



CLOUDGUARD

16 April 2024

# CLOUD MANAGEMENT EXTENSION

Administration Guide



# Check Point Copyright Notice

© 2019 - 2024 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 Cloud Management Extension Administration Guide



## Latest Version of this Document in English

Open the latest English version of this [document in a Web browser](#).  
Download the latest English 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
16 April 2024	Updated <a href="#">"Supported Configuration Template parameters" on page 33</a> Added <a href="#">"Autonomous Threat Prevention" on page 45</a>
21 March 2024	Updated <a href="#">"Automatically configure the NVA" on page 101</a>
17 March 2024	Updated <a href="#">"Parameters for GCP only" on page 32</a>
28 February 2024	Added <a href="#">"Configure Ingress Rules for NVA" on page 103</a>
25 February 2024	Updated <a href="#">"Supported Configuration Template parameters" on page 33</a>
25 December 2023	Updated <a href="#">"Troubleshooting" on page 106</a>
21 December 2023	Updated <a href="#">"Automatically configure the NVA" on page 101</a>
05 December 2023	Added <ul style="list-style-type: none"> <li>▪ <a href="#">"Repository Gateway Script" on page 100</a></li> <li>▪ <a href="#">"Objects Banner" on page 47</a></li> </ul>
27 November 2023	Updated <a href="#">"Management Parameters" on page 26</a>
12 November 2023	Added <a href="#">"Azure Virtual WAN" on page 101</a>
26 October 2023	Updated <ul style="list-style-type: none"> <li>▪ <a href="#">"Supported Configuration Template parameters" on page 33</a></li> <li>▪ <a href="#">"Implied Rules and Restrictive Policy" on page 46</a></li> <li>▪ <a href="#">"Autoprovision and Multi-Domain Log Server Configuration" on page 58</a></li> <li>▪ <a href="#">"Known Limitations" on page 73</a></li> </ul>

Date	Description
15 August 2023	<p>Updated</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Parameters for GCP only" on page 32</a></li> <li>▪ <a href="#">"Configuration Templates (gateway-configurations)" on page 32</a></li> <li>▪ <a href="#">"Configuring Network Group" on page 41</a></li> </ul> <p>Added</p> <ul style="list-style-type: none"> <li>▪ AWS Automatic Policy in <a href="#">"Supported Configuration Template parameters" on page 33</a></li> <li>▪ <a href="#">"Default-features" on page 42</a></li> </ul>
21 June 2023	<p>Updated:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Managing Multiple-Autoscaling Solutions with One Security Management Server" on page 48</a></li> <li>▪ <a href="#">"Implied Rules and Restrictive Policy" on page 46</a></li> </ul>
02 May 2023	<p>Updated:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Scale-Out" on page 15</a></li> <li>▪ <a href="#">"Supported Configuration Template parameters" on page 33</a></li> <li>▪ <a href="#">"Managing Auto-Scale with One Multi-Domain Server" on page 52</a></li> </ul> <p>Added <a href="#">"Implied Rules and Restrictive Policy" on page 46</a></p>
23 April 2023	<p>Updated:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Managing Multiple-Autoscaling Solutions with One Security Management Server" on page 48</a></li> </ul>
29 March 2023	<p>Updated:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Troubleshooting" on page 106</a></li> </ul>
22 March 2023	<p>Updated:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Supported Configuration Template parameters" on page 33</a></li> </ul>
07 March 2023	<p>Updated:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"CME Authentication" on page 21</a></li> <li>▪ <a href="#">"Configuring Name Prefix for Provisioned Gateways" on page 40</a></li> </ul>
01 February 2023	<p>Updated:</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Managing Multiple-Autoscaling Solutions with One Security Management Server" on page 48</a></li> </ul>

Date	Description
29 December 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Troubleshooting" on page 106</a></li> <li>▪ <a href="#">"Troubleshooting" on page 106</a></li> </ul>
19 December 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Use Case 2 - Working with Multiple Domains in the Multi-Domain Server and Multiple-Cloud Accounts" on page 53</a></li> </ul>
05 December 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Troubleshooting" on page 106</a></li> </ul>
24 October 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Schema" on page 25</a></li> <li>▪ <a href="#">"Management Parameters" on page 26</a></li> <li>▪ <a href="#">"Supported Configuration Template parameters" on page 33</a></li> </ul>
06 October 2022	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Schema" on page 25</a></li> </ul>
20 September 2022	Updated: <ul style="list-style-type: none"> <li>▪ Removed "-sg" flag in <a href="#">"Parameters for AWS only" on page 29</a></li> <li>▪ Added "-ca" and "-pp" flags in <a href="#">"Supported Configuration Template parameters" on page 33</a></li> </ul>
10 August 2022	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Configuring Network Group" on page 41</a></li> </ul> Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Automatic NAT and Access Rules" on page 65</a> &gt; Important Note</li> <li>▪ <a href="#">"Known Limitations" on page 73</a></li> </ul>
10 July 2022	Added: <ul style="list-style-type: none"> <li>▪ Autonomous Threat Prevention (ATP) support in <a href="#">"Supported Configuration Template parameters" on page 33</a></li> </ul>
31 May 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Supported Solutions and Features" on page 14</a></li> </ul>

Date	Description
26 April 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Using the autoprovisioning Command Line Configuration Tool" on page 24</a></li> </ul>
31 March 2022	<ul style="list-style-type: none"> <li>▪ Added description of the necessary steps for <a href="#">"CME Authentication" on page 21</a> with different public cloud platforms</li> <li>▪ Updated <a href="#">"Controllers (accounts)" on page 28</a></li> </ul>
08 March 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Overview of Cloud Management Extension (CME)" on page 14</a></li> </ul>
30 January 2022	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"CME Monitoring" on page 81</a> &gt; General Parameters</li> </ul>
17 January 2022	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"CME Monitoring" on page 81</a></li> </ul>
28 December 2021	Updated: <ul style="list-style-type: none"> <li>▪ CME configuration parameters</li> </ul>
29 October 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"AWS Security Hub" on page 91</a> - Removed all information about "custom Hotfix"</li> </ul>
25 October 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Configuration Templates (gateway-configurations)" on page 32</a> - Added the <code>-hc</code> option</li> </ul>
23 September 2021	Improved formatting and document layout
19 September 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Configuration Templates (gateway-configurations)" on page 32</a> - Removed the FQDN parameter</li> </ul>
02 August 2021	Improved formatting and document layout

Date	Description
18 July 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Configuration Templates (gateway-configurations)" on page 32</a></li> <li>▪ <a href="#">"The CME Logs" on page 20</a></li> </ul>
08 July 2021	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"CME API" on page 45</a></li> </ul> Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Troubleshooting" on page 106</a></li> </ul>
15 June 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Configuration Templates (gateway-configurations)" on page 32</a></li> </ul>
24 May 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Limitations" on page 108</a></li> </ul>
09 May 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Automatic NAT and Access Rules" on page 65</a></li> </ul>
08 March 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"AWS Security Hub" on page 91</a> - Added option to send Threat Prevention events</li> </ul>
08 March 2021	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Automatic NAT and Access Rules" on page 65</a></li> </ul>
18 February 2021	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Limitations" on page 80</a> - Removed support for VMware NSX-T</li> </ul>
27 July 2020	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Google Cloud Security Command Center (CSCC)" on page 83</a></li> </ul>
15 July 2020	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Limitations" on page 80</a> - Added a limitation</li> </ul>
20 April 2020	Removed: <ul style="list-style-type: none"> <li>▪ The Threat Emulation Software Blade and Flag</li> </ul>



Date	Description
29 March 2020	Added: <ul style="list-style-type: none"><li data-bbox="443 275 1142 309">■ The Threat Emulation Software Blade and Flag</li></ul> Updated: <ul style="list-style-type: none"><li data-bbox="443 398 1102 432">■ <i>"Limitations" on page 80</i> - Added a limitation</li></ul>
23 December 2019	Updated: <ul style="list-style-type: none"><li data-bbox="443 539 1289 573">■ <i>"Controllers (accounts)" on page 28</i> - Added an exception</li><li data-bbox="443 580 1102 613">■ <i>"Limitations" on page 80</i> - Added a limitation</li></ul>
04 November 2019	Added: <ul style="list-style-type: none"><li data-bbox="443 719 1390 752">■ <i>"Configuring Name Prefix for Provisioned Gateways" on page 40</i></li></ul>
15 August 2019	First release of this document

# Table of Contents

---

<b>Overview of Cloud Management Extension (CME)</b> .....	<b>14</b>
Supported Solutions and Features .....	14
CME configuration file .....	14
Scale-In and Scale-Out Events .....	15
Scale-In .....	15
Scale-Out .....	15
<b>Installing and Updating CME</b> .....	<b>17</b>
<b>CME Structure and Configurations</b> .....	<b>18</b>
CME Directories and Files .....	18
About CME Service Commands .....	19
Locating the Configuration Files .....	19
The CME Logs .....	20
CME Authentication .....	21
AWS .....	21
Azure .....	21
GCP .....	22
Using the <code>cme_menu</code> Command Line Configuration Tool .....	23
Using the <code>autoprov_cfg</code> Command Line Configuration Tool .....	24
Schema .....	25
Delay .....	25
Management .....	26
Management Parameters .....	26
Controllers (accounts) .....	28
General Parameters .....	29
Parameters for AWS only .....	29
Parameters for Azure only .....	31
Parameters for NSX only .....	31

---

---

Parameters for Nutanix only .....	31
Parameters for GCP only .....	32
Configuration Templates (gateway-configurations) .....	32
Supported Configuration Template parameters .....	33
Configuring Name Prefix for Provisioned Gateways .....	40
Configuring Network Group .....	41
Default-features .....	42
Enabling and Disabling Software Blades .....	43
Autonomous Threat Prevention .....	45
CME API .....	45
Configuring the tgw_menu .....	45
Implied Rules and Restrictive Policy .....	46
Objects Banner .....	47
<b>Managing Multiple-Autoscaling Solutions with One Security Management Server .....</b>	<b>48</b>
<b>Managing Auto-Scale with One Multi-Domain Server .....</b>	<b>52</b>
Important Notes .....	52
Use Case 1 - Working with a Single Domain in the Multi-Domain Server .....	52
Use Case 2 - Working with Multiple Domains in the Multi-Domain Server and Multiple-Cloud Accounts .....	53
Use Case 3 - Working with Multiple Domains in the Multi-Domain Server and a Single Cloud Account .....	55
Global Policy on a Multi-Domain Server .....	56
Autoprovision and Multi-Domain Log Server Configuration .....	58
<b>Managing Autoscaling with Management High Availability .....</b>	<b>60</b>
Security Management Server High Availability .....	60
Multi-Domain Server High Availability .....	62
<b>Automatic NAT and Access Rules .....</b>	<b>65</b>
Prerequisites .....	65
Mandatory Configuration .....	66
NAT Rule Generated .....	67
Access Rule Generated .....	68

---

---

Customizing Original and Translated Services in the NAT Rule .....	69
Customizing Original Source in the NAT Rule .....	70
Enabling Automatic NAT and Access Rules in CME .....	71
(Optional) Automatic Rule Placement .....	72
Known Limitations .....	73
<b>Automatic Hotfix Deployment .....</b>	<b>74</b>
Configuring the Automatic Hotfix Deployment .....	74
Disabling Automatic Hotfix Deployment .....	77
Viewing Configuration Parameters .....	78
Viewing Package Deployment Status .....	79
Limitations .....	80
<b>CME Monitoring .....</b>	<b>81</b>
<b>Google Cloud Security Command Center (CSCC) .....</b>	<b>83</b>
Prerequisites .....	83
Configuring CSCC on the Google Cloud Platform (GCP) .....	84
Configuring CloudGuard Network to Send Events to CSCC .....	85
Enabling CSCC on the Security Management Server .....	87
Disabling CSCC on the Security Management Server .....	87
Viewing the CSCC Status .....	88
Configuring Debug Mode .....	88
Additional Information about CloudGuard Network in CSCC .....	89
Log Exporter .....	89
Limitations .....	90
<b>AWS Security Hub .....</b>	<b>91</b>
Prerequisites .....	91
Subscribing to the Check Point CloudGuard Network in AWS Security Hub .....	92
Configuring the Check Point Security Management Server to Send Events to the AWS Security Hub .....	93
Enabling Security Hub on the Security Management Server .....	95
Disabling Security Hub on the Security Management Server .....	96

---

---

Displaying the Security Hub Integration Status .....	96
Configuring Debug Mode .....	97
Additional Information about CloudGuard Network in Security Hub .....	98
Accessing Security Hub Logs for Troubleshooting .....	98
Log Exporter .....	98
Limitations .....	99
<b>Repository Gateway Script .....</b>	<b>100</b>
<b>Azure Virtual WAN .....</b>	<b>101</b>
Automatically configure the NVA .....	101
Configure Ingress Rules for NVA .....	103
Using the Ingress User Interface .....	104
<b>Troubleshooting .....</b>	<b>106</b>
General troubleshooting guidelines .....	106
CME Log Collector .....	107
<b>Limitations .....</b>	<b>108</b>

# Overview of Cloud Management Extension (CME)

CME is a tool that runs on Check Point's Security Management Server and Multi-Domain Security Management Server. CME allows cloud-native integration between Check Point CloudGuard Network solutions and Cloud platforms.

As a Service, it continuously monitors CloudGuard Network solutions deployed in different cloud vendors and synchronizes them with the Security Management Server.

## Supported Solutions and Features

- CloudGuard Network for Azure VMSS
- CloudGuard Network for AWS ASG
- CloudGuard Network for GCP MIG
- Automatic Hotfix Deployment for autoscaling solutions
- CloudGuard Network for AWS Transit VPC
- CloudGuard Network for AWS Transit Gateway
- CloudGuard Network for NSX-T. For more information, see the [CloudGuard Network for NSX-T Security Gateway Deployment Guide](#)



**Note** - CME supports Check Point Management Server versions R80.20 and higher.

## CME configuration file

The CME configuration file has three fields which are detailed in the "[CME Structure and Configurations](#)" on page 18 section:

1. **Controllers** - Cloud accounts for communication with a specific cloud provider. These include the parameters necessary to connect with your cloud application.
2. **Management** - Parameters of the Check Point Management Server.
3. **Templates** - The individual scale sets configured in the account.

