



QUANTUM

23 April 2024

# QUANTUM MAESTRO

R81.20

Administration Guide



# Check Point Copyright Notice

© 2022 - 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 R81.20 Quantum Maestro Administration Guide

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



## Latest Version of this Document in English

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



## Feedback

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

## Revision History

Date	Description
11 February 2024	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Maestro Fastforward" on page 335</a></li> </ul>
05 December	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Shared Uplink Ports" on page 134</a></li> </ul>
26 November 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Configuring the Port Settings" on page 79</a> - the Orchestrator ports support the speeds "25G" and "4x25G"</li> <li>▪ <a href="#">"Viewing the Port Settings" on page 86</a> - the Orchestrator ports support the speeds "25G" and "4x25G"</li> <li>▪ <a href="#">"Configuring the Number of Orchestrators on a Maestro Site" on page 60</a></li> <li>▪ <a href="#">"Viewing the Number of Orchestrators on a Maestro Site" on page 60</a></li> <li>▪ <a href="#">"Installing a Hotfix Package on Orchestrators" on page 433</a> - CPUSE online installation is not supported</li> <li>▪ <a href="#">"Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device" on page 545</a></li> </ul> Removed: <ul style="list-style-type: none"> <li>▪ Performance Hogs (asg_perf_hogs) - these tests are part of the HCP tool (<a href="#">sk171436</a>)</li> </ul>
02 October 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Troubleshooting" on page 529</a></li> </ul>
14 September 2023	Updated: <p>(added clarifications in the Important Notes for Dual Site)</p> <ul style="list-style-type: none"> <li>▪ <a href="#">"Upgrading Maestro Environment - Zero Downtime" on page 453</a></li> <li>▪ <a href="#">"Upgrading Maestro Environment - Minimum Downtime" on page 480</a></li> </ul>
24 July 2023	Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Shared Uplink Ports" on page 134</a></li> </ul>
13 July 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Monitoring System and Component Status (asg monitor)" on page 265</a></li> <li>▪ <a href="#">"Showing Hardware State (asg stat)" on page 255</a></li> </ul>

Date	Description
01 May 2023	Removed: <ul style="list-style-type: none"> <li>▪ "Working with Session Control (asg_session_control)" - this command is not supported</li> </ul>
07 April 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Upgrading Maestro Environment - Zero Downtime" on page 453</a> Added a sub-step to install the Recommended Take of the R81.20 Quantum Maestro Orchestrator</li> <li>▪ <a href="#">"Upgrading Maestro Environment - Minimum Downtime" on page 480</a> Added a sub-step to install the Recommended Take of the R81.20 Quantum Maestro Orchestrator</li> <li>▪ <a href="#">"Collecting System Diagnostics (smo verifiers)" on page 280</a></li> </ul> Added: <ul style="list-style-type: none"> <li>▪ <a href="#">"Collecting System Information" on page 529</a></li> </ul> Removed: <ul style="list-style-type: none"> <li>▪ "Collecting System Information (asg_info)" - this command was deprecated in R81.20</li> </ul>
19 April 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Step 5 - Special Configuration Scenarios" on page 108</a></li> </ul>
07 April 2023	Updated the instructions about disabling and enabling the SMO Image Cloning: <ul style="list-style-type: none"> <li>▪ <a href="#">"Configuring Security Groups in Gaia Portal" on page 44</a></li> <li>▪ <a href="#">"Configuring Security Groups in Gaia Clish" on page 57</a></li> <li>▪ <a href="#">"Installing and Uninstalling a Hotfix on Security Group Members" on page 435</a></li> <li>▪ <a href="#">"Upgrading Maestro Environment - Zero Downtime" on page 453</a></li> <li>▪ <a href="#">"Upgrading Maestro Environment - Minimum Downtime" on page 480</a></li> <li>▪ <a href="#">"Rolling Back a Failed Upgrade of a Security Group - After Partial Upgrade" on page 510</a></li> <li>▪ <a href="#">"Rolling Back a Failed Upgrade of a Security Group - Zero Downtime" on page 513</a></li> <li>▪ <a href="#">"Rolling Back a Failed Upgrade of a Security Group - Minimum Downtime" on page 521</a></li> </ul>
04 April 2023	Updated: <ul style="list-style-type: none"> <li>▪ <a href="#">"Multi-blade Traffic Capture (tcpdump)" on page 220</a></li> </ul>

Date	Description
07 March 2023	Removed: <ul style="list-style-type: none"> <li>▪ Information about the "<code>asg_bond -v</code>" command because it is not supported</li> </ul>
05 March 2023	Updated: <ul style="list-style-type: none"> <li>▪ <i>"Introduction" on page 17</i> - added a link to <a href="#">sk180461 - License for Maestro setup - R81.20 new features</a></li> </ul>
02 March 2023	Removed: <ul style="list-style-type: none"> <li>▪ The chapter "IP Block and URL Block Features" - these features are not supported</li> </ul>
28 February 2023	Updated: <ul style="list-style-type: none"> <li>▪ <i>"Maestro Fastforward" on page 335</i></li> </ul>
02 February 2023	Updated: <ul style="list-style-type: none"> <li>▪ <i>"Policy Management on Security Group Members" on page 27</i></li> </ul>
24 January 2023	Updated: <ul style="list-style-type: none"> <li>▪ <i>"Maestro Fastforward" on page 335</i></li> </ul>
16 January 2023	Updated: <ul style="list-style-type: none"> <li>▪ <i>"Workflow for Configuring Security Groups" on page 38</i></li> </ul>
27 December 2022	Updated: <ul style="list-style-type: none"> <li>▪ <i>"Maestro Fastforward" on page 335</i></li> </ul>
18 December 2022	Updated: <ul style="list-style-type: none"> <li>▪ <i>"General Diagnostic in Security Groups" on page 530</i></li> </ul>
15 December 2022	Updated: <ul style="list-style-type: none"> <li>▪ <i>"General Diagnostic in Security Groups" on page 530</i></li> <li>▪ <i>"Packet Drop Monitoring (<code>drop_monitor</code>)" on page 250</i></li> </ul>

Date	Description
05 December 2022	<p>Added:</p> <ul style="list-style-type: none"><li>▪ <a href="#">"Rolling Back a Failed Upgrade of a Security Group - Zero Downtime" on page 513</a></li></ul> <p>Updated:</p> <ul style="list-style-type: none"><li>▪ <a href="#">"Upgrading Maestro Environment - Zero Downtime" on page 453</a></li><li>▪ <a href="#">"Maestro Auto-Scaling" on page 325</a></li></ul>
20 November 2022	First release of this document

# Table of Contents

---

<b>Introduction</b> .....	<b>17</b>
Important Links .....	17
<b>Getting Started</b> .....	<b>18</b>
<b>Security Group Concepts</b> .....	<b>19</b>
Single Management Object (SMO) and Policies .....	19
Single Management Object .....	19
Installing and Uninstalling Policies .....	22
Working with Policies (asg policy) .....	23
Policy Management on Security Group Members .....	27
Synchronizing Policy and Configuration Between Security Group Members .....	28
Understanding the Configuration File List .....	29
MAC Addresses and Bit Conventions .....	31
MAC Address Resolver (asg_mac_resolver) .....	34
<b>Configuring Security Groups</b> .....	<b>35</b>
General Workflow .....	35
Step 1 - Configuration Procedure .....	38
Workflow for Configuring Security Groups .....	38
Summary of Configuration Options .....	40
Configuring Security Groups in Gaia Portal .....	44
Configuring Security Groups in Gaia Clish .....	57
Step 2 - Configuring Gaia Settings of a Security Group .....	92
Step 3 - Configuration in SmartConsole .....	94
Step 4 - License Installation .....	104
Step 5 - Special Configuration Scenarios .....	108
Configuring Weights for Security Group Members .....	108
Introduction .....	108
Limitations .....	108

---



---

Calculating the Security Group Member Weight .....	109
Configuring the Security Group Member Weights .....	110
Monitoring the Security Group Member Weights .....	111
Best Practices .....	112
Configuring Bond Interface on the Management Ports .....	113
Configuring Bond Interface on Uplink Ports .....	117
Configuring VLAN Interfaces on top of a Bond Interface on Uplink Ports .....	120
Procedure .....	120
Example .....	125
Configuring VLAN Interfaces on Uplink Ports .....	129
Introduction .....	129
Viewing VLAN Interfaces on Uplink Ports in Gaia Portal .....	130
Viewing VLAN Interfaces on Uplink Ports in Gaia Clish .....	131
Configuring More Than 4000 VLAN Interfaces on Orchestrators .....	132
Shared Uplink Ports .....	134
Prerequisites .....	134
Known Limitations .....	134
Requirements for LACP bond that contains shared interfaces .....	134
Configuration .....	135
Configuring an LACP bond that contains shared uplink interfaces .....	135
LACP bond verification .....	137
Removing subordinate interfaces from LACP bonds .....	137
Removing an LACP bond that contains shared uplink interfaces from a Security Group .....	139
<b>Managing Security Groups .....</b>	<b>140</b>
Connecting to a Specific Security Group Member (member) .....	140
Global Commands .....	144
Working with Global Commands .....	144
Check Point Global Commands .....	146
General Global Commands .....	149

---

---

Global Operating System Commands .....	157
Backing Up and Restoring Gaia Configuration .....	163
Working with Security Group Gaia gClish Configuration (asg_config) .....	164
Configuring Security Group Members (asg_blade_config) .....	166
Working with the Distribution Mode .....	168
Background .....	168
Automatic Distribution Configuration (Auto-Topology) .....	169
Manual Distribution Configuration (Manual-General) .....	170
Setting and Showing the Distribution Configuration (set distribution configuration) ...	171
Configuring the Interface Distribution Mode (set distribution interface) .....	173
Showing Distribution Status (show distribution status) .....	175
Running a Verification Test (show distribution verification) .....	177
Configuring the Layer 4 Distribution Mode and Masks (set distribution l4-mode) .....	178
Configuring the Cluster State (g_clusterXL_admin) .....	180
Configuring a Unique MAC Identifier (asg_unique_mac_utility) .....	182
Background .....	182
Configuring the Unique MAC Identifier Manually .....	183
Options of the Unique MAC Identifier Utility .....	183
Working with the ARP Table (asg_arp) .....	185
The 'asg_arp' Command .....	185
Example Default Output .....	186
Example Verbose Output .....	187
Example Output for Verifying MAC Addresses .....	187
Verifying ARP Entries .....	187
Example Legacy Output .....	188
Working with the GARP Chunk Mechanism .....	189
Description .....	189
Configuration .....	190
Verification .....	191
NAT and the Correction Layer on a VSX Gateway .....	192

---

---

NAT and the Correction Layer on a Security Gateway .....	193
IPS Management During a Cluster Failover .....	194
<b>IPv6 Neighbor Discovery .....</b>	<b>195</b>
<b>Logging and Monitoring .....</b>	<b>196</b>
CPView .....	196
Overview of CPView .....	196
CPView User Interface .....	196
Using CPView .....	197
Network Monitoring .....	198
Working with Interface Status (asg if) .....	198
Global View of All Interfaces (show interfaces) .....	201
Monitoring Traffic (asg_ifconfig) .....	202
Monitoring Multicast Traffic .....	209
Showing Multicast Routing (asg_mrout) .....	209
Showing PIM Information (asg_pim) .....	212
Showing IGMP Information (asg_igmp) .....	215
Monitoring VPN Tunnels .....	218
SmartConsole .....	218
SNMP .....	218
CLI Tools .....	218
Traceroute (asg_tracert) .....	219
Multi-blade Traffic Capture (tcpdump) .....	220
Monitoring Management Interfaces Link State .....	223
Performance Monitoring and Control .....	225
Monitoring Performance (asg perf) .....	225
Setting Port Priority .....	241
Searching for a Connection (asg search) .....	242
Description .....	242
Searching in the Non-Interactive Mode .....	242
Searching in the Interactive Mode .....	246

---

---

Showing the Number of Firewall and SecureXL Connections (asg_conns) .....	248
Packet Drop Monitoring (drop_monitor) .....	250
Hardware Monitoring and Control .....	255
Showing Hardware State (asg stat) .....	255
Monitoring System and Component Status (asg monitor) .....	265
Configuring Alert Thresholds (set chassis alert_threshold) .....	268
Monitoring System Resources (asg resource) .....	271
Configuring Alerts for Security Group Member and Security Group Events (asg alert) .....	277
Collecting System Diagnostics (smo verifiers) .....	280
Diagnostic Tests .....	280
Showing the Tests .....	282
Showing the Last Run Diagnostic Tests .....	283
Running all Diagnostic Tests .....	284
Running Specific Diagnostic Tests .....	285
Collecting Diagnostic Information for a Report Specified Section .....	287
Error Types .....	288
Changing Compliance Thresholds .....	289
Changing the Default Test Behavior of the 'asg diag resource verifier' .....	289
Troubleshooting Failures .....	291
Alert Modes .....	295
Diagnostic Events .....	295
Important Notes .....	296
Known Limitations of the SMO Verifiers Test .....	300
System Monitoring .....	301
Showing System Serial Numbers (asg_serial_info) .....	301
Showing the Security Group Version (ver) .....	302
Showing System Messages (show smo log) .....	303
Configuring a Dedicated Logging Port .....	304
Log Server Distribution (asg_log_servers) .....	306

---

---

Viewing a Log File (asg log) .....	309
Monitoring Virtual Systems (cpha_vsx_util monitor) .....	312
Software Blades Update Verification (asg_swb_update_verifier) .....	313
Working with SNMP .....	316
Monitoring Quantum Maestro Orchestrators over SNMP .....	316
Enabling SNMP Monitoring on Quantum Maestro Orchestrators .....	316
Supported SNMP OIDs for Quantum Maestro Orchestrators .....	317
Supported SNMP Trap OIDs for Quantum Maestro Orchestrators .....	318
Monitoring Security Groups over SNMP .....	320
Enabling SNMP Monitoring of Security Groups .....	320
Supported SNMP OIDs for Security Groups .....	321
Supported SNMP Trap OIDs for Security Groups .....	321
SNMP Monitoring of Security Groups in VSX Mode .....	321
Common SNMP OIDs for Security Groups .....	322
<b>System Optimization .....</b>	<b>325</b>
Maestro Auto-Scaling .....	325
Overview .....	325
Prerequisites .....	325
Limitations .....	325
Terms .....	326
Configuration .....	326
Monitoring on Orchestrator .....	330
Troubleshooting .....	333
Maestro Fastforward .....	335
Introduction .....	335
How It Works .....	336
FAQ .....	336
Topologies .....	337
Configuration .....	337
Monitoring .....	344

---

---

Considerations for Administrators .....	346
Routing Mechanism .....	347
Policy Mechanism .....	347
Special Considerations .....	351
Known Limitations .....	354
Troubleshooting .....	357
Configuring Services to Synchronize After a Delay .....	360
Firewall Connections Table Size for VSX Gateway .....	363
Forwarding specific inbound-connections to the SMO (asg_excp_conf) .....	364
<b>Configuring Security Group High Availability .....</b>	<b>374</b>
Setting Security Group Weights (High Availability Factors) .....	374
Setting the Quality Grade Differential .....	376
<b>Configuring Identity Based Access Control and Threat Prevention .....</b>	<b>377</b>
<b>Deploying a Security Group in Monitor Mode .....</b>	<b>378</b>
Introduction to Monitor Mode .....	378
Example Topology for Monitor Mode .....	379
Supported Software Blades in Monitor Mode .....	380
Limitations in Monitor Mode .....	382
Configuring a Security Group in Gateway mode in Monitor Mode .....	383
Configuring a Security Group in VSX mode in Monitor Mode .....	394
Configuring Specific Software Blades for Monitor Mode .....	405
Configuring the Threat Prevention Software Blades for Monitor Mode .....	406
Configuring the Application Control and URL Filtering Software Blades for Monitor Mode .....	408
Configuring the Data Loss Prevention Software Blade for Monitor Mode .....	409
Configuring the Security Group in Monitor Mode Behind a Proxy Server .....	411
<b>Deploying a Security Group in Bridge Mode .....</b>	<b>412</b>
Introduction to Bridge Mode .....	412
Example Topology for Bridge Mode .....	413
Supported Software Blades in Bridge Mode .....	414

---

---

Limitations in Bridge Mode .....	416
Configuring a Security Group in Bridge Mode .....	417
Accept, or Drop Ethernet Frames with Specific Protocols .....	426
Routing and Bridge Interfaces .....	428
IPv6 Neighbor Discovery .....	429
Managing Ethernet Protocols .....	430
<b>Installing and Uninstalling a Hotfix .....</b>	<b>432</b>
Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators .....	432
Installing a Hotfix Package on Orchestrators .....	433
Uninstalling a Hotfix Package on Orchestrators .....	434
Deleting a Hotfix Package on Orchestrators .....	434
Installing and Uninstalling a Hotfix on Security Group Members .....	435
Installing a Hotfix Package on Security Group Members .....	436
Uninstalling a Hotfix Package on Security Group Members .....	446
<b>Upgrading Maestro to R81.20 .....</b>	<b>453</b>
Upgrading Maestro Environment - Zero Downtime .....	453
Upgrading Maestro Environment - Minimum Downtime .....	480
Rolling Back a Failed Upgrade of a Maestro Orchestrator .....	507
Rolling Back a Failed Upgrade of a Security Group - After Partial Upgrade .....	510
Rolling Back a Failed Upgrade of a Security Group - Zero Downtime .....	513
Rolling Back If Only Some of the Security Group Members Were Upgraded .....	513
Rolling Back the Whole Security Group .....	516
Rolling Back the Whole Security Group - With Downtime .....	519
Rolling Back a Failed Upgrade of a Security Group - Minimum Downtime .....	521
Rolling Back If Only Some of the Security Group Members Were Upgraded .....	521
Rolling Back the Whole Security Group - Zero Downtime .....	524
Rolling Back the Whole Security Group - With Downtime .....	527
<b>Troubleshooting .....</b>	<b>529</b>
Collecting System Information .....	529
General Diagnostic in Security Groups .....	530

---

---

Configuration Verifiers .....	534
MAC Verification (mac_verifier) .....	534
Layer 2 Bridge Verifier (asg_br_verifier, asg_brs_verifier) .....	536
Verifying VSX Gateway Configuration (asg_vsx_verify) .....	538
Log and Configuration Files .....	541
Installing the Gaia Operating System on a Quantum Maestro Orchestrator .....	544
Reset an Orchestrator to Factory Defaults .....	544
Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device .....	545
Replacing a Quantum Maestro Orchestrator .....	546
<b>Glossary .....</b>	<b>547</b>



# Introduction

Quantum Maestro Orchestrator is a scalable Network Security System built to secure the largest networks in the world by orchestrating multiple Check Point Security Appliances into a unified system.

The Quantum Maestro Orchestrator provides:

- Security of infinite scale
- Redundancy - Quantum Maestro Orchestrator automatically distributes traffic between the Security Appliances assigned to Security Groups
- Ability to connect more Security Appliances and use their resources easily in the existing Security Groups

## Important Links

For more information and the software, see the R81.20 Home Page: [sk177624](#).

- Read the Scalable Platforms Known Limitations in [sk148074](#).
- Read the R81.20 Known Limitations in [sk174965](#).
- To learn about the differences between different Scalable Platform versions, see [sk173183](#).
- Read [sk180461](#) for information about Maestro licensing features in R81.20.

# Getting Started

This Administration Guide describes:

- Security Group Concepts
- Configuration of Security Groups
- Optimization of Security Groups
- Upgrade of Security Groups and Orchestrators
- Troubleshooting

## Workflow:

1. Install the Quantum Maestro Orchestrators, the Security Appliances, and connect all cables.

Follow the [Quantum Maestro Getting Started Guide](#).

2. Get familiar with Security Group concepts:

See ["Security Group Concepts" on page 19](#).

3. Configure the required Security Groups.

See:

- ["Configuring Security Groups" on page 35](#).
- ["Managing Security Groups" on page 140](#)
- ["Deploying a Security Group in Monitor Mode" on page 378](#)
- ["Deploying a Security Group in Bridge Mode" on page 412](#)

4. Learn how to monitor your Security Groups:

See ["Logging and Monitoring" on page 196](#).

5. Learn how to optimize your Security Groups:

See ["System Optimization" on page 325](#).

6. Learn how to install Hotfixes on your Security Groups:

See ["Installing and Uninstalling a Hotfix" on page 432](#).

7. Learn how to troubleshoot your Security Groups:

See ["Troubleshooting" on page 529](#).

# Security Group Concepts

This section describes some of the Security Group concepts.

## Single Management Object (SMO) and Policies

*In This Section:*

---

Single Management Object .....	19
Installing and Uninstalling Policies .....	22
Working with Policies (asg policy) .....	23

---

### Single Management Object

Single Management Object (SMO) is a Check Point technology that manages the Security Group as one large Security Gateway with one management IP address.

One Security Group Member, the SMO Master, handles all management tasks, such as Security Gateway configuration, policy installation, remote connections, and logging

are handled. The SMO Master updates all other Security Group Members.

The Active Security Group Member with the lowest ID number is automatically assigned to be the SMO.

Use the "asg stat -i tasks" command to identify the SMO and see how tasks are distributed on the Security Group Members (see ["Showing Hardware State \(asg stat\)" on page 255](#)).

#### Example output in a Single Site configuration

The SMO task runs on the Security Group Member #1, on which you ran this command (see the string "(local)").

```
[Expert@HostName-ch0x-0x:0]# asg stat -i tasks
-----
| Task (Task ID)      |                               Chassis 1 |
-----
| SMO (0)           |                               1(local) |
| General (1)         |                               1(local) |
| LACP (2)            |                               1(local) |
| CH Monitor (3)     |                               1(local) |
| DR Manager (4)     |                               1(local) |
| UIPC (5)            |                               1(local) |
| Alert (6)           |                               1(local) |
-----
[Expert@HostName-ch0x-0x:0]#
```

## Example output in a Dual Site configuration

The SMO task runs on Site #2 - on the Security Group Member #3, on which you ran this command (see the string "(local)").

```
[Expert@HostName-ch0x-0x:0]# asg stat -i tasks
-----
| Task (Task ID)      |          Chassis 1          |          Chassis 2          |
-----
| SMO (0)           |                               |          3 (local)         |
| General (1)         |                2            |          3 (local)         |
| LACP (2)            |                2            |          3 (local)         |
| CH Monitor (3)     |                2            |          3 (local)         |
| DR Manager (4)     |                               |          3 (local)         |
| UIPC (5)            |                2            |          3 (local)         |
| Alert (6)           |                               |          3 (local)         |
-----

[Expert@HostName-ch0x-0x:0]#
[Expert@HostName-ch0x-0x:0]# member 2_4
Moving to member 2_4
... ..
[Expert@HostName-ch0x-0x:0]# asg stat -i tasks
-----
| Task (Task ID)      |          Chassis 1          |          Chassis 2          |
-----
| SMO (0)           |                               |                3           |
| General (1)         |                2            |                3           |
| LACP (2)            |                2            |                3           |
| CH Monitor (3)     |                2            |                3           |
| DR Manager (4)     |                               |                3           |
| UIPC (5)            |                2            |                3           |
| Alert (6)           |                               |                3           |
-----

[Expert@HostName-ch0x-0x:0]#
```

Example output from all Security Group Members (in our example, there are two on each Site):

```
[Expert@HostName-ch0x-0x:0]# g_all asg stat -i tasks
```

```
1_01:
```

Task (Task ID)	Chassis 1	Chassis 2
<b>SMO</b> (0)	<b>1(local)</b>	
General (1)	1(local)	1
LACP (2)	1(local)	1
CH Monitor (3)	1(local)	1
DR Manager (4)	1(local)	
UIPC (5)	1(local)	1
Alert (6)	1(local)	

```
1_02:
```

Task (Task ID)	Chassis 1	Chassis 2
<b>SMO</b> (0)	1	
General (1)	1	1
LACP (2)	1	1
CH Monitor (3)	1	1
DR Manager (4)	1	
UIPC (5)	1	1
Alert (6)	1	

```
2_01:
```

Task (Task ID)	Chassis 1	Chassis 2
<b>SMO</b> (0)	1	
General (1)	1	1(local)
LACP (2)	1	1(local)
CH Monitor (3)	1	1(local)
DR Manager (4)	1	
UIPC (5)	1	1(local)
Alert (6)	1	

```
2_02:
```

Task (Task ID)	Chassis 1	Chassis 2
<b>SMO</b> (0)	1	
General (1)	1	1
LACP (2)	1	1
CH Monitor (3)	1	1
DR Manager (4)	1	
UIPC (5)	1	1
Alert (6)	1	

```
[Expert@HostName-ch0x-0x:0]#
```

# Installing and Uninstalling Policies


## Installing a Policy

To install a policy on the Security Group, click **Install Policy** in SmartConsole.

The policy installation process includes these steps:

1. The Management Server installs the policy on the SMO Master.
2. The SMO Master copies the policy to all Security Group Members in the Security Group.
3. Each Security Group Member in the Security Group installs the policy locally.

During the policy installation, each Security Group Member sends and receives policy status updates to and from the other Security Group Members in the Security Group. This is because the Security Group Members must install their policies in a synchronized manner.

 **Note** - When you create a Security Group, its Security Group Members enforce an initial policy that allows only the implied rules necessary for management.

## Uninstalling a Policy

**Note** - You cannot uninstall policies from a Security Group in SmartConsole.

Step	Instructions
1	Connect over a serial port to the SMO in the Security Group.
2	Log in to the Gaia gClish.
3	Uninstall the policy: <pre>asg policy unload</pre> See " <a href="#">Working with Policies (asg policy)</a> " on the next page.

## Working with Policies (asg policy)

### Description

Use the "asg policy" command in Gaia gClish or the Expert mode to perform policy-related actions.

### Syntax

```
asg policy -h
```


```
asg policy {verify | verify_amw} [-vs <VS IDs>] [-a] [-v]
```

```
asg policy unload [--disable_pnotes] [-a]
```

```
asg policy unload --ip_forward
```

- ★ **Best Practice** - Run these commands over a serial connection to Security Group Members in the Security Group.

## Parameters

Parameter	Description
-h	Shows the built-in help.
verify	Confirms that the correct policies are installed on all Security Group Members in the Security Group.
verify_amw	Confirms that the correct Anti-Malware policies are installed on all Security Group Members in the Security Group.
unload	Uninstalls the policy from all Security Group Members in the Security Group.
-vs <VS IDs>	<p>Applies to Virtual Systems as specified by the &lt;VS IDs&gt;. &lt;VS IDs&gt; can be:</p> <ul style="list-style-type: none"> <li>▪ No &lt;VS IDs&gt; specified (default) - Applies to the context of the current Virtual System</li> <li>▪ One Virtual System</li> <li>▪ A comma-separated list of Virtual Systems (for example, 1, 2, 4, 5)</li> <li>▪ A range of Virtual Systems (for example, 3-5)</li> <li>▪ all - Shows all Virtual Systems</li> </ul> <p>This parameter is only applicable in a VSX environment.</p>
-v	Shows detailed verification results for Security Group Members.
-a	Runs the verification on Security Group Members in both UP and DOWN states.
--disable_pnotes	<p>Security Group Members stay in the state "UP" without an installed policy.</p> <p> <b>Important</b> - If you omit this option, Security Group Members go into the DOWN state until the policy is installed again!</p>
--ip_forward	Enables IP forwarding.



## Examples

### Example 1 - Detailed verification results for Security Group Members

```
[Expert@HostName-ch0x-0x:0]# asg policy verify -v
+-----+
|Policy Verification|
+-----+-----+-----+-----+-----+
|SGM   |Policy Name      |Policy Date   |Policy Signature |Status  |
+-----+-----+-----+-----+-----+
|1_01  |Standard         |27Feb19 08:56 |e17c177f7        |Success|
+-----+-----+-----+-----+-----+
|1_02  |Standard         |27Feb19 08:56 |e17c177f7        |Success|
+-----+-----+-----+-----+-----+

+-----+
|Summary|
+-----+
|Policy Verification completed successfully|
+-----+
[Expert@HostName-ch0x-0x:0]#
```

### Example 2 - Detailed verification results for for each Virtual System on Security Group Members

```
[Expert@HostName-ch0x-0x:0]# asg policy verify -vs all -v
+-----+
|Policy Verification|
+-----+-----+-----+-----+-----+
|VS   |SGM   |Policy Name      |Policy Date   |Policy Signature |Status  |
+-----+-----+-----+-----+-----+
|0    |1_01  |Standard         |27Feb19 08:56 |996eee5e6        |Success|
|    |1_03  |Standard         |27Feb19 08:56 |996eee5e6        |Success|
|    |1_04  |Standard         |27Feb19 08:56 |996eee5e6        |Success|
|    |1_05  |Standard         |27Feb19 08:56 |996eee5e6        |Success|
|    |1_06  |Standard         |27Feb19 08:56 |996eee5e6        |Success|
|    |1_11  |Standard         |27Feb19 08:56 |996eee5e6        |Success|
|    |1_12  |Standard         |27Feb19 08:56 |996eee5e6        |Success|
+-----+-----+-----+-----+-----+
|1    |1_01  |Standard         |27Nov12 13:03 |836fa2ec1        |Success|
|    |1_03  |Standard         |27Nov12 13:03 |836fa2ec1        |Success|
|    |1_04  |Standard         |27Nov12 13:03 |836fa2ec1        |Success|
|    |1_05  |Standard         |27Nov12 13:03 |836fa2ec1        |Success|
|    |1_06  |Standard         |27Nov12 13:03 |836fa2ec1        |Success|
|    |1_11  |Standard         |27Nov12 13:03 |836fa2ec1        |Success|
|    |1_12  |Standard         |27Nov12 13:03 |836fa2ec1        |Success|
+-----+-----+-----+-----+-----+
|2    |1_01  |Standard         |27Feb19 08:56 |10eef9ced        |Success|
|    |1_03  |Standard         |27Feb19 08:56 |10eef9ced        |Success|
|    |1_04  |Standard         |27Feb19 08:56 |10eef9ced        |Success|
|    |1_05  |Standard         |27Feb19 08:56 |10eef9ced        |Success|
|    |1_06  |Standard         |27Feb19 08:56 |10eef9ced        |Success|
|    |1_11  |Standard         |27Feb19 08:56 |10eef9ced        |Success|
|    |1_12  |Standard         |27Feb19 08:56 |10eef9ced        |Success|
+-----+-----+-----+-----+-----+

+-----+
|Summary|
+-----+
|Policy Verification completed successfully|
+-----+
[Expert@HostName-ch0x-0x:0]#
```

**Example 3 - Uninstall of a Policy**

```
[Expert@HostName-ch0x-0x:0]# asg policy unload
You are about to perform unload policy on blades: all
All SGMs will be in DOWN state, beside local SGM. It is recommended to run the procedure
via serial connection

Are you sure? (Y - yes, any other key - no) y

Unload policy requires auditing
Enter your full name: John Doe
Enter reason for unload policy [Maintenance]:
WARNING: Unload policy on blades: all, User: John Doe, Reason: Maintenance
+-----+
|Unload policy          |
+-----+-----+
|SGM                    |Status          |
+-----+-----+
|1_3                    |Success        |
+-----+-----+
|1_2                    |Success        |
+-----+-----+
|1_1                    |Success        |
+-----+-----+
|2_3                    |Success        |
+-----+-----+
|2_2                    |Success        |
+-----+-----+
|2_1                    |Success        |
+-----+-----+

+-----+-----+
|Summary                |
+-----+-----+
|Unload policy completed successfully |
+-----+-----+
[Expert@HostName-ch0x-0x:0]#
```

# Policy Management on Security Group Members

## *In This Section:*

---

Synchronizing Policy and Configuration Between Security Group Members .....	28
Understanding the Configuration File List .....	29
MAC Addresses and Bit Conventions .....	31
MAC Address Resolver (asg_mac_resolver) .....	34

---

Because the Security Group works as one large Security Gateway, all Security Group Members are configured with the same policy.

When you install a policy from the Management Server, it first installs the policy on the SMO Security Group Member.

The SMO copies the policy and Security Group Member configuration to all Security Group Members in the state "UP".

When the Security Group Member enters the state "UP", it automatically gets the installed policy and configurations that are installed, from the SMO.

When there is only one Security Group Member in the state "UP", it is possible there is no SMO. Then, that Security Group Member uses its local policy and configuration.

If there are problems with the policy or configuration on the Security Group Member, you can manually copy the information from a different Security Group Member.

The Security Group Member configuration has these components:

- Firewall policy, which includes the Rule Base.
- Set of configuration files defined in the `/etc/xfer_file_list` file.

This file contains the location of all related configuration files.

It also defines the action to take if the copied file is different from the one on the local Security Group Member.

## Synchronizing Policy and Configuration Between Security Group Members


Use the "asg\_blade\_config pull\_config" command in Gaia gClish to synchronize the policies manually.

Optionally, it can configure files from a specified source Security Group Member to the target Security Group Member.

The target Security Group Member is the Security Group Member you use to run this command.

To synchronize Security Group Members manually:

Step	Instructions
1	Run in Gaia gClish: <pre>asg_blade_config pull_config</pre>
2	Do <b>one</b> of these: <ul style="list-style-type: none"> <li>▪ Reboot the <b>target</b> Security Group Member:               <pre>reboot -b &lt;Security Group Member ID&gt;</pre> </li> <li>▪ Start the Check Point services and remove the ClusterXL Critical Device "admin_down":               <pre>cpstart clusterXL_admin up</pre> </li> </ul>

 **Note** - You can run the "asg stat -i all\_sync\_ips" command in Gaia gClish to get a list of all synchronization IP addresses on the Security Group Member.

## Understanding the Configuration File List

The `/etc/xfer_file_list` file contains pointers to the related configuration files on the Security Group Member. Each record defines the path to a configuration file, followed by the action to take if the imported file is different from the local file. This table shows an example of the record structure.

Context	File name and path	Action
<code>global_context</code>	<code>\$FWDIR/boot/modules/fwkernel.conf</code>	<code>/bin/false</code>

The context field defines the type of configuration file:

- `global_context` - Security Gateway configuration file
- `all_vs_context` - Virtual Systems configuration file

The action field defines the action to take when the imported (copied) file is different than the local file:

- `/bin/true` - Reboot is **not** required
- `/bin/false` - Reboot **is** required
- String enclosed in double quotes - Name of a "callback script" that selects the applicable action.

