, configure devices, monitor products and events, install updates, and so on.

SmartDashboard

Legacy Check Point GUI client used to create and manage the security settings in versions R77.30 and lower. In versions R80.X and higher is still used to configure specific legacy settings.

SmartProvisioning

Check Point Software Blade on a Management Server (the actual name is "Provisioning") that manages large-scale deployments of Check Point Security Gateways using configuration profiles. Synonyms: Large-Scale Management, SmartLSM, LSM.

SmartUpdate

Legacy Check Point GUI client used to manage licenses and contracts in a Check Point environment.

SNAT

Source Network Address Translation (Source NAT).

Software Blade

Specific security solution (module): (1) On a Security Gateway, each Software Blade inspects specific characteristics of the traffic (2) On a Management Server, each Software Blade enables different management capabilities.

Standalone

Configuration in which the Security Gateway and the Security Management Server products are installed and configured on the same server.

Subscribed Security Gateways

All Security Gateways on the Management Server are subscribed to the Default License Pool (unless configured differently) and get their licenses automatically. The user can exclude each Security Gateway from the automatic license distribution.

T

Tenant for ACI

Group of users, to isolate access to resources in Cisco ACI. Also known as Project.

Threat Emulation

Check Point Software Blade on a Security Gateway that monitors the behavior of files in a sandbox to determine whether or not they are malicious. Acronym: TE.

Threat Extraction

Check Point Software Blade on a Security Gateway that removes malicious content from files. Acronym: TEX.

Total Quota

The total license pool quota is the sum of all Central Licenses' cores.

U

Updatable Object

Network object that represents an external service, such as Microsoft 365, AWS, Geo locations, and more.

URL Filtering

Check Point Software Blade on a Security Gateway that allows granular control over which web sites can be accessed by a given group of users, computers or networks. Acronym: URLF.

User Directory

Check Point Software Blade on a Management Server that integrates LDAP and other external user management servers with Check Point products and security solutions.

V

Virtual Network

Environment of logically connected Virtual Machines.

VMware ESXi

A VMware® physical hypervisor server that hosts one or more Virtual Machines and other virtual objects. All references to ESX are also relevant for ESXi unless specifically noted otherwise.

VMware Global NSX-T

VMware Global NSX-T refers to the capabilities of NSX-T Federation, which uses a Global Manager to provide a centralized management plane for multiple, geographically dispersed NSX-T deployments (Local Managers). This allows for consistent policy enforcement and simplified operations across multiple data centers or cloud regions.

VMware NSX

VMware NSX is a network virtualization and security platform that enables the virtual cloud network, a software-defined approach to networking that extends across data centers, clouds, and application frameworks

VMware NSX-T

VMware NSX-T is a network virtualization and security platform that operates within a single data center or cloud environment. It provides software-defined networking, security (like distributed firewall and micro-segmentation), and load balancing for virtualized workloads, containers, and bare-metal servers.

VMware NSX Manager

Basic network and security functionality for virtual computer environments. A VMware® product family for SDN of Virtual Machines on the cloud (previously known as vShield).

VMware vCenter

Centralized management tool for VMware® vSphere. It manages many ESX servers and Virtual Machines from different ESX servers, from one console application.

VMware vSphere

VMware® cloud computing virtualization operating system. The vSphere Web Client is the GUI to manage Virtual Machines and their objects.

vNIC

Virtual Network Interface Card. Software-based abstraction of a physical interface that supplies network connectivity for Virtual Machines.

vsec_lic_cli

The Central License tool (vsec_lic_cli) runs on Management Servers and Multi-Domain Servers. It deploys and manages licenses for all subscribed Security Gateways. The tool can be used only in the Expert mode of the Management Server CLI.

vSwitch

A software abstraction of a physical Ethernet switch. It can connect to physical switches through physical network adapters to join virtual networks with physical networks. It can also be a Distributed Virtual Switch (dvSwitch), for definition and use on multiple ESXi hosts.

VSX

Virtual System Extension. Check Point virtual networking solution, hosted on a computer or cluster with virtual abstractions of Check Point Security Gateways and other network devices. These Virtual Devices provide the same functionality as their physical counterparts.

VSX Gateway

Physical server that hosts VSX virtual networks, including all Virtual Devices that provide the functionality of physical network devices. It holds at least one Virtual System, which is called VS0.

Z

Zero Phishing

Check Point Software Blade on a Security Gateway (R81.20 and higher) that provides real-time phishing prevention based on URLs. Acronym: ZPH.