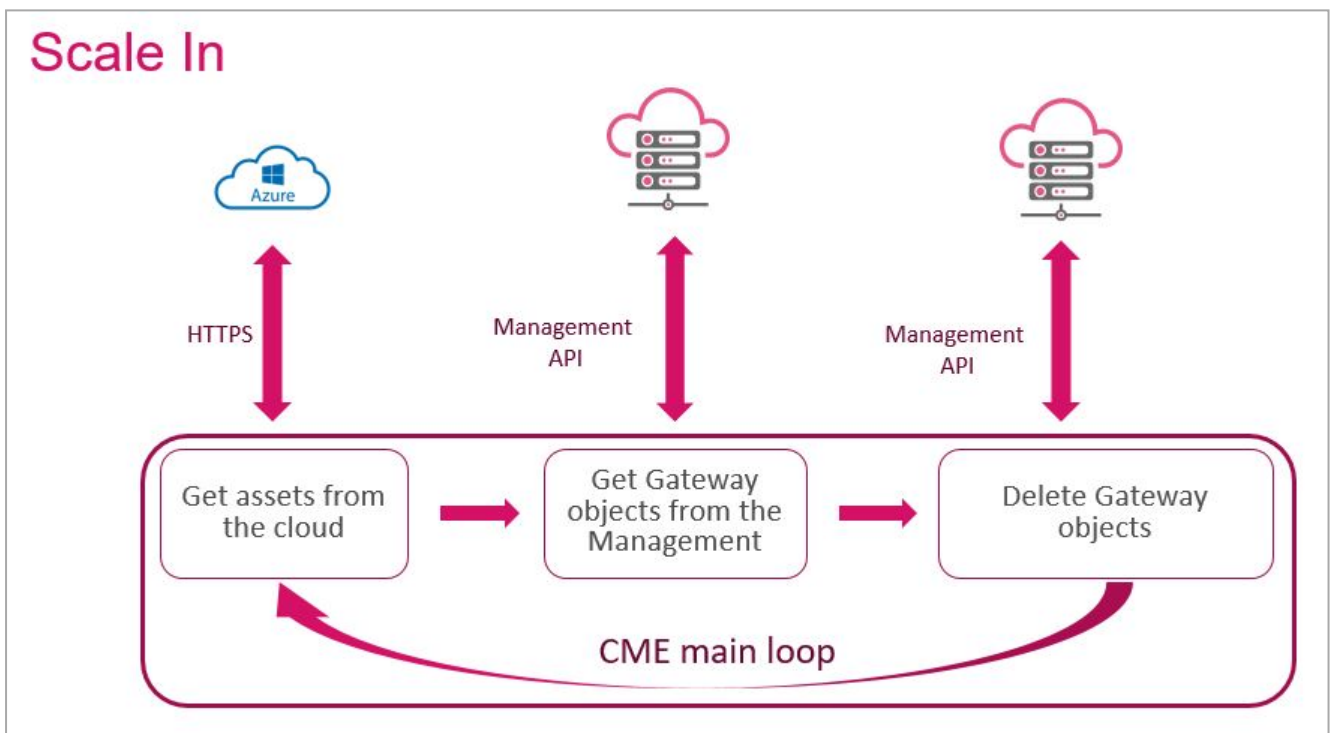
## Scale-In and Scale-Out Events

Scale sets automatically increase the number of VM instances as application demand increases (Scale-Out) and reduce the number of VM instances as demand decreases (Scale-In).

CME continually scans, and on each iteration, the load dictates if a scale-out or a scale-in event occurs, or if CME detects a demand that is not too high or too low for the current size of the set, there is no change.

### Scale-In

A scale-in event occurs as a result of a decrease in the current load. When a scale-in event triggers, CME designates one or more gateways as candidates for termination. The External Load Balancer stops forwarding new connections to these gateways, and Autoscale ends them. CME detects that these CloudGuard Network Security Gateways are stopped and automatically deletes these gateways from the Check Point Security Management Server's database.



### Scale-Out

A scale-out event occurs if the current load increases. When a scale-out event is triggered:

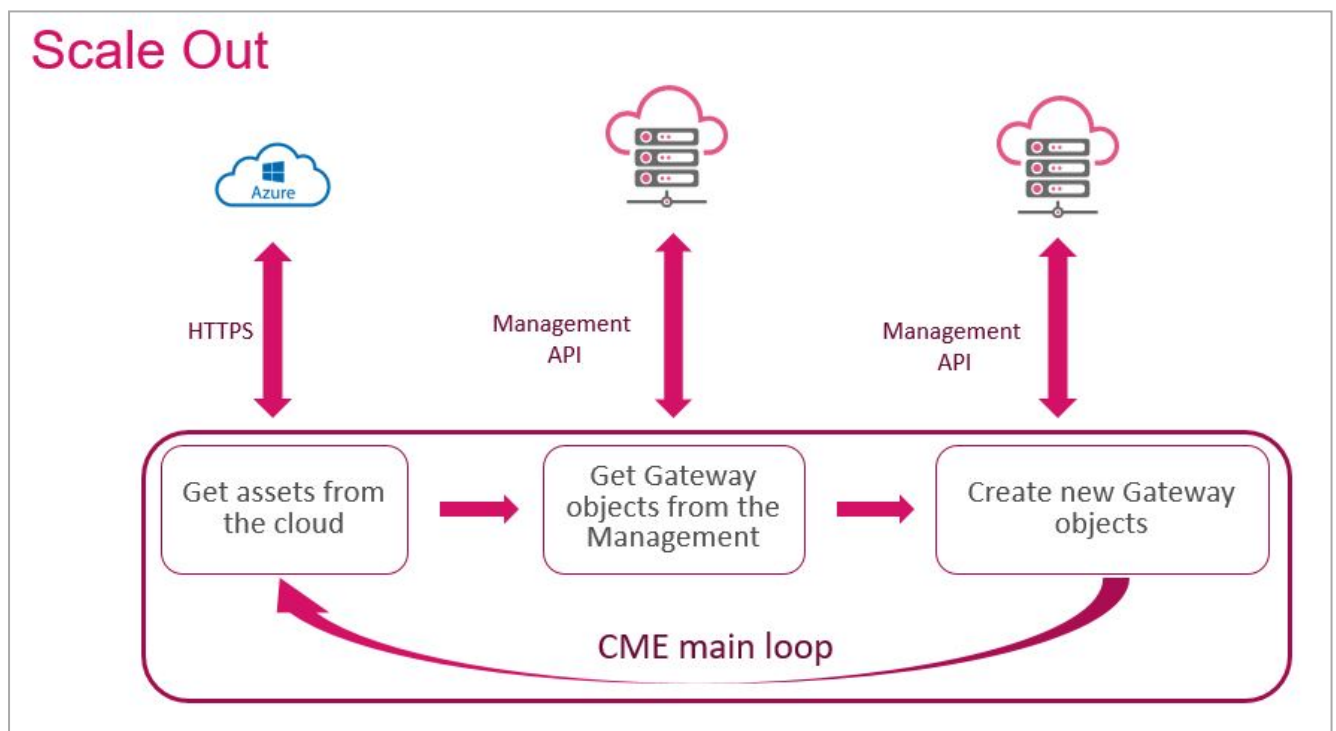
- The cloud provider auto-scale launches one or more new instances of the Check Point CloudGuard Network Security Gateways.

- The new instances of CloudGuard Network Security Gateways automatically run the Check Point First Time Configuration Wizard and then reboot.

During the scale-out, CME detects that new CloudGuard Network Security Gateway instances were launched. CME waits until the CloudGuard Network Security Gateways complete to deploy and then automatically:

- Initializes a Secure Internal Communication (SIC) channel with these CloudGuard Network Security Gateways.
- Install a restrictive access policy that has only a drop-all cleanup rule on these CloudGuard Network Security Gateways. For more information see ["Implied Rules and Restrictive Policy" on page 46](#).
- Do more configurations if needed, for example, blade configuration, run user custom scripts, create automatic Access/NAT rules, and more.
- Installs a Security Policy on these CloudGuard Network Security Gateways.

After the Security Policy installation, these CloudGuard Network Security Gateways start to reply to health probes. The Load Balancer then starts to forward new connections to them. The newly created CloudGuard Network Security Gateways report their status and send logs to CME.





# Installing and Updating CME

The CME package is available for online or for offline installation.



## Notes:

- We recommend to always install an updated version of CME when available.
- On some public cloud Management Servers, the CME is already pre-installed.  
We recommend to follow the instructions in [sk157492](#) to update CME to the latest version.

## To install/update the CME utility:

1. Go to [sk157492](#).
2. Download the latest CME package for your Management Server version.
3. Follow the **Installation Instructions** in the SK article to install CME.

# CME Structure and Configurations

These sections explain the main concepts of CME configuration.

## CME Directories and Files

- The CME is located in this directory on the Security Management or Multi-Domain Security Management Server:

```
/opt/CPcme/
```

- To execute the configuration tool for autoscaling solutions (such as Azure VMSS, AWS ASG, and GCP MIG) run this command in Expert mode:

```
autoprov_cfg
```

A more detailed description of `autoprov_cfg` is described in ["Using the autoprov\\_cfg Command Line Configuration Tool" on page 24](#).

- Run this command in Expert mode to execute command line configurations menu:

```
cme_menu
```

For each CME feature that requires the CME Menu, see the specific instructions in the related chapter.

- Configuration tool for AWS Transit Gateway:

```
tgw_menu
```

For a more detailed description of the `tgw-menu` features, see ["Configuring the tgw\\_menu" on page 45](#).

# About CME Service Commands

After a successful installation, CME runs the 'cme' service.

Function	Run this Command
Stop the service	<code>service cme stop</code>
Start the service	<code>service cme start</code>
Restart the service	<code>service cme restart</code>
Test the service	<code>service cme test</code>
Get the status of the service	<code>service cme status</code>

## Locating the Configuration Files

CME primary configuration file is `autoprovision.json`, and CME maintains backup files for it:

- `autoprovision.json.bak` - when there is a configuration change.
- `autoprovision.json.bak_schema` - when CME schema version is updated - See Schema section.

To find the CME configuration files use one of these directories:

- On a Security Management Server: `$FWDIR/conf/`
- On a Multi-Domain Security Management Server: `$MDSDIR/conf`

The configuration files are synchronized between the primary and secondary server in a Management High Availability environment.

# The CME Logs

The CME log files are:

- Primary CME Service log: `/var/log/CPcme/cme.log*`
- CME command line menu log: `/var/log/CPcme/cme_menu.log`

More logs used by Check Point Support:

- `rest_infra.log`
- `cme_api.log`
- `gunicorn_server.log`
- `diagnostics.log`

See "[CME Log Collector](#)" on page 107.

# CME Authentication

This section describes the necessary steps for CME authentication with different public cloud platforms.

## AWS

Refer to [sk130372](#) > 3. **Creating an AWS IAM User and IAM Role** section.

AWS Controller (account) connects to these URLs:

- [https://ec2.<region\\_code>.amazonaws.com](https://ec2.<region_code>.amazonaws.com)
- [https://elasticloadbalancing.<region\\_code>.amazonaws.com](https://elasticloadbalancing.<region_code>.amazonaws.com)

For example: <https://ec2.ap-northeast-2.amazonaws.com/>

## Azure

### Create a Microsoft Entra ID (formerly Azure AD) and Service Principal

With the Microsoft Entra ID and Service Principal, the Check Point Security Management Server monitors the creation and status of the VMSS, so it can complete the provision of these gateways.

1. Connect to [portal.azure.com](https://portal.azure.com).
2. Click **Active Directory** -> **App registrations** -> **New registration**.
3. Create new registration:
  - a. Select a meaningful Name.
  - b. Supported account types - Select **Single tenant**.
  - c. Redirect URL - Select **Web**, and type <https://localhost/vmss-name> - instead of: [vmss-name](https://localhost/vmss-name). It can be any name.
  - d. Click **Register**.
  - e. Open **Certificates and secrets** pane -> click **New secret key**.
  - f. Add the duration for the key.
  - g. Backup the key. **You cannot look at the key later**. Save it now.

After you create the application, write down these values, for "Configure the Check Point Security Management Server"

- Application ID

```
client_id
```

- Key value

```
client_secret
```

- Tenant ID

```
tenant
```

- Directory ID

**Note** - We recommend that you set the key to **never expire**.

### Permissions:

Give the Azure Active Directory application a minimum role of **Reader** to the VMSS and the VNET as explained [here](#).

Azure Controller (account) connects to these URLs:

- AzureCloud
  - <https://login.windows.net>
  - <https://management.azure.com>
- AzureChinaCloud
  - <https://login.chinacloudapi.cn>
  - <https://management.chinacloudapi.cn>
- AzureUSGovernment
  - <https://login.microsoftonline.us>
  - <https://management.usgovcloudapi.net>

## GCP

### Create a Google Cloud Platform (GCP) Service Account

The GCP Service account is used by the Check Point Security Management Server to monitor the creation and state of the autoscaling Managed Instance Group. This allows the Management Server to complete the provisioning of these gateways.

**To create a GCP service account:**

1. Go to <https://cloud.google.com/iam/docs/creating-managing-service-accounts>.

Use these parameters:

Name	check-point-autoprovision
Role	Compute Engine \ Compute Viewer

2. Click **Create Key > JSON** (as the key type). A `.json` file is downloaded to your computer).

*Note* - This `.json` file is used later as the credentials file in "[CME Structure and Configurations](#)" on page 18.

**Permissions:**

"Compute viewer"

GCP Controller (account) connects to this URL:

<https://www.googleapis.com/>

## Using the `cme_menu` Command Line Configuration Tool

- The `cme_menu` is a command line based menu to configure CME components and features.
- To start the menu, run `cme_menu` when logged into Expert mode on the Security Management or Multi-Domain Security Management Server.
- Use the instructions in this guide to configure the CME with the `cme_menu` as needed.

# Using the `autoprov_cfg` Command Line Configuration Tool

- The `autoprov_cfg` is a command-line tool to configure autoscaling solutions, such as Azure VMSS, AWS ASG, and GCP MIG.
- Refer to the specific solutions administration guide for specific information about how to use `autoprov_cfg`.
- For instructions about how to use the `autoprov_cfg`, run:

```
autoprov_cfg -h
```

- Commands summary:

Command	Description
<code>init</code>	Initialize auto-provision with Management, a Configuration Template, and a Controller (account) configuration
<code>show</code>	Show all or specific configuration settings
<code>add</code>	<ol style="list-style-type: none"> <li>1. Add a new Configuration Template or a Controller</li> <li>2. Add a new configuration to the Management or to a Configuration Template or a Controller</li> </ol>
<code>set</code>	Set values in an existing configuration of Management, Configuration Template or a Controller
<code>delete</code>	<ol style="list-style-type: none"> <li>1. Remove a Configuration Template or a Controller</li> <li>2. Remove a configuration from the Management or from a Configuration Template or a Controller</li> </ol>
<code>-v</code>	Show the version of CME
<code>-h</code>	Shows specific help documentation

- Specific help documentation is available for each option that you select.

For example, this command shows the available initialization parameters for AWS and their definition:

```
autoprov_cfg init AWS -h
```



# Schema

1. Starting from CME Take 212, the CME configuration has a schema version.
2. This attribute ensures that only compatible CME runs with the given CME configuration.
3. CME does not run when the schema version in the CME configuration is not compatible.
4. Example scenarios that can cause incompatibility:
  - a. Revert to older CME Take.
  - b. Upgrade - export configuration and importing it on a machine with an older CME Take.
  - c. High Availability Management/Multi Domain servers where the CME on the two members is not from the same take.
5. CME adds/updates a schema version parameter automatically and stores a backup of the previous configuration file in the `autoprovision.json.bak_schema` file.
6. To show the current schema version value, look for the schema value in CME configuration:

```
autoprov_cfg show all
```
7. This is a read-only parameter.
8. This attribute ensures that only compatible CME runs with the given CME configuration.