**Example - Configuration file list**

```
[Expert@HostName-ch0x-0x:0]# g_cat /etc/xfer_file_list
#The Columns are:
#1) global_context or all_vs_context - VSX support.
#   It separates the files relevant to all VSs (all_vs_context) from those which are only
#   relevant for VS0 (global_context)
#   In a security gateway mode, there is no difference between the two values
#2) File location in the SMO - where to pull the files from
#3) Action to perform after the file is copied, if it's different.
#   The result of the operation determines if a reboot is needed after the operation - 1
#   for reboot, 0 for no reboot
#   Please Notice - /bin/false => reboot, /bin/true => don't reboot
#4) [Optional] A local path to copy the file to, needed if different from the source

global_context /opt/CPda/bin/policy.xml /bin/true
global_context /etc/upgrade_pkg-0.1-cp989000001.i386.rpm "rpm -U --force --nodeps
/etc/upgrade_pkg-0.1-cp989000001.i386.rpm"
global_context /etc/sysconfig/image.md5 "/usr/lib/smo/libclone.tcl --clone --rsip --xfer --
reboot"
global_context $PPKDIR/boot/modules/sim_aff.conf "sim affinityload"
global_context $PPKDIR/boot/modules/simkern.conf /bin/false
global_context $FWDIR/boot/boot.conf /bin/false
global_context $FWDIR/boot/modules/fwkern.conf /bin/false
all_vs_context $FWDIR/conf/fwauthd.conf /bin/false
all_vs_context $FWDIR/conf/discntd.if /bin/false
#global_context /var/opt/fw.boot/ha_boot.conf /bin/false
global_context /config/active /usr/bin/confd_clone /config/db/cloned_db
global_context /tmp/sms_rate_limit.tmp /bin/true
global_context /tmp/sms_history.tmp /bin/true
global_context /home/admin/.ssh/known_hosts /bin/true
global_context /etc/passwd /bin/true
global_context /etc/shadow /bin/true
... output is cut for brevity ...
global_context /etc/smodb.json "/usr/lib/smo/libclone_smodb.tcl clone_smodb_apply"
/tmp/smo_smodb.json
global_context $FWDIR/conf/prioq.conf /bin/false
global_context /web/templates/httpd-ssl.conf.templ /usr/scripts/generate_httpd-ssl_conf.sh
all_vs_context $FWDIR/conf/fwaccel_dos_rate_on_install /bin/false
all_vs_context $FWDIR/conf/fwaccel6_dos_rate_on_install /bin/false
global_context $FWDIR/database/sam_policy.db $SMODIR/scripts/compare_samp_db.tcl /tmp/sam_
policy.db.new
global_context $FWDIR/database/sam_policy.mng /bin/false
all_vs_context $FWDIR/conf/icap_client_blade_configuration.C /bin/true
global_context $CPDIR/conf/chassis_priority_db.C /bin/true
[Expert@HostName-ch0x-0x:0]#
```

## MAC Addresses and Bit Conventions

MAC addresses on the system are divided into these types - BMAC, VMAC, and SMAC:

### BMAC

A MAC address assigned to all interfaces with the naming convention "BPEthX".

This is unique for each Security Group Member.

It does not rely on the interface index number.

Bit convention for the BMAC type:

Bit range	Instructions
1	Distinguishes between VMAC and other MAC addresses. This is used to prevent possible collisions with VMAC space. Possible values are: <ul style="list-style-type: none"> <li>▪ 0 - BMAC or SMAC</li> <li>▪ 1 - VMAC</li> </ul>
2-8	Security Group Member ID (starting from 1). This is limited to 127.
9-13	Always zero.
14	Distinguishes between BMAC and SMAC addresses. This is used to prevent possible collisions with SMAC space. Possible values: <ul style="list-style-type: none"> <li>▪ 0 - BMAC</li> <li>▪ 1 - SMAC</li> </ul>
15-16	Absolute interface number. This is taken from the interface name. When the BPEthX format is used, X is the interface number. This is limited to four interfaces.

## VMAC

A MAC address assigned to all interfaces with the naming convention "ethX-YZ".

This is unique for each Site.

It does not rely on the interface index number.

Bit convention for the VMAC type:

Bit range	Instructions
1	Distinguishes between VMAC and other MAC addresses. This is used to prevent possible collisions with VMAC space. Possible values are: <ul style="list-style-type: none"><li>▪ 0 - BMAC or SMAC</li><li>▪ 1 - VMAC</li></ul>
2-3	Site ID. Limited to 2 Sites.
4-8	Switch number. Limited to 32 switches.
9-16	Port number. Limited to 256 for each switch.



**SMAC**

A MAC address assigned to Sync interfaces.

This is unique for each Security Group Member.

It does not rely on the interface index number.

Bit convention for the SMAC type:

Bit range	Instructions
1	Distinguishes between VMAC and other MAC addresses. This is used to prevent possible collisions with VMAC space. Possible values are: <ul style="list-style-type: none"> <li>▪ 0 - BMAC or SMAC</li> <li>▪ 1 - VMAC</li> </ul>
2-8	Security Group Member ID (starting from 1). This is limited to 127.
9-13	Always zero.
14	Distinguishes between BMAC and SMAC addresses. This is used to prevent possible collisions with SMAC space. Possible values: <ul style="list-style-type: none"> <li>▪ 0 - BMAC</li> <li>▪ 1 - SMAC</li> </ul>
15	Always zero.
16	Sync interface. Possible values are: <ul style="list-style-type: none"> <li>▪ 0 - Sync1</li> <li>▪ 1 - Sync2</li> </ul>

# MAC Address Resolver (asg\_mac\_resolver)

## Description

Use the "asg\_mac\_resolver" command in Gaia gClish or the Expert mode to make sure that all types of MAC addresses (BMAC, VMAC, and SMAC) are correct.

From the MAC address you provide, the "asg\_mac\_resolver" command determines the:

- MAC type
- Site ID
- Security Group Member ID
- Assigned interface

## Syntax

```
asg_mac_resolver <MAC address>
```

## Example

```
[Expert@HostName-ch0x-0x:0]# asg_mac_resolver 00:1C:7F:01:00:FE  
[00:1C:7F:01:00:FE, BMAC] [Chassis ID: 1] [SGM ID: 1] [Interface: BPEth0]  
[Expert@HostName-ch0x-0x:0]#
```



### Notes:

- The specified MAC Address comes from BPEth0 on Security Group Member #1 on the Site #1.
- 00:1C:7F:01:00:FE is the Magic MAC attribute, which is identified by "FE".
- The index length is 16 bits (2 Bytes) identified by 01:00 x x x x x x x x x x x x x x x.

# Configuring Security Groups


This section provides a workflow and step-by-step instructions for configuring Security Groups.

## General Workflow

### Notes:

- It is assumed that you already installed the Quantum Maestro Orchestrators, the Security Appliances, and connected all cables. See the [Quantum Maestro Getting Started Guide](#).
- When you create a new Security Group on a Maestro Orchestrator, it is not possible to configure the Gaia GRUB Password in the Security Group wizard on the Maestro Orchestrator.  
You can configure the Gaia GRUB Password only after you complete the Gaia First Time Configuration Wizard on the Security Group. See the [R81.20 Gaia Administration Guide](#) > Chapter "System Management" > Section "System Passwords".

### 1. Configure the applicable Security Groups on the Quantum Maestro Orchestrators

-  **Note** - Configure only one of the installed Quantum Maestro Orchestrators. The Quantum Maestro Orchestrators synchronize the configuration automatically with each other.

#### Each Security Group must contain:

- a. One or more Security Appliances.

**Note** - The Quantum Maestro Orchestrators automatically assign the corresponding Downlink ports.

- b. Applicable ports on the Quantum Maestro Orchestrators:




- A dedicated Management port, which connects the Security Group to the Management Server (for example, `eth1-Mgmt1`).
- Uplink ports, to which you connected the external traffic and internal traffic networks.


#### You can configure Security Groups in:

- Gaia Portal (see ["Configuring Security Groups in Gaia Portal" on page 44](#)).
- Gaia Clish (see ["Configuring Security Groups in Gaia Clish" on page 57](#)).

See ["Summary of Configuration Options" on page 40](#).


**Perform these steps:**

Step	Instructions
a	Create a new Security Group.
b	Add the Network Configuration to the Security Group.
c	Configure the First Time Wizard settings in the Security Group.  <b>Note</b> - This First Time Wizard configures only a limited number of settings.
d	Assign the available Security Appliances to the Security Group.  <b>Important:</b> <ul style="list-style-type: none"> <li>▪ You can assign only supported Security Appliances to the same Security Group - see <a href="#">sk162373</a>.</li> <li>▪ Security Appliances assigned to the Security Group automatically reboot after you apply the configuration.</li> </ul>  <b>Best Practice for Dual Site</b> - Assign the same number (as possible) of Security Appliances from each site to the Security Group. If a failover occurs between the sites, Security Appliances on the new Active site must be able to process all the traffic.
e	Assign the applicable Quantum Maestro Orchestrator ports to the Security Group (Uplink ports and a Management interface).

-  **Best Practice** - Create a Gaia Backup on the Quantum Maestro Orchestrators to save the configuration. For more information, see the [R81.20 Gaia Administration Guide](#) > Chapter *Maintenance* > Section *System Backup*.

**2. Configure the Gaia Operating System settings in the new Security Group**

See "[Step 2 - Configuring Gaia Settings of a Security Group](#)" on page 92.

-  **Best Practice** - Create a Gaia Backup on the Security Group to save the configuration. For more information, see the [R81.20 Gaia Administration Guide](#) > Chapter *Maintenance* > Section *System Backup*.

**3. Configure the settings in SmartConsole**

See "[Step 3 - Configuration in SmartConsole](#)" on page 94.

- For a Security Group in **Gateway** mode:
  - a. Create one Security Gateway object.
  - b. Configure the applicable Security Policy.
  - c. Install the Security Policy on the Security Gateway object.
- For a Security Group in **VSX** mode:
  - a. Create one VSX Gateway object.
  - b. Create the objects of Virtual Systems.
  - c. Configure the applicable Security Policies for the Virtual Systems.
  - d. Install the Security Policies on the Virtual Systems.

#### 4. Install licenses

See ["Step 4 - License Installation" on page 104](#).

#### 5. Make sure the traffic passes as expected

Initiate connections that must pass through this Security Group.

#### 6. Configure special settings, if required

See:

- ["Step 5 - Special Configuration Scenarios" on page 108](#)
- ["Configuring Security Group High Availability" on page 374](#)
- ["Managing Security Groups" on page 140](#)
- ["System Optimization" on page 325](#)
- ["Deploying a Security Group in Monitor Mode" on page 378](#)
- ["Deploying a Security Group in Bridge Mode" on page 412](#)

# Step 1 - Configuration Procedure

You can configure Security Groups on Quantum Maestro Orchestrators:

- In Gaia Portal (see ["Configuring Security Groups in Gaia Portal" on page 44](#))
- In Gaia Clish (see ["Configuring Security Groups in Gaia Clish" on page 57](#))

See ["Summary of Configuration Options" on page 40](#).





## Workflow for Configuring Security Groups


You can configure Security Groups on a Quantum Maestro Orchestrator:

- In Gaia Portal - see ["Configuring Security Groups in Gaia Portal" on page 44](#)
- In Gaia Clish - see ["Configuring Security Groups in Gaia Clish" on page 57](#)

See ["Summary of Configuration Options" on page 40](#).

**Workflow:**

Step	Instructions
1	<p>Create a new Security Group.</p> <p> <b>Note</b> - Configure only one of the installed Quantum Maestro Orchestrators. The Quantum Maestro Orchestrators synchronize the configuration automatically with each other.</p> <p> <b>Best Practice</b> - Configure the <b>First Time Wizard settings</b> in the new Security Group.</p>
2	<p>Assign the applicable Security Appliances to the Security Group.</p> <p> <b>Important:</b></p> <ul style="list-style-type: none"> <li>▪ You can assign only supported Security Appliances to the same Security Group - see <a href="#">sk162373</a>.</li> <li>▪ You must disable SMO Image Cloning in the Security Group <b>before</b> you assign to this Security Group an appliance of a different model than the other assigned appliances (Known Limitation PMTR-71298).</li> <li>▪ Security Appliances assigned to the Security Group automatically reboot after you apply the configuration.</li> </ul> <p> <b>Best Practice for Dual Site</b> - Assign the same number (as possible) of Security Appliances from each site to the Security Group. If a failover occurs between the sites, Security Appliances on the new Active site must be able to process all the traffic.</p>

Step	Instructions
3	<p>Assign the applicable Quantum Maestro Orchestrator ports to the Security Group:</p> <ul style="list-style-type: none"><li>▪ Uplink ports</li><li>▪ A Management interface</li></ul>
4	<p>Verify and apply the configuration.</p>
5	<p>If you did not configure the <b>First Time Wizard settings</b> when you created a Security Group, you must run the Gaia First Time Configuration Wizard on the Security Group.</p> <ol style="list-style-type: none"><li>a. With a web browser, connect to the Gaia Portal of the Security Group: <div data-bbox="395 663 1460 725" style="border: 1px solid black; padding: 2px;"><code>https://&lt;IP Address of Security Group&gt;</code></div></li><li> <b>Important</b> - This connection goes through the Quantum Maestro Orchestrator's management interface you assigned to this Security Group.</li><li>b. The Gaia First Time Configuration Wizard starts. Follow the instructions on the screen.</li></ol>

## Summary of Configuration Options

Table: Summary of configuration options in Quantum Maestro Orchestrators

Configuration Option	In Gaia Portal	In Gaia Clish*
Configuring the number of Maestro sites (Single Site or Dual Site)	N / A	See <a href="#">"Configuring the Number of Maestro Sites" on page 59</a>
Viewing the configured number of Maestro sites	<ol style="list-style-type: none"> <li>1. Click <b>Orchestrator</b> page.</li> <li>2. In the <b>Topology</b> pane, open the Security Groups.</li> </ol>	See <a href="#">"Viewing the Number of Maestro Sites" on page 59</a>
Configuring the Site ID in the Dual Site deployment	N / A	See <a href="#">"Configuring the Site ID in Dual Site Deployment" on page 60</a>
Viewing the Site ID in the Dual Site deployment	N / A	See <a href="#">"Viewing the Site ID in Dual Site Deployment" on page 61</a>
Configuring the number of Orchestrators on a Maestro Site	N / A	See <a href="#">"Configuring the Number of Orchestrators on a Maestro Site" on page 60</a>
Viewing the configured number of Orchestrators on a Maestro Site	N / A	See <a href="#">"Viewing the Number of Orchestrators on a Maestro Site" on page 60</a>
Creating a New Security Group	See <a href="#">"Creating a New Security Group" on page 46</a>	See <a href="#">"Creating a New Security Group" on page 63</a>
Deleting a Security Group	See <a href="#">"Deleting a Security Group" on page 47</a>	See <a href="#">"Creating a New Security Group" on page 63</a>
Adding the Network Configuration to a Security Group	See <a href="#">"Adding the Network Configuration and First Time Wizard settings to a Security Group" on page 48</a>	See <a href="#">"Adding the Network Configuration to a Security Group" on page 65</a>
Removing the Network Configuration from a Security Group	See <a href="#">"Removing the Network Configuration and First Time Wizard settings from a Security Group" on page 49</a>	See <a href="#">"Removing the Network Configuration from a Security Group" on page 66</a>



Table: Summary of configuration options in Quantum Maestro Orchestrators (continued)


Configuration Option	In Gaia Portal	In Gaia Clish*
Configuring the First Time Wizard settings in a Security Group	See <a href="#">"Adding the Network Configuration and First Time Wizard settings to a Security Group" on page 48</a>	See <a href="#">"Configuring First Time Wizard settings in a Security Group" on page 67</a>
Removing the First Time Wizard settings from a Security Group	See <a href="#">"Removing the Network Configuration and First Time Wizard settings from a Security Group" on page 49</a>	See <a href="#">"Removing First Time Wizard settings from a Security Group" on page 68</a>
Assigning available Security Appliances to a Security Group	See <a href="#">"Assigning Available Security Appliances to a Security Group" on page 50</a>	See <a href="#">"Assigning One Security Appliance to a Security Group" on page 69</a>
Removing one Security Appliance from a Security Group	See <a href="#">"Removing One Security Appliance from a Security Group" on page 51</a>	See <a href="#">"Removing One Security Appliance from a Security Group" on page 71</a>
Removing all Security Appliances from a Security Group	See <a href="#">"Removing All Security Appliances from a Security Group" on page 52</a>	N / A
Moving Security Appliances from one Security Group to a different Security Group	See <a href="#">"Moving Security Appliances from One Security Group to a Different Security Group" on page 53</a>	N / A
Assigning Interfaces to a Security Group	See <a href="#">"Assigning Interfaces to a Security Group" on page 54</a>	See <a href="#">"Assigning One Interface to a Security Group" on page 73</a>
Removing one interface from a Security Group	See <a href="#">"Removing One Interface from a Security Group" on page 54</a>	See <a href="#">"Removing One Interface from a Security Group" on page 74</a>
Removing all interfaces from a Security Group	See <a href="#">"Removing All Interfaces from a Security Group" on page 55</a>	N / A
Moving interfaces from one Security Group to a different Security Group	See <a href="#">"Moving Interfaces from One Security Group to a Different Security Group" on page 55</a>	N / A

Table: Summary of configuration options in Quantum Maestro Orchestrators (continued)

Configuration Option	In Gaia Portal	In Gaia Clish*
Adding VLAN interfaces on Uplink ports	N / A	See <a href="#">"Configuring VLAN Interfaces on Uplink Ports" on page 129</a>
Viewing VLAN interfaces on Uplink ports	See <a href="#">"Configuring VLAN Interfaces on Uplink Ports" on page 129</a> Follow these steps: <ol style="list-style-type: none"> <li>1. Click <b>Orchestrator</b> page.</li> <li>2. See the <b>Unassigned Interfaces</b> column.</li> </ol> or these steps: <ol style="list-style-type: none"> <li>1. Click <b>Orchestrator</b> page.</li> <li>2. Click the <b>[+]</b> on the left side of the applicable Security Group.</li> <li>3. Click the <b>[+]</b> on the left side of the <b>Interfaces</b> section.</li> </ol>	See <a href="#">"Viewing VLAN Interfaces on Uplink Ports" on page 75</a> See <a href="#">"Configuring VLAN Interfaces on Uplink Ports" on page 129</a>
Verifying the configuration changes in Security Groups	Automatic	See <a href="#">"Verifying the Configuration Changes" on page 76</a>
Applying the configuration changes to Security Groups	In the bottom left corner, click <b>Apply</b> .	See <a href="#">"Applying the Configuration Changes" on page 77</a>
Deleting configuration changes in Security Groups that were not applied yet	In the bottom left corner, click <b>Refresh</b> .	See <a href="#">"Deleting Configuration Changes That Were Not Applied Yet" on page 78</a>
Configuring the port settings	N / A	See <a href="#">"Configuring the Port Settings" on page 79</a>
Viewing the port settings	N / A	See <a href="#">"Viewing the Port Settings" on page 86</a>

Table: Summary of configuration options in Quantum Maestro Orchestrators (continued)


Configuration Option	In Gaia Portal	In Gaia Clish*
Viewing the Security Group settings	<p>Follow these steps:</p> <ol style="list-style-type: none"> <li>1. Click <b>Orchestrator</b> page.</li> <li>2. In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b>.</li> <li>3. Click the <b>[+]</b> on the left side of the applicable Security Group.</li> </ol>	See <a href="#">"Viewing the Security Group Settings" on page 90</a>

 **\*Important** - After every change in Gaia Clish, verify (see ["Verifying the Configuration Changes" on page 76](#)) and then apply (see ["Applying the Configuration Changes" on page 77](#)) the new configuration.

# Configuring Security Groups in Gaia Portal

This section provides the configuration instructions for Gaia Portal.

To start working in Gaia Portal on the Quantum Maestro Orchestrator:

Step	Instructions
1	<p>With a web browser, connect to the Gaia Portal on the Quantum Maestro Orchestrator:</p> <pre>https://&lt;IP Address of Orchestrator's MGMT Port&gt;</pre>
2	<p>Log in to the Gaia Portal with these default credentials:</p> <ul style="list-style-type: none"> <li>▪ Username - admin</li> <li>▪ Password - admin</li> </ul> <p> <b>Best Practice</b> - Change the default password as soon as possible. See the <a href="#">R81.20 Gaia Administration Guide</a> &gt; Chapter <i>User Management</i> &gt; Section <i>Change My Password</i>.</p>
3	From the left navigation tree, click <b>Orchestrator</b> page.

The **Topology** section contains the table that shows these sections (from left to right):

Item	Description
<b>Unassigned Gateways</b>	All detected Security Appliances that are not part of configured Security Groups. Quantum Maestro Orchestrator listens on the ports and automatically detects the connected Security Appliances.
<b>Topology</b>	Configured Security Groups with their assigned Security Appliances and ports.
<b>Unassigned Interfaces</b>	All interfaces on Quantum Maestro Orchestrators that are not part of configured Security Groups.






## Notes:

- Click the **Apply** button to save the changes in Security Groups.
- Click the **Refresh** button to load the latest configuration. For example, when you work with two Quantum Maestro Orchestrators for redundancy, and you change the configuration on another Quantum Maestro Orchestrator.
- You use the drag-and-drop action on the Security Appliance and port objects.
- When you hover the mouse cursor over a Security Appliance object, the tooltip shows the Security Appliance ID in the Security Group, Appliance Serial Number, and the corresponding Downlink port.

Applicable configuration procedures are provided below.

See ["Workflow for Configuring Security Groups" on page 38](#).

## Creating a New Security Group

Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	In the <b>Topology</b> column, right-click on the <b>Security Groups</b> and select <b>New Security Group</b> .
3	Enter the required <b>Management interface settings</b> .  <b>Best Practice</b> - Configure the <b>First Time Wizard settings</b> .
4	Click <b>OK</b> .
5	Click the <b>[+]</b> on the left side of the <b>Security Groups</b> and the new Security Group.
6	In the <b>Unassigned Gateways</b> column, select the applicable Security Appliances.  <b>Important</b> - You must assign at least one Security Appliance to the Security Group.  <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ You can assign only supported Security Appliances to the same Security Group - see <a href="#">sk162373</a>.</li> <li>▪ You must disable SMO Image Cloning in the Security Group <b>before</b> you assign to this Security Group an appliance of a different model than the other assigned appliances (Known Limitation PMTR-71298).</li> <li>▪ To select multiple Security Appliances, press and hold the <b>CTRL</b> key and left-click the objects with the mouse cursor.</li> </ul>
7	Drag-and-drop the selected Security Appliances from the <b>Unassigned Gateways</b> column to the <b>Gateways</b> section in the new Security Group.
8	In the <b>Unassigned Interfaces</b> column, select the applicable data and management interfaces.  <b>Note</b> - To select multiple interfaces, press and hold the <b>CTRL</b> key and left-click the objects with the mouse cursor.
9	Drag-and-drop the selected interfaces from the <b>Unassigned Interfaces</b> column to the <b>Interfaces</b> section in the new Security Group.
10	In the bottom left corner, click <b>Apply</b> .  <b>Important</b> - Security Appliances assigned to the Security Group automatically reboot after you apply the configuration.

 **Notes:**

- Every new Security Group you add, is called **Security Group N**, where the ordinal number *N* is assigned automatically starting from 1 (for example, if you already have "Security Group 1" and "Security Group 3", then the new Security Group is called "Security Group 2").
- Every Security Group contains two sections:
  - **Gateways** - contains the Check Point Security Gateways you assign to this Security Group.
  - **Interfaces** - contains the Orchestrator's interfaces you assign to this Security Group.
- You must make sure to assign the correct Security Gateways' interfaces to Security Groups.


### Deleting a Security Group

Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	In the <b>Topology</b> column, right-click on the Security Group.
3	From the menu, click <b>Delete Security Group</b> . <b>Important</b> - There is no prompt to confirm.
4	In the bottom left corner, click <b>Apply</b> .

## Adding the Network Configuration and First Time Wizard settings to a Security Group


Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	In the <b>Topology</b> column, right-click on the Security Group.
3	Click <b>Set Security Group configuration</b> .
4	<p>In the <b>Network settings</b> section:</p> <ol style="list-style-type: none"> <li>1. In the <b>IPv4 address</b> field, enter the IPv4 address of the Security Group. All Security Appliances in this Security Group use this IPv4 address as their Gaia management IP address. You use this IPv4 address in SmartConsole when you configure the corresponding Security Gateway object.</li> <li>2. In the <b>Subnet mask</b> field, enter the applicable IPv4 subnet mask. All Security Appliances in this Security Group use this IPv4 subnet mask for their Gaia management IP address. You use this IPv4 subnet mask in SmartConsole when you configure the corresponding Security Gateway object.</li> <li>3. In the <b>Default Gateway</b> field, enter the applicable IPv4 address. All Security Appliances in this Security Group use this IPv4 address as their default gateway.</li> </ol>
5	<p>In the <b>First Time Wizard settings</b> section, configure the initial settings for Security Appliances assigned to this Security Group.</p> <ol style="list-style-type: none"> <li>1. Select <b>Set FTW configuration</b>.</li> <li>2. In the <b>Host Name</b> field, enter a hostname.</li> <li>3. Select <b>Configure Admin Password</b>: <ol style="list-style-type: none"> <li>a. In the <b>Admin Password</b> field, enter the Expert mode password.</li> <li>b. In the <b>Confirm Admin Password</b> field, enter the same Expert mode password key again.</li> </ol> </li> <li>4. In the <b>SIC Password</b> field, enter a one-time activation key (between 4 and 127 characters long). You use this activation key in SmartConsole when you create the corresponding Security Gateway object.</li> <li>5. In the <b>Confirm SIC Password</b> field, enter the same one-time activation key again.</li> <li>6. Select <b>Install as VSX</b>, only if it is necessary to run all Security Appliances in this Security Group as VSX Gateways.</li> </ol>
6	Click <b>OK</b> .
7	In the bottom left corner, click <b>Apply</b> .



-  **Warning** - If you enable the **Set FTW configuration** option in an existing Security Group (in which you already ran the First Time Configuration Wizard), then the change applies only after you reset each Security Appliance in that Security Group to factory defaults.

#### Removing the Network Configuration and First Time Wizard settings from a Security Group

Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	In the <b>Topology</b> column, right-click on the Security Group.
3	From the menu, click <b>Clear network configuration</b> . <b>Important</b> - There is no prompt to confirm.
4	In the bottom left corner, click <b>Apply</b> .

-  **Note** - This configuration option is available only in the Gaia Portal.

## Assigning Available Security Appliances to a Security Group

### ★ Best Practice:

1. Before you add Security Appliances to an existing Security Group, enable the SMO Image Cloning feature in the Security Group.

This feature automatically clones all the required software packages to the new Security Appliances.

Run in Gaia gClish on the Security Group:



```
set smo image auto-clone state on
```

```
show smo image auto-clone state
```

2. After you added the Security Appliances, you must disable the SMO Image Cloning feature in the Security Group:

```
set smo image auto-clone state off
```

```
show smo image auto-clone state
```

Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	Click the <b>[+]</b> on the left side of the applicable Security Group.
3	In the <b>Unassigned Gateways</b> column, select the applicable Security Appliances.  <b>Note</b> - To select multiple Security Appliances, press and hold the <b>CTRL</b> key and left-click the objects with the mouse cursor.
4	Drag-and-drop the selected Security Appliances from the <b>Unassigned Gateways</b> column to the <b>Gateways</b> section in the applicable Security Group.  <b>Note</b> - If such operation is allowed, Gaia Portal shows a green plus icon. Otherwise, it shows a red blocking icon.
5	In the bottom left corner, click <b>Apply</b> .

### Important:

- You can assign only supported Security Appliances to the same Security Group - see [sk162373](#).
- You must disable SMO Image Cloning in the Security Group **before** you assign to this Security Group an appliance of a different model than the other assigned appliances (Known Limitation PMTR-71298).
- Security Appliances assigned to the Security Group automatically reboot after you apply the configuration.

- ★ **Best Practice for Dual Site** - Assign the same number (as possible) of Security Appliances from each site to the Security Group. If a failover occurs between the sites, Security Appliances on the new Active site must be able to process all the traffic.


### Removing One Security Appliance from a Security Group


Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	Click the <b>[+]</b> on the left side of the applicable Security Group.
3	Click the <b>[+]</b> on the left side of the <b>Gateways</b> section.
4	Select the Security Appliance it is necessary to remove from the Security Group.
5	Right-click on the selected Security Appliance.
6	From the menu, click <b>Detach Gateway</b> . <b>Important</b> - There is no prompt to confirm.
7	In the bottom left corner, click <b>Apply</b> .

- ⓘ **Important** - The Security Appliance must perform a reset to factory defaults and reboot after you remove it from a Security Group. This is to make sure that no security configuration is left behind.

## Removing All Security Appliances from a Security Group

Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	Click the <b>[+]</b> on the left side of the applicable Security Group.
3	Left-click on the <b>Gateways</b> section to select it.
4	Right-click on the <b>Gateways</b> section.
5	From the menu, click <b>Detach all Gateways</b> .
6	In the bottom left corner, click <b>Apply</b> .

 **Important** - The Security Appliances must perform a reset to factory defaults and reboot after you remove them from a Security Group. This is to make sure that no security configuration is left behind.

 **Note** - This configuration option is available only in the Gaia Portal.

## Moving Security Appliances from One Security Group to a Different Security Group

### ★ Best Practice:

1. Before you add Security Appliances to an existing Security Group, enable the SMO Image Cloning feature in the Security Group.

This feature automatically clones all the required software packages to the new Security Appliances.

Run in Gaia gClish on the Security Group:

```
set smo image auto-clone state on
```

```
show smo image auto-clone state
```

2. After you added the Security Appliances, you must disable the SMO Image Cloning feature in the Security Group:

```
set smo image auto-clone state off
```

```
show smo image auto-clone state
```

Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	Click the <b>[+]</b> on the left side of the applicable <i>source</i> Security Group.
3	Click the <b>[+]</b> on the left side of the applicable <i>target</i> Security Group.
4	Select the applicable Security Appliances. <b>Note</b> - To select multiple Security Appliances, press and hold the <b>CTRL</b> key and left-click the objects with the mouse cursor.
5	Drag-and-drop the selected Security Appliances from the <b>Gateways</b> section of the <i>source</i> Security Group to the <b>Gateways</b> section of the <i>target</i> Security Group. <b>Note</b> - If such operation is allowed, Gaia Portal shows a green plus icon. Otherwise, it shows a red blocking icon.
6	In the bottom left corner, click <b>Apply</b> .

**i Important** - The Security Appliance must perform a reset to factory defaults and reboot after you remove it from a Security Group. This is to make sure that no security configuration is left behind.

**i Note** - This configuration option is available only in the Gaia Portal.

### Assigning Interfaces to a Security Group


Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	Click the <b>[+]</b> on the left side of the applicable Security Group.
3	In the <b>Unassigned Interfaces</b> column, select the applicable interfaces. <b>Note</b> - To select multiple interfaces, press and hold the <b>CTRL</b> key and left-click the objects with the mouse cursor.
4	Drag-and-drop the selected interfaces from the <b>Unassigned Interfaces</b> column to the <b>Interfaces</b> section in the applicable Security Group. <b>Note</b> - If such operation is allowed, Gaia Portal shows a green plus icon. Otherwise, it shows a red blocking icon.
5	In the bottom left corner, click <b>Apply</b> .

### Removing One Interface from a Security Group

Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	Click the <b>[+]</b> on the left side of the applicable Security Group.
3	Click the <b>[+]</b> on the left side of the <b>Interfaces</b> section.
4	Right-click on the applicable interface.
5	From the menu, click <b>Detach Interface</b> . <b>Important</b> - There is no prompt to confirm.
6	In the bottom left corner, click <b>Apply</b> .


## Removing All Interfaces from a Security Group

Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	Click the <b>[+]</b> on the left side of the applicable Security Group.
3	Right-click on the <b>Interfaces</b> section.
4	From the menu, click <b>Detach Security Group Interfaces</b> . <b>Important</b> - There is no prompt to confirm.
5	In the bottom left corner, click <b>Apply</b> .

 **Note** - This configuration option is available only in the Gaia Portal.

## Moving Interfaces from One Security Group to a Different Security Group


Step	Instructions
1	In the <b>Topology</b> column, click the <b>[+]</b> on the left side of the <b>Security Groups</b> .
2	Click the <b>[+]</b> on the left side of the applicable <i>source</i> Security Group.
3	Click the <b>[+]</b> on the left side of the applicable <i>target</i> Security Group.
4	Select the applicable interfaces. <b>Note</b> - To select multiple interfaces, press and hold the <b>CTRL</b> key and left-click the objects with the mouse cursor.
5	Drag-and-drop the selected interfaces from the <b>Interfaces</b> section of the <i>source</i> Security Group to the <b>Interfaces</b> section of the <i>target</i> Security Group. <b>Note</b> - If such operation is allowed, Gaia Portal shows a green plus icon. Otherwise, it shows a red blocking icon.
6	In the bottom left corner, click <b>Apply</b> .

 **Note** - This configuration option is available only in the Gaia Portal.

## Viewing VLAN Interfaces on Uplink Ports

See "[Configuring VLAN Interfaces on Uplink Ports](#)" on page 129.

Step	Instructions
1	On the <b>Orchestrator</b> page, in the <b>Topology</b> section, expand <b>Security Groups</b> .
2	Expand your Security Group.
3	Expand <b>Interfaces</b> .
4	Put the mouse cursor on an interface. VLAN information appears in the tooltip.

 **Note** - If this is a Dual Site deployment, and the Security Group contains Security Appliances that are located only at one of the sites (for example, Site 2), then the tooltip that shows VLAN interfaces appears only in Gaia Portal of the Orchestrator (for example, on Site 2) that is located at the same site as Security Appliances.



# Configuring Security Groups in Gaia Clish

This section provides the configuration instructions for Gaia Clish.

To start working in Gaia Clish on the Quantum Maestro Orchestrator:

Step	Instructions
1	Connect to the Command Line on the Quantum Maestro Orchestrator (over SSH, or through the Console Port).
2	Log in to the Gaia Portal with these default credentials: <ul style="list-style-type: none"><li data-bbox="357 658 663 689">▪ Username - admin</li><li data-bbox="357 698 657 730">▪ Password - admin</li></ul> <p data-bbox="316 766 1422 880">★ <b>Best Practice</b> - Change the default password as soon as possible. See the <a href="#">R81.20 Gaia Administration Guide</a> &gt; Chapter <i>User Management</i> &gt; Section <i>Change My Password</i>.</p>

These are the main commands in Gaia Clish on Quantum Maestro Orchestrators:

Task	Syntax
Viewing the settings	<pre data-bbox="411 331 916 394">show maestro</pre> <p data-bbox="411 421 759 454"><b>Available sub-commands</b></p> <p data-bbox="411 465 916 499">To see all available sub-commands:</p> <ol data-bbox="443 528 576 562" style="list-style-type: none"> <li>1. Enter:</li> </ol> <pre data-bbox="491 568 916 631">show maestro</pre> <ol data-bbox="443 640 895 674" style="list-style-type: none"> <li>2. Press the <b>Esc</b> key two times.</li> </ol>
Configuring the settings	<pre data-bbox="411 719 916 781">add maestro</pre> <p data-bbox="411 808 759 842"><b>Available sub-commands</b></p> <p data-bbox="411 853 916 887">To see all available sub-commands:</p> <ol data-bbox="443 916 576 949" style="list-style-type: none"> <li>1. Enter:</li> </ol> <pre data-bbox="491 956 916 1019">add maestro</pre> <ol data-bbox="443 1028 895 1061" style="list-style-type: none"> <li>2. Press the <b>Esc</b> key two times.</li> </ol>
	<pre data-bbox="411 1106 916 1169">set maestro</pre> <p data-bbox="411 1196 759 1229"><b>Available sub-commands</b></p> <p data-bbox="411 1240 916 1274">To see all available sub-commands:</p> <ol data-bbox="443 1303 576 1337" style="list-style-type: none"> <li>1. Enter:</li> </ol> <pre data-bbox="491 1344 916 1406">set maestro</pre> <ol data-bbox="443 1415 887 1449" style="list-style-type: none"> <li>2. Press the <b>Esc</b> key two times</li> </ol>
Deleting the settings	<pre data-bbox="411 1494 916 1556">delete maestro</pre> <p data-bbox="411 1583 759 1617"><b>Available sub-commands</b></p> <p data-bbox="411 1628 916 1662">To see all available sub-commands:</p> <ol data-bbox="443 1691 576 1724" style="list-style-type: none"> <li>1. Enter:</li> </ol> <pre data-bbox="491 1731 916 1794">delete maestro</pre> <ol data-bbox="443 1803 887 1836" style="list-style-type: none"> <li>2. Press the <b>Esc</b> key two times</li> </ol>

**Notes:**

- For more information about the Gaia Clish, see the [R81.20 Gaia Administration Guide](#).
- After every change, verify (see "[Verifying the Configuration Changes](#)" on [page 76](#)) and then apply (see "[Applying the Configuration Changes](#)" on [page 77](#)) the new configuration.