# Delay

- The delay parameter sets the sleep time between CME iterations.
- The default delay value is 30 seconds.
- To see the current delay value, look for the delay value in CME configuration:

```
autoprov_cfg show all
```

- To edit the delay configuration, run:

```
autoprov_cfg set delay <NEW_TIME_IN_SEC>
```

# Management

- There is one Management configuration for CME.
- The Management configuration applies to each controller, and each template.

To see the current Management configurations, run:

```
autoprov_cfg show management
```

To edit the management configurations, run:

```
autoprov_cfg set management -h
```

## Management Parameters

Parameter	Value	Description
-mn	MANAGEMENT-NAME	The name of this CME management configuration. This name must match the management name configured for each deployed scale-set. Note - This name is configurable and not related to CPM management name.
-d	DOMAIN:	The domain name or the domain UID that manage CME. This parameter is mandatory for MDS environments when one domain manages CME. If more than one domain manages CME, you should remove this parameter and configure it in the controller part, as explained below in the controller section.

Parameter	Value	Description												
-cs	SCRIPT FULL PATH	<p>This parameter let you set a custom script to be executed on the Management Server in these scenarios:</p> <ol style="list-style-type: none"> <li>1. After the restrictive policy installation step (even if restrictive policy is skipped).</li> <li>2. After installing the policy specified in the Configuration Template.</li> <li>3. After removing a Security Gateway.</li> </ol> <p>In each of these scenarios, CME runs the script with different arguments as listed in the table below:</p> <table border="1"> <thead> <tr> <th>Scenario</th> <th>Arguments</th> <th>Example</th> </tr> </thead> <tbody> <tr> <td>Restrictive policy installation</td> <td>delete &lt;gateway name&gt;</td> <td>\$FWDIR/conf/mgmt-script.sh delete cloudguard-gateway1</td> </tr> <tr> <td>Configuration Template policy installation</td> <td>add &lt;gateway name&gt;</td> <td>\$FWDIR/conf/mgmt-script.sh add cloudguard-gateway1</td> </tr> <tr> <td>Security Gateway removal</td> <td>delete &lt;gateway name&gt;</td> <td>\$FWDIR/conf/mgmt-script.sh delete cloudguard-gateway1</td> </tr> </tbody> </table> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ CME expects to find the script in the <i>\$FWDIR/conf</i> directory. For example: <i>\$FWDIR/conf/mgmt-script.sh</i>.</li> <li>▪ The script must have only admin read permission. You can give this permission with the command:  <pre>chmod 400 \$FWDIR/conf/&lt;script filename&gt;</pre> </li> </ul> <p>You can download an example of the Custom Management Script from <a href="#">here</a>.  To add parameters to the script see CUSTOM_PARAMETERS in "<a href="#">Configuration Templates (gateway-configurations)</a>" on page 32 &gt; General Parameters.</p>	Scenario	Arguments	Example	Restrictive policy installation	delete <gateway name>	\$FWDIR/conf/mgmt-script.sh delete cloudguard-gateway1	Configuration Template policy installation	add <gateway name>	\$FWDIR/conf/mgmt-script.sh add cloudguard-gateway1	Security Gateway removal	delete <gateway name>	\$FWDIR/conf/mgmt-script.sh delete cloudguard-gateway1
Scenario	Arguments	Example												
Restrictive policy installation	delete <gateway name>	\$FWDIR/conf/mgmt-script.sh delete cloudguard-gateway1												
Configuration Template policy installation	add <gateway name>	\$FWDIR/conf/mgmt-script.sh add cloudguard-gateway1												
Security Gateway removal	delete <gateway name>	\$FWDIR/conf/mgmt-script.sh delete cloudguard-gateway1												

## Controllers (accounts)

- To connect to your cloud account and automatically provision Security Gateways deployed in the account, the Security Management Server needs cloud-specific information, such as credentials and regions.

This information is related to a controller in the automatic provisioning configuration.

- To see the current controllers used by the Management Server connected to the cloud environments, run:

```
autoprov_cfg show controllers
```

- To add a new controller to an existing automatic provisioning configuration, run:

```
autoprov_cfg add controller -h
```



**Important** - Each controller in the configuration must have unique credentials, with the exception of the MDS configuration.

## General Parameters

Parameter	Value	Description
-cn	CONTROLLER-NAME	The name of the cloud environment controller. The name must be unique.
-dto	DELETION-TOLERANCE:	The number of cycles until a Gateway object in SmartConsole is deleted.
-ct	CONTROLLER TEMPLATES	An optional list of templates that are linked to this specific controller. This parameter is mandatory for MDS environments with more than one domain configured. for example, TEMPLATE1-NAME TEMPLATE2-NAME
-cd	CONTROLLER DOMAIN	Specify the domain name or the domain UID that manage this controller. This parameter is mandatory for MDS environments with more than one domain configured.

## Parameters for AWS only

Parameter	Value	Description
-r	REGIONS	A comma-separated list of AWS regions in which the gateways are being deployed. For example: eu-west-1,us-east-1,eu-central-1
-ak	AWS ACCESS KEY:	AWS Access Key ID
-sk	AWS SECRET KEY	AWS Secret Key
-iam	-	Use this flag to specify if you use an IAM role profile
-fi	AWS CREDENTIALS FILE PATH	The path to a text file with the AWS credentials
-sr	STS ROLE	The STS Role ARN of a role to assume
-se	STS EXTERNAL ID	An optional STS External Id to use when assuming a role in account

Parameter	Value	Description
-sn	SUB-CREDENTIALS NAME	Sub account name. The name must be unique
-sak	AWS SUB-CREDENTIALS ACCESS KEY	AWS Access Key ID for the sub account
-ssk	AWS SUB-CREDENTIALS SECRET KEY	AWS Secret Key for a sub account
-sfi	AWS SUB-CREDENTIALS FILE PATH	The path to a text file containing AWS credentials for a sub account
-siam	-	Use this flag to specify whether to use an IAM role profile for a sub account
-ssr	AWS SUB-CREDENTIALS STS ROLE	STS Role ARN of a role to assume for a sub-account
-sse	AWS SUB-CREDENTIALS STS EXTERNAL ID	An optional STS External Id to use when assuming a role in this sub account
-com	COMMUNITIES	An optional comma-separated list of communities, which are allowed for VPN connections that this controller discovers. If this attribute is missing or its value is an empty list, it means that any community may be joined by VPN connections that belong to this controller. This is useful to prevent automatic addition of VPN connections to a community based on the customer gateway public IP address.
-sv	-	Use this flag to enable the auto-provisioning of VPN objects
-slb	-	Use this flag to enable the auto-provisioning of load balancer Access and NAT rules
-ss	-	Use this flag to enable scan subnets with Centralized GWLB solution

## Parameters for Azure only

Parameter	Value	Description
-sb	SUBSCRIPTION ID	The Azure subscription ID
-en	-:	An optional attribute that specifies Azure's environment type. The possible values are: <ul style="list-style-type: none"> <li>■ AzureCloud (default)</li> <li>■ AzureChinaCloud</li> <li>■ AzureGermanCloud</li> <li>■ AzureUSGovernment</li> </ul>
-at	TENANT ID	The Azure Active Directory tenant ID.
-aci	CLIENT ID	The service principal's client ID value.
-acs	CLIENT SECRET	The service principal's client secret value.

## Parameters for NSX only

Parameter	Value	Description
-nf	NSX FINGERPRINT	NSX-T manager fingerprint
-np	NSX MANAGER PASSWORD:	NSX-T manager password
-nu	NSX MANAGER USERNAME	NSX-T manager username
-nh	NSX MANAGER HOST	NSX-T manager host IP
-nsm	NSX SERVICE MANAGER PASSWORD	NSX service manager password
-nad	NSX AD AUTH	NSX-T manager ad auth

## Parameters for Nutanix only

Parameter	Value	Description
-nf	NUTANIX PRISM FINGERPRINT	Nutanix Prism fingerprint
-np	NUTANIX PRISM PASSWORD:	Nutanix Prism password

Parameter	Value	Description
-nu	NUTANIX PRISM USERNAME	Nutanix Prism username
-nh	NUTANIX PRISM IP	Nutanix Prism IP

## Parameters for GCP only

Parameter	Value	Description
-proj	GCP-PROJECT	The GCP project ID of the project in which you deploy the CloudGuard Security Gateways. For example, "ACME-Production".
-cr	GCP-SERVICE-ACCOUNT-KEY	Full path to GCP Service Account key file. The file has to be located in <i>\$FWDIR/conf</i> and only have admin read permissions. For example, <i>\$FWDIR/conf/ACME-Production13cebb.json</i> .
-crd	GCP-SERVICE-ACCOUNT-DATA	The content of GCP service account data encoded in base64.

## Configuration Templates (gateway-configurations)

- Information required to automatically provision Security Gateways, such as what policy to install and which Software Blades to enable, is placed in a configuration template in the automatic provisioning configuration.
- To see the current configuration templates that you can apply on Security Gateways, run:

```
autoprov_cfg show templates
```

- To add a new configuration template to an existing automatic provisioning configuration, run the command:

```
autoprov_cfg add template -tn <CONFIGURATION-TEMPLATE-NAME> -otp <SIC-KEY> -ver <VERSION> -po <POLICY-NAME>
```



## Supported Configuration Template parameters

### General Parameters

Parameter	Value	Description
-otp	ONE_TIME_PASSWORD	A random string consisting of a minimum of 8 alphanumeric characters.
-ver	GATEWAY_VERSION	The Security Gateway version.
-po	POLICY_NAME	The name of an existing security policy to install on the Security Gateways.
-rp	POLICY_NAME	<p>An optional name of an existing security policy to install on the new Security Gateways as the first policy (required for the internal CME workflow). When not provided, a default policy is used (It has a drop-all cleanup rule).</p> <p>Note: restrictive policy name ("-rp") cannot be the same as the policy name ("po").</p> <p>See also <a href="#">"Implied Rules and Restrictive Policy" on page 46</a>.</p>
-cg	CUSTOM_GATEWAY_SCRIPT	<p>A path of a script on the Management Server that will be run on the gateways after the policy installation.</p> <p>You can add parameters to the script by separating them with spaces. The script should be located in the directory:</p> <ul style="list-style-type: none"> <li>▪ <code>\$FWDIR/conf</code> on Security Management Server.</li> <li>▪ <code>\$FWDIR/conf</code> of the Global Domain in Multi-Domain Security Management Server.</li> </ul> <p>The directory must have only admin read permissions.</p> <p>For example: <code>'\$FWDIR/conf/gw-script.sh param1 param2 ...'</code></p> <p>Note: Use the single quotes in the command.</p> <p>You can set one custom gateway script for each template.</p> <p>If you configure Management Data Plane Separation (MDPS), ensure the script is compatible.</p>

Parameter	Value	Description
-cp	CUSTOM_PARAMETERS	<p>A list of <b>parameters</b> separated by spaces for the Custom Management script.</p> <p>For example: '\$FWDIR/conf/mgmt-script.sh param1 param2 ...'</p> <p>Note: Use the single quotes in the command.</p> <p>For more details about the Custom Management Script see <a href="#">"Management Parameters" on page 26</a>.</p>
-xff	-	Enable XFF headers in HTTP / HTTPS requests.
-g	GENERATION	<p>String or number that you can use to force reapplying a template configuration to existing Security Gateways.</p> <p>If generation is specified and its value is different than the previous value that was used for applying the template on a specific Security Gateway, then the template settings will be reapplied to the Security Gateway.</p>
-secn	SECTION_NAME	<p>Name of a rule section in the Access and NAT layers in the policy, where to insert the automatically generated rules.</p> <p>See Automatic Rule Placement:</p> <ol style="list-style-type: none"> <li>1. <a href="#">sk112575 - AWS Automatic Rule Placement</a></li> <li>2. <a href="#">"(Optional) Automatic Rule Placement" on page 72</a></li> </ol>
-pn	PREFIX_NAME	See <a href="#">"Configuring Name Prefix for Provisioned Gateways" on page 40</a> .
-nk	"KEY" "VALUE"	<p>Configure other attributes to add to the Management API command "set-simple-gateway" (API v1).</p> <p>For example: -nk "save-logs-locally" "true"</p>

## Software Blades

Parameter	Value	Description
-hi	-	Enable the HTTPS Inspection
-atp	-	<p>Enable the Autonomous Threat Prevention</p> <p><b>Important:</b> Threat Extraction &amp; Zero Phishing Threat Prevention blades are not supported, and you must add a manual Threat Prevention Global Exception rule to inactivate the blades.</p> <p>Refer to "<a href="#">Autonomous Threat Prevention</a>" on <a href="#">page 45</a> for instructions on how to create a Global Exception.</p> <p>Notes:</p> <ul style="list-style-type: none"> <li>▪ Threat Extraction &amp; Zero Phishing are not supported.</li> <li>▪ Minimum required version for Security Management Server or Multi Domain Server is R81.10.</li> <li>▪ Minimum required version for Security Gateways is R81.</li> </ul>
-ia	-	<p>Enable the Identity Awareness to support CloudGuard Controller.</p> <p>For more information on CloudGuard Controller, refer to <a href="#">R81.20 CloudGuard Controller Administration Guide</a>.</p>
-appi	-	Enable the Application Control
-ips	-	Enable the IPS
-uf	-	Enable the URL Filtering
-ab	-	Enable the Anti-Bot
-av	-	Enable the Anti-Virus
-te	-	Enable the Threat Emulation
-vpn	-	Enable the IPsec VPN
-ca	-	Enable the Content Awareness

Parameter	Value	Description
-vd	VPN-DOMAIN	Configure the group object for the VPN domain in the VPN Gateway (with "vpn": true). <ul style="list-style-type: none"><li>▪ If you use this parameter with an <b>empty</b> value, the template automatically configures an empty group as the Encryption Domain.</li><li>▪ If you do <b>not</b> use this parameter, the template automatically configures the Encryption Domain to IP addresses behind the VPN Gateways.</li></ul>
-con	COMMUNITY_NAME	Optional Star community in which to place the VPN Gateway (with "vpn": true) as a center

## Log Server parameters

Parameter	Value	Description
-sl	SEND_LOGS_TO_SERVER	A comma-separated list of Primary Log Servers names to send logs to. The configured Log Server act as a Log and Alert Server..
-sbl	SEND_LOGS_TO_BACKUP_SERVER	A comma-separated list of Backup Log Servers names to send logs to if the Primary Log Servers are unavailable.
-sa	SEND_ALERTS_TO_SERVER	A comma-separated list of Alert Log Servers names to send alerts to.

 **Notes:**

- As part of the Auto Scale instance provisioning cycle the install database action is executed on all defined Log Servers when:
  - CME Take 250 and higher is installed.
  - Log Server configurations were set in a template with CME Take 250 or higher.
- To install the database for Log Server configurations that are set with CME Take lower than 250:
  - Install CME Take 250 or higher.
  - Reconfigure the existing Log Server configurations (See ["Examples of using Log Servers parameters: " below](#))
- To use Log Server parameters, you must configure at least one Primary Log Server (with the -sl parameter).
- To remove all Primary Log Server(s) the Backup and Alert Log Servers must be removed first.
- If Primary/Backup/Alert Log Servers are configured with the **new key** parameter (-nk) and with Log Servers parameters (-sl, -sbl, -sa), the **new key** parameter is ignored.
- Log Server settings are not supported in the Smart-1 Cloud environment.

**Examples of using Log Servers parameters:**

- Scenario 1: Configure Primary, Backup and Alert Log Servers.

```
autoprov_cfg set template -tn example-template_a -sl " PLS_1, PLS_2" -sbl " BLS_3" -sa "ALS_4"
```

Where:

- PLS\_1 and PLS\_2 are Primary Log Servers.
  - BLS\_3 is a Backup Log Server.
  - ALS\_4 is an Alert Log Server.
- Scenario 2: Log Servers are configured as in the previous example. Then, you decide to configure an additional Backup Log Server - BLS\_5.

For these action, it is mandatory to reconfigure all Backup Log Servers:

```
autoprov_cfg set template -tn example-template_a -sbl " BLS_3, BLS_5"
```

Where:

BLS\_3 and BLS\_5 are Backup Log Servers.

New Log Server setting:

- PLS\_1 and PLS\_2 are Primary Log Servers.
  - BLS\_3 and BLS\_5 are Backup Log Servers.
  - ALS\_4 is an Alert Log Server.
- Scenario 3: Log Servers are configured as in the previous example. Then, you decide to delete the Log Servers configuration:

- Delete all Alert Servers:

```
autoprov_cfg delete template -tn template -sa
```

- Delete all Backup Log Servers:

```
autoprov_cfg delete template -tn template -sbl
```

- Delete all Primary Log Servers:

```
autoprov_cfg delete template -tn template -sl
```

**Note:** If all Log Servers settings are removed, the default behavior is restored (Management Server/Domain Management Server acts as Primary Log Server).

## Parameters for AWS only

Parameter	Value	Description
-aap	-	<p>AWS Automatic Policy - creates simplified automatic security policy rules for these solutions:</p> <ol style="list-style-type: none"> <li>1. AWS Auto Scaling</li> <li>2. AWS Centralized Gateway Load Balancer</li> <li>3. AWS Transit Gateway</li> </ol> <p>Note: The parameter has no effect when used in other solutions. You can use the parameter only to create a new Configuration Template (set/delete is not supported).</p>
-gtr	TGW_STATIC_ROUTES	<p>Comma-separated list of CIDR networks. For each CIDR network, a static route is created on each Security Gateway of the Transit Gateway Auto Scaling group.</p>
-gsr	TGW_SPOKE_ROUTES	<p>Comma-separated list of spoke CIDR networks. Each spoke CIDR network that is learned from the Transit Gateway over BGP is advertised again by the Security Gateways of the Transit Gateway Auto Scaling group to the AWS Transit Gateway.</p>
-vxr	TVPC_EXPORT_ROUTES	<p>Comma-separated list of names. Each name is for a BGP routemap that is also exported to the spokes. The user has to create and manage this routemap on all Transit Gateways. This routemap can contain any routes to export to the spoke. For example, the route of a corporate network cidr.</p>
-vsr	TVPC_SPOKE_ROUTES	<p>Name for a BGP routemap that contains all spoke CIDR networks. This routemap is automatically created on the Transit Gateway and exported to the spokes, to allow all spoke-to-spoke traffic.</p>
-dt	Supported values: TGW	<p>The type of the deployment of the CloudGuard Security Gateways.</p>

Parameter	Value	Description
-hc	HEALTH_CHECK_IP_RANGE	String with ip1 and ip2 that represents the range for the AWS gateway health checks, separated by comma. For example: "10.0.0.0,10.0.255.255"
-pp	proxy ports	An optional comma-separated list of proxy ports enabled on Auto Scale Group instances. For example: "8080,8443".

### Parameters for Azure only

Parameter	Value	Description
-an	-	Enable the automatic NAT rule generation on Azure.
-v6	-	Enable IPv6 Gaia support on Azure.

## Configuring Name Prefix for Provisioned Gateways

By default, CME provision the gateway objects using these naming convention:

- **AWS:** <CONTROLLER-NAME>--<SCALE-SET-INSTANCE-NAME>--<REGION-NAME>
- **Azure:** <CONTROLLER-NAME>--<SCALE-SET-INSTANCE-NAME>--<RESOURCE-GROUP-NAME>
- **GCP:** <CONTROLLER-NAME>--<SCALE-SET-INSTANCE-NAME>
- **Nutanix:** <CONTROLLER-NAME>--<VM-NAME>
- **NSX-T:** <CONTROLLER-NAME>--<VM-NAME>

To add the template name as a name prefix (that comes before the controller name), run:

```
autoprov_cfg set template -tn <CONFIGURATION-TEMPLATE-NAME> -pn ""
```

To add a unique name as a name prefix (that comes before the controller name), run:

```
autoprov_cfg set template -tn <CONFIGURATION-TEMPLATE-NAME> -pn <UNIQUE-NAME-PREFIX>
```



**Note** - Currently, the Automatic HF deployment does not support name-prefix.



# Configuring Network Group

CME automatically creates and updates a network group object with all the provisioned scale-set instances in the Security Management/Multi-Domain Server.

Network group object naming convention in the Security Management/Multi-Domain Server by cloud providers:

- **General:** CME\_<CONTROLLER-NAME>--<PLATFORM-UNIQUE-IDENTIFIER>
- **AWS:** CME\_<CONTROLLER-NAME>--<SCALE-SET-NAME>--<REGION-NAME>
- **GCP:** CME\_<CONTROLLER-NAME>--<SCALE-SET-NAME>
- **Azure:** CME\_<CONTROLLER-NAME>--<SCALE-SET-NAME>--<RESOURCE-GROUP-NAME>
- **Nutanix:** CME\_<CONTROLLER-NAME>--<NETWORK-FUNCTION-PROVIDER>
- **NSX-T:** CME\_<CONTROLLER-NAME>--<REGISTERED-SERVICE-NAME>

- **Long names:**

Because of object names restriction in the Security Management Server, for Network group objects with Platform Unique Identifier larger than 150 characters, the CME replaces it with the hash (SHA256) of the Platform Unique Identifier.

For example, in the GCP the group name is:

CME\_<CONTROLLER-NAME>--<SCALE-SET-NAME-HASH-VALUE>

- **Object comment:**

The comment of the Network Group objects (for new objects starting CME Take 243) is the clear/full name of the Network Group object.

You can use the Network Group object in these policies and policy columns:

- Access Control rule columns:
  - Source
  - Destination
  - Install On
- NAT rule columns:
  - Original Source
  - Original Destination

**i** Notes:

- If you use an empty network group object (a scale set has 0 instances) in Access Policy ("Install On" column), policy installation will fail.
- CME creates only one unique network group object for each scale set.

## Default-features

Default-features is a section in the CME configuration. It contains Configuration Template attributes, which are enabled automatically for each new Configuration Template.

**Default-features section:**

- Initializing CME with *autoprov\_cfg init* creates/copies the Default-features section based on:
  - If there is no CME configuration on this server, the Default-features section is being created with the latest available Default features.
  - If there is a CME configuration on the server, the Default-features section is copied (if it exists) from the former configuration.
- To view the existing Default-features, look for the Default-features value in the CME configuration:

```
autoprov_cfg show all
```

**New template creation:**

When you create a new Configuration Template, if the Default-features section exists, its attributes are automatically added to the template (without specifying its attributes in the command).

- i** **Note** - If an attribute has version limitations, it is added automatically only if the template's versions is applicable for the attribute.

To see the existing configuration template, run:

```
autoprov_cfg show template -tn <TEMPLATE NAME>
```

# Enabling and Disabling Software Blades

See "[Supported Configuration Template parameters](#)" on page 33 for parameter information.

To enable Software Blades in CLI on Security Gateways you plan to connect in the future

Step	Instructions
1	Connect to the command line on the Security Management Server.
2	Log in to the Expert mode.
3	<p>Enable the Software Blades:</p> <p><b>To enable one Software Blades at a time, run:</b></p> <pre>autoprov_cfg set template -tn "&lt;CONFIGURATION-TEMPLATE-NAME&gt;" -&lt;SOFTWARE-BLADE-NAME&gt;</pre> <p><b>Example:</b></p> <pre>autoprov_cfg set template -tn "my-configuration-template" -ips</pre> <p><b>To enable multiple Software Blades at a time, run:</b></p> <pre>autoprov_cfg set template -tn "&lt;CONFIGURATION-TEMPLATE-NAME&gt;" -&lt;SOFTWARE-BLADE-NAME-1&gt; -&lt;SOFTWARE-BLADE-NAME-2&gt; ... -&lt;SOFTWARE-BLADE-NAME-N&gt;</pre> <p><b>Example:</b></p> <pre>autoprov_cfg set template -tn "my-configuration-template" -ips -uf -hi</pre>

### To disable Software Blades in CLI on Security Gateways you plan to connect in the future

Step	Instructions
1	Connect to the command line on the Security Management Server.
2	Log in to the Expert mode.
3	<p>Enable the Software Blades:</p> <p><b>To enable one Software Blades at a time, run:</b></p> <pre>autoprov_cfg delete template -tn "&lt;CONFIGURATION-TEMPLATE-NAME&gt;" -&lt;SOFTWARE- BLADE-NAME&gt;</pre> <p><b>Example:</b></p> <pre>autoprov_cfg delete template -tn "my- configuration-template" -ips</pre> <p><b>To enable multiple Software Blades at a time, run:</b></p> <pre>autoprov_cfg delete template -tn "&lt;CONFIGURATION-TEMPLATE-NAME&gt;" -&lt;SOFTWARE- BLADE-NAME-1&gt; -&lt;SOFTWARE-BLADE-NAME-2&gt; ... - &lt;SOFTWARE-BLADE-NAME-N&gt;</pre> <p><b>Example:</b></p> <pre>autoprov_cfg delete template -tn "my- configuration-template" -ips -uf -hi</pre>

### To enable and, or disable Software Blades in SmartConsole on existing Security Gateways

Step	Instructions
1	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
2	Double-click the Security Gateway object.
3	<ul style="list-style-type: none"> <li>▪ Select the Software Blade to enable it.</li> <li>▪ Clear the Software Blade check box to disable it.</li> </ul>
4	Click <b>OK</b> .
5	Install the applicable policy on the Security Gateway.

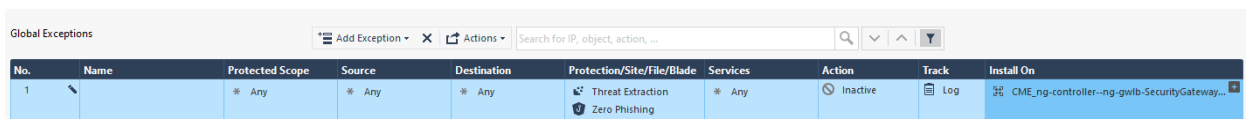
# Autonomous Threat Prevention

Autonomous Threat Prevention is an innovative Threat Prevention management model. For more details, refer to the [Threat Prevention Administration Guide](#) for your version.

Auto Scaling instances do not support Threat Extraction and Zero Phishing software blades.

To use Autonomous Threat Prevention, you must inactivate Threat Extraction and Zero Phishing:

1. Open SmartConsole and navigate to the **Security Policy** tab > **Threat Prevention** section > **Exceptions**.
2. Add new Global Exception:
  - a. In the **Protection/Site/File/Blade** column, add the Threat Extraction and Zero Phishing software blades.
  - b. In the **Action** column, select **Inactive**.
  - c. In the **Install On** column, select the Network Group object of Auto Scaling instances (refer to the ["Configuring Network Group" on page 41](#) section for more details).



No.	Name	Protected Scope	Source	Destination	Protection/Site/File/Blade	Services	Action	Track	Install On
1		* Any	* Any	* Any	Threat Extraction Zero Phishing	* Any	Inactive	Log	CME_ng-controller-ng-gwlb-SecurityGateway...

## CME API

With CME Management API you can configure the CME utility.

For more information, see the [CME API SwaggerHub documentation](#).

### Prerequisites:

- CME Take 139 or higher installed on the Check Point Management Server.
- Management API version 1.8 or higher installed on the Check Point Management Server (see the [Check Point Management API Reference](#)).

## Configuring the tgw\_menu

The Transit Gateway menu is a command-line based menu to configure the AWS Transit Gateway solution.

For more information, see the [CloudGuard Network for AWS Transit Gateway R80.20 and Higher Deployment Guide](#).

# Implied Rules and Restrictive Policy

A restrictive access policy package has only a drop-all cleanup rule. During Security Gateway provisioning cycle (scale out), CME can first install a restrictive policy package to prevent Security Gateway from answering load balancer's health probes.

- CME Take 250 and higher:

## Azure:

Gateway version	Load Balancer	Gateway Load Balancer	Application Gateway
All versions	SKIP	SKIP	INSTALL

## AWS:

Gateway version	Network Load Balancer	Gateway Load Balancer	Application Load Balancer
R81.10 and higher	SKIP	SKIP	INSTALL
R81 and lower	INSTALL	SKIP	INSTALL

## GCP

Gateway version	All Load Balancer types
R81.10 and higher	SKIP
R81 and lower	INSTALL

**Private Cloud Vendors (NSX-T, Nutanix):** CME installs restrictive policy on all solutions.

- CME Take 250 and lower:

CME always installs restrictive policy.

For CME Takes lower than 250, if the Implied Rules are disabled, it is required to configure a custom restrictive policy package and to set it in the Configuration Template.

For more details see:

- [sk179346 - Configuring Explicit Rules instead of Implied Rules](#)
- ["Supported Configuration Template parameters" on page 33](#)

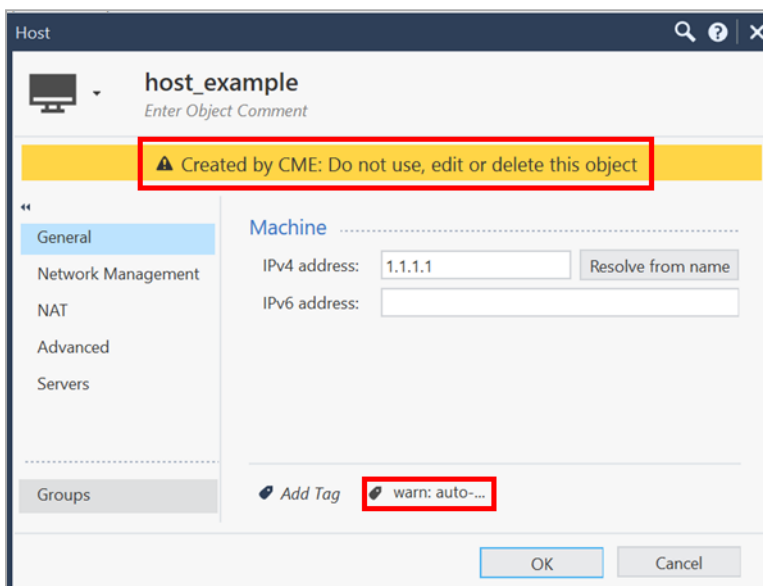
If it necessary to use the Multi-Domain Server Global Policy together with automatic provisioning, see ["Global Policy on a Multi-Domain Server" on page 56](#).