Applicable configuration procedures are provided below.

See "[Workflow for Configuring Security Groups](#)" on [page 38](#).

**Configuring the Number of Maestro Sites****Description**

This command configures the number of Maestro sites - Single Site (value 1), or Dual Site (value 2).

**Syntax**

```
set maestro configuration orchestrator-site-amount {1 | 2}
```

**Viewing the Number of Maestro Sites****Description**

This command shows the configured number of Maestro sites.

**Syntax**

```
show maestro configuration orchestrator-site-amount
```

**Example**

```
MHO> show maestro configuration orchestrator-site-amount
Number of configured Orchestrators Sites in this Maestro
deployment is 2.
MHO>
```

## Configuring the Number of Orchestrators on a Maestro Site

### Description

This command configures the number of Orchestrators on a Maestro Site.

### Syntax

```
set maestro configuration orchestrator-amount {1 | 2}
```

## Viewing the Number of Orchestrators on a Maestro Site

### Description

This command shows the configured number of Orchestrators on a Maestro Site.

### Syntax

```
show maestro configuration orchestrator-amount
```

### Example

```
MHO> show maestro configuration orchestrator-amount
Number of configured Orchestrators in this Maestro deployment is
2.
MHO>
```

## Configuring the Site ID in Dual Site Deployment

### Description

This command configures the Site ID in Dual Site deployment.

The Quantum Maestro Orchestrators on a site that were installed earlier, must get the ID 1.

The Quantum Maestro Orchestrators on a site that were installed later, must get the ID 2.

### Syntax

```
set maestro configuration orchestrator-site-id {1 | 2}
```

## Viewing the Site ID in Dual Site Deployment

### Description

This command shows the configured Site ID in Dual Site deployment.

### Syntax

```
show maestro configuration orchestrator-site-id
```

## Configuring the Base Site Sync VLAN ID in Dual Site Deployment

### Description

This command configures the Base Site Sync VLAN ID. Quantum Maestro Orchestrators of the same site use this value to calculate internal VLAN ID used for internal synchronization between Quantum Maestro Orchestrators.

#### Important:

- The value of the Base Site Sync VLAN ID must be the same on all Quantum Maestro Orchestrators of the same site. The default value is 3600.
- Configure a different Base Site Sync VLAN ID, if the default Site Sync VLAN IDs (3600 and 3601) conflict with the existing VLAN IDs in your environment.

Quantum Maestro Orchestrators use this Base Site Sync VLAN ID internally to calculate their Site Sync VLAN IDs based on these formulas:

- For the first Quantum Maestro Orchestrator on the same Site (Orchestrator ID 1\_1 and Orchestrator ID 2\_1):

$$\langle \text{Site Sync VLAN ID} \rangle = \langle \text{Base Site Sync VLAN ID} \rangle + 0$$

- For the second Quantum Maestro Orchestrator on the same Site (Orchestrator ID 1\_2 and Orchestrator ID 2\_2):

$$\langle \text{Site Sync VLAN ID} \rangle = \langle \text{Base Site Sync VLAN ID} \rangle + 1$$

Example for the internal Site Sync VLAN ID calculation based on the default value of 3600:

Site ID	Site Sync VLAN ID on Orchestrator ID 1_1 and Orchestrator ID 2_1	Site Sync VLAN ID on Orchestrator ID 1_2 and Orchestrator ID 2_2
Site #1	3600	3601
Site #2	3600	3601

### Syntax

```
set maestro configuration orchestrator-site-vlan <Number>
```

## Viewing the Base Site Sync VLAN ID in Dual Site Deployment

### Description

This command shows the configured Base Site Sync VLAN ID in Dual Site deployment.

### Syntax

```
show maestro configuration orchestrator-site-vlan
```

## Creating a New Security Group

### Description

This command adds a Security Group with the specified ID on the Quantum Maestro Orchestrator.

**i Important** - You must assign Security Appliances and applicable interfaces. See the corresponding configuration procedures.

### Syntax

```
add maestro security-group id <Security Group ID>
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	<p>Specifies the Security Group ID.</p> <p>To see the existing IDs and the available ID, press the <b>Tab</b> key.</p> <p><b>i Important</b> - The largest shown ID is the next available ID.</p>

### Example - Security Groups with IDS 1 and 2 already exist, ID 3 is the next available ID

```
MHO> add maestro security-group id
1 2 3
MHO> add maestro security-group id 3
Successfully added security group 3
MHO>
```

## Deleting a Security Group

### Description

This command deletes a Security Group with the specified ID on the Quantum Maestro Orchestrator.

**Important** - There is no prompt to confirm.

### Syntax

```
delete maestro security-group id <Security Group ID>
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.

### Example

```
MHO> delete maestro security-group id  
1 2 3  
MHO> delete maestro security-group id 3  
Successfully deleted security group 3  
MHO>
```



## Adding the Network Configuration to a Security Group

### Description

This command adds the Network Configuration in a Security Group with the specified ID.

### Syntax

```
set maestro security-group id <Security Group ID> management-
connectivity ipv4-address <Security Group IPv4 Address> mask-
length <1-32> [default-gw <Default Gateway IPv4 Address>]
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.
<code>&lt;Security Group IPv4 Address&gt;</code>	Specifies the IPv4 address for the Security Group.
<code>&lt;Default Gateway IPv4 Address&gt;</code>	Specifies the IPv4 address of the Default Gateway for the Security Group.

### Example

```
MHO> set maestro security-group id 3 management-connectivity
ipv4-address 192.168.30.40 mask-length 24 default-gw
192.168.30.1
Successfully set management connectivity configuration for
security group 3
MHO>
```

## Removing the Network Configuration from a Security Group

### Description

This command removes the Network Configuration from a Security Group with the specified ID.

**Important** - There is no prompt to confirm.

### Syntax

```
delete maestro security-group id <Security Group ID> management-
connectivity
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.

### Example

```
MHO> delete maestro security-group id[TAB]
1 2 3
MHO> delete maestro security-group id 3 management-connectivity
Successfully deleted management connectivity configuration for
security group 3
MHO>
```

## Configuring First Time Wizard settings in a Security Group

### Description

This command configures the First Time Wizard settings in a Security Group with the specified ID.

These settings are used to perform initial configuration of Security Appliances assigned to this Security Group.

**Warning** - If you configure these settings in an existing Security Group (in which you already ran the First Time Configuration Wizard), then the change applies only after you reset each Security Appliance in that Security Group to factory defaults.

### Syntax

```
set maestro security-group id <Security Group ID> ftw-
configuration hostname <Hostname> sic <SIC Password> admin-
password <Admin Password> is-vsx {yes | no}
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.
<code>ftw-configuration</code>	Specifies the First Time Wizard settings for Security Appliances in the Security Group.
<code>hostname &lt;Hostname&gt;</code>	Specifies the hostname for Security Appliances.
<code>sic &lt;SIC Password&gt;</code>	Specifies the one-time activation key for Security Appliances. You use this activation key in SmartConsole when you create the corresponding Security Gateway object. The key is between 4 and 127 characters long.
<code>admin-password &lt;Admin Password&gt;</code>	Specifies the Expert mode password for the Security Group.
<code>is-vsx {yes   no}</code>	Specifies whether to configure the Security Appliances in VSX mode.

## Example

```
MHO> set maestro security-group id 3 ftw-configuration hostname
MyGwAppliance sic 123456 admin-password P@sswo4d is-vsx no
Successfully set FTW configuration to security group 3
MHO>
```

## Removing First Time Wizard settings from a Security Group

### Description

This command removes the First Time Wizard settings from a Security Group with the specified ID.

**Important** - There is no prompt to confirm.

### Syntax

```
delete maestro security-group id <Security Group ID> ftw-
configuration
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.

### Example

```
MHO> delete maestro security-group id[TAB]
1 2 3
MHO> delete maestro security-group id 3 ftw-configuration
Successfully deleted FTW configuration for security group 3
MHO>
```

## Assigning One Security Appliance to a Security Group

### ★ Best Practice:

1. Before you add Security Appliances to an existing Security Group, enable the SMO Image Cloning feature in the Security Group.

This feature automatically clones all the required software packages to the new Security Appliances.

Run in Gaia gClish on the Security Group:

```
set smo image auto-clone state on
```

```
show smo image auto-clone state
```

2. After you added the Security Appliances, you must disable the SMO Image Cloning feature in the Security Group:

```
set smo image auto-clone state off
```

```
show smo image auto-clone state
```

## Description

This command assigns a Security Appliance with the specified Serial Number to a Security Group with the specified ID.

### i Important:


- You can assign only supported Security Appliances to the same Security Group - see [sk162373](#).
- You must disable SMO Image Cloning in the Security Group **before** you assign to this Security Group an appliance of a different model than the other assigned appliances (Known Limitation PMTR-71298).
- Security Appliances assigned to the Security Group automatically reboot after you apply the configuration.

- ★ **Best Practice for Dual Site** - Assign the same number (as possible) of Security Appliances from each site to the Security Group. If a failover occurs between the sites, Security Appliances on the new Active site must be able to process all the traffic.

## Syntax

```
add maestro security-group id <Security Group ID> serial <Serial Number>
```

## Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.
<code>serial &lt;Serial Number&gt;</code>	Assigns one Security Appliance specified by its Serial Number. To see the available Serial Numbers, press the <b>Tab</b> key.  <b>Important</b> - You can assign only appliances of the same model to the same Security Group.

## Example

```
MHO> add maestro security-group id 3 serial [TAB]
1234567890
MHO> add maestro security-group id 3 serial 1234567890
Successfully added gw 1234567890 to security group 7
MHO>
```

## Removing One Security Appliance from a Security Group

### Description

This command removes a Security Appliance with the specified Member ID or Serial Number from a Security Group with the specified ID.

#### Important:

- The Security Appliance must perform a reset to factory defaults and reboot after you remove it from a Security Group. This is to make sure that no security configuration is left behind.
- There is no prompt to confirm.

### Syntax to remove a Security Appliance with the specified Member ID

```
delete maestro security-group id <Security Group ID> member
<Member ID>
```

### Syntax to remove a Security Appliance with the specified Serial Number

```
delete maestro security-group id <Security Group ID> serial
<Serial Number>
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.
<code>member &lt;Member ID&gt;</code>	Specifies the Security Appliance by its Member ID in the Security Group. To see the available IDs, press the <b>Tab</b> key.
<code>serial &lt;Serial Number&gt;</code>	Specifies the Security Appliance by its Serial Number. To see the available Serial Numbers, press the <b>Tab</b> key.

### Example of removing a Security Appliance with the specified Member ID

```
MHO> delete maestro security-group id 3 member [TAB]
1 2 3 4
MHO> delete maestro security-group id 3 member 4
Successfully deleted member 4 from security group 3
MHO>
```

**Example of removing a Security Appliance with the specified Serial Number**

```
MHO> delete maestro security-group id 3 serial [TAB]
1234567890
MHO> delete maestro security-group id 3 serial 1234567890
Successfully deleted gw with 1322B01094 from security group 3
MHO>
```



## Assigning One Interface to a Security Group

### Description

This command assigns an interface with the specified name to a Security Group with the specified ID.

### Syntax

```
add maestro security-group id <Security Group ID> interface
<Interface Name>
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.
<code>interface &lt;Interface Name&gt;</code>	Assigns one interface specified by its name. To see the available interfaces, press the <b>Tab</b> key.

### Example

```
MHO> add maestro security-group id 3 interface [TAB]

eth1-Mgmt2 eth1-Mgmt3 eth1-Mgmt4 eth1-Mgmt6 eth1-Mgmt7 eth1-
Mgmt8
eth1-Mgmt9 eth1-10 eth1-11 eth1-12 eth1-13 eth1-14
eth1-15 eth1-16 eth1-17 eth1-18 eth1-19 eth1-20
eth1-21 eth1-22 eth1-23 eth1-24 eth1-25 eth1-26
eth1-48 eth1-49 eth1-51 eth1-53 eth1-55 eth1-57
eth1-59 eth1-61 eth1-63 eth2-Mgmt1 eth2-Mgmt2 eth2-Mgmt3
eth2-Mgmt4 eth2-06 eth2-07 eth2-08 eth2-09 eth2-10
eth2-11 eth2-12 eth2-13 eth2-14 eth2-15 eth2-16
eth2-17 eth2-18 eth2-19 eth2-20 eth2-21 eth2-22
eth2-23 eth2-24 eth2-25 eth2-26 eth2-48 eth2-49
eth2-51 eth2-53 eth2-55 eth2-57 eth2-59 eth2-61
eth2-63
MHO> add maestro security-group id 3 interface eth1-17
Successfully added interface eth1-17 to security group 3
MHO>
```

## Removing One Interface from a Security Group

### Description

This command removes an interface with the specified name from a Security Group with the specified ID.

### Syntax

```
delete maestro security-group id <Security Group ID> interface
<Interface Name>
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.
<code>interface &lt;Interface Name&gt;</code>	Removes one interface specified by its name. To see the available interfaces, press the <b>Tab</b> key.

### Example

```
MHO> delete maestro security-group id 3 interface [TAB]
eth1-Mgmt3 eth1-13 eth1-14 eth1-15 eth1-16 eth1-17
MHO> add maestro security-group id 3 interface eth1-17
Successfully deleted interface eth1-17 from security group 3
MHO>
```

## Viewing VLAN Interfaces on Uplink Ports

See "[Configuring VLAN Interfaces on Uplink Ports](#)" on page 129.

### Description

This command shows the Security Group configuration, including VLAN interfaces configured on the Uplink Ports.

### Syntax

```
show maestro security-group id <Security Group ID>
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the ID of the Security Group. To see the existing IDs, press the <b>Tab</b> key.

## Verifying the Configuration Changes

### Description

This command shows and verifies the validity of all the configuration changes you made, but did not apply yet to Security Groups or ports.

- ★ **Best Practice** - Run this command after all changes in the configuration of Security Groups or ports.

### Syntax

```
show maestro security-group verify-new-config
```

### Example 1 - No changes were made

```
MHO> show maestro security-group verify-new-config
The following changes will take place:
Temporary topology file not exists
MHO>
```

### Example 2 - Some changes were made

```
MHO> add maestro security-group id 3
Successfully added security group 3
MHO>
MHO> show maestro security-group verify-new-config
The following changes will take place:
Security Group 1
  - No changes
Security Group 2
  - Removed Gateway 1_2 serial 1234567890. GW is rebooting.
Security Group 3
  - Security group created
  - Added Gateway 1_1 serial 1234567890
  - Added interface eth1-Mgmt4
MHO>
```

## Applying the Configuration Changes

### Description

This command applies all the configuration changes you made, but did not apply yet to Security Groups or ports.

**i Important** - You must run this command after you make changes in the configuration of Security Groups or ports.

### Syntax

```
set maestro security-group apply-new-config
```

### Example

```
MHO> set maestro security-group apply-new-config
You are about to perform "set maestro security-group apply-new-
config"
The following changes will take place:
Security Group 1
  - No changes

Are you sure? (Y - yes, any other key - no) y

"set maestro security-group apply-new-config" requires auditing
Enter your full name: johndoe
Enter reason for "set maestro security-group apply-new-config"
[Configuration]: test
CRITICAL: "set maestro security-group apply-new-config", User:
johndoe, Reason: test
Are you sure? (Y - yes, any other key - no) y

Action Summary
-----

Security Group 1
  - No changes
MHO>
```

## Deleting Configuration Changes That Were Not Applied Yet

### Description

This command deletes all the configuration changes you made, but did not apply yet to Security Groups or ports.

**Important** - There is no prompt to confirm.

### Syntax

```
delete maestro security-group new-config
```

### Example

```
MHO> delete maestro security-group new-config  
Successfully deleted new topology configuration  
MHO>
```

## Configuring the Port Settings


### Description

These commands let you configure different settings on the Quantum Maestro Orchestrator's ports.

### Syntax

```
set maestro port <Port ID>
    admin-state {up | down}
    mtu 68-10236
    qsfp-mode {1G | 10G | 4x10G | 4x25G | 25G | 40G | 100G}
    type {downlink | uplink | management | site_sync | ssm_
sync} [no-confirmation]
```


## Parameters

Parameter	Description
<code>&lt;Port ID&gt;</code>	<p>Specifies the port to configure. The format is three numbers separated with a slash: <code>&lt;Quantum Maestro Orchestrator ID&gt;/&lt;Port Label&gt;/&lt;Port Split ID&gt;</code></p> <p>Examples:</p> <ul style="list-style-type: none"> <li>▪ 1/3/1</li> <li>▪ 2/20/1</li> </ul> <p>Notes:</p> <ul style="list-style-type: none"> <li>▪ <code>&lt;Quantum Maestro Orchestrator ID&gt;</code> is 1 if you connect only one Quantum Maestro Orchestrator. When you connect two Quantum Maestro Orchestrators for redundancy, the <code>&lt;Quantum Maestro Orchestrator ID&gt;</code> is 1 on the first Quantum Maestro Orchestrator and 2 on the second Quantum Maestro Orchestrator.</li> <li>▪ <code>&lt;Port Label&gt;</code> is the number of the physical port on the front panel. On MHO-140, there are exceptions for ports 51, 53, 55, and 56.</li> <li>▪ The default value of the <code>&lt;Port Split ID&gt;</code> is 1, if you did not split the port with a breakout cable.</li> <li>▪ To see the available Port IDs, enter the command <code>set maestro port</code> and press the <b>Tab</b> key.</li> <li>▪ To see the Port IDs and the names Gaia OS assigned to them, connect to the Gaia Portal on the Quantum Maestro Orchestrator and click <b>Orchestrator</b> page. For the default mapping, see the <a href="#">Quantum Maestro Getting Started Guide</a> - Section <i>Maestro Hyperscale Orchestrator Ports and Gaia OS Interfaces</i>.</li> </ul>
<code>admin-state</code>	<p>Configures the port administrative state:</p> <ul style="list-style-type: none"> <li>▪ up - Enabled</li> <li>▪ down - Disabled</li> </ul> <p> <b>Important</b> - This change does <b>not</b> survive reboot of the Orchestrator (Known Limitation MBS-11339).</p>
<code>mtu</code>	<p>Configures the port MTU. Valid range: 68 - 10236 bytes. Default: 10236 bytes.</p>



Parameter	Description
qsfp-mode	<p>Configures the QSFP mode:</p> <ul style="list-style-type: none"> <li>■ 1G - Port works with the 1 GbE speed (only 10 GbE ports support this mode).</li> <li>■ 10G - Port works with the 10 GbE speed.</li> <li>■ 4x10G - Split of a 40 GbE port into four ports that work with the 10 GbE speed each.</li> <li>■ 4x25G - Split of a 100 GbE port into four ports that work with the 25 GbE speed each.</li> <li>■ 25G - Port works with the 25 GbE speed.</li> <li>■ 40G - Port works with the 40 GbE speed.</li> <li>■ 100G - Port works with the 100 GbE speed.</li> </ul> <p><b>!</b> <b>Important</b></p> <ul style="list-style-type: none"> <li>■ On MHO-175 ports, you can configure only these modes: <ul style="list-style-type: none"> <li>• 4x10G, 4x25G, 25G, 40G, or 100G</li> </ul> </li> <li>■ On MHO-170 ports, you can configure only these modes: <ul style="list-style-type: none"> <li>• Ports with odd <i>&lt;Port Label&gt;</i> numbers (x/1/y, x/3/y, x/5/y, and so on): 4x10G, 4x25G, 25G, 40G, or 100G</li> <li>• Ports with even <i>&lt;Port Label&gt;</i> numbers (x/2/y, x/4/y, x/6/y, and so on): 25G, 40G, or 100G</li> </ul> </li> <li>■ On MHO-140 ports, you can configure only these port modes: <ul style="list-style-type: none"> <li>• Ports with the <i>&lt;Port Label&gt;</i> from x/1/y to x/48/y: 1G, 10G, or 25G</li> <li>• Ports with the <i>&lt;Port Label&gt;</i> x/49/y, x/51/y, x/53/y, and x/55/y: 4x10G, 4x25G, 25G, 40G, or 100G</li> <li>• Ports with the <i>&lt;Port Label&gt;</i> x/50/y, x/52/y, x/54/y, and x/56/y: 25G, 40G, or 100G</li> </ul> </li> </ul>

Parameter	Description
type	<p>Configures the port type:</p> <ul style="list-style-type: none"><li>▪ <code>downlink</code> - Connects to Check Point Security Appliances</li><li>▪ <code>uplink</code> - Connects to external and internal production networks</li><li>▪ <code>management</code> - Connects to a Management Server that manages the applicable Security Group</li><li>▪ <code>site_sync</code> - External synchronization in Dual Site deployment - between peer Orchestrators on different sites</li><li>▪ <code>ssm_sync</code> - Internal synchronization in Dual Site deployment - between peer Orchestrators on the same site</li></ul> <p>The parameter "<code>no-confirmation</code>" is optional. If specified, the command does not ask you for confirmation and audit information.</p>

Parameter	Description
	<p> <b>Important:</b></p> <ul style="list-style-type: none"> <li>■ On MHO-175, you can configure only these port types: <ul style="list-style-type: none"> <li>• Port 1: <ul style="list-style-type: none"> <li>◦ management</li> <li>◦ downlink</li> </ul> </li> <li>• Ports 2 and higher: <ul style="list-style-type: none"> <li>◦ uplink</li> <li>◦ downlink</li> <li>◦ site_sync</li> <li>◦ ssm_sync</li> </ul> </li> </ul> </li> <li>■ On MHO-170, you can configure only these port types: <ul style="list-style-type: none"> <li>• Port 1 and Port 2: <ul style="list-style-type: none"> <li>◦ management</li> <li>◦ downlink</li> </ul> </li> <li>• Ports 3 and higher: <ul style="list-style-type: none"> <li>◦ uplink</li> <li>◦ downlink</li> <li>◦ site_sync</li> <li>◦ ssm_sync</li> </ul> </li> </ul> </li> <li>■ On MHO-140, you can configure only these port types: <ul style="list-style-type: none"> <li>• Port 1, Port 2, Port 3, and Port 4: <ul style="list-style-type: none"> <li>◦ management</li> <li>◦ downlink</li> </ul> </li> <li>• Ports 5 and higher: <ul style="list-style-type: none"> <li>◦ uplink</li> <li>◦ downlink</li> <li>◦ site_sync</li> <li>◦ ssm_sync</li> </ul> </li> </ul> </li> <li>■ You cannot change the "ssm_sync" type of the dedicated Internal Synchronization port: <ul style="list-style-type: none"> <li>• MHO-175 - Port 32</li> <li>• MHO-170 - Port 32</li> <li>• MHO-140 - Port 48</li> </ul> </li> </ul>

**Example 1 - Viewing all available ports**

```
MHO> set maestro port [press the TAB key]
1/42/1 1/48/1 1/43/1 1/55/1 1/56/1 1/49/1 1/51/1 1/24/1 1/25/1
1/26/1 1/27/1 1/20/1 1/21/1 1/22/1 1/23/1 1/46/1 1/47/1 1/44/1
1/45/1 1/28/1 1/29/1 1/40/1 1/41/1 1/1/1 1/3/1 1/2/1 1/5/1
1/4/1 1/7/1 1/6/1 1/9/1 1/8/1 1/50/1 1/39/1 1/38/1 1/54/1
1/11/1 1/10/1 1/13/1 1/12/1 1/15/1 1/14/1 1/17/1 1/16/1 1/19/1
1/18/1 1/31/1 1/30/1 1/37/1 1/36/1 1/35/1 1/34/1 1/33/1 1/52/1
1/32/1 1/53/1
MHO>
```

**Example 2 - Changing the port administrative state**

```
MHO> set maestro port 1/20/1 admin-state down
You are about to perform "set maestro port 1/20/1 admin-state
down"
Action might lead to traffic impact

Are you sure? (Y - yes, any other key - no) y
Successfully set port 20 admin-state to down
MHO>
```

**Example 3 - Changing the port MTU**

```
MHO> set maestro port 1/20/1 mtu 10236
You are about to perform "set maestro port 1/20/1 mtu 10236"
Action might lead to traffic impact

Are you sure? (Y - yes, any other key - no) y
Successfully set port 20 mtu to 10236
MHO>
```

**Example 4 - Changing the port QSFP mode**

```
MHO> set maestro port 1/20/1 qsfp-mode 10G
You are about to perform "set maestro port 1/20/1 qsfp-mode 10G"
Action might lead to traffic impact

Are you sure? (Y - yes, any other key - no) y
Successfully set port 20 qsfp-mode to 10G success
MHO>
```

## Example 5 - Changing the port type

```
MHO> set maestro port 1/20/1 type uplink
You are about to perform "set maestro port 1/20/1 type uplink"
Are you sure? (Y - yes, any other key - no) y

"set maestro port 1/20/1 type uplink" requires auditing
Enter your full name: johndoe
Enter reason for "set maestro port 1/20/1 type uplink" [Maintenance]: test
WARNING: "set maestro port 1/20/1 type uplink", User: johndoe, Reason: test
Are you sure? (Y - yes, any other key - no) y

Successfully set port 1/20/1 type to uplink
MHO>
MHO> exit
[Expert@MHO:0]#
```

## Example 6 - Changing the port type with automatic confirmation

```
MHO> set maestro port 1/20/1 type uplink no-confirmation
You are about to perform "set maestro port 1/20/1 type uplink no-confirmation"
Are you sure? (Y - yes, any other key - no) y

"set maestro port 1/20/1 type uplink no-confirmation" requires auditing
Enter your full name: johndoe
Enter reason for "set maestro port 1/20/1 type uplink no-confirmation" [Maintenance]: test
WARNING: "set maestro port 1/20/1 type uplink no-confirmation", User: johndoe, Reason: test

Successfully set port 1/20/1 type to uplink
MHO>
MHO> exit
[Expert@MHO:0]#
```

## Viewing the Port Settings

### Description

These commands show the configured settings on the Quantum Maestro Orchestrator's ports.

### Syntax

```
show maestro port <Port ID>
  admin-state
  mtu
  optic-info
  qsfp-mode
  type
  vlans
```

## Parameters

Parameter	Description
<code>&lt;Port ID&gt;</code>	<p>Specifies the port to configure. The format is three numbers separated with a slash: <code>&lt;Quantum Maestro Orchestrator ID&gt;/&lt;Port Label&gt;/&lt;Port Split ID&gt;</code></p> <p>Examples:</p> <ul style="list-style-type: none"> <li>▪ 1/3/1</li> <li>▪ 2/6/1</li> </ul> <p>Notes:</p> <ul style="list-style-type: none"> <li>▪ If the port is not split with a breakout cable, then the default value of the <code>&lt;Port Split ID&gt;</code> is 1.</li> <li>▪ To see the available Port IDs, press the <b>Tab</b> key.</li> <li>▪ To see the Port IDs and the names Gaia OS assigned to them, connect to the Gaia Portal on the Quantum Maestro Orchestrator and click <b>Orchestrator</b> page. For the default mapping, see the <a href="#">Quantum Maestro Getting Started Guide</a> &gt; Section <i>Quantum Maestro Orchestrator Ports and Gaia OS Interfaces</i>.</li> </ul>
<code>admin-state</code>	<p>Shows the port administrative state:</p> <ul style="list-style-type: none"> <li>▪ up - Enabled</li> <li>▪ down - Disabled</li> </ul>
<code>mtu</code>	Shows the port MTU.
<code>optic-info</code>	Shows the information about the QSFP transceiver.
<code>qsfp-mode</code>	<p>Shows the QSFP mode:</p> <ul style="list-style-type: none"> <li>▪ 1G - Port works with the 1 GbE speed (only 10 GbE ports support this mode).</li> <li>▪ 10G - Port works with the 10 GbE speed.</li> <li>▪ 4x10G - Split of a 40 GbE port into four ports that work with the 10 GbE speed each.</li> <li>▪ 4x25G - Split of a 100 GbE port into four ports that work with the 25 GbE speed each.</li> <li>▪ 25G - Port works with the 25 GbE speed.</li> <li>▪ 40G - Port works with the 40 GbE speed.</li> <li>▪ 100G - Port works with the 100 GbE speed.</li> </ul>

Parameter	Description
type	<p>Shows the port type:</p> <ul style="list-style-type: none"> <li>▪ uplink - Connects to external and internal production networks</li> <li>▪ downlink - Connects to Check Point Security Appliances</li> <li>▪ management - Connects to a Management Server that manages the applicable Security Group</li> <li>▪ site_sync - External synchronization in Dual Site deployment - between peer Orchestrators on different sites</li> <li>▪ ssm_sync - Internal synchronization in Dual Site deployment - between peer Orchestrators on the same site</li> </ul>
vlan	Shows the VLAN IDs configured on this port.

### Example 1 - Viewing all available ports

```
MHO> show maestro port [TAB]
1/42/1 1/48/1 1/43/1 1/55/1 1/56/1 1/49/1 1/51/1 1/24/1 1/25/1
1/26/1 1/27/1 1/20/1 1/21/1 1/22/1 1/23/1 1/46/1 1/47/1 1/44/1
1/45/1 1/28/1 1/29/1 1/40/1 1/41/1 1/1/1 1/3/1 1/2/1 1/5/1
1/4/1 1/7/1 1/6/1 1/9/1 1/8/1 1/50/1 1/39/1 1/38/1 1/54/1
1/11/1 1/10/1 1/13/1 1/12/1 1/15/1 1/14/1 1/17/1 1/16/1 1/19/1
1/18/1 1/31/1 1/30/1 1/37/1 1/36/1 1/35/1 1/34/1 1/33/1 1/52/1
1/32/1 1/53/1
MHO>
```

### Example 2 - Viewing the port administrative state

```
MHO> show maestro port 1/4/1 admin-state
Port 1/4/1 admin-state is down
MHO>

MHO> show maestro port 1/27/1 admin-state
Port 1/27/1 admin-state is up
MHO>
```

### Example 3 - Viewing the port MTU

```
MHO> show maestro port 1/27/1 mtu
Port 27 mtu is 10236
MHO>
```



**Example 4 - Viewing the QSFP transceiver information**

```
MHO> show maestro port 1/27/1 optic-info
Port:27
Vendor Name:Gigalight
Serial Number:GE18190022
Part Number:GPP-PC192-3001CP
Check Point Part Number:NIY4471
Enforcement:Supported
Check Point SKU:CPAC-DAC-10G-1M-B
Material ID:320904
Product Type:10GBASE-CU-1M
Speed:10G
MHO>
```

**Example 5 - Viewing the port QSFP mode**

```
MHO> show maestro port 1/27/1 qsfm-mode
Port 27 qsfm-mode is 10G
MHO>
MHO> show maestro port 1/55/1 qsfm-mode
Port 55 qsfm-mode is 100G
MHO>
```

**Example 6 - Viewing the port type**

```
MHO> show maestro port 1/1/1 type
Port 1/4/1 type is management
MHO>
MHO> show maestro port 1/27/1 type
Port 1/27/1 type is downlink
MHO>
MHO> show maestro port 1/55/1 type
Port 1/55/1 type is uplink
MHO>
```

**Example 7 - Viewing the VLAN IDs**

```
MHO> show maestro port 1/20/1 vlans
Port 1/20/1 vlans are: 100 200
MHO>
```

## Viewing the Security Group Settings

### Description

This command shows the Security Group settings on the Quantum Maestro Orchestrator.