## Objects Banner

Starting from CME Take 252, objects created by CME have a warning banner.

To show the warning banner, CME creates and attaches a tag to objects.

Example of a warning banner for a host object created by CME:



# Managing Multiple-Autoscaling Solutions with One Security Management Server

## Background:

Configurations on a Security Management Server can have:

- Multiple Controllers
- Multiple Templates

## Each controller can:

- Represent single cloud environments (such as a single Azure Service Principal)
- Manage multiple Check Point Autoscaling solutions with either one configuration template, or with multiple configuration templates

## Each template:

- Represents one Check Point security configuration for a new Security Gateway (such as policy name, active Software Blades, SIC, and so on).
- When a new Security Gateway instance is detected by the autoprovision process, it uses the name of the template to determine the final Security Gateway configurations.



**Configuration:**

When you run the "autoprov\_cfg <Cloud Environment Name>" command on your Security Management Server, it configures one Management Server with one controller and one template.

This setup lets you manage one cloud environment with one Check Point security configuration for all Check Point autoscaling solutions found on it.

Example of the "autoprov\_cfg init" command to initialize the autoprovision configuration:

```
autoprov_cfg init "<Cloud-Name>" -mn "<Management-Name>" -tn
"<Template-Name>" -otp "<SIC-key>" -ver R80.20 -po "<Policy-Name>"
-cn "<Controller-Name>" -sb "<Azure-Subscription>" -at "<Tenant-
ID>" -aci "<Client-ID>" -acs "<Client-Secret>"
```

You can manage multiple Check Point autoscaling solutions.

To manage multiple Check Point autoscaling solutions, you must add a controller to represent each cloud platform.

**Example command that shows how to add a *new* controller:**

```
autoprov_cfg add controller Azure -cn "<Name>" -sb "<Azure-
Subscription>" [- en {AzureCloud,AzureChinaCloud,AzureGermanCloud,
AzureUSGovernment}] -at "<Tenant-ID>" -aci "<Client-ID>" -acs
"<Client-Secret>"
```



**Important** - Run this command for each new cloud environment, except the environment you used in the "autoprov\_cfg init" command.



**Note** - Optional values, such as configuring <Controller Templates> (add and, or change credentials template to customer environments) in the CME configuration file. Each Controller has its own set of cloud environment credentials. Give a meaningful name to each environment to distinguish between them.

**To edit the *existing* controller, run these commands:**

```
autoprov_cfg set controller
```

```
autoprov_cfg delete controller
```



**Note** - To remove all the CloudGuard Network Security Gateways related to this controller, scale in the scale set to 0 instances, wait for CME to delete the matching gateway objects from the Security Management Server, and only afterward delete the controller.

**To manage multiple autoscaling solutions with different security configurations:**

For every different Check Point security configuration, add a new template to represent it.

**To add a new template for each unique security configuration, use this command:**

- For R80.20

```
autoprov_cfg add template -tn "<Other-Template-Name>" -otp  
"<SIC-key>" -ver R80.20 -po "<Other-Policy-Name>"
```

- For R80.10

```
autoprov_cfg add template -tn "<Other-Template-Name>" -otp  
"<SIC-key>" -ver R80.10 -po "<Other-Policy-Name>"
```

** Notes:**

- Run this command for each template, except the template you used in the "autoprov\_cfg init" command.
- **Before** you scale out new Security Gateways, you must configure a Security Policy called <Other-Policy-Name> in SmartConsole.
- You can configure multiple autoscaling solution with a single template. For each autoscaling solution, enter the same values for the resource tags x-chkp-management and x-chkp-template.

To edit the existing template, run these commands:

```
autoprov_cfg set template
```

```
autoprov_cfg delete template
```

 **Notes:**

- Run the "autoprov\_cfg -h" command for more information about uses and examples.

For example:

```
autoprov_cfg init Azure -h
```

```
autoprov_cfg add controller Azure -h
```

- Run the "autoprov\_cfg show" command to confirm your configuration.
- If you followed the instructions in this guide correctly, then in Azure:
  - Each VMSS resource tag matches the *<Management-Name>* and the respective *<Template-Name>*.

```
x-chkp-management = <Management-Name>
x-chkp-template = {<Configuration-Template1-Name> |
<Configuration-Template-Other-Name>} to which the
VMSS is a subject
```

- The subscription of the VMSS matches the Subscription ID in the respective controller.
- The respective Controller Service Principal has a proper access role according to the Administration Guide.

# Managing Auto-Scale with One Multi-Domain Server

Automatic provisioning enables the management of Scale set gateways deployed in cloud environments by a Check Point Multi-Domain Server.

## Multi-Domain Server in Public Cloud:

If the Multi-Domain Server is installed in the Public Cloud, refer to the relevant article:

- [sk154436 - MDS / MDSM \(Multi-Domain Management\) Deployment on Azure](#)
- [sk143213 - Multi-Domain Management Deployment on AWS](#)
- [sk174186 - Multi-Domain Management Deployment on Google Cloud Platform](#)

## Important Notes

- The Security Multi-Domain Server login credentials must allow the script to access all the applicable Domain Management Servers.
- One instance of the CME service is responsible for provision in all the Domain Management Servers.
- For the `autoprov_cfg` commands to take effect, you must restart the CME service.

Run this command in the Expert mode to restart the CME service:

```
service cme restart
```

## Use Case 1 - Working with a Single Domain in the Multi-Domain Server

Rather than a Security Management Server, a Single Domain Management Server (in the Multi-Domain Server) does the provisioning.

For this use case, you must specify the Domain of the Domain Management Server, run:

```
autoprov_cfg set management -d <DOMAIN-NAME>
```



**Note** - In the Multi-Domain Server, replace the `<DOMAIN-NAME>` with the name of the applicable Domain Management Server.

## Use Case 2 - Working with Multiple Domains in the Multi-Domain Server and Multiple-Cloud Accounts

For this use case, it is assumed that for each Domain Management Server, there is a different dedicated cloud account.

The presumption is that, based on the given cloud credentials, each of the accounts returns a mutually exclusive set of objects. Different sets of credentials must not return the same instance. For example, if the two different cloud accounts return the same CloudGuard Network Security Gateway instance, the CME service tries to provision it two times - one time for each of the different cloud accounts.

For this use case, you must specify a Domain for each of the controllers used to connect to your cloud environments. (A controller contains configuration required to connect to a cloud environment, such as credentials, regions, or a subscription ID).

To specify a name for each controller, run:

```
autoprov_cfg set controller <CONTROLLER-TYPE/VENDOR> -cn  
<CONTROLLER-NAME> -cd <DOMAIN-NAME>
```

### Notes:

- Replace the *<CONTROLLER-NAME>* with the name of the controller used to connect to your cloud environment.
- Replace the *<DOMAIN-NAME>* with the name of an existing Domain.
- Multiple controllers can have the same *<DOMAIN-NAME>* value. This means that objects retrieved by the controllers, are configured in the same Domain.

The configuration and policy of a CloudGuard Network Security Gateway is determined by:

- A configuration template that you can create and edit with the `autoprov_cfg` CLI configuration tool.
- A tag on the instance or Virtual Machine with the configuration template name.

By default, any Security Gateway may be tagged with the name of any existing configuration template which is then provisioned with the parameters.

If particular templates must only be used by a specific Domain, you can run this command to enforce it:

```
autoprov_cfg set controller Azure -cn <CONTROLLER-NAME> -ct  
<CONFIGURATION-TEMPLATES-NAMES>
```

 **Notes:**

- Replace the `<CONTROLLER-NAME>` with the name of the controller (the one that you specified a Domain for).
- Replace the `<CONFIGURATION-TEMPLATES-NAMES>` with a list of configuration template names that can be used by that specific Domain (for example, `TEMPLATE1-NAME TEMPLATE2-NAME`).
- If you replace Domains for a controller, you must first scale out the new Security Gateways, and then remove the previous Security Gateways.

## Use Case 3 - Working with Multiple Domains in the Multi-Domain Server and a Single Cloud Account

Sometimes the environment requires that all the cloud objects be managed by one cloud account, but the security management is divided across multiple Domains.

It is possible to configure multiple controllers with the same credentials, but specify a different Domain for each controller. As explained in the use case "Working with Multiple Domains in the Multi-Domain Server and Multiple Cloud Accounts", this causes multiple controllers to retrieve the same CloudGuard Network Security Gateway and to provision the same Security Gateway in multiple Domains.

The solution is to configure exclusive templates for each Domain Management Server. To avoid duplication of attributes shared by multiple configuration templates, it is possible to configure a prototype configuration template. Multiple exclusive configuration templates use this prototype configuration template.

These example commands specify a prototype configuration template with a Security Policy, Security Gateway version, and a SIC Activation Key.

Example that shows how to configure a exclusive template for each Management Domain Server.

```
autoprov_cfg add template -tn <BASE-CONFIGURATION-TEMPLATE-NAME> -
po <POLICY-NAME> -ver <VERSION> -otp <SIC-ACTIVATION-KEY>
```

```
autoprov_cfg set template -tn <EXCLUSIVE-CONFIGURATION-TEMPLATE-
NAME> -pr <BASE-CONFIGURATION-TEMPLATE-NAME>
```

### Notes:

- Replace the `<BASE-CONFIGURATION-TEMPLATE-NAME>` with a name to represent the prototype configuration template (for example, `base-template`).
- Replace the `<POLICY-NAME>` with the name of a Security Policy to install on the Security Gateways (for example, `Standard`).
- Replace the `<VERSION>` with the Check Point version on the Security Gateway (for example, `R80.20`).
- Replace the `<SIC-ACTIVATION-KEY>` with the Secure Internal Communication (SIC) key.
- Replace the `<EXCLUSIVE-CONFIGURATION-TEMPLATE-NAME>` with the name of the exclusive configuration template, which uses the prototype configuration template values. You must run the second command one time for each exclusive template.

After you configure a set of templates dedicated for each Domain Management Server, you can specify the templates for each controller as explained in the use case "Working with Multiple Domains in the Multi-Domain Server and Multiple Cloud Accounts". Each of the controllers, that share credentials, retrieves the same set of Security Gateways. But, the controllers skip the provisioning for the Security Gateways, of which the template tag does not match the configuration templates list enforced on the controller.

## Global Policy on a Multi-Domain Server

This section applies if it necessary to use the Global Policy together with automatic provisioning.

When you deploy a new Security Gateway, it installs an internal restrictive access policy. This policy is intended to drop all traffic.

Any rules you configure in the Global Policy automatically conflict with the restrictive policy. As a result, the Global Policy installation fails.

It is possible to use a custom restrictive policy, which is manually excluded from the Global Policy Assignment -do these steps:

Step	Description
1	<p>Create a Global Policy in the Global Domain:</p> <ol style="list-style-type: none"> <li>a. Connect with SmartConsole to the Multi-Domain Server.</li> <li>b. In the SmartConsole login window, select <b>Global Domain</b>.</li> <li>c. Create a Security Policy with the required rules.</li> <li>d. Publish the SmartConsole session.</li> </ol>
2	<p>Create a new restrictive policy in each Domain:</p> <ol style="list-style-type: none"> <li>a. Connect with SmartConsole to the Multi-Domain Server.</li> <li>b. In the SmartConsole login window, select the <b>Domain</b>.</li> <li>c. Create a restrictive Access Control Policy. Because this policy is for internal purposes, we recommend this rule: <b>Source</b> = *Any <b>Destination</b> = *Any <b>Action</b> = Drop</li> <li>d. Publish the SmartConsole session.</li> <li>e. Do Steps 2b-2d again for <b>each</b> Domain.</li> </ol>



Step	Description
3	<p>Do not include the restrictive policy created in Step 2:</p> <ol style="list-style-type: none"> <li>Connect with SmartConsole to the Multi-Domain Server.</li> <li>In SmartConsole login window, select the <b>MDS</b>.</li> <li>Go to <b>Multi-Domain &gt; Global Assignments</b>.</li> <li>Under <b>Access Control</b>, select <b>Advanced</b>.</li> <li>Click <b>Assign Global Access Control Policy to all domain policies except</b>.</li> <li>Select the restrictive policy object you created in Step 2.</li> </ol>
4	<p>Set the newly created restrictive policy as the default restrictive policy:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Multi-Domain Server (on SSH or console).</li> <li>Log in to the Expert mode.</li> <li>For each Domain, set the name of the restrictive policy package you created in Step 2 as the default restrictive policy:</li> </ol> <pre data-bbox="316 864 1461 967"> autoprov_cfg set template -tn &lt;CONFIGURATION-TEMPLATE-NAME&gt; -rp &lt;RESTRICTIVE-POLICY-PACKAGE-NAME&gt; </pre>

 **Notes:**

- Replace the `<CONFIGURATION-TEMPLATE-NAME>` with the name of the applicable configuration template.
- Replace the `<RESTRICTIVE-POLICY-PACKAGE-NAME>` with the name of the restrictive policy package you created in Step 2.

# Autoprovision and Multi-Domain Log Server Configuration

This section applies if it necessary to add a Multi-Domain Log Server together with automatic provisioning.

**Important** - Before you can create a Domain Log Server, a Domain must have a minimum of one configured Domain Management Server.

To add a Domain Log Server:

1. Stop the CME service.

```
service cme stop
```

2. Add a Domain Log Server.

3. Start the CME service:

```
service cme start
```

You can configure a template to forward the security logs from the Security Gateway to the applicable Domain Log Server:

```
autoprov_cfg set template <CONFIGURATION-TEMPLATE-NAME> -sl <SEND-LOGS-TO-DLS-NAME>
```

By default, alerts are not sent to the Domain Log Server.

You can configure a template to forward the security logs from the Security Gateway to the applicable Domain Backup Log Server:

```
autoprov_cfg set template <CONFIGURATION-TEMPLATE-NAME> -sbl <SEND-LOGS-TO-DBLS-NAME>
```

You can configure the template to forward the alerts also from the Security Gateway to the applicable Domain Log Server:

```
autoprov_cfg set template <CONFIGURATION-TEMPLATE-NAME> -sa <SEND-ALERTS-TO-DLS-NAME>
```

**Notes:**

- Replace the `<CONFIGURATION-TEMPLATE-NAME>` with the name of the applicable configuration template.
- Replace the `<SEND-LOGS-TO-DLS-NAME>`, `<SEND-ALERTS-TO-DLS-NAME>`, `<SEND-LOGS-TO-DBLS-NAME>` with the name of the Domain Log Server object as configured in SmartConsole.
- Refer to the section for more details regarding Log Server settings.

# Managing Autoscaling with Management High Availability

## Security Management Server High Availability

You can deploy and configure a Secondary Security Management Server as a Standby Security Management Server to provide High Availability in case of a failure or of unexpected downtime on the Primary Security Management Server.

For more information, see the [Security Management Administration Guide](#) for your version > section *Management High Availability*.