### Syntax

```
show maestro security-group id <Security Group ID>
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the Security Group ID. To see the existing IDs, press the <b>Tab</b> key.



**Example**

```
MHO> show maestro security-group id 1
name: 1
- uplinks:
  - eth1-05:
    - physical: Port 1/5/1
  - eth1-Mgmt1:
    - physical: Port 1/1/1
  - eth2-05:
    - physical: Port 2/5/1
- mgmt_ip: 192.168.19.52
- sic_pass: 12345
- hostname: MyGW1
- default_gw: 192.168.19.1
- is_vsx: false
- gateways:
  - 1:
    - serial: 2222222222
    - model: Check Point16000
  - 3:
    - serial: 3333333333
    - model: Check Point16000
  - 2:
    - serial: 4444444444
    - model: Check Point16000
  - 4:
    - serial: 5555555555
    - model: Check Point16000
- mgmt_netmask: 24
MHO>
```

## Step 2 - Configuring Gaia Settings of a Security Group

This section provides instructions for configuring Gaia settings of a Security Group.



### Configuring Gaia Settings of a Security Group in Gaia Portal

Step	Instructions
1	<p>With a web browser, connect to the Gaia Portal of the Security Group:</p> <pre>https://&lt;IP Address of Security Group&gt;</pre> <p> <b>Important</b> - This connection goes through the Quantum Maestro Orchestrator's management interface you assigned to this Security Group.</p>
2	<p>Log in with these default credentials:</p> <ul style="list-style-type: none"> <li>▪ Username - admin</li> <li>▪ Password - admin</li> </ul>
3	<p>Change the default Gaia password to a new password:</p> <ol style="list-style-type: none"> <li>a. From the left tree, click <b>User Management &gt; Users</b>.</li> <li>b. Select the <b>admin</b> user.</li> <li>c. Click <b>Reset Password</b>.</li> <li>d. Enter the new password.</li> <li>e. Click <b>OK</b>.</li> </ol>
4	<p>From the left tree, click <b>Network Management &gt; Network Interfaces</b>.</p>
5	<p>Configure the applicable settings (for example, create a Bond or a VLAN interface) and IP addresses for the Uplink ports.</p> <p> <b>Important</b> - In VSX mode, you must configure all IP addresses in SmartConsole only.</p>
6	<p>Configure other applicable Gaia settings. For example: Time Zone, DNS servers, Proxy server, Static Routes.</p>

For more information, see the [R81.20 Gaia Administration Guide](#).

### Configuring Gaia Settings of a Security Group in Gaia gClish

 **Note** - The commands you run in the Gaia gClish apply to all Security Appliances in this Security Group.

Step	Instructions
1	<p>Connect to the command line of the Security Group over SSH at <i>&lt;IP Address of Security Group&gt;</i>.</p> <p>When you log in, the Gaia gClish opens by default.</p> <p> <b>Important</b> - This connection goes through the Quantum Maestro Orchestrator's management interface you assigned to this Security Group.</p>
2	<p>Log in with these default credentials:</p> <ul style="list-style-type: none"> <li>▪ Username - admin</li> <li>▪ Password - admin</li> </ul>
3	<p>Change the default Gaia password to a new password:</p> <pre style="border: 1px solid black; padding: 5px;">set user admin password</pre>
4	<p>Configure the applicable settings (for example, create a Bond or a VLAN interface) and IP addresses for the Uplink ports.</p> <p> <b>Important</b> - In VSX mode, you must configure all IP addresses in SmartConsole only.</p>
5	<p>Configure other applicable Gaia settings.</p> <p>For example: Time Zone, DNS servers, Proxy server, Static Routes.</p>

For more information, see:

- [R81.20 Gaia Administration Guide](#)
- ["Connecting to a Specific Security Group Member \(member\)" on page 140](#)

# Step 3 - Configuration in SmartConsole


## Configuring a Security Gateway object and its policy

### 1. Create one Security Gateway object

You can configure a Security Gateway object in SmartConsole in one of these modes - **Wizard Mode**, or **Classic Mode**:


#### Configuring a Security Gateway object in SmartConsole in Wizard Mode

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new Security Gateway object in one of these ways: <ul style="list-style-type: none"> <li>▪ From the top toolbar, click <b>New (*) &gt; Gateway</b>.</li> <li>▪ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; New Gateway</b>.</li> <li>▪ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Gateway</b>.</li> </ul>
4	In the <b>Check Point Security Gateway Creation</b> window, click <b>Wizard Mode</b> .
5	On the <b>General Properties</b> page: <ol style="list-style-type: none"> <li>a. In the <b>Gateway name</b> field, enter a name for this Security Gateway object.</li> <li>b. In the <b>Gateway platform</b> field, select <b>Maestro</b>.</li> <li>c. In the <b>Gateway IP address</b> section, enter the same IPv4 address that you configured for the Security Group on the Quantum Maestro Orchestrator.</li> <li>d. Click <b>Next</b>.</li> </ol>
6	On the <b>Trusted Communication</b> page: <ol style="list-style-type: none"> <li>a. Select <b>Initiate trusted communication now</b>, enter the same Activation Key you entered in the <b>First Time Wizard settings</b> of the Security Group on the Quantum Maestro Orchestrator.</li> <li>b. Click <b>Next</b>.</li> </ol>

Step	Instructions
7	<p>On the <b>End</b> page:</p> <ol style="list-style-type: none"> <li>Examine the <b>Configuration Summary</b>.</li> <li>Select <b>Edit Gateway properties for further configuration</b>.</li> <li>Click <b>Finish</b>.</li> </ol> <p><b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
8	<p>On the <b>Network Security</b> tab, enable the desired Software Blades.</p> <p> <b>Important</b> - Do not select anything on the <b>Management</b> tab.</p>
9	Click <b>OK</b> .
10	Publish the SmartConsole session.

### Configuring a Security Gateway object in SmartConsole in Classic Mode

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>▪ From the top toolbar, click <b>New (*) &gt; Gateway</b>.</li> <li>▪ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; New Gateway</b>.</li> <li>▪ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Gateway</b>.</li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b>.</p> <p><b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
5	In the <b>Name</b> field, enter a name for this Security Gateway object.
6	In the <b>IPv4 address</b> and <b>IPv6 address</b> fields, enter the same IPv4 address that you configured for the Security Group on the Quantum Maestro Orchestrator.

Step	Instructions
7	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group:</p> <ol style="list-style-type: none"> <li>Near the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>In the <b>Platform</b> field, select <b>Open server / Appliance</b>.</li> <li>In the <b>Activation Key</b> field, enter the same Activation Key you entered in the <b>First Time Wizard settings</b> of the Security Group on the Quantum Maestro Orchestrator.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>OK</b>.</li> </ol>
8	<p>In the <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>In the <b>Hardware</b> field, select <b>Maestro</b>.</li> <li>In the <b>Version</b> field, select <b>R80.20SP</b>.</li> <li>In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
9	<p>On the <b>Network Security</b> tab, enable the desired Software Blades.</p> <p> <b>Important</b> - Do not select anything on the <b>Management</b> tab.</p>
10	Click <b>OK</b> .
11	Publish the SmartConsole session.

For more information, see the [R81.20 Security Management Administration Guide](#).

## 2. Configure a Security Policy in SmartConsole

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click <b>Security Policies</b> .



Step	Instructions
3	Create a new policy and configure the applicable layers: <ol style="list-style-type: none"> <li>At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>Click <b>Close</b>.</li> <li>On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>
4	Create the applicable Access Control Policy.
6	Create the applicable Threat Prevention Policy.
7	Publish the SmartConsole session.

For more information, see:

- [R81.20 Security Management Administration Guide](#)
- [R81.20 Threat Prevention Administration Guide](#)
- Applicable *Administration Guides* on the [R81.20 Home Page](#).


### 3. Install the Security Policy in SmartConsole

Step	Instructions
1	Install the Access Control Policy on the Security Gateway object: <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable policy for this Security Gateway object.</li> <li>Select only the Access Control Policy.</li> <li>Click <b>Install</b>.</li> </ol>
2	Install the Threat Prevention Policy on the Security Gateway object: <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable policy for this Security Gateway object.</li> <li>Select only the Threat Prevention Policy.</li> <li>Click <b>Install</b>.</li> </ol>

## Configuring a VSX Gateway object and its policies

## 1. Configure a VSX Gateway object in SmartConsole

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server or <i>Main Domain Management Server</i> that should manage this Security Group.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new VSX Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>▪ From the top toolbar, click <b>New (*) &gt; VSX &gt; Gateway</b>.</li> <li>▪ In the top left corner, click <b>Objects menu &gt; More object types &gt; Network Object &gt; Gateways and Servers &gt; VSX &gt; New Gateway</b>.</li> <li>▪ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; VSX &gt; Gateway</b>.</li> </ul> <p>The <b>VSX Gateway Wizard</b> opens.</p>
4	<p>On the <b>VSX Gateway General Properties (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>a. In the <b>Enter the VSX Gateway Name</b> field, enter the desired name for this VSX Gateway object.</li> <li>b. In the <b>Enter the VSX Gateway IPv4</b> field, enter the same IPv4 address that you configured on the <b>Management Connection</b> page of the VSX Gateway's First Time Configuration Wizard.</li> <li>c. In the <b>Enter the VSX Gateway IPv6</b> field, enter the same IPv6 address that you configured on the <b>Management Connection</b> page of the VSX Gateway's First Time Configuration Wizard.</li> <li>d. In the <b>Select the VSX Gateway Version</b> field, select <b>R80.20SP</b>.</li> <li>e. Click <b>Next</b>.</li> </ol>
5	<p>On the <b>Virtual Systems Creation Templates (Select the Creation Template most suitable for your VSX deployment)</b> page:</p> <ol style="list-style-type: none"> <li>a. Select the applicable template.</li> <li>b. Click <b>Next</b>.</li> </ol>

Step	Instructions
6	<p>On the <b>VSX Gateway General Properties (Secure Internal Communication)</b> page:</p> <ol style="list-style-type: none"> <li>In the <b>Activation Key</b> field, enter the same Activation Key you entered in the <b>First Time Wizard settings</b> of the Security Group on the Quantum Maestro Orchestrator.</li> <li>In the <b>Confirm Activation Key</b> field, enter the same Activation Key again.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>Next</b>.</li> </ol>
7	<p>On the <b>VSX Gateway Interfaces (Physical Interfaces Usage)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the list of the interfaces - it must show all the Uplink ports you assigned to this Security Group.</li> <li>If you plan to connect more than one Virtual System directly to the same Uplink port, you must select <b>VLAN Trunk</b> for that physical Uplink port.</li> <li>Click <b>Next</b>.</li> </ol>
8	<p>On the <b>Virtual Network Device Configuration (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>You can select <b>Create a Virtual Network Device</b> and configure the first desired Virtual System at this time (we recommend to do this later).</li> <li>Click <b>Next</b>.</li> </ol>
9	<p>On the <b>VSX Gateway Management (Specify the management access rules)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the default access rules.</li> <li>Select the applicable default access rules.</li> <li>Configure the applicable source objects, if needed.</li> <li>Click <b>Next</b>.</li> </ol> <p> <b>Important</b> - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.</p>
10	<p>On the <b>VSX Gateway Creation Finalization</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Finish</b> and wait for the operation to finish.</li> <li>Click <b>View Report</b> for more information.</li> <li>Click <b>Close</b>.</li> </ol>

Step	Instructions
11	Examine the VSX configuration: <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Log in to the Expert mode.</li> <li>Run:               <div data-bbox="549 405 1460 468" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>vsx stat -v</pre> </div> </li> </ol>
12	Open the VSX Gateway object.
13	On the <b>General Properties</b> page, click the <b>Network Security</b> tab.
14	Enable the desired Software Blades for the VSX Gateway object itself (context of VS0). Refer to: <ul style="list-style-type: none"> <li>▪ <a href="#">sk79700: VSX supported features on R75.40VS and above</a></li> <li>▪ <a href="#">sk106496: Software Blades updates on VSXR75.40VS and above - FAQ</a></li> <li>▪ Applicable <i>Administration Guides</i> on the <a href="#">R81.20 Home Page</a></li> </ul>
15	Click <b>OK</b> to push the updated VSX Configuration. Click <b>View Report</b> for more information.
16	Examine the VSX configuration: <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Log in to the Expert mode.</li> <li>Run:               <div data-bbox="549 1256 1460 1319" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>vsx stat -v</pre> </div> </li> </ol>
17	Install policy on the VSX Gateway object: <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the default policy for this VSX Gateway object.                This policy is called:               <div data-bbox="549 1570 1460 1632" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <pre>&lt;Name of VSX Gateway object&gt;_VSX</pre> </div> </li> <li>Click <b>Install</b>.</li> </ol>

Step	Instructions
18	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"><li>Connect to the command line on the Security Group.</li><li>Log in to the Expert mode.</li><li>Run:</li></ol> <pre data-bbox="549 405 1460 468">vsx stat -v</pre>

## 2. Configure Virtual Systems and their Security Policies in SmartConsole

Step	Instructions
1	Connect with the SmartConsole to the Security Management Server, or each <i>Target</i> Domain Management Server that should manage each Virtual System.
2	Configure the desired Virtual Systems on this Security Group.
3	Create the applicable Access Control Policy for these Virtual Systems.
4	Create the applicable Threat Prevention Policy for these Virtual Systems.
5	Publish the SmartConsole session.
6	Install the configured Security Policies on these Virtual Systems.
7	Install the Access Control Policy on these Virtual Systems: <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable policy for the Virtual System object.</li> <li>Select only the Access Control Policy.</li> <li>Click <b>Install</b>.</li> </ol>
8	Install the Threat Prevention Policy on these Virtual Systems: <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable policy for the Virtual System object.</li> <li>Select only the Threat Prevention Policy.</li> <li>Click <b>Install</b>.</li> </ol>
9	Examine the VSX configuration: <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Log in to the Expert mode.</li> <li>Run:               <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>vsx stat -v</pre> </div> </li> </ol>

For more information, see:

- [R81.20 Security Management Administration Guide](#)
- [R81.20 VSX Administration Guide](#)
- Applicable *Administration Guides* on the [R81.20 Home Page](#)

## Step 4 - License Installation

1. Quantum Maestro Orchestrators do not require a license.
2. Generate a Security Gateway license for each Security Appliance you connect to a Quantum Maestro Orchestrator.

### Procedure

Prepare this summary table for all Security Appliances:

Appliance	IPv4 Address of Sync interface (License IP Address)	MAC Address of Mgmt interface (License CK)
Your description	IPv4 Address of the <b>Sync</b> interface on this appliance	MAC Address of the <b>Mgmt</b> interface on this appliance

Steps:

Step	Instructions
A	Connect to the command line on each Security Appliance.
B	Log in to the Expert mode.
C	Get the <b>IPv4 Address</b> of the <b>Sync</b> interface (copy the value of "inet addr"): <b>Note</b> - You must generate the license for this IPv4 address. <pre>ifconfig Sync   head -n 2</pre>
D	Get the <b>MAC Address</b> of the <b>Mgmt</b> interface (copy the value of "HWaddr"): <b>Note</b> - When you generate the license, you must use this MAC Address as the license CK. <pre>ifconfig Mgmt   grep Mgmt</pre>
E	Generate the license as described in <a href="#">sk163323</a> .

3. If the applicable license exists in the License Repository on the Check Point Management Server, it installs the licenses automatically.
  - If the Check Point Management Server is connected to the Internet, it pulls the licenses from the User Center.




- If the Check Point Management Server is **not** connected to the Internet, then follow the procedures below.

 **Note** - In Dual Site, these steps install the licenses on all sites automatically.

### Part 1 - Install the license on the Security Group Member that runs as the Single Management Object (SMO)

Step	Instructions
A	Connect to the command line on the Security Group.
B	Log in to the Expert mode.
C	Get the IP address of the Sync interface on the SMO: <pre>asg_blade_config get_smo_ip</pre>
D	Install the license for the IPv4 address of the SMO <b>192.0.2.X</b> (see "Notes" below): <pre>cplic put &lt;applicable string&gt;</pre>
E	Make sure the license is installed: <pre>g_cplic print</pre>

### Part 2 - Install the license on a specific Security Group Member that is not the SMO

 **Important** - You must follow these steps for **each** Security Appliance in the Security Group.

Step	Instructions
A	Connect to the Gaia OS of the Security Group or Quantum Maestro Orchestrator.
B	Log in to the Expert mode.
C	Connect to a specific Security Appliance with this command: <pre>member &lt;Security Group ID&gt; &lt;Member ID&gt;</pre> <p>See <a href="#">"Connecting to a Specific Security Group Member (member)" on page 140</a></p>
D	Get the IPv4 Address of the Sync interface: <pre>ifconfig Sync   head -n 2</pre>

Step	Instructions
E	<p>Install the license for the IPv4 address of the Sync interface <b>192.0.2.X</b> on this specific appliance (see "Notes" below):</p> <pre>cplic put &lt;applicable string&gt;</pre>
F	<p>Create a copy of the <code>\$CPDIR/conf/cp.license</code> file:</p> <pre>cp -v \$CPDIR/conf/cp.license /var/log/cp.license.copy</pre>
G	<p>Make sure the copy of the license file is the same as the original license file:</p> <pre>md5sum \$CPDIR/conf/cp.license /var/log/cp.license.copy</pre>
H	<p>Transfer the copy of the license file from this Security Group Member to the SMO:</p> <pre>asg_cp2blades -b 1_01 /var/log/cp.license.copy</pre>
I	<p>Delete all data from the current license file <code>\$CPDIR/conf/cp.license</code> on this Security Group Member:</p> <pre>cat \$CPDIR/conf/cp.license echo &gt; \$CPDIR/conf/cp.license cat \$CPDIR/conf/cp.license</pre>
J	<p>Connect to the Security Group Member that runs as SMO:</p> <pre>member &lt;Security Group ID&gt; &lt;SMO Member ID&gt;</pre>
K	<p>Add the content of the license file you copied earlier from a specific Security Group Member to the license file on the SMO:</p> <pre>cat \$CPDIR/conf/cp.license cat /var/log/cp.license.copy &gt;&gt; \$CPDIR/conf/cp.license cat \$CPDIR/conf/cp.license</pre>
L	<p>Wait for at least 6 minutes.</p>

Step	Instructions
M	<p data-bbox="507 241 1406 309">Make sure the license is installed on the specific Security Group Member:</p> <pre data-bbox="512 322 1460 383">g_cplic print</pre>

 **Notes:**


- Check Point User Center sends you an email with the full "cplic put" command.  
You can also see the full syntax in the generated license details in the User Center.
- On the Management Server, each Security Group is one Security Gateway object.  
Therefore, each Security Group consumes a Management license of one Security Gateway.

# Step 5 - Special Configuration Scenarios

This section contains special configuration scenarios:

- Weights for Security Group Members when different models of Security Appliances are assigned to the same Security Group
- Bond interfaces
- VLAN interfaces
- Bridge Mode

## Configuring Weights for Security Group Members

 **Note** - Do not confuse this section with "[Configuring Security Group High Availability](#)" on page 374 that is related to the hardware monitoring.

### Introduction

Starting in R81.10, you can assign different models of Security Appliances (mix of appliance models) to the same Security Group - see [sk162373](#).

To make sure all Security Group Members are loaded as equally as possible, you can configure relative weights to Security Group Members.

As a result, traffic is distributed between the Security Group Members according to these relative weights.

### Limitations

- In R81.20, it is not supported to configure Auto Scaling Settings if a Maestro Security Group contains different Appliance models.
- If a Security Group contains Security Appliance of different models, you must disable the SMO Image Cloning in the Security Group (Known Limitation PMTR-71298) in Gaia gClish:

```
set smo image auto-clone state off
show smo image auto-clone state
```

## Calculating the Security Group Member Weight

### Default Weight for each Security Group Member:

$$\frac{\text{Number of CPU Cores on this Security Group Member}}{\text{Total Number of CPU Cores on all Security Group Members}} \times 100\%$$


### Custom Weight for a Security Group Member:

$$\frac{\text{Local Weight of this Security Group Member}}{\text{Sum of all Weights of all Security Group Members}} \times 100\%$$

### Examples for a Security Group that has three Security Group Members - M1, M2, and M3:

Required Traffic Assignment	Configuration Workflow
M3 - 15% M2 - 15% M1 - 70%	M3 - assign a number between 0 and 512 M2 - assign the same number you assigned to M3 M1 - assign the number that is 7-fold of the number assigned to M2 / M3
M3 - 10% M2 - 10% M1 - 80%	M3 - assign the same number between 0 and 512 M2 - assign the same number you assigned to M3 M1 - assign the number that is 8-fold of the number assigned to M2 / M3
M3 - 10% M2 - 20% M1 - 70%	M3 - assign a number between 0 and 512 M2 - assign the number that is 2-fold of the number assigned to M3 M1 - assign the number that is 7-fold of the number assigned to M3

## Configuring the Security Group Member Weights

Step	Instructions
1	Connect to the command line on the Security Group.
2	If your default shell is <code>/etc/bash</code> (Expert mode), then go to Gaia gClish: <pre>gclish</pre>
3	Configure the required weight: <pre>set smo security-group sgm-weight id &lt;SGM IDs&gt; weight {default   0-512}</pre>
4	Apply the new configuration: <pre>set smo security-group sgm-weight apply</pre> <p> <b>Important</b> - As a result of the calculation, some connections might move between the Security Group Members.</p>

### Parameters:

Parameter	Description
<code>sgm-weight id &lt;SGM IDs&gt;</code>	Applies to Security Group Members as specified by the <code>&lt;SGM IDs&gt;</code> . <code>&lt;SGM IDs&gt;</code> can be: <ul style="list-style-type: none"> <li>▪ No <code>&lt;SGM IDs&gt;</code> specified, or <code>all</code> Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, <code>1_1</code>)</li> </ul>
<code>weight {default   0-512}</code>	Specifies the weight.

## Monitoring the Security Group Member Weights

Step	Instructions
1	Connect to the command line on the Security Group.
2	If your default shell is <code>/etc/bash</code> (Expert mode), then go to Gaia gClish: <pre>gclish</pre>
3	Examine the weights: <pre>show smo security-group sgm-weight &lt;SGM IDs&gt;</pre>

### Example 1:

```
[Global] HostName-ch01-01> show smo security-group sgm-weight all
SGM weights are:
1_01: 8 (33.33%)
1_02: 16 (66.67%)
[Global] HostName-ch01-01>
```

### Example 2:

```
[Global] HostName-ch01-01> show smo security-group sgm-weight 1_2
SGM 1_2 weight is: 16 (66.67%)
[Global] HostName-ch01-01>
```

## Best Practices

- Do **not** assign Security Appliance models that differ significantly in their CPU power to the same Security Group.
- In Dual Site, use the same Security Appliance models for the same Security Group Members on each site.

Example:

- Security Group Member with ID 1 on Site 1 (1\_1) and Security Group Member with ID 1 on Site 2 (2\_1) should be the same.
  - Security Group Member with ID 2 on Site 1 (1\_2) and Security Group Member with ID 2 on Site 2 (2\_2) should be the same.
- If you assign different models of Security Appliances to the same Security Group, then all Security Group Members have the same number of CoreXL Firewall instances (`fw_worker`).

By default, the number of CoreXL Firewall instances is configured according to the SMO Security Group Member.

We recommend the maximal number of CoreXL Firewall instances in the Security Group does not exceed this number:

```
2 x (Number of CPU cores on the weakest Security Group Member)
```



## Configuring Bond Interface on the Management Ports

**Important** - If this Security Group is configured in VSX mode, follow this workflow:

1. In Gaia gClish, temporarily disable the VSX mode:

```
set vsx off
```

2. Configure a Bond Interface on the Management Ports as described below.
3. In Gaia gClish, enable the VSX mode:

```
set vsx on
```

### Use Case - Creating a New Security Group from Scratch

**Note** - You can perform Steps 2 - 5 in either Gaia Portal (see "[Configuring Security Groups in Gaia Portal](#)" on page 44), or Gaia Clish (see "[Configuring Security Groups in Gaia Clish](#)" on page 57).

Step	Instructions
1	Connect to one of the Quantum Maestro Orchestrators.
2	Create a new Security Group: <ol style="list-style-type: none"> <li>a. In the <b>Network settings</b> section, enter a dummy IP address configuration.</li> <li>b. Do not configure the <b>First Time Wizard settings</b>.</li> </ol>
3	Assign two available management interfaces <code>ethM-MgmtX</code> and <code>ethN-MgmtY</code> to the Security Group.
4	Assign the applicable Security Appliances to the Security Group.
5	Assign the applicable Uplink ports to the Security Group.
6	Connect through the console port to the Security Appliance with Member ID 1 in this Security Group.
7	Log in to the Expert mode.
8	Go to the Gaia gClish: <pre>gclish</pre>
9	Check which <code>eth#-Mgmt#</code> interface has the IP address you assigned to the Security Group. In our example, we assume it is <code>ethM-MgmtX</code> .

Step	Instructions
10	Add a new Bonding group with this syntax: <pre>add bonding group &lt;Bond ID&gt; mgmt</pre>
11	Add the free <code>ethN-MgmtY</code> interface (without an IP address) to the bonding group with this syntax: <pre>add bonding group &lt;Bond ID&gt; mgmt interface ethN-MgmtY</pre>
12	Assign the real IP address (you wish to use for this Security Group) to the Bonding group with this syntax: <pre>set interface magg&lt;Bond ID&gt; ipv4-address &lt;Real IPv4 Address&gt; mask-length &lt;Mask Length&gt;</pre>
13	Set the Bonding group as the new Gaia Management Interface: <pre>set management interface magg&lt;Bond ID&gt;</pre>
14	Delete the dummy IP address from the <code>ethM-MgmtX</code> interface: <pre>delete interface ethM-MgmtX ipv4-address</pre>
15	Add the free <code>ethM-MgmtX</code> interface (without an IP address) to the bonding group with this syntax: <pre>add bonding group &lt;Bond ID&gt; mgmt interface ethM-MgmtX</pre>
16	Connect to one of the Quantum Maestro Orchestrators.
17	Make sure the Security Group settings are correct.
18	In a web browser, connect to the Management IP address of the Security Group and complete the First Time Configuration Wizard manually.

### Use Case - Editing an Existing Security Group

Step	Instructions
1	Connect to one of the Quantum Maestro Orchestrators.

Step	Instructions
2	<p>Assign a second available management interface <code>ethN-MgmtY</code> to the Security Group.</p> <p>You can perform this step in Gaia Portal (see <a href="#">"Configuring Security Groups in Gaia Portal" on page 44</a>), or Gaia Clish (see <a href="#">"Configuring Security Groups in Gaia Clish" on page 57</a>).</p> <p>In our example, we assume that the interface <code>ethM-MgmtX</code> is already assigned.</p>
3	<p>Connect through the console port to the Security Appliance with Member ID 1 in this Security Group.</p>
4	<p>Log in to the Expert mode.</p>
5	<p>Go to the Gaia gClish:</p> <pre data-bbox="352 779 1460 846">gclish</pre>
6	<p>Change the IP address on the <code>ethM-MgmtX</code> interface to some dummy IP address:</p> <pre data-bbox="352 965 1460 1070">set interface ethM-MgmtX ipv4-address &lt;Dummy IPv4 Address&gt; mask-length &lt;Mask Length&gt;</pre>
7	<p>Add a new Bonding group with this syntax:</p> <pre data-bbox="352 1149 1460 1216">add bonding group &lt;Bond ID&gt; mgmt</pre>
8	<p>Add the free <code>ethN-MgmtY</code> interface (without an IP address) to the bonding group with this syntax:</p> <pre data-bbox="352 1339 1460 1406">add bonding group &lt;Bond ID&gt; mgmt interface ethN-MgmtY</pre>
9	<p>Assign the real IP address to the Bonding group with this syntax:</p> <pre data-bbox="352 1473 1460 1579">set interface magg&lt;Bond ID&gt; ipv4-address &lt;Real IPv4 Address&gt; mask-length &lt;Mask Length&gt;</pre>
10	<p>Set the Bonding group as the new Gaia Management Interface:</p> <pre data-bbox="352 1664 1460 1731">set management interface magg&lt;Bond ID&gt;</pre>
11	<p>Delete the dummy IP address from the <code>ethM-MgmtX</code> interface:</p> <pre data-bbox="352 1798 1460 1865">delete interface ethM-MgmtX ipv4-address</pre>

Step	Instructions
12	<p>Add the free <code>ethM-MgmtX</code> interface (without an IP address) to the bonding group with this syntax:</p> <pre data-bbox="352 320 1461 383">add bonding group &lt;Bond ID&gt; mgmt interface ethM-MgmtX</pre>
13	Connect to one of the Quantum Maestro Orchestrators.
14	Make sure the Security Group settings are correct.
15	<p>In SmartConsole:</p> <ol style="list-style-type: none"><li>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</li><li>Open the Security Gateway object.</li><li>From the left tree, click <b>Network Management</b>.</li><li>Click <b>Get Interfaces &gt; Get Interfaces With Topology</b>.</li><li>Examine the configuration and accept it.</li><li>Click <b>OK</b>.</li><li>Install the applicable Access Control Policy.</li></ol>

## Configuring Bond Interface on Uplink Ports

### 1. Assign the applicable Uplink ports to the applicable Security Group

You perform this step on one of the Quantum Maestro Orchestrators.

You can perform this step in either Gaia Portal, or Gaia Clish of the Quantum Maestro Orchestrator.

#### In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal on one of the Quantum Maestro Orchestrators.
2	Assign the applicable Uplink ports to the applicable Security Group. See <a href="#">"Assigning Interfaces to a Security Group" on page 54</a> .
3	In the bottom left corner, click <b>Apply</b> .


#### In Gaia Clish

Step	Instructions
1	Connect to the command line on one of the Quantum Maestro Orchestrators.
2	Log in to the Gaia Clish.
3	Assign the applicable Uplink ports to the applicable Security Group. See <a href="#">"Assigning One Interface to a Security Group" on page 73</a> .
4	Verify the new configuration. See <a href="#">"Verifying the Configuration Changes" on page 76</a> .
5	Apply the new configuration. See <a href="#">"Applying the Configuration Changes" on page 77</a> .


### 2. Configure the Bond interface on top of the Uplink ports

You can perform this step in either Gaia Portal, or Gaia gClish of the Security Group.

## In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal of the Security Group.
2	Configure the Bond interface on top of the Uplink ports.
3	In Gateway mode only: Assign the IP address to this Bond interface.  <b>Important</b> - In VSX mode, you must assign the IP address in SmartConsole in the VSX Gateway object, or applicable Virtual System object.

## In Gaia gClish

Step	Instructions
1	Connect to the command line of the Security Group.
2	Log in to the Expert mode.
3	Go to the Gaia gClish: <input type="text" value="gclish"/>
4	Configure the Bond interface on top of the Uplink ports.
5	In Gateway mode only: Assign the IP address to this Bond interface.  <b>Important</b> - In VSX mode, you must assign the IP address in SmartConsole in the VSX Gateway object, or applicable Virtual System object.


For more information, see the [R81.20 Gaia Administration Guide](#).

### 3. Configure the Security Gateway or VSX Gateway object in SmartConsole

- If you already created a **Security Gateway** object for this Security Group:

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the applicable Security Gateway object.
4	From the left tree, click <b>Network Management</b> .
5	Click <b>Get Interfaces &gt; Get Interfaces Without Topology</b> .
6	Click <b>OK</b> .
7	Install the Access Control Policy on this Security Gateway object.

- If you already created a **VSX Gateway** object for this Security Group:

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the applicable VSX Gateway object.
4	From the left tree, click <b>Physical Interfaces</b> .
5	Click <b>Add</b> .
6	Add the new interface.  <b>Important</b> - Enter the same name (case sensitive) you see in the Gaia settings of this Security Group.
7	Click <b>OK</b> .
8	Install the Access Control Policy on this VSX Gateway object.
9	Configure the Bond interface in the applicable Virtual System.
10	Install the Access Control Policy on the applicable Virtual System object.

**Note** - For more information, see the [R81.20 VSX Administration Guide](#).

# Configuring VLAN Interfaces on top of a Bond Interface on Uplink Ports

## *In This Section:*

---

Procedure .....	120
Example .....	125

---

This section shows how to configure VLAN Interfaces on top of a Bond Interface that is configured on Uplink Ports.

## Procedure

1. Add the required VLAN tags and assign the Uplink ports to the applicable Security Group

You can perform this step in either Gaia Portal, or Gaia Clish of the Quantum Maestro Orchestrator.

### In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal on one of the Quantum Maestro Orchestrators.
2	Add VLAN tags on the applicable Uplink Ports. See " <a href="#">Configuring Security Groups in Gaia Portal</a> " on page 44.
3	Assign the applicable Uplink ports with VLAN tags to the applicable Security Group. See " <a href="#">Assigning Interfaces to a Security Group</a> " on page 54.
4	In the bottom left corner, click <b>Apply</b> .

### In Gaia Clish

Step	Instructions
1	Connect to the command line on one of the Quantum Maestro Orchestrators.
2	Log in to the Gaia Clish.




Step	Instructions
3	Add VLAN tags on the applicable Uplink Ports. See <a href="#">"Configuring Security Groups in Gaia Clish" on page 57.</a>
4	Assign the applicable Uplink ports to the applicable Security Group. See <a href="#">"Assigning One Interface to a Security Group" on page 73.</a>
5	Verify the new configuration. See <a href="#">"Verifying the Configuration Changes" on page 76.</a>
6	Apply the new configuration. See <a href="#">"Applying the Configuration Changes" on page 77.</a>

## 2. Configure the Bond interface and VLAN interfaces on the Bond interface in the Security Group


You can perform this step in either Gaia Portal, or Gaia gClish of the Security Group.

### In Gaia Portal

Step	Instructions
1	Connect with a web browser to the Gaia Portal of the Security Group.
2	Configure the Bond interface on top of the Uplink ports.
3	Add the same VLAN interfaces on the Bond interface, which you added in the Quantum Maestro Orchestrator.
4	In Gateway mode only: Assign the IP addresses to these VLAN interfaces.  <b>Important</b> - In VSX mode, you must assign the IP addresses in SmartConsole in the VSX Gateway object or applicable Virtual System object.

### In Gaia gClish

Step	Instructions
1	Connect to the command line of the Security Group.
2	Log in to the Expert mode.

Step	Instructions
3	Go to the Gaia gClish: <input type="text" value="gclish"/>
4	Configure the Bond interface on top of the Uplink ports.
5	Add the same VLAN interfaces on the Bond interface, which you added in the Quantum Maestro Orchestrator.
6	In Gateway mode only: Assign the IP addresses to these VLAN interfaces.  <b>Important</b> - In VSX mode, you must assign the IP addresses in SmartConsole in the VSX Gateway object or applicable Virtual System object.

For more information, see the [R81.20 Gaia Administration Guide](#).


### 3. Configure the Security Gateway or VSX Gateway object in SmartConsole

- If you already created a **Security Gateway** object for this Security Group:

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the applicable Security Gateway object.
4	From the left tree, click <b>Network Management</b> .
5	Click <b>Get Interfaces &gt; Get Interfaces Without Topology</b> .
6	Click <b>OK</b> .
7	Install the Access Control Policy on this Security Gateway object.

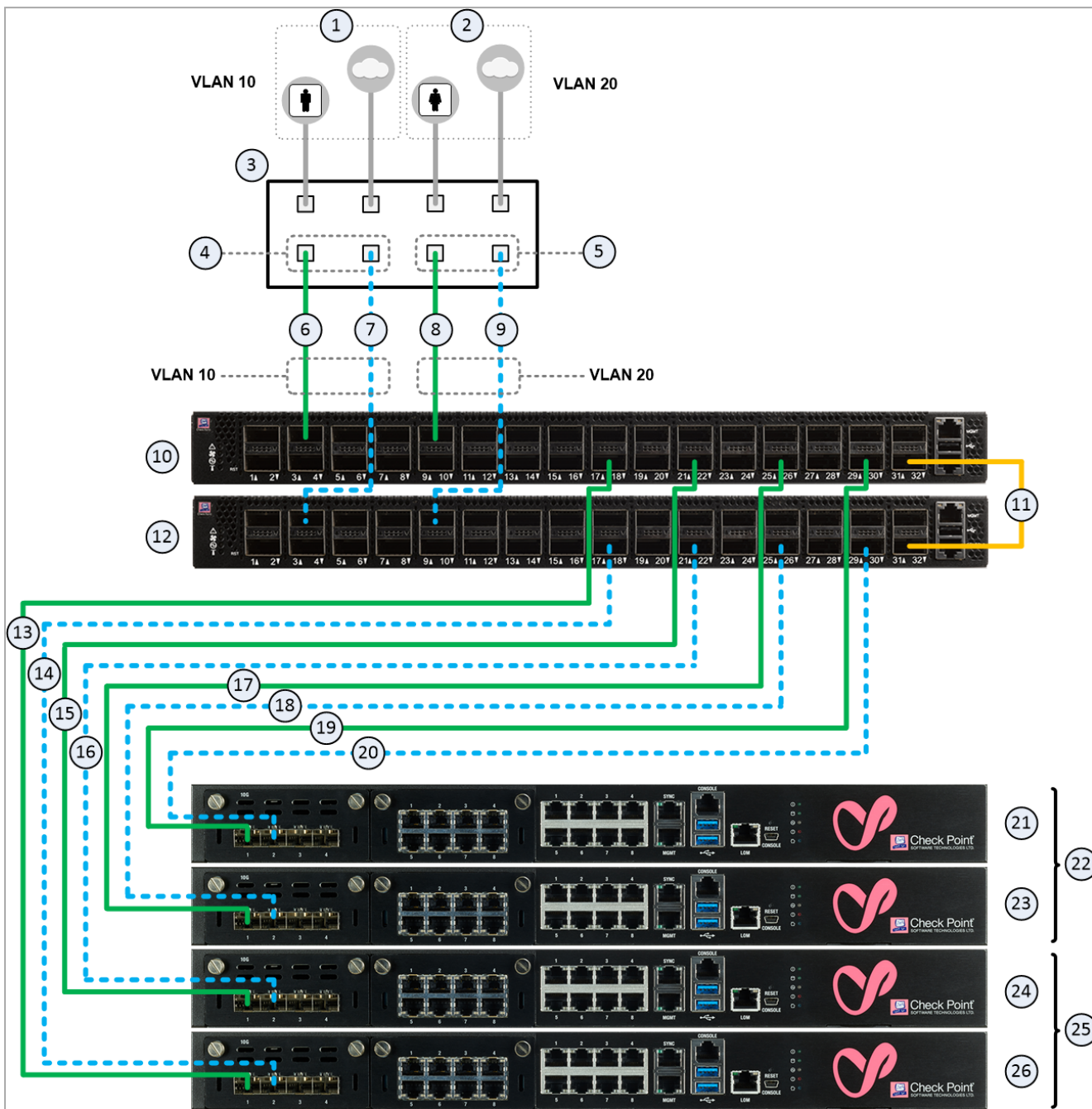
- If you already created a **VSX Gateway** object for this Security Group:

Note - For more information, see the [R81.20 VSX Administration Guide](#).

Step	Instructions
1	Connect with SmartConsole to the Management Server.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the applicable VSX Gateway object.
4	From the left tree, click <b>Physical Interfaces</b> .
5	Click <b>Add</b> .
6	Add the new Bond interface.  <b>Important</b> - Enter the same name (case sensitive) you see in the Gaia settings of this Security Group.
7	In the <b>VLAN Trunk</b> column, check the box for this Bond interface.
8	Click <b>OK</b> .
9	Install the Access Control Policy on this VSX Gateway object.
10	Configure the VLAN interfaces in the applicable Virtual System.
11	Install the Access Control Policy on the applicable Virtual System object.

## Example

This example is based on the default configuration of MHO-170:




## Explanations

Table: Explanations

Item	Description
1	Network 1 in VLAN 10 connected to ports on the Networking Device (3).
2	Network 2 in VLAN 20 connected to ports on the Networking Device (3).
3	Networking Device (router or switch) that connects your Network 1 and Network 2 to the Quantum Maestro Orchestrators (10 and 12) with Bond interfaces (Link Aggregation).
4	Bond interface that connects Network 1 to the Quantum Maestro Orchestrators (10 and 12). This Bond interface provides a redundant Uplink connection for the traffic inspected by the Security Appliances (26 and 24) in the applicable Security Group (25).
5	Bond interface that connects Network 2 to the Quantum Maestro Orchestrators (10 and 12). This Bond interface provides a redundant Uplink connection for the traffic inspected by the Security Appliances (23 and 21) in the applicable Security Group (22).
6	A DAC cable, Fiber cable (with transceivers), or Breakout cable that connects a first slave of the first Bond (4) on the Networking Device (3) to the first Quantum Maestro Orchestrator (10). This cable connects to the Uplink port 3 (interface <code>eth1-05</code> ), which must be configured with the VLAN tag 10.
7	A DAC cable, Fiber cable (with transceivers), or Breakout cable that connects a second slave of the first Bond (4) on the Networking Device (3) to the first Quantum Maestro Orchestrator (12). This cable connects to the Uplink port 3 (interface <code>eth2-05</code> ), which must be configured with the VLAN tag 10.
8	A DAC cable, Fiber cable (with transceivers), or Breakout cable that connects a first slave of the second Bond (5) on the Networking Device (3) to the second Quantum Maestro Orchestrator (10). This cable connects to the Uplink port 9 (interface <code>eth1-17</code> ), which must be configured with the VLAN tag 20.

Table: Explanations (continued)

Item	Description
9	<p>A DAC cable, Fiber cable (with transceivers), or Breakout cable that connects a second slave of the second Bond (5) on the Networking Device (3) to the second Quantum Maestro Orchestrator (12).</p> <p>This cable connects to the Uplink port 9 (interface <code>eth2-17</code>), which must be configured with the VLAN tag 20.</p>
10	First Quantum Maestro Orchestrator.
11	<p>A DAC that connects the dedicated Synchronization ports 32 on the Quantum Maestro Orchestrators (10 and 12).</p> <p> <b>Important</b> - This connection is only used to synchronize the configuration of Security Groups between the Quantum Maestro Orchestrators.</p>
12	Second Quantum Maestro Orchestrator.
13-20	DAC cables, Fiber cables (with transceivers), or Breakout cables that connect Downlink ports on Quantum Maestro Orchestrators to the Security Appliances.
21-23	All Security Appliances assigned to the Security Group 2.
24-26	All Security Appliances assigned to the Security Group 1.

## Example procedure

Step	Instructions
1	<p>Configure the required settings on one of the Quantum Maestro Orchestrators:</p> <ol style="list-style-type: none"> <li>1. Connect to one of the Quantum Maestro Orchestrators.</li> <li>2. Add VLAN tag 10 to the Port 1/3/1 (interface <code>eth1-05</code>).</li> <li>3. Add VLAN tag 10 to the Port 2/3/1 (interface <code>eth2-05</code>).</li> <li>4. Add VLAN tag 20 to the Port 1/9/1 (interface <code>eth1-17</code>).</li> <li>5. Add VLAN tag 20 to the Port 2/9/1 (interface <code>eth2-17</code>).</li> <li>6. Assign the Port 1/3/1 with VLAN tag 10 (interface <code>eth1-05.10</code>) to the Security Group 1.</li> <li>7. Assign the Port 2/3/1 with VLAN tag 10 (interface <code>eth2-05.10</code>) to the Security Group 1.</li> <li>8. Assign the Port 1/9/1 with VLAN tag 20 (interface <code>eth1-17.20</code>) to the Security Group 2.</li> <li>9. Assign the Port 2/9/1 with VLAN tag 20 (interface <code>eth2-17.20</code>) to the Security Group 2.</li> <li>10. Apply the configuration.</li> </ol>
2	<p>Configure the required settings in the Security Group 1:</p> <ol style="list-style-type: none"> <li>1. Connect to the Gaia of the Security Group 1.</li> <li>2. Configure a new interface Bond1 on top of the interfaces <code>eth1-05</code> and <code>eth2-05</code>.</li> <li>3. Add the VLAN tag 10 on top of the new interface Bond1 (<code>bond1.10</code>).</li> </ol>
3	<p>Configure the required settings in the Security Group 2:</p> <ol style="list-style-type: none"> <li>1. Connect to the Gaia of the Security Group 2.</li> <li>2. Configure a new interface Bond1 on top of the interfaces <code>eth1-17</code> and <code>eth2-17</code>.</li> <li>3. Add the VLAN tag 20 on top of the new interface Bond1 (<code>bond1.20</code>).</li> </ol>
4	<p>In SmartConsole, add the new interface (<code>bond1.XX</code>) to the Security Group object.</p>



# Configuring VLAN Interfaces on Uplink Ports

## Introduction

Starting in the R81.10 release for Quantum Maestro Orchestrators, Check Point integrated a major enhancement for the configuration of VLAN interfaces on the Uplink ports of a Quantum Maestro Orchestrator:

- Increased the number of supported VLAN interfaces on an Orchestrator:
  - No limit for each Uplink port.
  - The total supported number of VLAN interfaces is 9000 (more details are below).
- All distribution modes are now supported on Uplink ports.

You can use all VLAN interfaces instead of only General + Layer 4 distribution (see [sk165172](#)).

- All distribution modes are supported on each VLAN interface on an Uplink port, even if the Uplink port allows only specific VLAN interfaces.
- It is **no** longer required to configure the VLAN interfaces on an Orchestrator.

Workflow:

1. Assign the physical interface (e.g., eth1-05) to the applicable Security Group.
2. Configure the applicable IP address on the physical interface (e.g., eth1-05) or VLAN interfaces (e.g., eth1-05.100) on the Security Group.
3. In SmartConsole:
  - a. Open the Security Gateway object for this Security Group.
  - b. From the left tree, click the **Network Management** page.
  - c. Click **Get Interfaces > Get Interfaces Without Topology > click Accept**.
  - d. Configure the topology settings for each interface.
  - e. Install the Access Control Policy on the Security Gateway object.

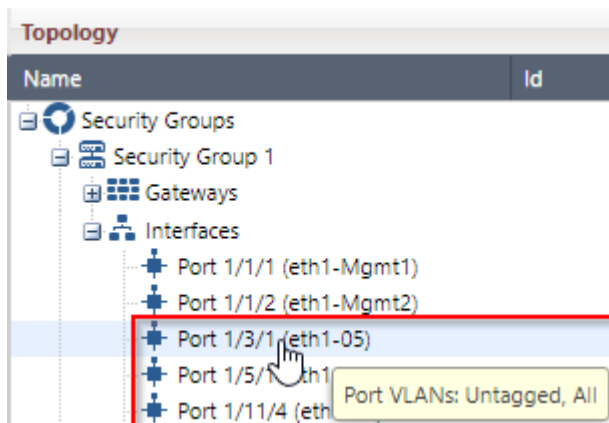
If there are changes in the configuration of the Security Group interfaces (for example, VLAN interfaces or distribution mode), then the Security Group automatically sends these changes to the Orchestrator. The Security Group does so after a policy installation or a manual change in Gaia gClish.

## Viewing VLAN Interfaces on Uplink Ports in Gaia Portal

Step	Instructions
1	On the <b>Orchestrator</b> page, in the <b>Topology</b> section, expand <b>Security Groups</b> .
2	Expand your Security Group.
3	Expand <b>Interfaces</b> .
4	Put the mouse cursor on an interface. VLAN information appears in the tooltip.

**Note** - If this is a Dual Site deployment, and the Security Group contains Security Appliances that are located only at one of the sites (for example, Site 2), then the tooltip that shows VLAN interfaces appears only in Gaia Portal of the Orchestrator (for example, on Site 2) that is located at the same site as Security Appliances.

### Example 1



Port:

- Port 1/3/1 (eth1-05)

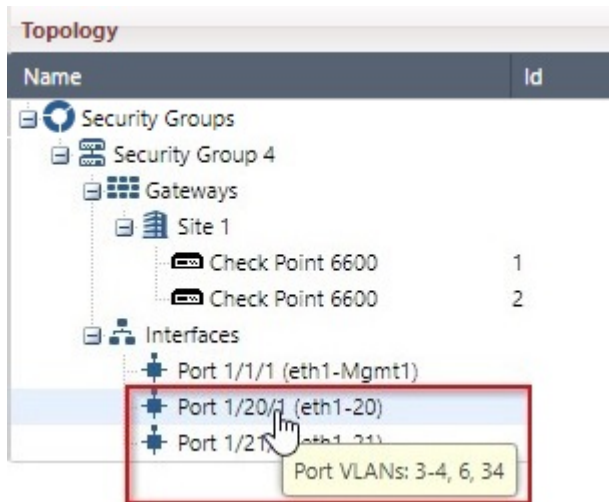
Tooltip:

- Port VLANs: Untagged, All

Explanation:

- The Orchestrator forwards to the Security Group 1 all untagged and all tagged packets that arrive at the Orchestrator port 1/3/1 (eth1-05). This is similar to a VLAN Trunk interface configured to allow all VLAN interfaces.

## Example 2



Port:

- Port 1/20/1 (eth1-20)

Tooltip:

- Port VLANs: 3-4, 6, 34

Explanation:

- The Orchestrator forwards to the Security Group 4 only packets with VLAN tags 3-4, 6, and 34 that arrive at the Orchestrator port 1/20/1 (eth1-20). This is similar to a VLAN Trunk interface configured to allow VLANs 3-4, 6, and 34.

## Viewing VLAN Interfaces on Uplink Ports in Gaia Clish

### Syntax

```
show maestro security-group id <Security Group ID>
```

### Parameters

Parameter	Description
<code>id &lt;Security Group ID&gt;</code>	Specifies the ID of the Security Group. To see the existing IDs, press the <b>Tab</b> key.

## Configuring More Than 4000 VLAN Interfaces on Orchestrators

If it is necessary to configure more than ~4000 VLAN interfaces on the Orchestrator, we recommend that you configure the physical interface on the Orchestrator as a VLAN trunk interface that allows all untagged and all tagged packet to be forwarded to the Security Group. This makes it possible for an internal automatic optimization to occur.

For a VLAN trunk interface to forward all tagged and all untagged packets, these conditions must be met:

- VLAN Trunk mode must be enabled (see the instructions before how to enable the VLAN Trunk mode).
- The distribution mode of all the VLAN interfaces on a specific physical interface must be the same (because this VLAN optimization occurs for each Orchestrator port).

### Example

Physical interface on the Orchestrator - eth1-20

VLAN interfaces - eth1-20.33, eth1-20.44, eth1-20.55, eth1-20.66

Each of these four VLAN interfaces must have the same distribution mode.

If one or more of the VLAN interfaces of this specific base interface (eth1-20) have a different distribution than other VLAN interfaces, the internal automatic optimization is disabled. This is part of the design because the total supported number of VLAN interfaces has a limit.

For example, if the distribution mode of eth1-20.55 is different, then the Orchestrator forwards only the packets with the VLAN tags 33, 44, and 66 are forwarded to the applicable Security Group.

In the above case, automatic optimization occurs (allows all tagged and untagged packets for eth1-20). Therefore, an interface with this optimization is only considered as one VLAN interface out of total supported 9000 VLAN interfaces for this Orchestrator.

This means that when this optimization occurs, the full VLAN range can be used on all the Orchestrator interfaces without the limitation of the total supported VLAN interfaces.

### To enable the VLAN Trunk mode:

#### Warnings:

- Do this procedure during a maintenance window.  
No traffic flows through Security Groups while the 'orchd' process restarts.
- All Orchestrators on your sites must run the same software version.

Step	Instructions
1	Connect to the command line on one of the Orchestrators.
2	Log in to Gaia Clish.
3	<p>Enable the VLAN Trunk mode:</p> <pre data-bbox="316 416 1225 517">set maestro configuration uplink-trunk-mode state enabled</pre>
4	<p>Examine the status of the VLAN Trunk mode:</p> <pre data-bbox="316 598 1225 698">show maestro configuration uplink-trunk-mode state</pre>
5	<p>Restart the Maestro daemon:</p> <ol style="list-style-type: none"><li data-bbox="347 804 1241 878">a. Connect to the command line on <b>each</b> Orchestrator on your sites.</li><li data-bbox="347 887 762 920">b. Log in to the Expert mode.</li><li data-bbox="347 929 778 963">c. Restart the 'orchd' process:<pre data-bbox="395 969 1225 1025">orchd restart</pre></li></ol>

## Shared Uplink Ports

You can assign each uplink interface to multiple Security Groups, with different VLANs assigned to the interface on each Security Group. For example: you can assign eth1-05 to Security Groups 3 and 4, with VLAN interface eth1-05.30 configured on Security Group 3, and VLAN interface eth1-05.40 configured on Security Group 4.

### Prerequisites

1. R81.20 must be installed on the Management Server.
2. R81.20 must be installed on the Maestro Orchestrators.
3. R81.20 must be installed on all Security Appliances in the Security Group.

### Known Limitations

- LACP mode is not supported on a MAGG (bond of Management interfaces), which is shared between different Security Groups.
- Having an LACP bond shared between multiple Security Groups decreases the segregation between these Security Groups.

For example, if Security Group 3 and Security Group 4 share eth1-05 and eth2-05 as subordinates of an LACP bond, and for some reason Security Group 3 stops sending LACP packets to the external switch, then traffic in VLAN interface eth1-05.40 could be affected. Using shared bonds in other bond modes (for example: XOR) does not decrease the segregation.

### Requirements for LACP bond that contains shared interfaces

If a shared uplink interface is part of an LACP bond in a Security Group, then this shared uplink interface must be part of an identical LACP bond in every Security Group to which it is assigned.

Example:

- eth1-05 is assigned to Security Group 3.
- eth1-05 is a subordinate of bond1.30, which is an LACP bond in Security Group 3.
- eth1-05 is assigned to Security Group 4.

In such a scenario, eth1-05 in Security Group 4 must also be part of an LACP bond.

In the configuration example above, this configuration would be **incorrect**:

bond1.30 is an LACP bond in Security Group 3, and it contains eth1-05

bond1.40 is a non-LACP bond in Security Group 4, and it contains eth1-05

Every LACP bond, which contains shared interfaces, must have exactly the same configuration in each Security Group to which it belongs. The LACP bond must have the same subordinate interfaces, and in the same order.

In the configuration example above, if the order of subordinate interfaces in bond1.30 is "eth1-05, eth2-05", then the order of subordinate interfaces in bond1.40 must also be "eth1-05, eth2-05".

## Configuration

### Configuring an LACP bond that contains shared uplink interfaces

To create a bond interface with subordinate interfaces that are shared between Security Groups, the shared uplinks feature must first be enabled on all the Security Groups sharing the bond, using Gaia Clish. Afterwards, the subordinate interfaces in the bond must be added to each Security Group through the Maestro Hyperscale Orchestrator's Gaia Portal or Gaia Clish. The bonds must be configured in each corresponding Security Group (using the Gaia gClish shell), with VLAN interfaces configured for each Security Group.

The Security Group with the lowest ID, which has been assigned the shared subordinate interfaces, is responsible for the LACP negotiation for these interfaces.

For example, to share a bond interface with subordinate interfaces eth1-05 and eth2-05 between Security Group 3 and Security Group 4:

1. On the Maestro Hyperscale Orchestrator:
  - a. Enable the shared uplinks feature on Security Group 3 and Security Group 4:

```
Mhol_1> set maestro security-group id 3 shared-uplinks
state enabled
Mhol_1> set maestro security-group id 4 shared-uplinks
state enabled
```

- b. Apply the configuration:


```
Mhol_1> set maestro security-group apply-new-config
```

2. On the Maestro Hyperscale Orchestrator (in Gaia Portal or Gaia Clish):
  - a. Assign interface eth1-05 to Security Group 3.
  - b. Assign interface eth2-05 to Security Group 3.
  - c. Assign interface eth1-05 to Security Group 4.
  - d. Assign interface eth2-05 to Security Group 4.
3. In both Security Group 3 and Security Group 4:

- a. Connect to the command line of the Security Group.
- b. Log in.
- c. If your default shell is the Expert mode, then go to Gaia gClish:

```
gclish
```

- d. Create a bonding group which contains the physical interfaces eth1-05 and eth2-05.

 **Note** - The bonding group ID does not have to be identical in the different Security Groups.

In Security Group 3, run:

```
[Global] sg3-ch01-01 > add bonding group 1 interface
eth1-05
[Global] sg3-ch01-01 > add bonding group 1 interface
eth2-05
[Global] sg3-ch01-01 > set bonding group 1 mode 8023AD
```

In Security Group 4, run:

```
[Global] sg4-ch01-01 > add bonding group 1 interface
eth1-05
[Global] sg4-ch01-01 > add bonding group 1 interface
eth2-05
[Global] sg4-ch01-01 > set bonding group 1 mode 8023AD
```

- e. Create a VLAN interface on top of the bond interface.

In Security Group 3, run:

```
[Global] sg3-ch01-01 > add interface bond1 vlan 30
```

In Security Group 4, run:

```
[Global] sg4-ch01-01 > add interface bond1 vlan 40
```

- f. Configure IP addresses for the bond VLAN interfaces.

#### 4. Update the Security Gateway objects in SmartConsole:

- a. From the left navigation panel, click **Gateways & Servers**.
- b. Open the Security Gateway object for **each** Security Group.
- c. In the left panel, click **Network Management > Topology**.



- d. From the top, click **Get Interfaces > Get Interfaces with topology**.
  - e. Click **Close** to approve the new topology (example: bond1.30).
  - f. If required, edit the interface to configure its topology settings.
  - g. Click **OK** to close the Security Gateway object.
5. Install the Access Control Policy.

This also updates the Orchestrator's configuration.

6. The Orchestrator starts to forward the tagged traffic to the Security Group.

According to the above configuration:

- Each packet that arrives at VLAN interfaces eth1-05.30 and eth2-05.30 is forwarded to Security Group 3.
- Each packet that arrives at VLAN interfaces eth1-05.40 and eth2-05.40 is forwarded to Security Group 4.

### Notes:

- No traffic goes through the bond until VLAN interfaces are configured on the Security Group, and the firewall policy is installed.
- An interface shared between two Security Groups cannot have the same VLAN configured on top of it in both Security Groups. In the example above, configuring bond1.30 on both Security Group 3 and Security Group 4 (when bond1 contains eth1-05 and eth2-05 as subordinates on both Security Groups), or configuring no VLAN on top of the bond in either Security Group, would be invalid.

## LACP bond verification

To make sure an LACP bond, which contains shared interfaces, is configured correctly, run this command from the Maestro Hyperscale Orchestrator (in the Expert mode):

```
lACP_verify
```

## Removing subordinate interfaces from LACP bonds

When a subordinate interface is added to an LACP bond interface, it is assigned an index called "Port Number".

For example, the first subordinate added to bond1 is assigned the Port Number 1, the second subordinate added to bond1 is assigned the Port Number 2, and so on.

When subordinate interfaces are removed from an LACP bond, the remaining subordinate interfaces in the bond keep sending LACP PDUs with the original Port Number that was assigned when each subordinate interface was added to the bond.

## Example

### 1. In Security Group 1:

- a. The physical interfaces were added to bond1 in this order: eth1-05, eth1-06, eth1-07, and eth1-08.

This means that eth1-05 has Port Number 1, eth1-06 has Port Number 2, eth1-07 has Port Number 3, and eth1-08 has Port Number 4.

- b. Later, subordinate interfaces eth1-05 and eth1-06 were removed from bond1.

In this scenario, subordinate interface eth1-07 still has Port Number 3, and subordinate interface eth1-08 still has Port Number 4 in the LACP PDUs they send to an external switch.

### 2. In Security Group 2:

- a. The physical interfaces were added to bond1 in this order: eth1-07 and eth1-08.

This means that eth1-07 has Port Number 1, and eth1-08 has Port Number 2.

- b. No subordinate interfaces were removed from bond1.

In this scenario, subordinate interface eth1-07 has Port Number 1, and subordinate interface eth1-08 has Port Number 2 in the LACP PDUs they send to an external switch.

This inconsistency can cause traffic loss. Therefore, all bonds that use shared subordinates must be created exactly in the same way. In the example above, this means that the bonds in Security Group 1 and Security Group 2 must be created as follows:

- In Security Group 1:
  - a. Create bond1.
  - b. Add eth1-07 to bond1.
  - c. Add eth1-08 to bond1.
- In Security Group 2:
  - a. Create bond1.
  - b. Add eth1-07 to bond1.
  - c. Add eth1-08 to bond1.

If subordinate interfaces eth1-05 and eth1-06 must be removed from bond1 in Security Group 1, then bond1 in Security Group 1 must be recreated from scratch to match the configuration of bond1 in Security Group 2.

## Removing an LACP bond that contains shared uplink interfaces from a Security Group

To remove a bond interface with subordinate interfaces that are shared between Security Groups, first the bond interface must be removed from the Security Group, and only afterwards from the Orchestrator.

Example:

- In Security Group 3:
  1. bond1 is an LACP bond.
  2. bond1 contains subordinate interfaces eth1-05 and eth2-05.
  3. bond1.30 is a VLAN interface on top of bond1.

Goal:

Remove bond1 in Security Group 4.

Procedure:

1. In Security Group 4:
  - a. Connect to the command line of Security Group 4.
  - b. Log in.
  - c. Go to the Gaia gClish shell.
  - d. Remove the VLAN interface from bond1.

```
[Global] sg4-ch01-01 > delete interface bond1 vlan 40
```

- e. Remove the subordinate interfaces from bond1"

```
[Global] sg4-ch01-01 > delete bonding group 1 interface eth1-05  
[Global] sg4-ch01-01 > delete bonding group 1 interface eth2-05
```

- f. Remove the bond:

```
[Global] sg4-ch01-01 > delete bonding group 1
```

2. On the Maestro Hyperscale Orchestrator (in Gaia Portal or Gaia Clish):
  - a. Remove interface eth1-05 from Security Group 4.
  - b. Remove interface eth2-05 from Security Group 4.

# Managing Security Groups

This section provides basic information about managing Security Groups.

## Connecting to a Specific Security Group Member (member)

You can connect to the command line of a specific Security Group Member in a Security Group in several ways.

### Connecting from the Quantum Maestro Orchestrator to a Security Group Member in a Security Group

Step	Instructions
1	Connect to the command line on the Quantum Maestro Orchestrator.
2	<p>Examine the configured Security Group and its Security Group Members.</p> <ul style="list-style-type: none"> <li>In the Gaia Clish, run:           <pre>show maestro security-group id &lt;Security Group ID&gt;</pre> </li> <li>In the Expert mode, run:           <pre>clish -c "show maestro security-group id &lt;Security Group ID&gt;"</pre> </li> </ul>
3	Make sure to log in to the Expert mode.
4	<p>Connect to a Security Group Member in the Security Group with <i>one</i> of these commands:</p> <pre>member &lt;Security Group ID&gt; &lt;Member ID&gt;</pre> <pre>m &lt;Security Group ID&gt; &lt;Member ID&gt;</pre>
5	Log in.

#### Example:

```
[Expert@Orch:0]# member 1 3
Moving to member 3 in security group 1 (198.51.101.3)
admin@198.51.101.1's password: *****
Last login: Mon Jan 28 17:05:23 2019 from 198.51.101.126
You have logged into the system.
[Expert@SG1-ch01-03:0]#
```

## Connecting from one Security Group Member to another Security Group Member in the same Security Group

Step	Instructions
1	Connect to the command line of the Security Group over SSH at: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <code>&lt;IP Address of Security Group&gt;</code> </div> <p><b>i Important</b> - This connection goes through the Quantum Maestro Orchestrator management interface you assigned to this Security Group.</p>
2	Log in to the Expert mode.
3	Connect to a Security Group Member in the same Security Group with one of these commands: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <code>member &lt;Member ID&gt;</code> </div> <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <code>m &lt;Member ID&gt;</code> </div>

### Example:

```
[Expert@SG1-ch01-03:0]# m 2
Moving to member 1_2
This system is for authorized use only.
Last login: Mon Jan 28 17:07:45 2019 from 192.0.2.1
You have logged into the system.
[Expert@SG1-ch01-02:0]#
```

### **i** Notes:

- To go back to the previous Security Group Member, run the `exit` command.
- You open many SSH sessions to Security Group Members.
- When you connect to a Security Group Member from the Quantum Maestro Orchestrator or from another Security Group Member, the new SSH connection goes over an internal Quantum Maestro Orchestrator network.

## Connecting from the Quantum Maestro Orchestrator to a Security Group Member in a Security Group


Step	Instructions
1	Connect to the command line on the Quantum Maestro Orchestrator.

Step	Instructions
2	<p>Examine the configured Security Group and its Security Group Members.</p> <ul style="list-style-type: none"> <li>■ In the Gaia Clish, run:           <pre>show maestro security-group id &lt;Security Group ID&gt;</pre> </li> <li>■ In the Expert mode, run:           <pre>clish -c "show maestro security-group id &lt;Security Group ID&gt;"</pre> </li> </ul>
3	Make sure to log in to the Expert mode.
4	<p>Connect to a Security Group Member in the Security Group with <i>one</i> of these commands:</p> <pre>member &lt;Security Group ID&gt; &lt;Member ID&gt;</pre> <pre>m &lt;Security Group ID&gt; &lt;Member ID&gt;</pre>
5	Log in.

**Example:**

```
[Expert@Orch:0]# member 1 3
Moving to member 3 in security group 1 (198.51.101.3)
admin@198.51.101.1's password: *****
Last login: Mon Jan 28 17:05:23 2019 from 198.51.101.126
You have logged into the system.
[Expert@SG1-ch01-03:0]#
```

**Connecting from one Security Group Member to another Security Group Member in the same Security Group**

Step	Instructions
1	<p>Connect to the command line of the Security Group over SSH at:</p> <pre>&lt;IP Address of Security Group&gt;</pre> <p> <b>Important</b> - This connection goes through the Quantum Maestro Orchestrator management interface you assigned to this Security Group.</p>
2	Log in to the Expert mode.

Step	Instructions
3	<p>Connect to a Security Group Member in the same Security Group with one of these commands:</p> <pre data-bbox="352 320 1458 383">member &lt;Member ID&gt;</pre> <pre data-bbox="352 383 1458 445">m &lt;Member ID&gt;</pre>

**Example:**

```
[Expert@SG1-ch01-03:0]# m 2
Moving to member 1_2
This system is for authorized use only.
Last login: Mon Jan 28 17:07:45 2019 from 192.0.2.1
You have logged into the system.
[Expert@SG1-ch01-02:0]#
```

**Notes:**

- To go back to the previous Security Group Member, run the `exit` command.
- You open many SSH sessions to Security Group Members.
- When you connect to a Security Group Member from the Quantum Maestro Orchestrator or from another Security Group Member, the new SSH connection goes over an internal Quantum Maestro Orchestrator network.

# Global Commands

## *In This Section:*

---

Working with Global Commands .....	144
Check Point Global Commands .....	146
General Global Commands .....	149
Global Operating System Commands .....	157

---

The Gaia operating system includes a set of global commands that apply to all or specified Security Group Members.

## Working with Global Commands

### Background

- Gaia gClish commands apply globally to all Security Group Members, by default.
- Gaia gClish commands do not apply to Security Group Members that are in the DOWN state in the Security Group.

If you run a "set" command while a Security Group Member is in the DOWN state, the command does not update that Security Group Member.

The Security Group Member synchronizes its database during startup and applies the changes after reboot.

- Gaia Clish commands apply only to the specific Security Group Member.

For these commands, see the [R81.20 Gaia Administration Guide](#).



## Global Commands

Command	Instructions
auditlog	<ul style="list-style-type: none"> <li>▪ Enabled by default.</li> <li>▪ All commands are recorded in the audit log.</li> <li>▪ To learn more about the audit log, see <i>Looking at the Audit Log</i>.</li> </ul>
config-lock	<ul style="list-style-type: none"> <li>▪ Protects the Gaia gClish database by locking it. Each Security Group Member has one lock.</li> <li>▪ To set Gaia gClish operations for an Security Group Member, the Security Group Member must hold the "config-lock".</li> <li>▪ To set the "config-lock", run: <div data-bbox="480 663 1461 728" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre>set config-lock on override</pre> </div> </li> <li>▪ Gaia gClish traffic runs on the Sync interface, TCP port 1129.</li> </ul>
blade-range	<ul style="list-style-type: none"> <li>▪ Runs commands on specified Security Group Members.</li> <li>▪ Runs Gaia gClish embedded commands only on this subset of Security Group Members.</li> <li>▪ We do not recommend that you use the <code>blade-range</code> command, because all Security Group Members must have identical configurations.</li> </ul>

# Check Point Global Commands

These global commands apply to more than one Security Group Member. These global commands let you work with Security Gateway and SecureXL.

**fw, fw6**

## Description

The `fw` and `fw6` commands are global scripts that run the `fw` and `fw6` commands on each Security Group Member.

## Syntax

Shell	Syntax
Gaia Clish	<code>fw</code>
Gaia gClish	<code>fw6</code>
Expert mode	<code>g_fw</code> <code>g_fw6</code>

## Examples

### Example 1

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> fw ctl
-- 2 blades: 1_01 1_02 --
Usage: fw ctl command args...
Commands: install, uninstall, pstat, iflist, arp, debug, kdebug, bench
         chain, conn, multik, conntab, fwghtab_bl_stats
[Global] HostName-ch01-01 >
```

### Example 2

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> fw ctl iflist
-- 6 blades: 1_01 1_02 1_03 2_01 2_02 2_03 --
0 : BPEth0
1 : BPEth1
2 : eth1-Mgmt4
3 : eth2-Mgmt4
4 : eth1-01
5 : eth1-CIN
6 : eth2-CIN
8 : eth2-01
16 : Sync
17 : eth1-Mgmt1
18 : eth2-Mgmt1
[Global] HostName-ch01-01 >
```

**fw dbgfile****Description**

Use the "fw dbgfile" commands in Gaia gClish to debug how the Security Group inspect traffic.

**Syntax to collect the debug**

```
fw dbgfile collect -f <Debug Output File> [-buf <Buffer Size>]
[-m <Debug Module 1> <Debug Flags 1> [-m <Debug Module 2> <Debug
Flags 2>] ... [-m <Debug Module N> <Debug Flags N>]]
```

**Syntax to show the collected debug**

```
fw dbgfile view [<Debug Output File>] [-o <Debug Output File>]
```

**Parameters**

Parameter	Description
collect	Collects the Security Gateway debug information.
view	Shows the collected debug information.
<Debug Output File>	Specifies the full path and the name of the debug output file.
-buf <Buffer Size>	Specifies the debug buffer size. Always set the maximal size 8200.
-m <Debug Module 1> Debug Flags 1> [-m <Debug Module 2> <Debug Flags 2>] ... [-m <Debug Module N> <Debug Flags N>]	Specifies Security Gateway debug modules and debug flags in those modules. You can specify more than one debug module.
-o <Debug Output File>	Specifies the full path and the name of the debug output file to read.

## Examples

### Example - Collect debug information

```
[Global] HostName-ch01-01 > fw dbgfile collect -f /var/log/debug.txt -buf 8200 -m fw + conn -m kiss + pmdump
```

### Example - Show the collected debug information

```
[Global] HostName-ch01-01 > fw dbgfile view /var/log/debug.txt
```

**i** **Important** - For complete debug procedure, see the [R81.20 Quantum Security Gateway Guide](#) > Chapter *Kernel Debug on Security Groups*.

## fwaccel, fwaccel6

### Description

The `fwaccel` commands control the acceleration for IPv4 traffic.

The `fwaccel6` commands control the acceleration for IPv6 traffic.

### Syntax

Shell	Syntax for IPv4	Syntax for IPv6
Gaia Clish Gaia gClish	<code>fwaccel help</code>	<code>fwaccel6 help</code>
Expert mode	<code>g_fwaccel help</code>	<code>g_fwaccel6 help</code>

### Parameters and Options

For more information, see the [R81.20 Performance Tuning Administration Guide](#) > Chapter *SecureXL* > Section *SecureXL Commands and Debug* - Subsection '*fwaccel*' and '*fwaccel6*'.

## General Global Commands

Global commands apply to more than one Security Group Member.

These commands are available in Gaia Clish and Gaia gClish:

In Gaia Clish and Gaia gClish	In the Expert mode
update_conf_file	g_update_conf_file
global	global_help
asg_cp2blades	asg_cp2blades
asg_clear_table	asg_clear_table

Below are some global commands

### Viewing the List of Global Commands (global help)

#### Description

Use the "global help" command in Gaia gClish to show the list of global commands you can use in Gaia gClish.

#### Syntax

```
global help
```

#### Examples

##### Example output in Gateway mode

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> global help
Usage: <command_name> [-b SGMs] [-a -l -r --] <native command arguments>
Executes the specified command on specified blades.

Optional Arguments:
  -b blades: in one of the following formats
            1_1,1_4 or 1_1-1_4 or 1_01,1_03-1_08,1_10
            all (default)
            chassis1
            chassis2
            chassis_active
  -a       : Force execution on all SGMs (incl. down SGMs).
  -l       : Execute only on local blade.
  -r       : Execute only on remote SGMs.

Command list:
snapshot_show_current snapshot_recover fwaccel6_m fwaccel6 fw6 unlock update_conf_file mv fwaccel_m ethtool md5sum dmesg cp
tcpdump cat tail clusterXL_admin reboot ls fwaccel vpn fw netstat cpstop cpstart cplic asg
[Global] HostName-ch01-01>
```

## Example output in VSX mode

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> global help
Usage: <command_name> [-b SGMs] [-a -l -r --] <native command arguments>
Executes the specified command on specified blades.

Optional Arguments:
  -b blades: in one of the following formats
        1_1,1_4 or 1_1-1_4 or 1_01,1_03-1_08,1_10
        all (default)
        chassis1
        chassis2
        chassis_active
  -a      : Force execution on all SGMs (incl. down SGMs).
  -l      : Execute only on local blade.
  -r      : Execute only on remote SGMs.