### Notes:

- The Network Security Group must enable these ports on both Security Management Servers:
  - Port 18211 - Used for SIC with the Secondary Security Management Server.
  - Port 18221 - Used for synchronization between the Security Management Servers.
  - Port 18192 - Used for internal connection between the Security Management Servers.
- Use the same template, *Check Point Security Management*, to deploy a Standby Security Management Server. During the deployment, select the installation type configured manually. Next, configure the second Virtual Machine as a Secondary Security Management Server. See the Security Management Administration Guide for your version > section *Configuring a Secondary Server in SmartConsole*.

While the Secondary Security Management Server acts as a Standby server, make sure that the `autoprovisioning` script does not run on the Standby server.

To do this, run these commands in Expert mode on the Standby server:

```
service cme stop
chkconfig --del cme
```

**To demote the Active Security Management Server to the Standby role:**

Step	Description
1	Disable autoscaling.

Step	Description
2	Connect to the command line on the Active Security Management Server.
3	Log in to the Expert mode.
4	Run these commands: <pre>service cme stop</pre> <pre>chkconfig --del cme</pre>
5	Change the Active Security Management Server to the Standby: <ol style="list-style-type: none"><li>Connect with SmartConsole to the Active Security Management Server.</li><li>Click <b>Menu &gt; Management High Availability</b>.</li><li>Use the <b>Action</b> button to change the Active server to Standby.</li></ol> <p>For more information, see the Security Management Administration Guide for your version &gt; section <i>Changing a Server to Active or Standby</i>).</p>
6	Enable autoscaling.

# Multi-Domain Server High Availability

You can deploy and configure a Secondary Multi-Domain Server as a Standby Multi-Domain Server to provide High Availability in case of a failure, or of unexpected downtime on the Primary Multi-Domain Server.

Make sure to read the ["Managing Auto-Scale with One Multi-Domain Server" on page 52](#).



## Important:

- The Security Multi-Domain Server log in credentials should allow the script to access all the applicable Domain Management Servers in each Multi-Domain Server.
- There must be two instances of the CME service that are responsible for provisioning in all the Domain Management Servers and in each Multi-Domain Server.
- Configure the first deployed Multi-Domain Server as Primary in the First Time Configuration Wizard.
- Configure all other deployed Multi-Domain Servers as Secondary in the First Time Configuration Wizard.
- CME service script must run on both Primary and Secondary Multi-Domain Servers.
- To add a new Domain Management Server in an existing Domain:

Step	Description
1	In the existing Domain, determine which Multi-Domain Server runs the Active Domain Management Server.
2	Stop the CME service on that Multi-Domain Server: <pre>service cme stop</pre>
3	Add a new Domain Management Server on an applicable Multi-Domain Server.
4	Start the CME service on the Multi-Domain Server (the same Multi-Domain Server on which you stopped the CME service): <pre>service cme start</pre>

- If you demote the Active Domain Management Server to Standby role and then promote the Standby Domain Management Server to the Active role in the same Domain, you must restart the CME service on the Multi-Domain Server that runs the new Active Domain Management Server.

Run this command in Expert mode to restart the CME service:

```
service cme restart
```

- All configuration updates on the Primary Multi-Domain Server require the restart of the CME service on all the Secondary Multi-Domain Servers.
- To restart the autoprovision service on all Primary and Secondary Multi-Domain Servers:

Step	Description
1	Connect to the command line on each Secondary Multi-Domain Server.
2	Log in to the Expert mode.
3	Make sure that the configuration file is already synchronized from the Primary Multi-Domain Server: <pre>autoprov_cfg show all</pre>
4	Restart the CME service. <pre>service cme restart</pre>

- To add a Multi-Domain Log Server, see the CME and ["Autoprovision and Multi-Domain Log Server Configuration" on page 58](#).

- To add a new Domain Log Server in an existing Domain:

Step	Description
1	In SmartConsole, determine which Multi-Domain Server runs the Active Domain Management Server in the existing Domain.
2	Connect to the command line on that Multi-Domain Server.
3	Log in to the Expert mode.
4	Stop the CME service on that Multi-Domain Server: <pre>service cme stop</pre>
5	In SmartConsole, add a new Domain Log Server on an applicable Multi-Domain Server.
6	Start the CME service on the Multi-Domain Server (the same Multi-Domain Server on which you stopped the CME service): <pre>service cme start</pre>



# Automatic NAT and Access Rules

Automatic NAT and Access rules for CloudGuard Auto Scaling automatically configure the NAT and Access rules in the Security Policy based on the Internal Application gateway's listeners and tags.



**Important** - This configuration is only for:

- VMSS in Azure that uses the Application gateway.
- AWS Auto Scale Group solutions

For AWS, this feature is part of the CloudGuard Auto Scaling for AWS solution, see [CloudGuard Network for AWS Auto Scale Group Deployment Guide](#).

## Prerequisites



- CME Take 137 or higher installed on the Security Management Server or Multi-Domain Server.
- CME controller used for this VMSS with reader permissions for Application gateway resources in Azure.
- A deployed CloudGuard for Azure VMSS solution that uses both an external and internal Application gateway.

For more information, see the [Virtual Machine Scale Sets \(VMSS\) for Azure R80.10 and Higher Administration Guide](#) > Section *Deploy Internal Application Gateway*.

# Mandatory Configuration

To enable this feature, these tags are required on the internal Application gateway:


Key	Value	Example
x-chkp-management	The name of the Management Server	my-management
x-chkp-template	The name of the configuration template selected when the Virtual Machine Scale Sets (VMSS) for Azure was setup.	my-configuration-template

-  **Note** - When this feature is enabled, CME starts to configure NAT and Access rules for Application gateways with the above tags that match the current management and configuration template. See ["Enabling Automatic NAT and Access Rules in CME" on page 71](#).
-  **Best Practice** - To prevent unexpected behavior, we recommend to stop CME before this configuration, and to restart it after the configuration is complete.

# NAT Rule Generated

No	Original Source	Original Destination	Original Services	Translated Source	Translated Destination	Translated Services	Installed On
1	See below for more information	LocalGateway External	See below for more information	LocalGateway Internal NAT Method: Hide	The Internal Application gateway frontend IP private address	Listener port and protocol. See below for more information.	VMSS instance

## Default Values

Column	Values
<b>Original Source</b>	<p>The traffic to the VMSS instances is initiated from the external Application gateway subnet.</p> <p>By default, the original source is the internal Application gateway VNET. To change this, see <a href="#">"Customizing Original Source in the NAT Rule" on page 70</a>.</p> <p> <b>Important</b> - In an environment with VNET peering (the external and internal Application gateways are on different VNETS). <b>You must</b> change the <b>Original Source</b> to be the external Application gateway subnet or VNET.</p>
<b>Original Services</b>	<p>If the listener listens to protocol HTTP using port 80 or HTTPS using port 443, the original service port is:</p> <ul style="list-style-type: none"> <li>▪ 9080 for port 80</li> <li>▪ 9443 for port 443</li> </ul> <p>If not, the original service is the same as the listener Protocol and Port.</p>

Column	Values												
<b>Translated Services</b>	<p>To change the Original Services, see "<a href="#">Customizing Original and Translated Services in the NAT Rule</a>" on the next page.</p> <p>Example:</p> <table border="1"> <thead> <tr> <th>Listener Protocol and Port</th> <th>Original Service</th> <th>Translated Service</th> </tr> </thead> <tbody> <tr> <td>HTTP and port 81</td> <td>HTTP and port 81</td> <td>HTTP and port 81</td> </tr> <tr> <td>HTTP and port 80</td> <td>HTTP and port 9080</td> <td>HTTP and port 80</td> </tr> <tr> <td>HTTP and port 443</td> <td>HTTP and port 9443</td> <td>HTTP and port 443</td> </tr> </tbody> </table>	Listener Protocol and Port	Original Service	Translated Service	HTTP and port 81	HTTP and port 81	HTTP and port 81	HTTP and port 80	HTTP and port 9080	HTTP and port 80	HTTP and port 443	HTTP and port 9443	HTTP and port 443
Listener Protocol and Port	Original Service	Translated Service											
HTTP and port 81	HTTP and port 81	HTTP and port 81											
HTTP and port 80	HTTP and port 9080	HTTP and port 80											
HTTP and port 443	HTTP and port 9443	HTTP and port 443											

## Access Rule Generated

Source	Destination	VPN	Services & Applications	Action	Track	Install On
The same as the <b>Original Source</b> in the corresponding NAT rule	LocalGatewayExternal	Any	The same as the <b>Original Services</b> in the corresponding NAT rule	Accept	Log	VMSS instance

See the [Virtual Machine Scale Sets \(VMSS\) for Azure R80.10 and Higher Administration Guide](#) > Section *Creating Dynamic Objects LocalGatewayInternal and LocalGatewayExternal*.

# Customizing Original and Translated Services in the NAT Rule

To customize the ports for **Original Services**, or to configure multiple internal Application gateways to listen to other ports, tag the internal Application gateway as follows:

Key	Value	Example
x-chkp-forwarding	A space-separated list of <PROTOCOL>-<ORIGINAL-PORT>-<DESTINATION-PORT> items to represent the forwarding rules it is necessary to use	<ul style="list-style-type: none"> <li>■ HTTP-9081-80</li> <li>■ HTTP-9081-80</li> <li>■ HTTPS-9444-443</li> </ul>

## Value Description

Attribute	Description
<PROTOCOL>	Allowed values: HTTP or HTTPS
<ORIGINAL-PORT>	The port, to which the external Application gateway forwards the traffic.
<DESTINATION-PORT>	The listener port on the internal Application gateway.

If the <DESTINATION-PORT> matches an existing internal Application gateway port, the **Original Services** in the NAT rule is a CPM service composed of <PROTOCOL> and <ORIGINAL-PORT>.

If there is no match, another rule is created that uses the tag value:

- **Original Services:** CPM service composed of <PROTOCOL> and <ORIGINAL-PORT>
- **Translated Services:** CPM service composed of <PROTOCOL> and <DESTINATION-PORT>

**Examples:**

Listener protocol and port	x-chkp-forwarding	Original Services	Translated Services
HTTP and port 81	HTTP-9981-81	HTTP and port 9981	HTTP and port 81
HTTP and port 81	HTTP-9999-99	HTTP and port 81	HTTP and port 81
		HTTP and port 9999	HTTP and port 99

## Customizing Original Source in the NAT Rule

To allow traffic from a specific IP addresses or networks based on their CIDRs, tag the internal Application gateways as follows:

- ★ **Best Practice** - We recommend to use this tag with the external Application gateway subnet.

Key	Value	Example
x-chkp-source-cidrs	A list of space-separated network/mask, from which the traffic is allowed	10.0.0.0/24 192.168.0.0/24

**Examples:**

VMSS VNET	x-chkp-source-cidrs	Original Source
10.0.0.0/16	Not configured	10.0.0.0/16
10.0.0.0/16	10.0.0.0/24	10.0.0.0/24

# Enabling Automatic NAT and Access Rules in CME

To enable Automatic NAT and Access rules, run:

```
autoprov_cfg set template -tn <CONFIGURATION-TEMPLATE-NAME> -an
```

When the feature is enabled, CME starts to configure NAT and Access rules based on the Application gateway's `x-chkp_management` and `x_chkp-template` tags.

To disable Automatic NAT and Access rules, run:

```
autoprov_cfg delete template -tn <CONFIGURATION-TEMPLATE-NAME> -an
```

After the feature is disabled:

1. CME removes the existing NAT and Access rules that were automatically created for this template.
2. CME does not add NAT and Access Rules for new instances.

## (Optional) Automatic Rule Placement

By default, automatic Access and NAT rules for each VMSS instance are added at the top of the rulebase.

Sometimes it is recommended to add the rules in a specific place in the policy rather than at the top.

This can be achieved by creating a section for these rules in SmartConsole, and specifying the section name in CME configuration.


### Procedure

1. In SmartConsole, in the applicable Security Policy, create a **New Section**:
  - a. To create a New Section, right-click on below a rule number.
  - b. Select **Create New Section**, click **Below**.
  - c. Enter the name for the New Section and make sure to record the name.
  - d. Publish the SmartConsole session.
2. Connect to command line on the Security Management Server.
3. Log in to the Expert mode.
4. Run this command:

```
autoprov_cfg set template -tn <CONFIGURATION-TEMPLATE-NAME>
-secn <SECTION-NAME>
```

- Replace *<CONFIGURATION-TEMPLATE-NAME>* with the name of the configuration template configured with the Automatic NAT and Access rules feature (for example, *my-configuration-template*).
- Replace *<SECTION-NAME>* with the name of the section created in Step 1.

If the section is specified in the configuration template, but not found in the rule base, the rule is added at the top by default.

 **Note** - The changes above occur only for new VMSS instances. The existing rules stay the same.

### To change the section name

To change the section in which new automatic Access and NAT rules are added, run:

```
autoprov_cfg set template -tn <CONFIGURATION-TEMPLATE-NAME> -
secn <SECTION-NAME>
```



## To remove the section name

To add the new automatic Access and NAT rules to the top of the rule base, run:

```
autoprov_cfg delete template -tn <CONFIGURATION-TEMPLATE-NAME> -  
secn
```

## Known Limitations

- The feature works only with:
  - Azure Application gateways
  - AWS Auto Scale Group solutions

Azure Load Balancers (layer 4) are currently not supported.

- These ports used with Auto Scaling groups in AWS are not supported:
  - x-chkp-ignore-ports
  - x-chkp-http-ports
  - x-chkp-https-ports
  - x-chkp-ssl-ports
  - x-chkp-source-object

# Automatic Hotfix Deployment

Automatic Hotfix Deployment for CloudGuard autoscaling solutions automatically deploys a preconfigured CPUSE Hotfix or Jumbo Hotfix Accumulator (JHF) when an instance scales out.

This feature allows you to do all the necessary configuration on the Management or Multi-Domain Management Server. You do not have to access each Security Gateway instance manually.

## Prerequisites:

- CME is installed on the Management or Multi-Domain Management Server.
- Autoprovision is enabled and configured for the autoscaling solution for which Automatic Hotfix Deployment is required.
- CDT (Central Deployment Tool), version 1.7 or higher installed on the Security Management or Multi-Domain Security Management Server.
- CPUSE is updated to the latest version on the Management or Multi-Domain Management Server.
- The CPUSE package to be installed on new scaled out instances is available on the Management or Multi-Domain Management Server.

## Configuring the Automatic Hotfix Deployment


### Step 1 - Installing the Central Deployment Tool (CDT)

1. Download CDT v1.7 or higher from [sk111158](#).
2. Install the Central Deployment Tool.




### Step 2 - Updating the CPUSE on the Management Server

To update the CPUSE agent, you can either perform a self-update (which is the simplest method), or manually upgrade, see [sk92449](#) - section 3-A "Download the latest build of the CPUSE Agent".