Command list:
cplic cpstart cpstop netstat fw vpn fwaccel ls reboot clusterXL_admin tail cat topdump cp dmesg md5sum ethtool fwaccel_m mv
update_conf_file unlock fwaccel6_m snapshot_recover snapshot_show_current asg
[Global] HostName-ch01-01>
```

## Updating Configuration Files (update\_conf\_file)

### Description

Use these commands to add, update, and remove parameters in configuration files.

**Important** - After you change the configuration files, you must reboot the Security Group with the "reboot -b all" command.

### Syntax

Shell	Syntax
Gaia gClish	<code>update_conf_file &lt;File Name&gt; &lt;Parameter Name&gt;=&lt;Parameter Value&gt;</code>
Expert mode	<code>g_update_conf_file &lt;File Name&gt; &lt;Parameter Name&gt;=&lt;Parameter Value&gt;</code>

### Important:

- There must not be a space in front of the equal sign (=).
- There must not be a space after the equal sign (=).

## Parameters

Parameter	Description
<i>&lt;File Name&gt;</i>	<p>Full path and name of the configuration file to update You do not need to specify the full path for these files (only specify the file name):</p> <ul style="list-style-type: none"> <li>■ <code>\$FWDIR/boot/modules/fwkernel.conf</code></li> <li>■ <code>\$PPKDIR/conf/simkernel.conf</code></li> </ul>
<i>&lt;Parameter Name&gt;</i>	Name of the parameter to configure.
<i>&lt;Parameter Value&gt;</i>	New value for the parameter to configure.

### Notes:

- These commands work with configuration files in a specified format. It is composed of lines, where each line defines one parameter:  
*<Parameter Name>=<Parameter Value>*  
The `$FWDIR/boot/modules/fwkernel.conf` and `$PPKDIR/conf/simkernel.conf` files use this format.
- If the specified configuration file does not exist, these commands create it.
- These commands make the required changes on all Security Group Members.  
It is not necessary to copy the updated file to other Security Group Members with the "asg\_cp2blades" command.

## Examples

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01>
[Global] HostName-ch01-01> update_conf_file /home/admin/MyConfFile.txt var1=hello
[Global] HostName-ch01-01>
[Global] HostName-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var1=hello

[Global] HostName-ch01-01> update_conf_file /home/admin/MyConfFile.txt var2=24h
[Global] HostName-ch01-01>
[Global] HostName-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var2=24h
var1=hello

[Global] HostName-ch01-01> update_conf_file /home/admin/MyConfFile.txt var1=goodbye
[Global] HostName-ch01-01>
[Global] HostName-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var2=24h
var1=goodbye

[Global] HostName-ch01-01> update_conf_file /home/admin/MyConfFile.txt var2=
[Global] HostName-ch01-01>
[Global] HostName-ch01-01> cat /home/admin/MyConfFile.txt
-*- 3 blades: 2_01 2_02 2_03 -*-
var1=goodbye
[Global] HostName-ch01-01>
```

## Setting Firewall Kernel Parameters (g\_fw ctl set)

### Description

Use these commands in the Expert mode to show or set the values of the specified Firewall kernel parameters.

### Syntax for viewing the current value of a kernel parameter

```
g_fw ctl get <Parameter Type> <Parameter Name>
```

### Syntax for setting a value of a kernel parameter

```
g_fw ctl set <Parameter Type> <Parameter Name> <Parameter Value>
```



## Parameters

Parameter	Description
get	Shows the specified parameter and its value.
set	Change the parameter value to the specified value.
<Parameter Type>	Type of the parameter: <ul style="list-style-type: none"> <li>▪ int - Accepts integer values</li> <li>▪ str - Accepts string values</li> </ul> <p><b>Note</b> - You must enter the correct parameter type.</p>
<Parameter Name>	Parameter name to configure.
<Parameter Value>	Parameter value to configure.

**i Note** - To make changes persistent, you must manually add the applicable kernel parameters and their values in the `$FWDIR/boot/modules/fwkernel.conf` file. Use the "g\_update\_conf\_file" command in the Expert mode. See "[Updating Configuration Files \(update\\_conf\\_file\)](#)" on page 150.

For more information, see the [R81.20 Quantum Security Gateway Guide](#) > Chapter *Working with Kernel Parameters on Security Groups*.

## Copying Files Between Security Group Members (asg\_cp2blades)

### Description

Use the "asg\_cp2blades" command in Gaia gClish or the Expert mode to copy files from the current Security Group Member to another Security Group Member.

### Syntax (for Gaia gClish and the Expert mode)

```
asg_cp2blades [-b <SGM IDs>] [-s] <Source Path> [<Destination Path>]
```

## Parameters

Parameter	Description
<code>-b &lt;SGM IDs&gt;</code>	<p>Applies to Security Group Members as specified by the <code>&lt;SGM IDs&gt;</code>.</p> <p><code>&lt;SGM IDs&gt;</code> can be:</p> <ul style="list-style-type: none"> <li>▪ No <code>&lt;SGM IDs&gt;</code> specified, or <code>all</code> Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, <code>1_1</code>)</li> </ul>
<code>-r</code>	Copy folders and directories that contain files.
<code>-s</code>	<p>Save a local copy of the old file on each Security Group Member. The copy is saved in the same directory as the new file. The old file has the same name with this at the end:</p> <p><code>*.bak.&lt;date&gt;.&lt;time&gt;</code></p>
<code>&lt;Source Path&gt;</code>	Full path and name of the file to copy.
<code>&lt;Destination Path&gt;</code>	<p>Full path of the destination.</p> <p>If not specified, the command copies the file to the relative source file location.</p>

## Example

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > asg_cp2blades /home/admin/note.txt
Operation completed successfully
[Global] HostName-ch01-01 >
[Global] HostName-ch01-01 > cat /home/admin/note.txt
-- 3 blades: 2_01 2_02 2_03 --
hello world
[Global] HostName-ch01-01>
```

## Deleting Connections from the Connections Table (`asg_clear_table`)

### Description

Use the "`asg_clear_table`" command in Gaia gClish or the Expert mode to delete connections from the Connections table on the Security Group Members.

The command runs up to 15 times, or until there are less than 50 connections left.

**Important** - If you are connected to the Security Group over SSH, your connection is disconnected.

**Syntax (for Gaia gClish and the Expert mode)**

```
asg_clear_table [-b <SGM IDs>]
```

**Parameters**

Parameter	Description
-b <SGM IDs>	<p>Applies to Security Group Members as specified by the &lt;SGM IDs&gt;. &lt;SGM IDs&gt; can be:</p> <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul> <p><b>Note</b> - With this option, you can only select Security Group Members from one Site.</p>

**Viewing Information about Interfaces on Security Group Members (show interface)****Description**

Use the "show interface" command in Gaia gClish to view information about the interfaces on the Security Group Members.

For more information, see the [R81.20 Gaia Administration Guide](#) > Chapter *Network Management* > Section *Network Interfaces*.

**Syntax**

```
show interfaces all
```

```
show interface <Options>
```

**Example**

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> show interface eth1-01 ipv4-address
1_01:
ipv4-address 4.4.4.10/24

1_02:
ipv4-address 4.4.4.10/24

1_03:
ipv4-address 4.4.4.10/24

1_04:
ipv4-address 4.4.4.10/24

1_05:
Blade 1_05 is down. See "/var/log/messages".

2_01:
ipv4-address 4.4.4.10/24

2_02:
ipv4-address 4.4.4.10/24

2_03:
ipv4-address 4.4.4.10/24

2_04:
ipv4-address 4.4.4.10/24

2_05:
ipv4-address 4.4.4.10/24
[Global] HostName-ch01-01>
```

## Global Operating System Commands

Global operating system commands are standard Linux commands that run on all or specified Security Group Members.

When you run a global command in Gaia gClish, the operating system runs a global script that is the standard Linux command on the Security Group Members.

When you run a command in the Expert mode, it works as a standard Linux command.

To use the global command in the Expert mode, run the global command script version as shown in this table:

Gaia gClish Command	Global Command in the Expert mode
arp	g_arp
cat	g_cat
cp	g_cp
dmesg	g_dmesg
ethtool	g_ethtool
ifconfig	asg_ifconfig
ls	g_ls
md5sum	g_md5sum
mv	g_mv
netstat	g_netstat
reboot	g_reboot
tail	g_tail
tcpdump	g_tcpdump
top	g_top

## Notes:

- The parameters and options for the standard Linux command are available for the global command.
- You can use one or more flags.
- Do **not** use these two flags together in the same command:
  - The "-l" flag - to execute the command only on the local Security Group Member
  - The "-r" flag - to execute the command only on the remote Security Group Member

## Syntax

- In Gaia Clish:

```
<Gaia gClish Command> [-b <SGM IDs>] <Command Options>
```

- In the Expert mode:

```
<Global Expert mode Command> [-b <SGM IDs>] <Command Options>
```

## Parameters

Parameter	Description
<i>&lt;Gaia gClish Command&gt;</i>	Standard command in Gaia gClish as appears in the table above.
<i>&lt;Global Expert mode Command&gt;</i>	Global command in the Expert mode as appears in the table above.
<i>-b &lt;SGM IDs&gt;</i>	<p>Applies to Security Group Members as specified by the <i>&lt;SGM IDs&gt;</i>.</p> <p><i>&lt;SGM IDs&gt;</i> can be:</p> <ul style="list-style-type: none"> <li>▪ No <i>&lt;SGM IDs&gt;</i> specified, or <code>all</code> Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, <code>1_1</code>)</li> </ul> <p><b>Note</b> - You can only select Security Group Members from one Site with this option.</p>
<i>&lt;Command Options&gt;</i>	Standard command options for the specified command.

Below are explanations about some of the global commands.

## Global 'ls'

### Description

The global `ls` command shows the file in the specified directory on all Security Group Members.

### Syntax

- In Gaia Clish:

```
ls [-b <SGM IDs>] <Command Options>
```

- In the Expert mode:

```
g_ls [-b <SGM IDs>] <Command Options>
```

### Example

This example runs the 'g\_ls' command in the Expert mode on Security Group Members 1\_1, 1\_2, and 1\_3.

The example output shows the combined results for these Security Group Members.

```
[Expert@HostName-ch0x-0x:0]# g_ls -b 1_1-1_3,2_1 /var/
-*- 4 blades: 1_01 1_02 1_03 -*-
CPbackup   ace      crash  lib    log    opt      run     suroot
CPsnapshot cache  empty  lock   mail   preserve spool   tmp
[Expert@HostName-ch0x-0x:0]#
```

## Global 'reboot'

### Description

The global `reboot` command reboots all Security Group Members.

### Syntax

- In Gaia Clish:

```
reboot [-a]
```

- In the Expert mode:

```
g_reboot [-a]
```

## Parameters

Parameter	Description
No Parameters	Reboots all Security Group Members that are in the state "UP".
-a	Reboots all Security Group Members that in the DOWN and the UP states.

## Global 'top'

### Description

The global `top` command:

- Shows CPU utilization in real time on Security Group Members.
- Uses the local Security Group Member configuration file (`~/ .toprc`) to format the output on the remote Security Group Members.

The command copies this file to the remote Security Group Members.

### Syntax

- In Gaia Clish:

```
top -h
```

```
top [local] [-f [-o <Output File>] [-n <Number of Iterations>]] -b <SGM IDs> [<Command Options>]
```

```
top [local] [s <Output File>] -b <SGM IDs> [<Command Options>]
```

- In the Expert mode:

```
g_top -h
```

```
g_top [local] [-f [-o <Output File>] [-n <Number of Iterations>]] -b <SGM IDs> [<Command Options>]
```

```
g_top [local] [s <Output File>] -b <SGM IDs> [<Command Options>]
```



## Parameters

Parameter	Description
-h	Shows the built-in help.
local	Uses the 'top' configuration file ( <code>~/ .toprc</code> ) on the local Security Group Member.
-f	Exports the output to a file. Default: <code>/vat/log/gtop.&lt;Time&gt;</code>
-o <i>&lt;Output File&gt;</i>	Specifies the path and name of the output file. Must use with the "-f" parameter.
-n <i>&lt;Number of Iterations&gt;</i>	The command saves the output the specified number of times. Default: 1 Must use with the "-f" parameter.
-s <i>&lt;Output File&gt;</i>	Shows the content of the output file <i>&lt;Output File&gt;</i> , in which the command saved its output earlier.
<i>&lt;Command Options&gt;</i>	Parameters of the standard <code>top</code> command. For more information, see the <code>top</code> command documentation.

## Configuring the 'g\_top' output

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: <input type="text" value="top"/>
4	Set the desired view (press <b>h</b> to see the built-in help).
5	Press <b>Shift+W</b> to save the 'top' configuration.
6	Run: <input type="text" value="g_top"/>

## Global 'arp'

### Description

The global `arp` command shows the ARP cache table on all Security Group Members.

### Syntax

- In Gaia Clish:

```
arp [-b <SGM IDs>] <Command Options>]
```

- In the Expert mode:

```
g_arp [-b <SGM IDs>] <Command Options>]
```

### Example - ARP table on all interfaces of all Security Group Members

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > arp
1_01:
Address      HWtype  HWaddress      Flags Mask    Iface
192.0.2.2   ether   00:1C:7F:02:04:FE  C             Sync
172.23.9.28 ether   00:14:22:09:D2:22  C             eth1-Mgmt4
192.0.2.3   ether   00:1C:7F:03:04:FE  C             Sync
1_02:
Address      HWtype  HWaddress      Flags Mask    Iface
192.0.2.3   ether   00:1C:7F:03:04:FE  C             Sync
172.23.9.28 ether   00:14:22:09:D2:22  C             eth1-Mgmt4
192.0.2.1   ether   00:1C:7F:01:04:FE  C             Sync
1_03:
Address      HWtype  HWaddress      Flags Mask    Iface
192.0.2.1   ether   00:1C:7F:01:04:FE  C             Sync
172.23.9.28 ether   00:14:22:09:D2:22  C             eth1-Mgmt4
192.0.2.2   ether   00:1C:7F:02:04:FE  C             Sync
[Global] HostName-ch01-01 >
```

# Backing Up and Restoring Gaia Configuration

For more information, see the [R81.20 Gaia Administration Guide](#):

- Chapter *Maintenance* > Section *System Backup*.
- Chapter *Maintenance* > Section *Snapshot Management*.

# Working with Security Group Gaia gClish Configuration (asg\_config)

## Description

Use the "asg\_config" command in Gaia gClish or Expert mode to:

- Show the current Gaia gClish configuration on all SGMs.
- Save the current Gaia gClish configuration of all SGMs to a file.

## Use cases:

- Copy the Gaia gClish configuration to a different Security Group.

For example, you can use the saved configuration from an existing Security Group to configure up a new Security Group.

- Quickly re-configure a Security Group that was reverted to factory defaults.

Before you revert to the factory default image, save the existing Gaia gClish configuration. Then use it to override the factory default settings.

## Syntax

```
asg_config show
```

```
asg_config save [-t] [<Output File>]
```

## Parameters

Parameter	Description
show	Show the existing Gaia gClish configuration.
save	Save the current Gaia gClish configuration to a file. If you do not include a path, the output file is saved to this directory: /home/admin/
-t	Adds a timestamp in Unix Epoch format to the file name.
<Output File>	Specifies the path and name of the output file. If you do not include a path, the output file is saved to this directory: /home/admin/

**Example - Save the current Gaia gClish configuration to the `/home/admin/myconfig` file**

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > asg_config save -t myconfgif
[Global] HostName-ch01-01 > exit
[Expert@HostName-ch0x-0x:0]# ls -l ~/myconfgif*
-rw-rw---- 1 admin root 75891 Feb 28 04:38 myconfgif.1551346686
[Expert@HostName-ch0x-0x:0]# date -d @1551346686
Thu Feb 28 04:38:06 EST 2019
[Expert@HostName-ch0x-0x:0]#
```

# Configuring Security Group Members (asg\_blade\_config)

## Description

Use the "asg\_blade\_config" command in the Expert mode to manage Security Group Members:

- Copy the Security Group Member configuration from the local Security Group Member to other Security Group Members in the Security Group
- Change the synchronization start IP address
- Reset the system uptime value
- Get a policy from the Management Server

## Syntax

```
asg_blade_config
  fetch_smc
  full_sync <IP Address>
  get_smo_ip
  is_in_pull_conf_group
  is_in_security_group
  pull_config
  reset_sic -reboot_all <Activation Key>
  set_sync_start_ip <Start IP Address>
  upgrade_cu
  upgrade_start <New Version> [cu]
  upgrade_stat
  upgrade_stop
```

## Parameters

Parameter	Description
<code>fetch_smc</code>	Fetches policy from Management Server and distributes it to all Security Group Members.
<code>full_sync &lt;IP Address&gt;</code>	Runs Full Sync with the remote Security Group Member, whose IP address is <i>&lt;IP Address&gt;</i> .
<code>get_smo_ip</code>	Gets the SMO IP address from the Cluster Control Protocol (CCP) packets sent in the Security Group.
<code>is_in_pull_conf_group</code>	Checks whether the Security Group Member is in the Pulling Configuration Group.
<code>is_in_security_group</code>	Checks whether the Security Group Member is in the Security Group.
<code>pull_config</code>	Pulls configuration from other Security Group Members.
<code>reset_sic -reboot_all &lt;Activation Key&gt;</code>	Starts a Secure Internal Communication (SIC) cleanup. You must enter the <i>&lt;Activation Key&gt;</i> . You use this key later in SmartConsole to establish Secure Internal Communication.
<code>set_sync_start_ip &lt;Start IP Address&gt;</code>	Changes the Sync start IP address of local Security Group Member to <i>&lt;Start IP Address&gt;</i> .
<code>upgrade_cu</code>	Enables the Connectivity Upgrade mode (runs an iteration).
<code>upgrade_start &lt;New Version&gt; [cu]</code>	Starts an upgrade procedure from the current version to the <i>&lt;New Version&gt;</i> . The "cu" parameter uses the Connectivity Upgrade mode.
<code>upgrade_stat</code>	Shows the upgrade procedure information.
<code>upgrade_stop</code>	Stops the upgrade procedure.

## Troubleshooting the asg\_blade\_config command

To troubleshoot problems associated with the "asg\_blade\_config" command, examine the logs listed in the `$FWDIR/log/blade_config` file.

For example, if a Security Group Member unexpectedly reboots, you can search the log file for the word `reboot` to learn why.

# Working with the Distribution Mode

## *In This Section:*

---

Background .....	168
Automatic Distribution Configuration (Auto-Topology) .....	169
Manual Distribution Configuration (Manual-General) .....	170
Setting and Showing the Distribution Configuration (set distribution configuration) ...	171
Configuring the Interface Distribution Mode (set distribution interface) .....	173
Showing Distribution Status (show distribution status) .....	175
Running a Verification Test (show distribution verification) .....	177
Configuring the Layer 4 Distribution Mode and Masks (set distribution l4-mode) .....	178

---

## Background

The Quantum Maestro Orchestrator uses the Distribution Mode to assign incoming traffic to Security Group Members in each Security Group.

By default, the Quantum Maestro Orchestrator automatically configures the Distribution Mode.

### Supported Distribution Modes

Mode	Instructions
<b>User (Internal)</b>	<p>Packets are assigned to a Security Group Member based on the packet's Destination IP address.</p> <p>If Layer 4 distribution is enabled, Quantum Maestro Orchestrator assigns packets to a Security Group Member based on the packet's Source Port and the Destination IP address.</p>
<b>Network (External)</b>	<p>Packets are assigned to a Security Group Member based on the packet's Source IP address.</p> <p>If Layer 4 distribution is enabled, Quantum Maestro Orchestrator assigns packets to a Security Group Member based on the packet's Source IP address and Destination Port.</p>



Mode	Instructions
<b>General</b>	<p>Quantum Maestro Orchestrators assign packets to a Security Group Member based on the packet's Source IP address and the Destination IP address.</p> <p>If Layer 4 distribution is enabled, Quantum Maestro Orchestrators assign packets to a Security Group Member based on the packet's Source IP address, Source Port, Destination IP address, and Destination Port.</p>
<b>Auto-Topology (Per-Port)</b>	Each port for a Security Group Member is configured separately in the User Mode or Network Mode.

 **Notes:**

- The default mode is **Auto-Topology ((Per-Port))** and the Layer 4 distribution is enabled.
- The **User ((Internal))** Mode and **Network ((External))** Mode can work together. The supported combinations are:
  - User Mode and User Mode
  - User Mode and Network Mode
  - Network Mode and Network Mode

In many scenarios, it is possible to optimize the combination of the User Mode and Network Mode to pass traffic through same Security Group Member from the two sides.

## Automatic Distribution Configuration (Auto-Topology)

By default, Security Groups work in the **General** Mode.

The best Distribution Mode is selected based on the Security Group topology as defined in SmartConsole in the Security Gateway object.

The Distribution Mode is automatically based on these interface types:

- Physical interfaces, except for management and synchronization interfaces
- VLAN
- Bond
- VLAN on top of Bond

## Manual Distribution Configuration (Manual-General)

In some deployments, you must manually configure a Distribution Mode to the **General**.

In other cases, it may be necessary to force the system to work in the **General** Mode.

When the Distribution Mode is manually configured (**Manual-General** Mode), the Distribution Mode of each SSM is **General**.

In this configuration, the topology of the interfaces is irrelevant.

- ★ **Best Practice** - Do **not** manually change the Distribution Mode of a Virtual System. This can cause performance degradation.

## Setting and Showing the Distribution Configuration (set distribution configuration)

Use these Gaia gClish commands on a Security Group to set and show the distribution configuration.

**i Important** - If the Security Group runs in a VSX mode, run the commands in the context of VS0 only. The commands apply immediately across all Virtual Systems.

### Syntax to show the Distribution Configuration

```
show distribution configuration
```

### Syntax to set the Distribution Configuration

```
set distribution configuration {auto-topology | manual-general}
ip-version {ipv4 | ipv6 | all} ip-mask <Mask>
```

### Parameters

Parameter	Notes
auto-topology	Configures the distribution mode to Auto-Topology (Per-Port).
manual-general	Configures the distribution mode to Manual General.
ipv4	Configures the distribution mode for IPv4 traffic only.
ipv6	Configures the distribution mode for IPv6 traffic only.
all	Configures the distribution mode for IPv4 and IPv6 traffic.


Parameter	Notes
ip-mask <Mask>	<p>Must be the same as the distribution matrix size. Must be specified in the Hex format. Follow these steps:</p> <ol style="list-style-type: none"> <li>1. Examine the distribution matrix size:           <pre data-bbox="560 416 1426 479">show distribution verification verbose</pre> <p>Examine the Matrix Size line. Example:</p> <pre data-bbox="560 568 1426 651">... Matrix Size 512 ...</pre> </li> <li>2. Exit from the Gaia gClish to the Expert mode.</li> <li>3. Convert the matrix size from the decimal to the hexadecimal format:           <pre data-bbox="560 786 1426 848">printf '%x\n' &lt;Matrix Size&gt;</pre> <p>Example:</p> <pre data-bbox="560 898 1426 981">[Expert@HostName-ch0x-0x:0]# printf '%x\n' 512 200 [Expert@HostName-ch0x-0x:0]#</pre> </li> <li>4. Go to the Gaia gClish:           <pre data-bbox="560 1025 1426 1088">gclish</pre> </li> <li>5. Configure the distribution mode with the required mask:           <pre data-bbox="560 1133 1426 1240">set distribution ... ip-mask &lt;Matrix Size in HEX&gt;</pre> <p>Example:</p> <pre data-bbox="560 1290 1426 1330">set distribution ... ip-mask 200</pre> </li> </ol>

# Configuring the Interface Distribution Mode (set distribution interface)

## Description

Use these Gaia gClish commands on a Security Group to:

- Set the interface Distribution Mode - For an interface when the system is not working in the General Mode
- Show the interface Distribution Mode - If it is assigned by Auto-Topology, or is manually configured

 **Note** - In VSX mode, you must go to the context of the applicable Virtual System before you can change the interface Distribution Mode.  
Run the "set virtual-system <VS ID>" command.

## Syntax to set the interface Distribution Mode

```
set distribution interface <Name of Interface> configuration {user
| network | policy}
```

## Syntax to show the interface Distribution Mode

```
show distribution interface <Name of Interface> configuration
```

## Parameters

Parameter	Description
<Name of Interface>	Interface name as assigned by the operating system.
user	Manually assign the <b>User (Internal)</b> Distribution Mode - based on the Destination IP address.
network	Manually assign the <b>Network (External)</b> Distribution Mode - based on the Source IP address.
policy	Use <b>Auto-Topology</b> to automatically assign the Distribution Mode according to the policy.

## Examples

### Example 1 - Set the Distribution Mode to Network (External)

```
[Global] HostName-ch01-01 > set distribution interface eth1-01
configuration network
/bin/distutil set_ifn_dist_mode eth1-01 external
```

### Example 2 - Set the Distribution Mode to use the Auto-Topology to assign traffic according to the policy

```
[Global] HostName-ch01-01 > set distribution interface eth1-01
configuration policy
/bin/distutil set_ifn_dist_mode eth1-01 policy
```

### Example 3 - Set the Distribution Mode to User (Internal)

```
[Global] HostName-ch01-01 > set distribution interface eth1-01
configuration user
/bin/distutil set_ifn_dist_mode eth1-01 internal
```

## Showing Distribution Status (show distribution status)

### Description

Use this Gaia gClish command on a Security Group to show the status report of the Distribution Mode.

### Syntax

```
show distribution status [verbose]
```

### Examples

#### Example 1 - Regular output

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> show distribution status
distribution:
  l4_mode: 'on'
  mode: general
matrix:
  actual_size: '512'
ports:
  eth1-05: policy-internal
  eth1-06: policy-internal
[Global] HostName-ch01-01>
```

#### Example 2 - Verbose output

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> show distribution verification verbose
Test:           Configuration:      Verification:      Result:
Mode            per-port                per-port           Passed
L4 Mode         on                       on                 Passed
Matrix Size     512                     512               Passed
eth2-08         policy-external         policy-external    Passed
eth1-08         policy-internal         policy-internal    Passed
eth2-07         policy-internal         policy-internal    Passed
eth2-06         policy-internal         policy-internal    Passed
eth1-05         manual-internal         manual-internal    Passed
eth1-06         policy-internal         policy-internal    Passed
eth1-07         policy-internal         policy-internal    Passed

Verification passed successfully
[Global] HostName-ch01-01>
```

## Explanation about the output

Field	Instructions
L4 Mode	Shows the Layer 4 distribution status: <ul style="list-style-type: none"><li>▪ <code>on</code> - enabled</li><li>▪ <code>off</code> - disabled</li></ul>
Mode	Shows the currently configured Distribution Mode: <ul style="list-style-type: none"><li>▪ <code>per-port</code> - Auto-Topology</li><li>▪ <code>user</code> - User (Internal)</li><li>▪ <code>network</code> - Network (External)</li><li>▪ <code>general</code> - General</li></ul>
Matrix Size	Shows the size of the Distribution Mode matrix.
Ports	Shows the Distribution Mode assignment for each interface.



## Running a Verification Test (show distribution verification)

### Description

Use this Gaia gClish command on a Security Group to run a verification test of the Distribution Mode configuration.

This test compares the Security Group configuration with the actual results.

You can see a summary or a verbose report of the test results.

### Syntax

```
show distribution verification [verbose]
```

### Examples

#### Example 1- Verbose output of successful tests

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show distribution verification verbose
Test:           Configuration:      Verification:      Result:
Mode            per-port                per-port          Passed
L4 Mode        off                    off               Passed
Matrix Size    512                    512              Passed
eth2-16        policy-internal        policy-internal   Passed
eth1-16        policy-internal        policy-internal   Passed
eth1-15        policy-external        policy-external   Passed
[Global] HostName-ch01-01 >
```

#### Example 2 - Verbose output of failed tests

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show distribution verification verbose
Test:           Configuration:      Verification:      Result:
Mode            per-port                per-port          Passed
L4 Mode        on                    off               Failed
Matrix Size    512                    0                Failed
eth1-05        policy-internal        policy-internal   Passed
eth1-06        policy-internal        policy-internal   Passed
eth2-05        policy-external        policy-external   Passed
eth2-06        manual-internal        policy-external   Failed

Verification failed with above errors
[Global] HostName-ch01-01 >
```

# Configuring the Layer 4 Distribution Mode and Masks (set distribution l4-mode)

## Description

Use these commands in Gaia gClish on a Security Group to:

- Enable Layer 4 distribution and set new masks for the IP address and the port
- Disable Layer 4 distribution
- Show Layer 4 Distribution Mode and masks

## Syntax

```
set distribution l4-mode enabled
set distribution l4-mode disabled
show distribution l4-mode
```

## Examples

### Example 1 - Configure the Layer 4 Distribution Mode

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> set distribution l4-mode enabled
1_01:
success

1_02:
success
[Global] HostName-ch01-01>
```

### Example 2 - Disable the Layer 4 Distribution Mode

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> set distribution l4-mode disabled
1_01:
success

1_02:
success
[Global] HostName-ch01-01>
```

**Example 3 - Show the current Layer 4 Distribution Mode**

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> show distribution l4-mode
1_01:
L4 Distribution: Enabled

1_02:
L4 Distribution: Enabled
[Global] HostName-ch01-01>
```

# Configuring the Cluster State (g\_clusterXL\_admin)

## Description

Use the "g\_clusterXL\_admin" command in the Expert mode to change the cluster state manually, to UP or DOWN, for one or more Security Group Members.

## Use Case

This command is useful for tests and debug.

- ★ **Best Practice** - Do not use this command in production environments, because it can cause performance degradation.

## Syntax

```
g_clusterXL_admin -h
```

```
g_clusterXL_admin -b <SGM IDs> {up | down [-a]} [-r]
```

## Parameters

Parameter	Description
-h	Shows the built-in help.
-b <SGM IDs>	Applies to Security Group Members as specified by the <SGM IDs>. <SGM IDs> can be: <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul>
up	Changes the cluster state to UP.
down	Changes the cluster state to DOWN.
-a	Synchronizes accelerated connections to other Security Group Members.
-r	Runs this command on all <SGM IDs>, except the local Security Group Member.

 **Notes:**

- When the Security Group Member is in the Administrative **DOWN** state:
  - Gaia gClish commands do not run on this Security Group Member.
  - Traffic is not sent to this Security Group Member.
  - The "asg stat" command shows this Security Group Member as "**DOWN (admin)**".
- When the cluster state of the Security Group Member is changed to Administrative **UP**, it automatically synchronizes the configuration from a different Security Group Member that is in the state "UP".
- This command cannot change the state of a Security Group Member to **UP** if it is in the **DOWN** state because of a software or hardware problem.
- The "g\_clusterXL\_admin" command generates log entries.  
To see these log entries, run:

```
asg log --file audit
```

**Example**

```
[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 2_03 up
You are about to perform blade_admin up on blades: 2_03
This action will change members state

Are you sure? (Y - yes, any other key - no) y

Blade_admin up requires auditing
Enter your full name: John Doe
Enter reason for blade_admin up [Maintenance]: test
WARNING: Blade_admin up on blades: 2_03, User: John Doe, Reason: test

Members outputs:
-- 1 blade: 2_03 --
Setting member to normal operation ...
Member current state is ACTIVE
[Expert@HostName-ch0x-0x:0]#
```

# Configuring a Unique MAC Identifier (asg\_unique\_mac\_utility)

## *In This Section:*

---

Background .....	182
Configuring the Unique MAC Identifier Manually .....	183
Options of the Unique MAC Identifier Utility .....	183

---

## Background

When there are more than one Security Group on a Layer 2 segment, the Unique MAC Identifier must be different for each Security Group.

The Unique MAC Identifier is assigned by default during the initial setup.

The last octet of the management interface MAC address is the Unique MAC Identifier.

The last octet of the management interface MAC address is set for these data interface types:

- Interfaces with names in the "ethX-YZ" format
- Bond interfaces
- VSX *wrp* interfaces
- VLAN interfaces

If there is no configured management interface, the Unique MAC Identifier is assigned the default value 254.

Use the "asg\_unique\_mac\_utility" command in Gaia gClish or the Expert mode to set:

- Data interface Unique MAC Identifier
- Host name

## Configuring the Unique MAC Identifier Manually

Step	Instructions
1	Connect to the command line on the Security Group.
2	Run this command in Gaia gClish or the Expert mode: <pre>asg_unique_mac_utility</pre>
3	Select an option from the menu and follow the instructions on the screen. <b>Example:</b> <pre>-----   Unique MAC Utility                                  -----    HOSTNAME [MySecurityGroup]                           Unique MAC [192]                                    -----   Choose one of the following options: ----- 1) Set Hostname with Unique MAC wizard 2) Apply Unique MAC from current HOSTNAME 3) Manual set Unique MAC 4) Exit</pre>
4	Reboot the Security Group to apply the new Unique MAC Identifier: <pre>reboot -b all</pre>

## Options of the Unique MAC Identifier Utility

The options for setting the Unique MAC Identifier are:

### "Set Hostname with Unique MAC wizard"

The "\_asg" suffix and the setup number, between 1 and 254, are added to the setup name.

**Example:**

Setup Name	Suffix	Setup number
My_SG	_asg	22

This creates a new host name with a Unique MAC Identifier of 22.

The setup number replaces the Unique MAC Identifier default value of 254.

New Host Name	Unique MAC Identifier
My_SG_asg22	22

After reboot, all data interface MAC addresses have the new Unique MAC Identifier value 16.

**Example:**

```
eth1-01 00:1C:7F:XY:ZW:16
```

**Note** - The last octet for `eth1-01`, shown in bold, is 16 hex (22 decimal).

**"Apply Unique MAC from current Hostname"**

Assign a new Unique MAC Identifier to the interfaces.

The new Unique MAC Identifier is created from the setup number in the host name.

The current host name must first comply with the setup name number convention:

```
/asg suffix/setup
```

**"Manual set Unique MAC"**

Set the Unique MAC Identifier to the default value of 254.



# Working with the ARP Table (asg\_arp)

## *In This Section:*

---

The 'asg_arp' Command .....	185
Example Default Output .....	186
Example Verbose Output .....	187
Example Output for Verifying MAC Addresses .....	187
Verifying ARP Entries .....	187
Example Legacy Output .....	188

---

## The 'asg\_arp' Command

### Description

The `asg_arp` command in the Expert mode shows the ARP cache for the whole Security Group or for the specified Security Group Member, interface, MAC address, and Host name.

This command shows summary or verbose information.

### Syntax

```
asg_arp -h
```

```
asg_arp [-b <SGM IDs>] [-v] [--verify] [-i <Name of Interface>] [-m <MAC Address>] [<Hostname>]
```

```
asg_arp --legacy
```

## Parameters

Parameter	Description
-h	Shows the built-in help.
-v	Verbose mode that shows detailed Security Group Member cache information.
-b <SGM IDs>	Applies to Security Group Members as specified by the <SGM IDs>. <SGM IDs> can be: <ul style="list-style-type: none"> <li>■ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>■ One Security Group Member (for example, 1_1)</li> </ul>
-i <Name of Interface>	Shows the ARP cache for the specified interface.
-m <MAC Address>	Shows the ARP cache for the specified MAC address.
<Hostname>	Shows the ARP cache for the specified host name.
--verify	Runs MAC address verification on all Maestro Sites and shows the results.
--legacy	Shows the ARP cache for each Security Group Member in the legacy format.

## Example Default Output

This example shows the ARP cash in the Default Mode:

```
[Expert@HostName-ch0x-0x:0]# asg_arp
Address          HWaddress        Iface
172.23.19.4      54:7F:EE:6A:D0:BC eth1-Mgmt2
1_01             00:1C:7F:01:04:FE Sync
1_2             00:1C:7F:02:04:FE Sync
ssm1             02:02:03:04:05:40 eth1-CIN
ssm2             04:02:03:04:05:40 eth2-CIN
[Expert@HostName-ch0x-0x:0]#
```

## Example Verbose Output

This example shows the ARP cash in the Verbose Mode:

```
[Expert@HostName-ch0x-0x:0]# asg_arp -v
Address          HWtype  HWaddress          Flags Mask  Iface          SGMs
172.23.19.4     ether   54:7F:EE:6A:D0:BC  C          eth1-Mgmt2     1_01
1_01            ether   00:1C:7F:01:04:FE  C          Sync           1_02
1_2            ether   00:1C:7F:02:04:FE  C          Sync           1_01
ssm1            ether   02:02:03:04:05:40  C          eth1-CIN       1_01,1_02
ssm2            ether   04:02:03:04:05:40  C          eth2-CIN       1_01
[Expert@HostName-ch0x-0x:0]#
```

## Example Output for Verifying MAC Addresses

This example shows the output of the MAC address verification (on a Single Chassis):

```
[Expert@HostName-ch0x-0x:0]# asg_arp --verify
Address          HWtype  HWaddress          Flags Mask  Iface          SGMs
172.23.19.4     ether   54:7F:EE:6A:D0:BC  C          eth1-Mgmt2     1_01
1_01            ether   00:1C:7F:01:04:FE  C          Sync           1_02
1_2            ether   00:1C:7F:02:04:FE  C          Sync           1_01
ssm1            ether   02:02:03:04:05:40  C          eth1-CIN       1_01,1_02
ssm2            ether   04:02:03:04:05:40  C          eth2-CIN       1_01

MAC address for IP 172.23.19.4 is inconsistent across the SGMs

-----
Collecting information from SGMs...
-----
Verifying FW1 mac magic value on all SGMs...
Success
-----
Verifying IPV4 and IPV6 kernel values...
Success
-----
Verifying FW1 mac magic value in /etc/smodb.json...
Success
-----
Verifying MAC address on local chassis (Chassis 1)...
Success
-----
[Expert@HostName-ch0x-0x:0]#
```

## Verifying ARP Entries

Use these commands to confirm that the Unique MAC value has changed.

For the Unique MAC database value, run this command in the Expert mode:

```
g_allc dbget chassis:private:magic_mac
```

Example:

```
[Expert@HostName-ch0x-0x:0]# g_allc dbget chassis:private:magic_mac
--* 4 sgms: 1_01 1_02 2_02 2_03 --*
22
```

For the Unique MAC Kernel value, run this command in Gaia gClish:

```
fw ctl get int fwha_mac_magic
```

Example:

```
[Global] HostName-ch01-01> fw ctl get int fwha_mac_magic
-- 4 sgms: 1_01 1_02 2_02 2_03 --
fwha_mac_magic = 22
[Global] HostName-ch01-01>
```

You can display the magic attribute for interfaces of the type `ethX-YZ` with the "ifconfig" command in the Expert mode.

Example:

```
[Expert@HostName-ch0x-0x:0]# ifconfig eth1-01
eth1-01 Link encap:Ethernet HWaddr 00:1C:7F:81:01:16
        inet6 addr: fe80::21c:7fff:fe81:116/64 Scope:Link
        UP BROADCAST RUNNING SLAVE MULTICAST MTU:1500 Metric:1
        RX packets:154820 errors:0 dropped:0 overruns:0 frame:0
        TX packets:23134 errors:0 dropped:0 overruns:0 carrier:0
        collisions:0 txqueuelen:0 RX bytes:15965660 (15.2 MiB)
        TX bytes:2003398 (1.9 MiB)
[Expert@HostName-ch0x-0x:0]#
```

## Example Legacy Output

This example shows ARP cache for each Security Group Member in the Legacy Mode output:

```
[Expert@HostName-ch0x-0x:0]# asg_arp --legacy
1_01:
Address                HWtype  HWaddress           Flags Mask           Iface
ssm2                   ether   04:02:03:04:05:40   C                    eth2-CIN
ssm1                   ether   02:02:03:04:05:40   C                    eth1-CIN
1_2
172.23.19.4           ether   54:7F:EE:6A:D0:BC   C                    eth1-Mgmt2
1_02:
Address                HWtype  HWaddress           Flags Mask           Iface
1_01                   ether   00:1C:7F:01:04:FE   C                    Sync
ssm1                   ether   02:02:03:04:05:40   C                    eth1-CIN
[Expert@HostName-ch0x-0x:0]#
```

# Working with the GARP Chunk Mechanism

## *In This Section:*

---

Description .....	189
Configuration .....	190
Verification .....	191

---

## Description

When Proxy ARP is enabled, the Firewall responds to ARP requests for hosts other than itself.

When failover occurs between Security Group Members, the new Active Security Group Member sends Gratuitous ARP (GARP) Requests with its own (new) MAC address to update the network ARP tables.

To prevent network congestion during failover, GARP Requests are sent in user defined groups called chunks.

Each chunk contains a predefined number of GARP Requests based on these parameters:

- The number of GARP Requests in each chunk (default is 1000 in each HTU).
- High Availability Time Unit (HTU) - the time interval (1 HTU = 0.1 sec), after which a chunk is sent.
- The chunk mechanism iterates on the proxy ARP IP addresses, and each time sends GARP Requests only for some of them until it completes the full list.

When the iteration sends the full list, it waits  $N$ HTUs and sends the list again.

## Configuration

**i Important** - To make the configuration permanent (to survive reboot), add the applicable kernel parameters to the `$FWDIR/boot/modules/fwkernel.conf` file with this command:

```
g_update_conf_file fwkernel.conf <Parameter>=<Value>
```

For example, to send 10 GARP Requests each second, set the value of the kernel parameter `fwkernel.refresh_arps_chunk` to 1:

```
g_fw_ctl set int fwkernel.refresh_arps_chunk 1
```

To send 50 GARP Requests each second, set the value of the kernel parameter `fwkernel.refresh_arps_chunk` to 5:

```
g_fw_ctl set int fwkernel.refresh_arps_chunk 5
```

Whenever the iteration is finished sending GARP Requests for the entire list, it waits `N` HTUs and sends the GARP Requests again.

The time between the iterations can be configured with these kernel parameters:

Kernel Parameter	Instructions
<code>fwkernel.periodic_send_garps_interval1</code>	<p>The default value is 1 HTU (0.1 second). The Security Group sends the GARP immediately after failover.</p> <p><b>i Important</b> - Do not change this value.</p>
<code>fwkernel.periodic_send_garps_interval2</code>	<p>The default value is 10 HTUs (1 second). After the iteration sends the GARP list, it waits for this period of time and sends it again.</p>
<code>fwkernel.periodic_send_garps_interval3</code>	<p>The default value is 20 HTUs (2 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.</p>
<code>fwkernel.periodic_send_garps_interval4</code>	<p>The default value is 50 HTUs (5 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.</p>
<code>fwkernel.periodic_send_garps_interval5</code>	<p>The default value is 100 HTUs (10 seconds). After the iteration sends the GARP list, it waits for this period of time and sends it again.</p>

To change an interval, run in the Expert mode:

```
g_fw ctl set int fwha_periodic_send_garps_interval<N> <Value>
```

To apply the intervals, run in the Expert mode:

```
g_fw ctl set int fwha_periodic_send_garps_apply_intervals 1
```

## Verification

To send GARP Requests manually, on the SMO, run in the Expert mode:

```
g_fw ctl set int test_arp_refresh 1
```

This causes GARP Requests to be sent (same as was failover).

To debug, run in the Expert mode:

```
g_fw ctl zdebug -m cluster + ch_conf | grep fw_refresh_arp_proxy_
on_failover
```

# NAT and the Correction Layer on a VSX Gateway

In a VSX Gateway, the guidelines in NAT and the Correction Layer on a Security Gateway apply to each Virtual System individually.

For best results, manage an entire session by a specified Virtual System on the same Security Group Member.

When a Virtual Switch (junction) connects several Virtual Systems, the same session can be handled by one Virtual System on one Security Group Member, and by another Virtual System on a different Security Group Member.

When a packet reaches a Virtual System from a junction, the system VSX Stateless Correction Layer checks the distribution again according to the Distribution Mode configured on the WRP interface. It can decide to forward the packet to a different Security Group Member.

In addition, on each Virtual System, the stateful Correction Layer can forward session packets, similar to the Security Gateway.

All forwarding operations have a performance impact. Therefore, the Distribution Mode configuration should minimize forwarding operations.

**To achieve optimal distribution between Security Group Members in a Security Group in VSX mode:**

NAT Rules	Guidelines
Not using NAT rules on any Virtual System	Set the Distribution Mode to <b>General</b> .
Using NAT rule on at least one Virtual System	<ul style="list-style-type: none"> <li>▪ On the Virtual Systems that use NAT rules:           <ul style="list-style-type: none"> <li>• Set the Distribution Mode to <b>User</b> for the networks hidden behind NAT.</li> <li>• Set the Distribution Mode to <b>Network</b> for the destination networks.</li> </ul> </li> <li>▪ On the remaining Virtual Systems that do not use NAT rules:           <ul style="list-style-type: none"> <li>• Set the Distribution Mode to <b>User</b> for the internal networks.</li> <li>• Set the Distribution Mode to <b>Network</b> for the external networks.</li> </ul> </li> </ul>



# NAT and the Correction Layer on a Security Gateway

For optimal system performance, one Security Group Member handles all traffic for a session.

With NAT, packets sent from the client to the server can be distributed to a different Security Group Member than packets from the same session sent from the server to the client.

The system Correction Layer must then forward the packet to the correct Security Group Member.

Configuring the Distribution Mode correctly keeps correction situations to a minimum and optimizes system performance.

**To achieve optimal distribution between Security Group Members in a Security Group in Gateway mode:**

NAT Rules	Guidelines
Not using NAT rules	Set the Distribution Mode to <b>General</b> .
Using NAT rule	<ul style="list-style-type: none"> <li>▪ Set the Distribution Mode to <b>User</b> for the networks hidden behind NAT.</li> <li>▪ Set the Distribution Mode to <b>Network</b> for the destination networks.</li> </ul>

# IPS Management During a Cluster Failover

You can configure how IPS is managed during a cluster failover.

This occurs when one Cluster Member takes over for a different Cluster Member to provide High Availability.

You must run this command in the Expert mode.

## Syntax to configure the IPS behavior during a cluster failover

```
asg_ips_failover_behavior {connectivity | security}
```

## Parameters

Parameter	Description
connectivity	Prefers connectivity (default). Keeps connections alive, even if IPS inspection cannot be guaranteed.
security	Prefers security. Closes connections, for which IPS inspection cannot be guaranteed.

## Syntax to view the configured IPS behavior during a cluster failover

```
fw ctl get int fwha_ips_reject_on_failover
```

Explanation:

Output	Current Configuration
fwha_ips_reject_on_failover = 0	Prefers connectivity
fwha_ips_reject_on_failover = 1	Prefers security

# IPv6 Neighbor Discovery

Neighbor discovery works over the ICMPv6 Neighbor Discovery protocol, which is the functional equivalent of the IPv4 ARP protocol.

ICMPv6 Neighbor Discovery Protocol must be explicitly permitted in the Access Control Rule Base for all bridged networks.

This is different from ARP. ARP traffic is Layer 2 only, therefore it permitted regardless of the Rule Base.

This is an example of an explicit Rule Base that permits ICMPv6 Neighbor Discovery protocol:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
IPv6 Neighbor Discovery	Network object that represents the Bridged Network	Network object that represents the Bridged Network	Any	neighbor-advertisement neighbor-solicitation router-advertisement router-solicitation redirect6	Accept	Log	Policy Targets

# Logging and Monitoring

This section provides instructions for monitoring the environment.

## CPView

### Overview of CPView

#### Description

CPView is a text based built-in utility on a Check Point computer.

CPView Utility shows statistical data that contain both general system information (CPU, Memory, Disk space) and information for different Software Blades (only on Security Group).

The CPView continuously updates the data in easy to access views.

On Security Group, you can use this statistical data to monitor the performance.

For more information, see [sk101878](#).

#### Syntax

```
cpview --help
```

### CPView User Interface

The CPView user interface has three sections:

Section	Description
<b>Header</b>	This view shows the time the statistics in the third view are collected. It updates when you refresh the statistics.
<b>Navigation</b>	This menu bar is interactive. Move between menus with the arrow keys and mouse. A menu can have sub-menus and they show under the menu bar.
<b>View</b>	This view shows the statistics collected in that view. These statistics update at the refresh rate.

## Using CPView

Use these keys to navigate the CPView:

Key	Description
Arrow keys	Moves between menus and views. Scrolls in a view.
Home	Returns to the <b>Overview</b> view.
Enter	Changes to the <b>View Mode</b> . On a menu with sub-menus, the <b>Enter</b> key moves you to the lowest level sub-menu.
Esc	Returns to the <b>Menu Mode</b> .
Q	Quits CPView.

Use these keys to change CPView interface options:

Key	Description
R	Opens a window where you can change the refresh rate. The default refresh rate is 2 seconds.
W	Changes between wide and normal display modes. In wide mode, CPView fits the screen horizontally.
S	Manually sets the number of rows or columns.
M	Switches on/off the mouse.
P	Pauses and resumes the collection of statistics.

Use these keys to save statistics, show help, and refresh statistics:

Key	Description
C	Saves the current page to a file. The file name format is: <code>cpview_&lt;ID of the cpview process&gt;.cap&lt;Number of the capture&gt;</code>
H	Shows a tooltip with CPView options.
Space bar	Immediately refreshes the statistics.

# Network Monitoring

You can monitor and log traffic.

## Working with Interface Status (asg if)

### Description

Use the "asg if" command in Gaia gClish or the Expert mode to:

- Enable and disable the interfaces
- Show information about interfaces:
  - IPv4, IPv6, and MAC address
  - Interface type
  - Link State
  - Speed
  - MTU
  - Duplex

### Syntax

```
asg if -h
```

```
asg if -i <Interface1>[,<Interface2>, ..., <InterfaceN>] [-v]  
[enable | disable]
```

```
asg if -ip <IP Address>
```

## Parameters

Parameter	Description
-h	Shows the built-in help.
No Parameters	Shows information about all interfaces.
-i <Interface1> [,< Interface2 >, ..., <InterfaceN>]	Shows information only about the interfaces specified by their names. <ul style="list-style-type: none"> <li>▪ You can specify one or more interfaces.</li> <li>▪ If you specify more than interface, you must separate their names by a comma without spaces. Example: <code>asg if -i Sync,eth1-Mgmt1</code></li> </ul>
-v	Shows verbose output. <b>Note</b> - This view is not supported for logical interfaces (for example, Bond, VLAN, and <code>ethX-MgmtY</code> interfaces).
enable	Enables the specified interfaces.
disable	Disables the specified interfaces.
-ip <IP Address>	Shows information only about one interface specified by its IPv4 or IPv6 address.

## Verbose Mode (asg if -v)

The Verbose Mode shows extended information, including information retrieved from the switch.

You can use the Verbose Mode for one interface or a comma-separated list of interfaces (without spaces).

This operation can take a few seconds for each interface.

### Example output

```
[Expert@HostName-ch0x-0x:0]# asg if -i eth1-01 -v
Collecting information, may take few seconds
-----+
|Interfaces Data                                     |
+-----+
|Interface|IPv4 Address      |Info      |State      |Speed  |MTU   |Duplex |
|         |MAC Address      |         | (ch1) / (ch2) |      |      |      |
|         |IPv6 Address (global)|         |         |      |      |      |
|         |IPv6 Address (local)|         |         |      |      |      |
+-----+
|eth1-01  |-                |Bond slave| (up) / (up) |10G    |1500  |Full   |
|         |00:1c:7f:a1:01:0|         |master:      |      |      |      |
|         |-                |         |bond1 (up) / (up)|      |      |      |
|         |-                |         |         |      |      |      |
+-----+
|Comment                                     |
+-----+
|internal interface                         |
+-----+
|Traffic                                     |
+-----+
|media          |In traffic |In pkt(uni/mul/brd)|Out traffic  |Out pkt(uni/mul/brd)|
+-----+
|FTLF8528P2BNV-EM |28.8Kbps  |0pps/38pps/5pps   |4.1Mbps     |0pps/355pps/0pps   |
+-----+
|Errors (total/pps)                                     |
+-----+
|OutDiscards          |InDiscards      |InErrors      |OutErrors      |
+-----+
|0/0                  |0/0              |0/0            |0/0            |
+-----+
[Expert@HostName-ch0x-0x:0]#
```



## Global View of All Interfaces (show interfaces)

Use the "show interfaces" command in Gaia gClish to show the current status of all defined interfaces on the system.

### Example

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> show interfaces
+-----+
| Interfaces Data
+-----+
| Interface | IPv4 Address | Info | State | Speed | MTU | Duplex |
|           | MAC Address  |      | (chl) |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| bond1     | 17.17.17.10  | Bond Master | (down) | NA     | NA  | NA     |
|           | 00:1c:7f:81:05:fe |          | slaves: |        |     |         |
|           |              |          | eth1-05 (down) |        |     |         |
|           |              |          | eth2-05 (down) |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| eth1-05   | -           | Bond slave | (down) | 10G    | 1500 | Full   |
|           | 00:1c:7f:81:05:fe |          | master: |        |     |         |
|           |              |          | bond1 (down) |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| eth2-05   | -           | Bond slave | (down) | 10G    | 1500 | Full   |
|           | 00:1c:7f:81:05:fe |          | master: |        |     |         |
|           |              |          | bond1 (down) |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| bond1.201 | 18.18.18.10  | Vlan      | (down) | NA     | NA  | NA     |
|           | 00:1c:7f:81:05:fe |          |        |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| br0       | -           | Bridge Mast | (up)   | NA     | NA  | NA     |
|           | 00:1c:7f:81:07:fe |          | ports: |        |     |         |
|           |              |          | eth2-07 (down) |        |     |         |
|           |              |          | eth1-07 (down) |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| eth1-07   | -           | Bridge port | (down) | 10G    | 1500 | Full   |
|           | 00:1c:7f:81:07:fe |          | master: |        |     |         |
|           |              |          | br0 (up) |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| eth2-07   | -           | Bridge port | (down) | 10G    | 1500 | Full   |
|           | 00:1c:7f:82:07:fe |          | master: |        |     |         |
|           |              |          | br0 (up) |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| eth1-01   | 15.15.15.10  | Ethernet  | (up)   | 10G    | 1500 | Full   |
|           | 00:1c:7f:81:01:fe |          |        |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| eth1-Mgmt4 | 172.23.9.67  | Ethernet  | (up)   | 10G    | 1500 | Full   |
|           | 00:d0:c9:ca:c7:fa |          |        |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| eth2-01   | 25.25.25.10  | Ethernet  | (up)   | 10G    | 1500 | Full   |
|           | 00:1c:7f:82:01:fe |          |        |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
| Sync      | 192.0.2.1    | Ethernet  | (up)   | 10G    | 1500 | Full   |
|           | 00:1c:7f:01:04:fe |          |        |        |     |         |
+-----+-----+-----+-----+-----+-----+-----+
[Global] HostName-ch01-01>
```



### Notes:

- This sample output shows that this Sync interface is a Bond-Master and if the interfaces are UP or DOWN.
- To add a comment to an interface, run in Gaia gClish:

```
> set interface <Name of Interface> comment "<Comment Text>"
```

# Monitoring Traffic (asg\_ifconfig)

## Description

The "asg\_ifconfig" command in Gaia gClish or the Expert mode collects traffic statistics from all or a specified range of Security Group Members.

The combined output shows the traffic distribution between Security Group Members and their interfaces (calculated during a certain period).

The "asg\_ifconfig" command has these modes:

Mode	Instructions
<b>Native</b>	This is the default setting. When you do not specify the "analyze" or "banalyze" option in the syntax, the command behaves almost in the same as the native Linux "ifconfig" command. However, the output shows statistics for all interfaces on all Security Group Members, and for interfaces on the local Security Group Member.
<b>Analyze</b>	Shows accumulated traffic information and traffic distribution between Security Group Members.
<b>Banalyze</b>	Shows accumulated traffic information and traffic distribution between interfaces.

### Notes:

- The parameters "analyze" and "banalyze" are mutually exclusive. You cannot specify them in the same command.
- If you run this command in the context of a Virtual System, you can only see the output that applies to that context.

## Syntax

```
asg_ifconfig -h
```

```
asg_ifconfig [-b <SGM IDs>] [<Name of Interface>] [analyze [-d <Delay>] [-a] [-v]]
```

```
asg_ifconfig [-b <SGM IDs>] [<Name of Interface>] [banalyze [-d <Delay>] [-a] [-v] [-rb] [-rd] [-rp] [-tb] [-td] [-tp]]
```

## Parameters

Parameter	Description																
-h	Shows the built-in help.																
-b <SGM IDs>	<p>Applies to Security Group Members as specified by the &lt;SGM IDs&gt;. &lt;SGM IDs&gt; can be:</p> <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul>																
<Name of Interface>	Specifies the name of the interface.																
analyze	<p>Shows accumulated traffic information and traffic distribution between the Security Group Members.</p> <p>Use the "-a", "-v", and "-d &lt;Delay&gt;" parameters to show traffic distribution between interfaces.</p>																
banalyze	<p>Shows accumulated traffic information and traffic distribution between the interfaces.</p> <p>Use the "-a", "-v", and "-d &lt;Delay&gt;" parameters to show traffic distribution between interfaces.</p> <p>By default, the traffic distribution table is not sorted.</p> <p>You can use these parameters to sort the traffic distribution table:</p> <ul style="list-style-type: none"> <li>▪ -rb - Sort the output by the number of received (RX) bytes</li> <li>▪ -rd - Sort the output by the number of received (RX) dropped packets</li> <li>▪ -rp - Sort the output by the number of received (RX) packets</li> <li>▪ -tb - Sort the output by the number of transmitted (TX) bytes</li> <li>▪ -td - Sort the output by the number of transmitted (TX) dropped packets</li> <li>▪ -tp - Sort the output by the number of transmitted (TX) packets</li> </ul> <p>For example, if you sort with the "-rb" option, the higher values appear at the top of the "RX bytes" column:</p> <table border="1" style="margin-left: 20px;"> <thead> <tr> <th>SGM ID</th> <th>RX packets</th> <th>RX bytes</th> <th>RX dropped</th> </tr> </thead> <tbody> <tr> <td>1_03</td> <td></td> <td>70%</td> <td></td> </tr> <tr> <td>1_02</td> <td></td> <td>20%</td> <td></td> </tr> <tr> <td>1_01</td> <td></td> <td>10%</td> <td></td> </tr> </tbody> </table>	SGM ID	RX packets	RX bytes	RX dropped	1_03		70%		1_02		20%		1_01		10%	
SGM ID	RX packets	RX bytes	RX dropped														
1_03		70%															
1_02		20%															
1_01		10%															
-d <Delay>	<p>Delay, in seconds, between data samples.</p> <p>Default: 5 seconds.</p>																

Parameter	Description
-a	Shows total traffic volume. By default (without "-a"), the output shows the average traffic volume per second.
-v	Verbose mode. Shows detailed information of each interface and the accumulated traffic information

## Examples

### Example 1 - Default output

This example shows the total traffic sent and received by the interface `eth2-01` for all Security Group Members on Site 1 (Active Site)..

By default, the output shows the average traffic volume per second.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg_ifconfig -b chassis1 eth2-01

as1_02:
eth2-01    Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX packets:94 errors:0 dropped:0 overruns:0 frame:0
           TX packets:63447 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:5305 (5.1 KiB)  TX bytes:5688078 (5.4 MiB)

1_03:
eth2-01    Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX packets:137 errors:0 dropped:0 overruns:0 frame:0
           TX packets:26336 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:7591 (7.4 KiB)  TX bytes:2355386 (2.2 MiB)

1_04:
eth2-01    Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX packets:124 errors:0 dropped:0 overruns:0 frame:0
           TX packets:3098 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:6897 (6.7 KiB)  TX bytes:378990 (370.1 KiB)

1_05:
eth2-01    Link encap:Ethernet  HWaddr 00:1C:7F:81:01:EA
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX packets:79 errors:0 dropped:0 overruns:0 frame:0
           TX packets:26370 errors:0 dropped:0 overruns:0 carrier:0
           collisions:0 txqueuelen:0
           RX bytes:4507 (4.4 KiB)  TX bytes:2216546 (2.1 MiB)
[Global] HostName-ch01-01>
```

## Example 2 - The 'analyze' mode

This example shows:

- The accumulated and detailed traffic volume statistics for the interface `eth2-Sync` for each Security Group Member.
- The total for all Security Group Members.
- The traffic distribution for each Security Group Member.
- The `-a` option shows the total traffic volume instead of the average volume per second.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg_ifconfig eth2-Sync analyze -v -a
Command is executed on SGMs: chassis_active

1_01:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:01:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:225018 bytes:36970520 (37.0 MiB)  dropped:0
           TX: packets:3522445 bytes:1381032583 (1.4 GiB)  dropped:0

1_02:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:02:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:221395 bytes:35947248 (35.9 MiB)  dropped:0
           TX: packets:4674143 bytes:1850315554 (1.9 GiB)  dropped:0

1_03:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:03:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:10 bytes:644 (644.0 b)  dropped:0
           TX: packets:67826313 bytes:7345458105 (7.3 GiB)  dropped:0

1_04:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:04:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:13 bytes:860 (860.0 b)  dropped:0
           TX: packets:68489217 bytes:7487476060 (7.5 GiB)  dropped:0

1_05:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:05:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:203386 bytes:19214238 (19.2 MiB)  dropped:0
           TX: packets:7164109 bytes:2740761091 (2.7 GiB)  dropped:0

== Accumulative ==
eth2-Sync  Link encap:Ethernet
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:649822 bytes:92133510 (92.1 MiB)  dropped:0
           TX: packets:151676227 bytes:20805043393 (20.8 GiB)  dropped:0

== Traffic Distribution ==

-----
      SGM ID  RX packets   RX bytes  RX dropped  TX packets   TX bytes  TX dropped
-----
      1_01    34.6%        40.1%      0.0%        2.3%        6.6%      0.0%
      1_02    34.1%        39.0%      0.0%        3.1%        8.9%      0.0%
      1_03     0.0%         0.0%      0.0%        44.7%       35.3%     0.0%
      1_04     0.0%         0.0%      0.0%        45.2%       36.0%     0.0%
      1_05    31.3%        20.9%      0.0%        4.7%       13.2%     0.0%
-----

[Global] HostName-ch01-01>
```

## Example 2 - The 'banalyze' mode

This example shows:

- The accumulated and detailed traffic volume statistics for the interface `eth2-Sync` on each Security Group Member.
- The total on each Security Group Member.
- The traffic distribution on each Security Group Member.
- The `-a` option shows the total traffic volume instead of the average volume per second.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg_ifconfig eth2-Sync banalyze -v -a
Command is executed on SGMs: chassis_active
```

```
1_01:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:01:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:225018 bytes:36970520 (37.0 MiB)  dropped:0
           TX: packets:3522445 bytes:1381032583 (1.4 GiB)  dropped:0
```

```
== Accumulative ==
           RX: packets:225018 bytes:36970520 (37.0 MiB)  dropped:0
           TX: packets:3522445 bytes:1381032583 (1.4 GiB)  dropped:0
```

```
== Traffic Distribution ==
```

```
-----
Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
-----
eth2-Sync  100.0%      100.0%      0.0%      100.0%      100.0%      0.0%
-----
```

```
1_02:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:02:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:221395 bytes:35947248 (35.9 MiB)  dropped:0
           TX: packets:4674143 bytes:1850315554 (1.9 GiB)  dropped:0
```

```
== Accumulative ==
           RX: packets:221395 bytes:35947248 (35.9 MiB)  dropped:0
           TX: packets:4674143 bytes:1850315554 (1.9 GiB)  dropped:0
```

```
== Traffic Distribution ==
```

```
-----
Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
-----
eth2-Sync  100.0%      100.0%      0.0%      100.0%      100.0%      0.0%
-----
```

```
1_03:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:03:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:10 bytes:644 (644.0 b)  dropped:0
           TX: packets:67826313 bytes:7345458105 (7.3 GiB)  dropped:0
```

```
== Accumulative ==
           RX: packets:10 bytes:644 (644.0 b)  dropped:0
           TX: packets:67826313 bytes:7345458105 (7.3 GiB)  dropped:0
```

```
== Traffic Distribution ==
```

```
-----
Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
-----
eth2-Sync  100.0%      100.0%      0.0%      100.0%      100.0%      0.0%
-----
```

```
1_04:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:04:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:13 bytes:860 (860.0 b)  dropped:0
           TX: packets:68489217 bytes:7487476060 (7.5 GiB)  dropped:0
```

```
== Accumulative ==
           RX: packets:13 bytes:860 (860.0 b)  dropped:0
           TX: packets:68489217 bytes:7487476060 (7.5 GiB)  dropped:0
```

```
== Traffic Distribution ==
```

```

-----
Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
-----
eth2-Sync 100.0%    100.0%    0.0%    100.0%    100.0%    0.0%
-----

1_05:
eth2-Sync  Link encap:Ethernet  HWaddr 00:1C:7F:05:04:FE
           UP BROADCAST RUNNING SLAVE MULTICAST  MTU:1500  Metric:1
           RX: packets:203386 bytes:19214238 (19.2 MiB)  dropped:0
           TX: packets:7164109 bytes:2740761091 (2.7 GiB)  dropped:0

== Accumulative ==
           RX: packets:203386 bytes:19214238 (19.2 MiB)  dropped:0
           TX: packets:7164109 bytes:2740761091 (2.7 GiB)  dropped:0

== Traffic Distribution ==

-----
Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
-----
eth2-Sync 100.0%    100.0%    0.0%    100.0%    100.0%    0.0%
-----

== All Blades ==
           RX: packets:649822 bytes:92133510 (92.1 MiB)  dropped:0
           TX: packets:148153782 bytes:20805043393 (20.8 GiB)  dropped:0

== Traffic Distribution == (all blades)

-----
Interface RX packets RX bytes RX dropped TX packets TX bytes TX dropped
-----
eth2-Sync 100.0%    100.0%    0.0%    100.0%    100.0%    0.0%
-----

[Global] HostName-ch01-01>

```



# Monitoring Multicast Traffic

## *In This Section:*

---

Showing Multicast Routing ( <code>asg_mroute</code> ) .....	209
Showing PIM Information ( <code>asg_pim</code> ) .....	212
Showing IGMP Information ( <code>asg_igmp</code> ) .....	215

---

Use these commands to show information about multicast traffic.

## Showing Multicast Routing (`asg_mroute`)

### Description

The "`asg_mroute`" command in Gaia gClish or the Expert mode shows this multicast routing information in a tabular format:

- **Source** - Source IP address
- **Dest** - Destination address
- **lif** - Source interface
- **Oif** - Outbound interface

You can filter the output for specified interfaces and Security Group Members.

### Syntax

```
asg_mroute -h
```

```
asg_mroute [-d <Destination Route>] [-s <Source Route>] [-i  
<Source Interface>] [-b <SGM IDs>]
```

## Parameters

Parameter	Description
-h	Shows the built-in help.
No Parameters	Shows all routes, interfaces and Security Group Members.
-d <i>&lt;Destination Route&gt;</i>	Specifies the destination multicast group IP address.
-s <i>&lt;Source Route&gt;</i>	Specifies the source IP address.
-i <i>&lt;Source Interface&gt;</i>	Specifies the source interface name.
-b <i>&lt;SGM IDs&gt;</i>	<p>Applies to Security Group Members as specified by the <i>&lt;SGM IDs&gt;</i>.</p> <p><i>&lt;SGM IDs&gt;</i> can be:</p> <ul style="list-style-type: none"> <li>▪ No <i>&lt;SGM IDs&gt;</i> specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul>

## Examples

### Example 1 - Shows all multicast routes for all interfaces and Security Group Members

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg_mroute
+-----+
|Multicast Routing (All SGMs)                                     |
+-----+-----+-----+-----+
|Source                |Dest                |Iif                |Oif                |
+-----+-----+-----+-----+
|12.12.12.1           |225.0.90.90        |eth1-01           |eth1-02           |
+-----+-----+-----+-----+
|22.22.22.1           |225.0.90.90        |eth1-02           |eth1-01           |
+-----+-----+-----+-----+
|22.22.22.1           |225.0.90.91        |eth1-02           |eth1-01           |
+-----+-----+-----+-----+
[Global] HostName-ch01-01>
```

### Example 2 - Shows only specific IP address, interfaces, destination IP address, or Security Group Members

```
[Expert@HostName-ch0x-0x:0]# asg_mroute -s 22.22.22.1 -i eth1-02 -d 225.0.90.91
+-----+
|Multicast Routing (All SGMs)                                     |
+-----+-----+-----+-----+
|Source                |Dest                |Iif                |Oif                |
+-----+-----+-----+-----+
|22.22.22.1           |225.0.90.91        |eth1-02           |eth2-01           |
+-----+-----+-----+-----+
[Expert@HostName-ch0x-0x:0]#
```

## Showing PIM Information (asg\_pim)

### Description

The `asg_pim` command in Gaia gClish or the Expert mode shows this PIM information in a tabular format:

- **Source** - Source IP address
- **Dest** - Destination IP address
- **Mode** - Both Dense Mode and Sparse Mode are supported
- **Flags** - Local source and MFC state indicators
- **In. intf** - Source interface
- **RPF** - Reverse Path Forwarding indicator
- **Out int** - Outbound interface
- **State** - Outbound interface state

You can filter the output for specified interfaces and Security Group Members.

### Syntax

```
asg_pim -h
```

```
asg_pim [-b <SGM IDs>] [-i <if>]
```

```
asg_pim neighbors [-n <neighbor>]
```

### Parameters

Parameter	Description
-h	Shows the built-in help.
No Parameters	Shows all routes, interfaces and Security Group Members.
-b <SGM IDs>	Applies to Security Group Members as specified by the <SGM IDs>. <SGM IDs> can be: <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul>
-i <if>	Shows only the specified source interface.

Parameter	Description
neighbors	<p>Runs verification tests to make sure that PIM neighbors are the same on all Security Group Members and shows this information:</p> <ul style="list-style-type: none"> <li>▪ <b>Verification</b> - Results of verification test</li> <li>▪ <b>Neighbor</b> - PIM neighbor</li> <li>▪ <b>Interface</b> - Interface name</li> <li>▪ <b>Holdtime</b> - Time in seconds to hold a connection open during peer negotiation</li> <li>▪ <b>Expires</b> - Minimum and Maximum expiration values for all Security Group Members</li> </ul>
-n <neighbor>	Shows only the specified PIM neighbor.

## Examples

### Example 1 - Shows PIM information and multicast routes for all interfaces and Security Group Members

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg_pim
-----+
|PIM (All SGMs)
-----+
|source      |dest      |Mode      |Flags|In. intf |RPF      |Out. intf |State  |
-----+-----+-----+-----+-----+-----+-----+-----+
|12.12.12.1  |225.0.90.90 |Dense-Mode|L|M  |eth1-01  |none     |      |      |
-----+-----+-----+-----+-----+-----+-----+-----+
|22.22.22.1  |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none     |eth1-01  |Forwarding|
-----+-----+-----+-----+-----+-----+-----+-----+
|22.22.22.1  |225.0.90.91 |Dense-Mode|L|M  |eth1-02  |none     |eth1-01  |Forwarding|
|              |              |              |      |          |          |eth2-01  |Forwarding|
-----+-----+-----+-----+-----+-----+-----+-----+
Flags: L - Local source, M - MFC State
[Global] HostName-ch01-01>
```

**Example 2 - Shows PIM Information for the specific interface on all Security Group Members**

```
[Expert@HostName-ch0x-0x:0]# asg_pim -i eth1-02 -b all
+-----+
|PIM (All SGMs)
+-----+
|SGM 1_01
+-----+
|source      |dest        |Mode      |Flags|In. intf |RPF      |Out. intf |State  |
+-----+-----+-----+-----+-----+-----+-----+-----+
|22.22.22.1  |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none     |eth1-01  |Forwarding|
+-----+-----+-----+-----+-----+-----+-----+-----+
|22.22.22.1  |225.0.90.91 |Dense-Mode|L    |eth1-02  |none     |eth1-01  |Forwarding|
|            |            |          |    |          |         |eth2-01  |Forwarding|
+-----+-----+-----+-----+-----+-----+-----+-----+
|SGM 1_02
+-----+
|source      |dest        |Mode      |Flags|In. intf |RPF      |Out. intf |State  |
+-----+-----+-----+-----+-----+-----+-----+-----+
|22.22.22.1  |225.0.90.90 |Dense-Mode|L|M  |eth1-02  |none     |eth1-01  |Forwarding|
+-----+-----+-----+-----+-----+-----+-----+-----+
|22.22.22.1  |225.0.90.91 |Dense-Mode|L|M  |eth1-02  |none     |eth1-01  |Forwarding|
|            |            |          |    |          |         |eth2-01  |Forwarding|
+-----+-----+-----+-----+-----+-----+-----+-----+
[Expert@HostName-ch0x-0x:0]#
```

**Example 3 - Shows PIM neighbors**

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg_pim neighbors
+-----+
|PIM Neighbors (All SGMs)
+-----+
|Verification:
|Neighbors Verification: Passed - Neighbors are identical on all blades
+-----+
|Neighbor      |Interface    |Holdtime   |Expires (min-max)
+-----+-----+-----+-----+
|11.1.1.1      |bond1       |105        |11:36:45-11:37:59
+-----+-----+-----+-----+
[Global] HostName-ch01-01>
```

## Showing IGMP Information (asg\_igmp)

### Description

Use the `asg_igmp` command in Gaia gClish or the Expert mode to show IGMP information in a tabular format.