## Step 3 - Enabling and Configuring Automatic Hotfix Deployment

Step	Description
1	Configure the template.
2	Connect to the command line on the Security Management Server.
3	Transfer the downloaded Hotfix or Jumbo Hotfix Accumulator package to a directory in the Security Management Server. This Hotfix package is configured to be deployed automatically on scaled-out instances.
4	Log in to the Expert mode..
5	Launch the CME menu: <pre>cme_menu</pre>
6	<ol style="list-style-type: none"> <li>Select the cloud platform where the relevant autoscaling solution is deployed in the CME menu main page.</li> <li>Select <b>Automatic HotfixDeployment</b>.</li> </ol>
7	<p>Enable the Automatic <b>HotfixDeployment</b> feature:</p> <ol style="list-style-type: none"> <li>Select <b>Enable and Configure Automatic HotfixDeployment</b>.</li> <li>Enter the requested parameters (see the parameter table below for details).</li> </ol>
8	Repeat Step 6, as needed, for each template.
9	<p>Confirm the configuration, and then restart the CME service, run:</p> <pre>CME service has to be restarted to apply configurations. Restart now? 1 - Yes</pre> <p> <b>Note</b> - To restart the service manually, run:</p> <pre>service cme restart</pre>


## Parameters

Parameter	Description	Possible Values
configuration-template-name	<p>Name of the configuration template with the relevant autoscaling solution.</p> <p> <b>Note</b> - If CME was not configured as described, then this feature cannot be enabled.</p>	Template number as displayed on-screen
package-path	The package's <b>absolute</b> path to be deployed on the scale-out instances. The package must be located on the Management Server.	"/home/admin/Check_Point_R80_10_JUMBO_HF_Bundle_T169_FULL.tgz"
is-mandatory	<p>In case of package deployment failure, whether or not the deployment is a mandatory condition, in order to allow the scale-out instance to continue the setup configuration.</p> <p> <b>Note</b> - If the package deployment fails and you select "Yes", then the instance tries to deploy the package again. This may cause the other instances to not start the CME.</p>	<p>1 - Yes</p> <p>2 - No</p>
package-source	<p>Package delivery method to the scale set instance.</p> <ul style="list-style-type: none"> <li>▪ Local - Package is sent from the Management Server to the scaled-out instances.</li> <li>▪ Cloud - The scale set instance downloads the package from the Check Point Cloud.</li> </ul> <p> <b>Note</b> - A package with the same filename must be available in the Check Point Cloud.</p>	<p>1 - Cloud</p> <p>2 - Local</p>

# Disabling Automatic Hotfix Deployment

You can disable Automatic Hotfix Deployment for scale out instances you plan to connect in the future.

## Procedure

Step	Description
1	Connect to the command line on the Security Management Server.
2	Log in to the Expert mode.
3	Launch the CME menu: <pre>cme_menu</pre>
4	<ol style="list-style-type: none"> <li>Select the cloud platform where the relevant autoscaling solution is deployed in the CME menu main page.</li> <li>Select Automatic HotfixDeployment.</li> </ol>
5	Select <b>Disable Automatic HotfixDeployment</b>
6	Select the template on which you want to disable the feature.
7	<p>Confirm the operation:</p> <pre>CME service has to be restarted to apply configurations. Restart now? 1 - Yes</pre> <p> <b>Note</b> - To restart the service manually, run:</p> <pre>service cme restart</pre>

# Viewing Configuration Parameters

## Procedure

Step	Description
1	Connect to the command line on the Security Management Server.
2	Log in to the Expert mode.
3	Launch the CME menu: <input type="text" value="cme_menu"/>
4	<ol style="list-style-type: none"><li>Select the cloud platform where the relevant autoscaling solution is deployed in the CME menu main page.</li><li>Select Automatic HotfixDeployment.</li></ol>
5	Select <b>Display HotfixDeployment status</b> .
6	Select the template to be used to show the configuration parameters.

# Viewing Package Deployment Status

## Procedure

Step	Description
1	Connect to the command line on the Security Management Server.
2	Log in to the Expert mode.
3	Launch the CME menu: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;">cme_menu</div>
4	<ol style="list-style-type: none"> <li>a. Select the cloud platform where the relevant autoscaling solution is deployed in the CME menu main page.</li> <li>b. Select Automatic HotfixDeployment.</li> </ol>
5	Select <b>Display Automatic HotfixDeployment Configurations</b> .
6	Select the template to be used to show the configuration parameters.

## Output Parameters

Parameter	Description	Possible Values
Instance Name	The name of instance	Azure-Production--exampleVMSS_11--EXAMPLE-VMSS
IP Address	The IP address of the specific instance	"192.168.0.4"
Status	<p>The Hotfix package installation status for the specific instance:</p> <ul style="list-style-type: none"> <li>▪ <b>Installed</b> - The package successfully installed.</li> <li>▪ <b>Not Installed</b> - The package was not installed.</li> <li>▪ <b>Not Applicable</b> - The package is not compatible with the instance.</li> <li>▪ <b>Error</b> - There was an error retrieving the status of the instance.</li> </ul>	<p>Installed            Not Installed            Not Applicable            Error</p>

# Limitations

- The package is only installed on new instances.

To install the package on all existing instances, do these steps:

1. Remove instances that do not contain the package.
2. Scale out new instances.
3. Wait for the provisioning to finish.

- Supported cloud platforms: Azure, AWS, GCP.

- Central Deployment Tool:

- Because Automatic Hotfix Deployment relies on CDT, see *CDT Limitations* in [sk111158](#).
- CDT version 1.9 is not compatible with Auto-HF in CME.
- When another CDT operation is in progress, you cannot use the Display Hotfix deployment status option.

If you do, it shows an error message.

The solution is to wait until the CDT operation is finished, and then try the Display Hotfix deployment status again.

- When scaling out several instances, the package is not installed in parallel.
- Enabling Automatic Hotfix Deployment significantly increase the time until a scaled-out instance finishes provisioning.

This is due to the time it takes for a Hotfix or Jumbo Hotfix Accumulator to be installed.

- Only Hotfixes and Jumbo Hotfixes are supported.

Minor and Major upgrades are not supported.

- Automatic HF deployment does not support name-prefix.



# CME Monitoring

CME is integrated with Check Point logs in order to improve logging and monitoring.

### Prerequisites

- CME Take 178 or higher installed on the Security Management or Multi-Domain Security Management Server. Run this command in Expert mode to verify the Take:

```
autoprov_cfg -v
```

- CME Take 51 or higher installed on the Security Management or Multi-Domain Security Management Server. Run this command in Expert mode to verify the take:

```
autoupdatercli show | grep -A 6 Infra_AutoUpdate
```


To monitor CME logs, use one of these options:

- Filter the logs in the SmartConsole with this query syntax: `blade:"CME"`
- Configure Log Exporter to export all logs that belong to CME Blade.

See the [Logging and Monitoring R81.10 Administration Guide](#) > Log Exporter > Configuring Log Exporter in CLI > Log Exporter Advanced Configuration in CLI for more information.

For example on how to export CME logs to Splunk log server, run in Expert mode:

```
cp_log_export add name <exporter name> target-server <log server IP> target-port <log server port> protocol tcp format splunk filter-blade-in CME
```

-  **Note** - In Multi-Domain Security Management environment, logs are displayed with respect to the environment, which means the domain's logs are displayed in the domain's console.

### Log description:

Category	Description
General events	CME general information such as service start/stop and configuration changes (MDS global level only).
Autoscale-Group related events	Cloud account information such as scale-in/out success or failure.
Autoprovision process events	Provisioning information such as add/remove gateway instance success or failure.

# Google Cloud Security Command Center (CSCC)

You can configure your CloudGuard Network Security instances to send Threat Prevention events to the Google Cloud Security Command Center (CSCC).


CSCC is Google's platform used to manage security risks.

After the configuration is finished, the Check Point Security Management Server assigns port 37227 to receive security events from the Security Gateways that it manages. It then sends the events to CSCC.

For more information, see the [GCP CSCC documentation](#).

## Prerequisites

- Latest version of CME installed on the Security Management Server.
- Supports only the Security Management Server and Security Management Server High Availability. There is **no** support for Multi-Domain Servers.

 **Note** - The Security Management Server must have outbound internet connectivity to send Google Cloud Security Command Center (CSCC) APIs.

# Configuring CSCC on the Google Cloud Platform (GCP)

## Step: 1 Create a Service Account

A service account is a non-human user that needs to authenticate and give access to data in Google's APIs link.

### To create a service account:

1. From your Google projects, log in to your Google account > go to **IAM & admin > Service Accounts**.
2. Click **Create Service Account**.
3. Select a name for the service account > click **Create**.
4. Click **Edit > Create Key**.  
Create a private key in JSON format, and keep it.
5. In the **IAM** field, add this role to your service account:  
**Compute Viewer**
6. Click **Save**.
7. Log in to your GCP organization.
8. In the **IAM** field, add these roles to the service account:  
**Security Center Findings Editor**
9. Click **Save**.

**Step 2: Select CloudGuard IaaS as a Security Source:**

Use these steps to allow CloudGuard Network to publish relevant findings to your GCP account:

1. Log in to your organization > in the **Security** field, go to **Security Command Center**
2. Click **Add Security Source**.
3. Select **Check Point CloudGuard Network Integration for Cloud SCC**.
4. To register, click **Visit Check Point Software Technologies site**.
5. Select the GCP Service Account connected to the GCP project created in "[Step: 1 Create a Service Account](#)" on the previous page.
6. Copy the **Source ID** value. This value is for the configuration on CloudGuard Network.

## Configuring CloudGuard Network to Send Events to CSCC

Use these steps to configure the Check Point Security Management Server to send findings to your Google CSCC account.

**Procedure**

1. Install the latest CME version. See "[Installing and Updating CME](#)" on page 17.
2. Configure the CME service on the Security Management Server. See "[CME Structure and Configurations](#)" on page 18.
3. Transfer the JSON file of the service account (created in "[Step: 1 Create a Service Account](#)" on the previous page) to a directory on the Security Management Server.
4. Connect to the command line on the Security Management Server.
5. Log in to the Expert mode.
6. Launch the CME menu:

```
cme_menu
```

7. Select the **Cloud Security Control Center (CSCC)** section:
  - a. From the CME menu main page, select **GCP**.
  - b. From the **GCP** Configuration tab, select **Cloud Security Command Center (CSCC)**.
8. Enable the **Cloud Security Control Center (CSCC)** feature:

- a. Select **Configure CSCC for CloudGuard IaaS**.
- b. Enter the requested parameters.
- c. **Optional:** Decide if to enable the feature immediately, or not.

### Parameters

Parameter	Value	Description
organization-id	1111s	The organization number that allows events to be sent to CSCC. For more information, see <a href="#">Creating and managing organizations</a> .
project-id	My-project	The name of the project that you need to allow CSCC. For more information, see <a href="#">Locate the Project ID</a> .
source-id	123456	The source ID that is assigned to CloudGuard IaaS. This value must be copied from <b>Select CloudGuard Network as a security source</b> step.
service-account-key-path	"/home/admin/CSCC/s-a-key.json"	Parameter received in the GCP Configuration, (Step 1) - It allows CloudGuard IaaS to extract applicable security information from your instances.

## Enabling CSCC on the Security Management Server

You can activate CSCC feature only after the configuration is complete.

### Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:

```
cme_menu
```

4. Select **Cloud Security Control Center (CSCC)**.
  - a. On the CME menu home page, select **GCP**.
  - b. In the **GCP** Configuration tab, select **Cloud Security Control Center (CSCC)**.
5. Activate **Cloud Security Control Center (CSCC)** > select **Enable CSCC**.

## Disabling CSCC on the Security Management Server

If you disable the feature it stops the Security Management Server from sending logs to GCP.

### Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:

```
cme_menu
```

4. Select the **Cloud Security Control Center (CSCC)** section.
  - a. On the CME menu home page, select **GCP**.
  - b. In the **GCP** Configuration tab, select **Cloud Security Control Center (CSCC)**.
5. Select **Disable CSCC**.

## Viewing the CSCC Status

You can see the status of CSCC on the Security Management Server.

### Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:

```
cme_menu
```

4. Select the **Cloud Security Control Center (CSCC)** section.
  - a. On the CME menu home page, select **GCP**.
  - b. In the **GCP Configuration** tab, select **Cloud Security Control Center (CSCC)**.
5. Click **Cloud Security Control Center (CSCC)** > select **Display CSCC**.

## Configuring Debug Mode

When Debug mode is activated, then detailed logs of the CME internal state are generated and saved to a file.



**Note** - The Debug mode is disabled by default.

### Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:

```
cme_menu
```

4. Select the **Cloud Security Control Center (CSCC)** section.
  - a. On the CME menu home page, select **GCP**.
  - b. On the **GCP Configuration** tab, select **Cloud Security Control Center (CSCC)**.
5. Select **CSCCDebug Mode Configuration**.
  - To activate debug mode, select **Enable CSCC Mode Configuration**.
  - To stop debug mode, select **Disable CSCC Mode Configuration**.



# Additional Information about CloudGuard Network in CSCC

CloudGuard IaaS sends security events reported by these Software Blades:

- IPS
- Anti-Bot
- Anti-Virus
- Email Security and Anti-Spam

The Software Blade is displayed in the **Category** field.

Use these options to see more information:

- External URL link that opens the related log in smart view.
- **Source Properties** tab.

## Log Exporter

As part of the configuration to send security events, the Log Exporter feature is used.

A new Log Exporter instance is added and monitored by the `cpwd` with the name:  
`EXPORTER.CME_LOG_REPORTER`

For more information about the Log Exporter, see [sk122323](#).

# Limitations

- This feature is for Check Point Security Management Server versions R80.40 and higher.
- Multi-Domain Servers are not supported.
- These scenarios are not supported:
  - Two or more GCP Instances with the same private IP addresses in the same project.  
In this case, one of the instances is displayed in the CSCC Finding.
  - On-Premises appliances with a source IP the same as the IP address of an instance in the configured GCP project.  
In this case, the resource name of the GCP instance is displayed in the **Findings**.
- GCP Instance information is updated each 30 minutes.
- Only compute instances are supported.
- Only active states are reported.
- The feature does not work with manual modifications.  
All the modifications must be done with the `cme_menu`.
- For CME limitations, see [sk157492](#).
- For Log Exporter limitations, see [sk122323](#).

# AWS Security Hub


You can configure your Check Point Security Management Servers to send Threat Prevention events to the AWS Security Hub.

The AWS Security Hub service gives you a comprehensive view of your security alerts and security posture across your AWS accounts.

For more information, see the [AWS Security Hub documentation](#).

## Prerequisites

- This feature is for Check Point Security Management Server version R80.30 with Jumbo Hotfix Accumulator 226 and higher.
- CME installed on the Security Management Server with support for AWS Security Hub, see [sk157492](#).
- Supports only the Security Management Server (or Security Management Server High Availability) with Log Server. There is no support for Multi-Domain Security Management Servers or for a dedicated Log Server.

 **Note** - To use the AWS Security Hub APIs, the Security Management Server must have outbound internet connectivity.

# Subscribing to the Check Point CloudGuard Network in AWS Security Hub

## Step 1: Configure the Integration

1. Enable Security Hub service in your AWS account and region.
2. Click **Integrations**.
3. Search for: "check point"
4. Select "**Check Point CloudGuard IaaS**".
5. Click **Accept findings**.

## Step 2: Configure the IAM Roles

For Check Point Security Management Server to send security logs to the AWS Security Hub service, it is necessary to attach the appropriate permissions to the IAM role attached to the instance profile, or the IAM role of the user credentials.

- For Security Management Server in AWS - If you want to use the IAM role profile of the management as credentials:

In the IAM policy of the IAM role attached to the Security Management Server, add a statement to **allow** action `securityhub:BatchImportFindings` to **any** resource.

- For On-Premises Security Management Server - Use the user's **Access&Secret** key as credentials:

In the user's IAM policy, add a statement to **allow** action `securityhub:BatchImportFindings` to **any** resource.

# Configuring the Check Point Security Management Server to Send Events to the AWS Security Hub

Use these steps to configure the Check Point Security Management Server to send findings to your AWS Security Hub account.

## Procedure

1. Install the latest CME version. See ["Installing and Updating CME" on page 17](#).
2. Connect to the command line on the Security Management Server.
3. Log in to the Expert mode.
4. Launch the CME menu:

```
cme_menu
```

5. Select the Security Hub section:
  - a. From the CME menu main page, select **AWS**.
  - b. From the AWS Configuration tab, select **Security Hub**.
6. Configure the Security Hub feature:

- a. Select **Configure Security Hub**.
- b. Enter the requested parameters:

Parameter	Example Value	Description
<code>account-id</code>	123456789123	A 12-digit number that uniquely identifies your AWS account.
<code>credentials</code>	IAM	One of these: <ul style="list-style-type: none"> <li>▪ IAM - to use the IAM role profile.</li> <li>▪ Path to a text file that contains the AWS credentials in this format:               <div style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>AWSAccessKeyId=&lt;AWS-ACCESS-KEY&gt; AWSecretKey=&lt;AWS-SECRET-KEY&gt;</pre> </div> </li> </ul>
<code>region</code>	eu-west-1	The region name to which you want to send security hub findings.

- c. **Optional:** Decide if to enable this feature immediately.

# Enabling Security Hub on the Security Management Server

You can activate the Security Hub feature only after the configuration is complete.

## Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:

```
cme_menu
```

4. Select the **Security Hub** section:
  - a. On the CME menu home page, select **AWS**.
  - b. In the AWS Configuration tab, select **Security Hub**.
5. Activate the **Security Hub** > select **Enable Security Hub**.

After the Security Hub is configured and enabled on the Security Management Server, it is possible to make sure that the status shows "**Security Hub Service is currently enabled and sending logs to AWS**". See "[Displaying the Security Hub Integration Status](#)" on the next page.

# Disabling Security Hub on the Security Management Server

If you disable the feature, it stops the Security Management Server from sending logs to AWS Security Hub service.

## Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:

```
cme_menu
```

4. Select the **Security Hub** section:
  - a. On the CME menu home page, select **AWS**.
  - b. In the AWS Configuration tab, select **Security Hub**.
5. Disable **Security Hub** > select **Disable Security Hub**.

# Displaying the Security Hub Integration Status

You can see the status of Security Hub integration on the Security Management Server.

## Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:


```
cme_menu
```

4. Select the **Security Hub** section:
  - a. On the CME menu home page, select **AWS**.
  - b. In the AWS Configuration tab, select **Security Hub**.
5. To display the Security Hub Status, select **Security Hub Status**.



# Configuring Debug Mode

When Debug mode is activated, detailed logs of the Security Hub internal state are generated and saved to a file.

 **Note** - The Debug mode is disabled by default.

## Procedure

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:

```
cme_menu
```

4. Select the **Security Hub** section:
  - a. On the CME menu home page, select **AWS**.
  - b. In the AWS Configuration tab, select **Security Hub**.
5. Select **Configure Security Hub Debug Mode**.
  - To activate debug mode, select **Enable Security Hub debug mode**.
  - To stop debug mode, select **Disable Security Hub debug mode**.

# Additional Information about CloudGuard Network in Security Hub

Only logs from these Software Blades and features are sent to AWS Security Hub:

- IPS
- Anti-Bot
- Anti-Virus
- Threat Emulation
- Threat Extraction
- MTA

For more information about **Finding**, select the **Finding ID** and see **ProductFields**.



## Notes:

- **GeneratorId** represents the Security Management Server's host name.
- **CreatedAt** time is concurrent to the host time.
- To filter in AWS, use: **Product name is "CloudGuard Network"** to see all Check Point CloudGuard Network findings.
- For Security Management Server High Availability:
  - The configuration is synched between the *Active* and *Standby* servers.
  - After failover, enable the Security Hub feature in the **Active** Security Management Server.

## Accessing Security Hub Logs for Troubleshooting

These are the log files on the Management Server:

```
/var/log/CPcme/cme_log_reporter.log*
```

## Log Exporter

As part of the configuration to send security events, the Log Exporter feature is used.

A new Log Exporter instance is added and monitored by the `cpwd` with the name:

```
EXPORTER.CME_LOG_REPORTER
```

For more information about the Log Exporter, see [sk122323](#).

# Limitations

- Multi-Domain Security Management Servers or dedicated Log Servers are not supported.
- Only *Active* states are reported.
- The feature does not work with manual modifications. Use the "`cme_menu`" command for all modifications.
- AWS limitations:
  - The maximum allowed size for a **Finding** is 240 kilobytes.  
A Finding larger than 240 kilobytes is dropped.
  - The *Findings* are uploaded to AWS in bulks.  
A bulk is up to 100 *Findings*.
  - AWS limits the **ProductFields** to 50 elements only.  
To view the full log, use SmartConsole.
- For CME limitations, see [sk157492](#).
- For Log Exporter limitations, see [sk122323](#).

# Repository Gateway Script

In CME API v1.1, you can add a repository script to your configuration template that runs on the Security Gateways after the policy installation.

1. Use the [add-repository-script management API](#) to add the script to the script repository on the Management Server.

For example:

```
url: POST https://{managementIP}/web_api/v1.9/add-
repository-script
body: {"name": "create_route", "script-body": "#!/bin/bash
clish -c lock database override clish -c set static-route
10.24.2.0/32 nexthop gateway address 10.24.0.0 on clish -c
save config"}
```

**Note** - For Multi-Domain Security Management server, add the script for each Domain.

You can run the API call using the `mgmt_cli` tool, Web Services, SmartConsole CLI, or Gaia CLI.

2. Publish the session with the [publish management API](#).
3. After the script is successfully added to the script repository on the Management Server, you can add the repository script to your template. For more information, see [CME API SwaggerHub documentation](#).

For example:

```
url: PUT https://{managementIP}/web_api/v1.8/cme-
api/v1.1/gwConfigurations/<azure/gcp/aws>/<template-name>
body: "repository_gateway_scripts": [{"name": "create_route"}]
```

Script with parameters:

```
url: PUT https://{managementIP}/web_api/v1.8/cme-
api/v1.1/gwConfigurations/<azure/gcp/aws>/<template-name>
body: "repository_gateway_scripts": [{"name": "repo_script",
"parameters": "param1 param2"}]
```

**Note** - For CME API in Postman, you can use this [Postman Collection](#).

# Azure Virtual WAN

You can configure your NVA Gateways in the Security Management Server with CME.

For more information, see the [Azure Virtual WAN Deployment Guide](#) > Deploying new CloudGuard Network Security NVA.

## Automatically configure the NVA

### Requirements:

- A regular Security Management server (Not Smart-1 Cloud) or Multi-Domain Security Management Server with CME Take 261 and higher, with a valid license.
- CME Take 240 and higher installed on the Security Management server.
- Make sure you have a service principal with reader permission for the NVA's Managed Resource Group.

### Procedure:

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Run the command:

```
cme_menu
```

4. On the Menu select **Azure (1) > vWAN (2) > Configure NVA gateways on management server (1)**
5. Enter the requested parameters.

You can see logs in the file: `/var/log/CPcme/cme_menu.log`.

6. After you enter the parameters, the script starts to run. Wait for the script to complete.

### To run the script manually:

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Run the command:

```
python3 /opt/CPCme/features/vWAN/vWAN_automatic_script.py
"tenant="<Active-Directory-Tenant-ID>" "client_id="<Client-
ID>" "client_secret="<Client-Secret>" "subscription="<Azure-
Subscription>" "managed_app_resource_group_name="<Managed-App-
Resource-Group-Name>" "nva_name="<NVA-name>" "sic_key="<SIC-
key>" "policy="<Policy-Name>" "atp="<True/False>"
```

#### For example:

```
python3 /opt/CPCme/features/vWAN/vWAN_automatic_script.py
"tenant="7113cebb-911c-4122-aa5c-34db449380f7" "client_
id="82fb1445-f40e-46dc-9cd3-c065e14f132b" "client_
secret="xxx" "subscription="98e34f37-ece4-4cdc-97dc-
44a074f84aff" "managed_app_resource_group_name="mrg-vwan-
managed-app-12340424143321" "nva_nam="nvaGw" "sic_
key="SIC123456" "policy="Standard"
```

#### 4. Wait for the script to complete.

#### Parameters for NVA configuration:

Parameter Name	Default Value	Description
tenant	TENANT ID	The Azure Active Directory tenant ID.
client_id	CLIENT ID	The service principal's client ID value.
client_secret	CLIENT SECRET	The service principal's client secret value.
subscription	SUBSCRIPTION ID	The Azure subscription ID.
managed_app_resource_group_name	MANAGED APP RESOURCE GROUP NAME	The managed app resource group name. Go to your Virtual WAN resource group > Enter the managed application resource > In the overview section copy the "Managed resource group" value.
nva_name	NVA NAME	NVA (Network virtual appliance) name. Go to your Virtual WAN resource group > Enter the virtual WAN resource > Enter the Hub > Enter Network Virtual Appliance > Copy Checkpoint's NVA name.
sic_key	SIC KEY	SIC key to the security management server.
policy	POLICY NAME	The name of an existing security policy to install on the Security Gateways.

Parameter Name	Default Value	Description
atp	True	Optional. Available in CME Take 239 and higher. Enable the Autonomous Threat Prevention blades.

## Configure Ingress Rules for NVA

Ingress rules enable ingress traffic through the NVA, and with the ingress menu, you can configure ingress rules on the Security Management Server and on the Azure side.

The ingress menu creates NSG rules on the Azure side and NAT and access rules on the Security Management Server side to enable ingress traffic.

Each generated NAT rule is located in a dedicated NAT section called **Automatic Generated Rules: vWAN**, and each generated access rule is located in a dedicated inline rule called **vwan\_access\_layer (automatic)**.



**Important** - Do not change the NAT and access rules manually.

### Requirements

- A regular Security Management Server (Not Smart-1 Cloud) with a valid license.
- NVA instances configured in SmartConsole with the **{tags=vwan}** comment.
- NVA must have a minimum of one public IP address attached to it.
- CME Take 261 and higher installed on the Security Management Server.
- CME account (controller) with a service principle assigned to:
  - NVA's **Managed resource group** with **Reader** and **Network Contributor** roles.
  - Relevant public IP addresses (or their resource group) with **Reader** role.
- Terminal with a minimum of 150 characters in width and 40 characters in height (150 columns and 40 lines).
- Terminal emulator that supports line drawings. Confirmed terminals:
  - MobaXterm
  - Windows Command Line
  - Windows Terminal
  - SecureCRT
  - Putty (Need to enable VT100 line drawing support)

### Procedure:

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Run the command: `cme_menu`
4. On the menu, select **Azure (1) > vWAN (2) > Configure Ingress Rules (Preview) (5)**.
5. Enter the requested parameters. After you enter the parameters, the ingress menu User Interface starts.

### Parameters for NVA configuration:

Parameter Name	Description
Account (CME controller)	The Azure account you use to connect to the cloud for data about NVAs.
Domain	The relevant domain name, only for a Multi-Domain Management server environment.
Policy Package	The policy package name to create the ingress NAT and Access rules in.
NVA	The NVA you configure with the ingress rules.

## Using the Ingress User Interface

The ingress menu starts after you provide the initial parameters.

In this menu, you can create or edit the ingress rules. Changes are published, and the relevant policy package is installed only when you press the **Publish** button.

Use the keyboard to navigate and control the menu. The mouse does not work on it.


### Controls:

- Use the **arrow keys** to navigate between the button and inputs. The relevant input/button is marked in yellow when you select it.
- Use the **Enter key** to select an element.
- When you select an input, its background changes to white, and you can edit it in this mode.  
  
(Some inputs accept certain characters; for example, IP inputs accept characters that are relevant for IP addresses).
- To exit the menu press **Ctrl + C**.

### To add a rule:

Select **Add Rule** > Enter the relevant details > Press **add**.




 **Note** - When you create a new rule, you must add or discard the rule before you can navigate to a different rule.

**To delete a rule:**

Select an existing rule > Press **Delete**.

**To edit a rule:**

Select an existing rule > Navigate to the desired input > Press **Enter** > make changes > Press **ESC** to deselect and save.

 **Note** - Invalid values are marked in red, and you can only deselect a rule once you fix the values.

**To publish the changes and rules:**

Press **Publish** to publish the changes. If there is an issue, it shows in the message box, and details are added to the logs.

Once the publishing process is completed successfully, press any key to exit the menu.

You can see logs in the file: `/var/log/CPcme/cme_menu.log`.

# Troubleshooting

For the most common troubleshooting issues, refer to [ATRG: CME \(Cloud Management Extension\) for CloudGuard](#).

## General troubleshooting guidelines

Run these commands on the Security Management Server or Multi-Domain Server (in the Expert mode) to test the CME service.

Command	Description
<code>service cme stop</code>	Stops the main CME service.
<code>service cme test</code>	Starts the test. Examines the output of this command to confirm that the setup works properly.
<code>service cme start</code>	Starts the main CME service (if it was stopped before the test).

- Make sure that the clock on the Security Management Server is set correctly.

The best way to set the clock is with the NTP.

You need a synchronized clock to make API calls into a cloud environment.

- Review logs are created by the CME on the Management Server:

```
/var/log/CPCme/cme.log*
```

- To enable or disable **Debug** mode:

- Connect to the command line on the Security Management Server.
- Log in to the Expert mode.
- Launch the CME menu:

```
cme_menu
```

- Navigate to **Debug Mode**.
- Select **Enable Debug mode**.



**Note** - The Debug mode significantly increases the number of logs messages written to the CME log files.

## CME Log Collector

When contacting [Check Point Support](#), collect the CME files using CME Log Collector (supported in CME Take 155 and higher).

CME Log Collector is a utility that collects CME important files into a single TGZ file.

This file allows analyzing customer setups from a remote location.

To use it:

1. Connect to the command line on the Security Management Server.
2. Log in to the Expert mode.
3. Launch the CME menu:

```
cme_menu
```

4. Navigate to **Debug Mode**.
5. Select **CME Log Collecting**.
6. Select a path for the file

**Best Practice** - We recommend to enable CME debug mode for a few CME cycles before collecting CME files.

# Limitations

Refer to [sk157492](#) for an up-to-date list of CME limitations.