You can filter the output for specified interfaces and Security Group Members. If no Security Group Member is specified, the command runs a verification to make sure that IGMP data is the same on all Security Group Members:

- Group verification - Confirms the groups exist on all Security Group Members. If a group is missing on some Security Group Members, a message shows which group is missing on which blade.
- Global properties - Confirms the flags, address and other information are the same on all Security Group Members.
- Interfaces - Confirms that all blades have the same interfaces and that they are in the same state (UP or DOWN). If inconsistencies are detected, a warning message shows.

### Syntax

```
asg_igmp -h
```

```
asg_igmp [-i <interface>] [-b <SGM IDs>]
```

### Parameters

Parameter	Description
-h	Shows the built-in help.
-i <interface>	Source interface name.
-b <SGM IDs>	Applies to Security Group Members as specified by the <SGM IDs>. <SGM IDs> can be: <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or <code>all</code> Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, <code>1_1</code>)</li> </ul>

## Examples

### Example 1 - Shows IGMP information and multicast routes for all interfaces and Security Group Members

Note - In this example, the verification detected an interface inconsistency.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg_igmp

Collecting IGMP information, may take few seconds...
+-----+
|IGMP (All SGMs)                                     |
+-----+
|Interface: eth1-01                                  |
+-----+
|Verification:                                       |
|Group Verification: Passed - Information is identical on all blades |
|Global Properties Verification: Passed - Information is identical on all blades |
+-----+
|Group          |Age      |Expire   |
+-----+-----+-----+
|225.0.90.91    |2m       |4m       |
+-----+-----+-----+
|Flags          |IGMP Ver|Query Interval|Query Response Interval|protocol|Advertise Address|
+-----+-----+-----+-----+-----+-----+
|Querier        |2        |125      |10          |PIM     |12.12.12.10     |
+-----+-----+-----+-----+-----+

+-----+
|Interface: eth1-02                                  |
+-----+
|Verification:                                       |
|Group Verification: Failed - Found inconsistency between blades |
| -Group 225.0.90.92: missing in blades 1_02 |
|Global Properties Verification: Passed - Information is identical on all blades |
+-----+
|Group          |Age      |Expire   |
+-----+-----+-----+
|225.0.90.92    |2m       |3m       |
+-----+-----+-----+
|Flags          |IGMP Ver|Query Interval|Query Response Interval|protocol|Advertise Address|
+-----+-----+-----+-----+-----+-----+
|Querier        |2        |125      |10          |PIM     |22.22.22.10     |
+-----+-----+-----+-----+-----+

+-----+
|Interface: eth2-01                                  |
+-----+
|Verification:                                       |
|Group Verification: Passed - Information is identical on all blades |
|Global Properties Verification: Passed - Information is identical on all blades |
+-----+
|Group          |Age      |Expire   |
+-----+-----+-----+
|225.0.90.90    |2m       |3m       |
+-----+-----+-----+
|Flags          |IGMP Ver|Query Interval|Query Response Interval|protocol|Advertise Address|
+-----+-----+-----+-----+-----+-----+
|Querier        |2        |125      |10          |PIM     |2.2.2.10        |
+-----+-----+-----+-----+-----+

NOTE: Inconsistency found in interfaces configuration between blades
Inconsistent interfaces: eth1-02
[Global] HostName-ch01-01>
```



**Example 2 - Shows IGMP Information for a specified interface**

```
[Expert@HostName-ch0x-0x:0]# asg_igmp -i bond1.3
Collecting IGMP information, may take few seconds...
+-----+
|IGMP (All SGMs)                                     |
+-----+
|Interface: bond1.3                                  |
+-----+
|Verification                                         |
|Group Verification: Passed - Information is identical on all blades |
|Global Properties Verification: Passed - Information is identical on all blades |
+-----+
|Group          |Age          |Expire       |
+-----+-----+-----+
|225.0.90.90    |46m         |3m           |
+-----+-----+-----+
|Flags          |IGMP Ver    |Query Interval |Query Response Interval |protocol |Advertise Address|
+-----+-----+-----+-----+-----+-----+
|Querier        |2           |125           |10                       |PIM     |12.12.12.11     |
+-----+-----+-----+-----+-----+
[Expert@HostName-ch0x-0x:0]#
```

# Monitoring VPN Tunnels

Because VPN tunnels synchronize between all Security Group Members, use traditional tools to monitor tunnels.

## SmartConsole


You must **not** activate the **Monitoring** Software Blade in the Security Gateway (Security Group) object.

You can still see VPN tunnel status and details information in SmartConsole.

## SNMP

- You can use the OID sub-tree **tunnelTable** (.1.3.6.1.4.1.2620.500.9002 ) in the Check Point MIB to see the VPN status.
- For VSX environments, search for the *SNMP Monitoring* section in the [R81.20 VSX Administration Guide](#) for VSX-related SNMP information.

## CLI Tools

 **Note** - In a VSX environment, you must run these commands from the context of the applicable Virtual System.

Use these commands:

- To see VPN statistics for each Security Group Member, run in the Expert mode:

```
cpstat -f all vpn
```

- To monitor VPN tunnels for each Security Group Member, run in the Expert mode:

```
vpn tu
```

VPN tunnels are synchronized to all Security Group Members. Therefore, you can run this command from the scope of one Security Group Member.

- To monitor VPN tunnels in the non-interactive mode, run in Gaia gClish:

```
vpn shell tunnels
```

# Traceroute (asg\_tracert)

## Description

Use the "asg\_tracert" command in Gaia gClish or the Expert mode to show correct `tracert` results on the Security Group.

The native "tracert" cannot handle the "tracert" pings correctly because of the stickiness mechanism used in the Security Group Firewall.

The "asg\_tracert" command supports all native options and parameters of the `tracert` command.

## Syntax

```
asg_tracert <IP Address> [<tracert Options>]
```

## Parameters

Parameter	Description
<IP Address>	Specifies the destination IP address.
<tracert Options>	Specifies the native <code>tracert</code> command options.

## Example

```
[Expert@HostName-ch0x-0x:0]# asg_tracert 100.100.100.99
  traceroute to 100.100.100.99 (100.100.100.99), 30 hops max, 40 byte packets
  1  (20.20.20.20)  0.722 ms  0.286 ms  0.231 ms
  2  (100.100.100.99) 1.441 ms  0.428 ms  0.395 ms
[Expert@HostName-ch0x-0x:0]#
```

# Multi-blade Traffic Capture (tcpdump)

## Description

Use the "tcpdump" commands in Gaia gClish to capture and show traffic that is sent and received by Security Group Members in the Security Group.

These commands are enhancements to the standard `tcpdump` utility:

Command	Description
<code>tcpdump -mcap</code>	Saves packets from specified Security Group Members to a capture file.
<code>tcpdump -view</code>	Shows packets from the specified capture file, including the Security Group Member ID.



**Note** - Use the "g\_tcpdump" command in the Expert mode.

## Syntax

```
tcpdump [-b <SGM IDs>] -mcap -w <Output File> [<tcpdump Options>]
```

```
tcpdump -view -r <Input File> [<tcpdump Options>]
```



**Note** - To stop the capture and save the data to the capture file, press **CTRL+C** at the prompt.

## Parameters

Parameter	Description
<code>-b &lt;SGM IDs&gt;</code>	<p>Applies to Security Group Members as specified by the <code>&lt;SGM IDs&gt;</code>. <code>&lt;SGM IDs&gt;</code> can be:</p> <ul style="list-style-type: none"> <li>▪ No <code>&lt;SGM IDs&gt;</code> specified, or <code>all</code> Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, <code>1_1</code>)</li> </ul>

Parameter	Description
<code>-w &lt;Output File&gt;</code>	<p>Saves the captured packets at the specified path in a file with the specified the name.</p> <p>This output file contains captured packets from all specified Security Group Members.</p> <p>In the same directory, the command saves additional output files for each Security Group Member.</p> <p>The names of these additional files are: <code>&lt;SGM ID&gt;_&lt;Specified Name of Output File&gt;</code></p> <p>Example:</p> <ul style="list-style-type: none"> <li>▪ The specified full path is: /tmp/capture.cap</li> <li>▪ The additional capture files are: /tmp/1_1_capture.cap /tmp/1_2_capture.cap /tmp/1_3_capture.cap and so on</li> </ul>
<code>-r &lt;Input File&gt;</code>	<p>Reads the captured packets (in the <code>tcpdump</code> format) from the specified path from a file with the specified the name.</p>
<code>&lt;tcpdump Options&gt;</code>	<p>Standard <code>tcpdump</code> parameters.</p> <p>See the <code>tcpdump</code> manual page - <a href="https://linux.die.net/man/8/tcpdump">https://linux.die.net/man/8/tcpdump</a>.</p>

## Examples

### Example 1 - Capture packets on all Security Group Members

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > tcpdump -mcap -w /tmp/capture.cap
Capturing packets...
Write "stop" and press enter to stop the packets capture process.
1_01:
tcpdump: listening on eth1-Mgmt4, link-type EN10MB (Ethernet), capture size 96 bytes

Clarification about this output:
At this moment, an administrator pressed the CTRL+C keys

stop
Received user request to stop the packets capture process.

Copying captured packets from all SGMs...
Merging captured packets from SGMs to /tmp/capture.cap...
Done.
[Global] HostName-ch01-01>
```

### Example 2 - Capture packets from specified Security Group Members and interfaces

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > tcpdump -b 1_1,1_3,2_1 -mcap -w /tmp/capture.cap -nnni eth1-Mgmt4
... ..
[Global] HostName-ch01-01 >
```

### Example 3 - Show captured packets from a file

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> tcpdump -view -r /tmp/capture.cap
Reading from file /tmp/capture.cap, link-type EN10MB (Ethernet)
[1_3] 14:11:57.971587 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
[2_3] 14:12:07.625171 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
[2_3] 14:12:09.974195 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 37
[2_1] 14:12:09.989745 IP 0.0.0.0.cp-cluster > 172.16.6.0.cp-cluster: UDP, length 45
[2_3] 14:12:10.022995 IP 0.0.0.0.cp-cluster > 172.23.9.0.cp-cluster: UDP, length 32
... ..
[Global] HostName-ch01-01>
```

## Monitoring Management Interfaces Link State

By default, Security Group monitors the link state only on data ports (`eth<X>-<YZ>`).

The Management Monitor feature uses SNMP to monitor management ports on the Quantum Maestro Orchestrators.

The link state is sent to all Security Group Members.

The Management Monitor feature is disabled by default.

To enable this feature, run the `set chassis high-availability mgmt-monitoring on` command in Gaia gClish of the Security Group.

When the Management Monitor feature is enabled:

- The monitored management ports are included in the Security Group grade mechanism, according to the predefined factors (default is 11).
- The output of the `asg stat -v` command shows the Management ports.  
See the `Chassis Parameters > Ports > Mgmt` line in the output example below.
- The `show interfaces` command in Gaia gClish shows the link state of management interfaces based on this feature mechanism.

## Example

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> show chassis high-availability mgmt-monitoring
off
[Global] HostName-ch01-01> set chassis high-availability mgmt-monitoring on
[Global] HostName-ch01-01>
[Global] HostName-ch01-01> show chassis high-availability mgmt-monitoring
on
[Global] HostName-ch01-01> asg stat -v
-----
| System Status - Maestro |
-----
| Up time           | 13:10:04 hours |
| SGMs              | 2 / 2          |
| Version           | R81.20 (Build Number XXX) |
-----
| SGM ID            | Chassis 1      |
|                   | ACTIVE         |
-----
| 1                 | ACTIVE         |
| 2                 | ACTIVE         |
-----
| Chassis Parameters |
-----
| Unit              | Chassis 1      | Weight |
-----
| SGMs              | 2 / 2          | 6      |
| Ports             |                |        |
|   Standard        | 8 / 8          | 11     |
|   Bond            | 0 / 0          | 11     |
|   Mgmt            | 1 / 1          | 11     |
|   Other           | 0 / 0          | 6      |
| Sensors           |                |        |
|   SSMs            | 2 / 2          | 11     |
|                   |                |        |
| Grade             | 73 / 73        | -      |
-----
| Synchronization   |
|   Sync to Active chassis: Enabled |
-----
[Global] HostName-ch01-01>
[Global] HostName-ch01-01> show interfaces
-----
+-----+
| Interfaces Data |
+-----+
-----+
| Interface      | IPv4 Address   | Info      | Link State | | |
| Speed|MTU  | Duplex|         |           |           |
|              | MAC Address   |           | (ch1)      |
+-----+-----+-----+-----+
| eth1-Mgmt1    | 172.23.19.53/24 | Ethernet  | (Up)       | 10G
| 1500 |Full  |         |           |           |
|              | 00:1c:7f:62:91:94 |         |           |
+-----+-----+-----+-----+
| Sync          | 192.0.2.1/24   | Ethernet  | (up)       | 10G
| 1500 |Full  |         |           |           |
|              | 00:1c:7f:01:04:fe |         |           |
+-----+-----+-----+-----+
+-----+
... .. output was truncated for brevity ... ..
```



# Performance Monitoring and Control

This section provides commands to monitor and control the performance of Security Group Members.

## Monitoring Performance (asg perf)

### Description

Use the "asg perf" command in Gaia gClish or the Expert mode to monitor continuously the key performance indicators and load statistics.

There are different commands for IPv4 and IPv6 traffic.

You can show the performance statistics for IPv4 traffic, IPv6 traffic, or for all traffic.

The command output automatically updates after a predefined interval (default is 10 seconds).

To stop the command and return to the command line, press the **e** key.

### Syntax

```
asg perf -h
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-k] [-v] [-vv] [-p] [{-4 | -6}] [-c]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-k] [-e] [--delay <Seconds>]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-v] [-vv [mem [{fwk | cpd | fwd | all_daemons}]]]
```

```
asg perf [-b <SGM IDs>] [-vs <VS IDs>] [-v] [-vv [cpu [{1m | 1h | 24h}]]]
```

### Parameters

Parameter	Description
-h	Shows the built-in help.

Parameter	Description
<code>-b &lt;SGM IDs&gt;</code>	<p>Applies to Security Group Members as specified by the <code>&lt;SGM IDs&gt;</code>.</p> <p><code>&lt;SGM IDs&gt;</code> can be:</p> <ul style="list-style-type: none"> <li>▪ No <code>&lt;SGM IDs&gt;</code> specified, or <code>all</code> Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, <code>1_1</code>)</li> </ul>
<code>-vs &lt;VS IDs&gt;</code>	<p>Applies to Virtual Systems as specified by the <code>&lt;VS IDs&gt;</code>.</p> <p><code>&lt;VS IDs&gt;</code> can be:</p> <ul style="list-style-type: none"> <li>▪ No <code>&lt;VS IDs&gt;</code> specified (default) - Applies to the context of the current Virtual System</li> <li>▪ One Virtual System</li> <li>▪ A comma-separated list of Virtual Systems (for example, <code>1, 2, 4, 5</code>)</li> <li>▪ A range of Virtual Systems (for example, <code>3-5</code>)</li> <li>▪ <code>all</code> - Shows all Virtual Systems</li> </ul> <p>This parameter is only applicable in a VSX environment.</p>
<code>-v</code>	<p>Shows statistics for each Security Group Member. Adds a performance summary for each Security Group Member.</p>
<code>-vv</code>	<p>Shows statistics for each Virtual System. <b>Note</b> - This parameter is only relevant in a VSX environment.</p>
<code>mem [{fwk   cpd   fwd   all_daemons}]</code>	<p>Shows memory usage for each daemon. Use this with the <code>"-vv"</code> parameter. Valid values:</p> <ul style="list-style-type: none"> <li>▪ <code>fwk</code> (default)</li> <li>▪ <code>fwd</code></li> <li>▪ <code>cpd</code></li> <li>▪ <code>all_daemons</code></li> </ul>
<code>cpu [{1m   1h   24h}]</code>	<p>Shows CPU usage for a specified period of time. Use this with the <code>"-vv"</code> parameter. Valid values:</p> <ul style="list-style-type: none"> <li>▪ <code>1m</code> - The last 60 seconds (default)</li> <li>▪ <code>1h</code> - The last hour</li> <li>▪ <code>24h</code> - The last 24 hours</li> </ul>

Parameter	Description
-p	Shows detailed statistics and traffic distribution between these paths on the Active Site: <ul style="list-style-type: none"> <li>■ Acceleration path (SecureXL)</li> <li>■ Medium path (PXL)</li> <li>■ Slow path (Firewall)</li> </ul>
{-4   -6}	<ul style="list-style-type: none"> <li>■ -4 - Shows IPv4 information only.</li> <li>■ -6 - Shows IPv6 information only.</li> </ul> <p>If no value is specified, the combined performance information shows for both IPv4 and IPv6.</p>
-c	Shows percentages instead of absolute values.
-k	Shows peak (maximum) system performance values.
-e	Resets the peak values and deletes all peaks files and system history files.
--delay <Seconds>	Temporarily changes the update interval for the current "asg perf" session. Enter a delay value in seconds. The default delay is 10 seconds.

 **Notes:**

- The "-b <SGM IDs>" and "-vs <VS IDs>" parameters must be at the beginning of the command syntax.  
If both parameters are used, "-b <SGM IDs>" must be first.
- If your Security Group is **not** configured in VSX mode, the VSX-related commands are not available.  
They do not appear when you run the "asg perf -h" command.

## Examples

### Example 1 - Summary without Parameters (asg perf)

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf
Thu May 21 08:17:24 IDT 2015
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: 0
+-----+
|Performance Summary|
+-----+
|Name                |Value          |
+-----+
|Throughput          |751.6 K        |
|Packet rate         |733            |
|Connection rate     |3              |
|Concurrent connections|142           |
|Load average        |2%             |
|Acceleration load (avg/min/max)|1%/0%/4%      |
|Instances load (avg/min/max)|2%/0%/8%      |
|Memory usage        |10%           |
+-----+
* Instances / Acceleration Cores: 8 / 4
* Activated SWB: FW,IPS
[Global] HostName-ch01-01>
```

#### Notes:

- By default, absolute values are shown.
- Unless otherwise specified, the combined statistics for IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the Active Security Group Member only.

**Example 2 - Performance Summary (asg perf -v)**

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf -vs all -v -vv cpu 24h
Tue Oct 22 07:23:37 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-----+
|Performance Summary                                     |
+-----+-----+-----+
|Name                                                    |Value          |IPv4%          |
+-----+-----+-----+
|Throughput                                             |10.2 K         |100%           |
|Packet rate                                            |11             |100%           |
|Connection rate                                        |0              |N/A            |
|Concurrent connections                                |22             |100%           |
|Load average                                           |7%             |                |
|Acceleration load (avg/min/max)                       |6%/6%/6%      |                |
|Instances load (avg/min/max)                           |5%/4%/9%      |                |
|Memory usage                                           |55%            |                |
+-----+-----+-----+

+-----+
|Per SGM Distribution Summary                             |
+-----+-----+-----+-----+-----+-----+-----+
|SGM |Throughput |Packet |Conn. |Concu. |Accel. |Instances |Mem. |
|ID  |           |Rate   |Rate  |Conn   |Cores% |Cores%    |Usage|
+-----+-----+-----+-----+-----+-----+-----+
|1_01|10.2 K     |11     |0     |22     |6/6/6  |5/4/9     |55%  |
+-----+-----+-----+-----+-----+-----+-----+
|Total|10.2 K     |11     |0     |22     |6/6/6  |5/4/9     |55%  |
+-----+-----+-----+-----+-----+-----+-----+

+-----+
|Per VS CPU Usage Summary                               |
+-----+-----+-----+-----+
|VS ID|Avg. Cpu%|Min. Cpu%|Max. Cpu%|
|     |         |(SGM id) |(SGM id) |
+-----+-----+-----+-----+
| 0   |2        |1 (1_02) |2 (1_01) |
| 1   |0        |0 (1_01) |0 (1_04) |
+-----+-----+-----+-----+
* CPU stats is aggregated over the last 24hrs
[Global] HostName-ch01-01>
```

Make sure to enable the resource control monitoring on all Security Group Members.

Run in the Expert mode on the Security Group:

```
g_fw vsx resctrl monitor enable
```

By default, absolute values are shown.

**Notes:**

- Average, minimum and maximum values are calculated across all active Security Group Members.
- The Security Group Member ID with the minimum and maximum value shows in brackets for each Security Group Member.

- Unless otherwise specified, the combined statistics for both IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the active Security Group Member only.

### Example 3 - Detailed Statistics and Traffic Distribution (asg perf -p)

This example the output for the Virtual Systems 0 and 1.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf -vs 0-1 -p
Aggregated statistics (IPv4 and IPv6) of SGMs: all Virtual Systems: 0-1
+-----+
|Performance Summary|
+-----+-----+-----+
|Name                |Value                |IPv4%                |
+-----+-----+-----+
|Throughput          |1.7 K                |100%                 |
|Packet rate         |2                    |100%                 |
|Connection rate     |0                    |N/A                  |
|Concurrent connections|20                   |100%                 |
|Load average        |6%                   |                     |
|Acceleration load (avg/min/max)|5%/5%/5%           |                     |
|Instances load (avg/min/max)|5%/3%/10%           |                     |
|Memory usage        |57%                  |                     |
+-----+-----+-----+
=+-----+
|Per Path Distribution Summary|
+-----+-----+-----+-----+-----+
|                |Acceleration|Medium                |Firewall                |Dropped                |
+-----+-----+-----+-----+-----+
|Throughput      |0           |0                     |1.7 K                    |0                       |
|Packet rate     |0           |0                     |2                         |0                       |
|Connection rate |0           |0                     |0                         |                        |
|Concurrent conn.|10          |0                     |10                        |                        |
+-----+-----+-----+-----+-----+
[Global] HostName-ch01-01>
```

**Example 4 - Per Path Statistics (asg perf -p -v)**

This example shows detailed performance information for each Security Group Member and traffic distribution between different paths. It also shows VPN throughput and connections.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf -p -v
Tue Oct 22 07:31:31 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-----+
|Performance Summary|
+-----+
|Name|Value|
+-----+
|Throughput|3.3 G|
|Packet rate|6.2 M|
|Connection rate|0|
|Concurrent connections|3.4 K|
|Load average|54%|
|Acceleration load (avg/min/max)|58%/48%/68%|
|Instances load (avg/min/max)|3%/1%/5%|
|Memory usage|18%|
+-----+

+-----+
|Per SGM Distribution Summary|
+-----+
|SGM ID|Throughput|Packet rate|Conn.|Concurrent|Core usage|Core Instances|Memory|
| | | |Rate|Connections|avg/min/max %|avg/min/max %|Usage|
+-----+
|1_01|644.3 M|1.2 M|0|520|52/44/62|6/3/10|18%|
|1_02|526.7 M|997.1 K|0|512|61/51/68|2/0/5|18%|
|1_03|526.6 M|997.0 K|0|512|62/53/73|2/1/3|18%|
|1_04|526.7 M|997.0 K|0|804|54/48/60|2/1/3|18%|
|1_05|526.7 M|997.1 K|0|512|59/45/76|3/1/5|18%|
|1_06|526.7 M|997.1 K|0|512|61/52/70|4/4/5|18%|
+-----+
|Total|3.3 G|6.2 M|0|3.4 K|58/48/68|3/1/5|18%|
+-----+

+-----+
|Per Path Distribution Summary|
+-----+
| |Acceleration|Medium|Firewall|Dropped|
+-----+
|Throughput|3.2 G|0|2.1 M|117.6 M|
|Packet rate|6.0 M|0|1.4 K|222.8 K|
|Connection rate|0|0|0|0|
|Concurrent connections|3.2 K|0|156|0|
+-----+

+-----+
|VPN Performance|
+-----+
|VPN throughput|2.9 G|
|VPN connections|3.1 K|
+-----+
[Global] HostName-ch01-01>
```

**Example 5 - Virtual System Memory Summary with Performance Summary (asg perf -vs all -vv mem)**

The "-vv mem" parameter shows memory usage for each Virtual System across all active Security Group Members.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf -vs all -vv mem
Tue Jul 29 16:05:44 IDT 2014
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: all
+-----+
|Performance Summary                                     |
+-----+-----+
|Name                                                    |Value          |
+-----+-----+
|Throughput                                             |684.5 K       |
|Packet rate                                           |700           |
|Connection rate                                       |3             |
|Concurrent connections                               |144           |
|Load average                                          |2%            |
|Acceleration load (avg/min/max)                     |0%/0%/1%     |
|Instances load (avg/min/max)                         |2%/0%/12%    |
|Memory usage                                          |10%           |
+-----+-----+
* Instances / Acceleration Cores: 8 / 4
+-----+
|Per VS Memory Summary                                 |
+-----+-----+-----+-----+-----+-----+
| VS ID | User Space | Memory in | FWK memory | Total memory| CPU   |
|      | memory    | Kernel   |            |             | Usage % |
+-----+-----+-----+-----+-----+-----+
|  0 max|222.3M (1_01)|1.658G (1_04)|47.11M (1_04)|1.880G (1_04)| N/A   |
|      min|215.8M (1_03)|1.213G (1_01)|45.55M (1_03)|1.249G (1_01)| N/A   |
+-----+-----+-----+-----+-----+-----+
|  1 max|56.34M (1_02)| 0K (1_04) |31.16M (1_02)|56.34M (1_02)| N/A   |
|      min|54.24M (1_01)| 0K (1_04) |29.52M (1_03)|54.24M (1_01)| N/A   |
+-----+-----+-----+-----+-----+-----+
* Maximum and minimum values are calculated across all active SGMs
[Global] HostName-ch01-01>
```

**Notes:**

- The Security Group Member that uses the most user space memory on Virtual System 1 is Security Group Member 1\_01
- The Security Group Member that uses the least `fwk` daemon memory on Virtual System 3 is Security Group Member 1\_02
- This information shows only if `vsxmstat` is enabled for `perfanalyze use`
- Make sure that the `vsxmstat` feature is enabled (`vsxmstat status_raw`)



## Description

Use the "asg perf" command in Gaia gClish or the Expert mode to monitor continuously the key performance indicators and load statistics.

There are different commands for IPv4 and IPv6 traffic.

You can show the performance statistics for IPv4 traffic, IPv6 traffic, or for all traffic.

The command output automatically updates after a predefined interval (default is 10 seconds).

To stop the command and return to the command line, press the **e** key.

## Syntax

<code>asg perf -h</code>
<code>asg perf [-b &lt;SGM IDs&gt;] [-vs &lt;VS IDs&gt;] [-k] [-v] [-vv] [-p] [{-4   -6}] [-c]</code>
<code>asg perf [-b &lt;SGM IDs&gt;] [-vs &lt;VS IDs&gt;] [-k] [-e] [--delay &lt;Seconds&gt;]</code>
<code>asg perf [-b &lt;SGM IDs&gt;] [-vs &lt;VS IDs&gt;] [-v] [-vv [mem [{fwk   cpd   fwd   all_daemons}]]]</code>
<code>asg perf [-b &lt;SGM IDs&gt;] [-vs &lt;VS IDs&gt;] [-v] [-vv [cpu [{1m   1h   24h}]]]</code>

## Parameters

Parameter	Description
-h	Shows the built-in help.
-b <SGM IDs>	<p>Applies to Security Group Members as specified by the &lt;SGM IDs&gt;.</p> <p>&lt;SGM IDs&gt; can be:</p> <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or <code>all</code> Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, <code>1_1</code>)</li> </ul>

Parameter	Description
<code>-vs &lt;VS IDs&gt;</code>	<p>Applies to Virtual Systems as specified by the <code>&lt;VS IDs&gt;</code>. <code>&lt;VS IDs&gt;</code> can be:</p> <ul style="list-style-type: none"> <li>▪ No <code>&lt;VS IDs&gt;</code> specified (default) - Applies to the context of the current Virtual System</li> <li>▪ One Virtual System</li> <li>▪ A comma-separated list of Virtual Systems (for example, <code>1, 2, 4, 5</code>)</li> <li>▪ A range of Virtual Systems (for example, <code>3-5</code>)</li> <li>▪ <code>all</code> - Shows all Virtual Systems</li> </ul> <p>This parameter is only applicable in a VSX environment.</p>
<code>-v</code>	Shows statistics for each Security Group Member. Adds a performance summary for each Security Group Member.
<code>-vv</code>	Shows statistics for each Virtual System. <b>Note</b> - This parameter is only relevant in a VSX environment.
<code>mem [{fwk   cpd   fwd   all_daemons}]</code>	Shows memory usage for each daemon. Use this with the " <code>-vv</code> " parameter. Valid values: <ul style="list-style-type: none"> <li>▪ <code>fwk</code> (default)</li> <li>▪ <code>fwd</code></li> <li>▪ <code>cpd</code></li> <li>▪ <code>all_daemons</code></li> </ul>
<code>cpu [{1m   1h   24h}]</code>	Shows CPU usage for a specified period of time. Use this with the " <code>-vv</code> " parameter. Valid values: <ul style="list-style-type: none"> <li>▪ <code>1m</code> - The last 60 seconds (default)</li> <li>▪ <code>1h</code> - The last hour</li> <li>▪ <code>24h</code> - The last 24 hours</li> </ul>
<code>-p</code>	Shows detailed statistics and traffic distribution between these paths on the Active Site: <ul style="list-style-type: none"> <li>▪ Acceleration path (SecureXL)</li> <li>▪ Medium path (PXL)</li> <li>▪ Slow path (Firewall)</li> </ul>

Parameter	Description
{-4   -6}	<ul style="list-style-type: none"> <li>■ -4 - Shows IPv4 information only.</li> <li>■ -6 - Shows IPv6 information only.</li> </ul> <p>If no value is specified, the combined performance information shows for both IPv4 and IPv6.</p>
-c	Shows percentages instead of absolute values.
-k	Shows peak (maximum) system performance values.
-e	Resets the peak values and deletes all peaks files and system history files.
--delay <Seconds>	<p>Temporarily changes the update interval for the current "asg perf" session.</p> <p>Enter a delay value in seconds.</p> <p>The default delay is 10 seconds.</p>

 **Notes:**

- The "-b <SGM IDs>" and "-vs <VS IDs>" parameters must be at the beginning of the command syntax.  
If both parameters are used, "-b <SGM IDs>" must be first.
- If your Security Group is **not** configured in VSX mode, the VSX-related commands are not available.  
They do not appear when you run the "asg perf -h" command.

## Examples

### Example 1 - Summary without Parameters (asg perf)

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf
Thu May 21 08:17:24 IDT 2015
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: 0
+-----+
|Performance Summary|
+-----+
|Name|Value|
+-----+
|Throughput|751.6 K|
|Packet rate|733|
|Connection rate|3|
|Concurrent connections|142|
|Load average|2%|
|Acceleration load (avg/min/max)|1%/0%/4%|
|Instances load (avg/min/max)|2%/0%/8%|
|Memory usage|10%|
+-----+
* Instances / Acceleration Cores: 8 / 4
* Activated SWB: FW,IPS
[Global] HostName-ch01-01>
```

#### Notes:

- By default, absolute values are shown.
- Unless otherwise specified, the combined statistics for IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the Active Security Group Member only.

**Example 2 - Performance Summary (asg perf -v)**

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf -vs all -v -vv cpu 24h
Tue Oct 22 07:23:37 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-----+
|Performance Summary|
+-----+-----+-----+
|Name|Value|IPv4%|
+-----+-----+-----+
|Throughput|10.2 K|100%|
|Packet rate|11|100%|
|Connection rate|0|N/A|
|Concurrent connections|22|100%|
|Load average|7%|
|Acceleration load (avg/min/max)|6%/6%/6%|
|Instances load (avg/min/max)|5%/4%/9%|
|Memory usage|55%|
+-----+-----+-----+

+-----+
|Per SGM Distribution Summary|
+-----+-----+-----+-----+-----+-----+-----+
|SGM |Throughput |Packet |Conn. |Concu. |Accel. |Instances |Mem. |
|ID | |Rate |Rate |Conn |Cores% |Cores% |Usage%|
+-----+-----+-----+-----+-----+-----+-----+
|1_01 |10.2 K |11 |0 |22 |6/6/6 |5/4/9 |55% |
+-----+-----+-----+-----+-----+-----+-----+
|Total|10.2 K |11 |0 |22 |6/6/6 |5/4/9 |55% |
+-----+-----+-----+-----+-----+-----+

+-----+
|Per VS CPU Usage Summary|
+-----+-----+-----+-----+
|VS ID|Avg. Cpu%|Min. Cpu%|Max. Cpu%|
| | |(SGM id) |(SGM id) |
+-----+-----+-----+-----+
| 0 |2 |1 (1_02)|2 (1_01)|
| 1 |0 |0 (1_01)|0 (1_04)|
+-----+-----+-----+-----+
* CPU stats is aggregated over the last 24hrs
[Global] HostName-ch01-01>
```

Make sure to enable the resource control monitoring on all Security Group Members.

Run in the Expert mode on the Security Group:

```
g_fw vsx resctrl monitor enable
```

By default, absolute values are shown.

**Notes:**

- Average, minimum and maximum values are calculated across all active Security Group Members.
- The Security Group Member ID with the minimum and maximum value shows in brackets for each Security Group Member.

- Unless otherwise specified, the combined statistics for both IPv4 and IPv6 are shown.
- When no Security Group Members are specified, performance statistics are shown for the active Security Group Member only.

### Example 3 - Peak Values (asg perf -p)

This example shows peak values for one Virtual System.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf -vs 0-1 -p
Aggregated statistics (IPv4 and IPv6) of SGMs: all Virtual Systems: 0-1
+-----+
|Performance Summary|
+-----+-----+-----+
|Name                |Value          |IPv4%         |
+-----+-----+-----+
|Throughput          |1.7 K          |100%          |
|Packet rate         |2              |100%          |
|Connection rate     |0              |N/A           |
|Concurrent connections|20             |100%          |
|Load average        |6%             |              |
|Acceleration load (avg/min/max)|5%/5%/5%      |              |
|Instances load (avg/min/max)|5%/3%/10%     |              |
|Memory usage        |57%            |              |
+-----+-----+-----+
=+-----+
|Per Path Distribution Summary|
+-----+-----+-----+-----+
|          |Acceleration|Medium        |Firewall      |Dropped      |
+-----+-----+-----+-----+
|Throughput|0            |0             |1.7 K         |0            |
|Packet rate|0           |0             |2             |0            |
|Connection rate|0         |0             |0             |             |
|Concurrent conn. |10        |0             |10            |             |
+-----+-----+-----+-----+
[Global] HostName-ch01-01>
```

### Example 4 - Per Path Statistics (asg perf -p -v)

This example shows detailed performance information for each Security Group Member and traffic distribution between different paths. It also shows VPN throughput and connections.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf -p -v
Tue Oct 22 07:31:31 IST 2013
Aggregated statistics (IPv4 and IPv6) of SGMs: chassis_active Virtual Systems: 0
+-----+
|Performance Summary|
+-----+
|Name|Value|
+-----+
|Throughput|3.3 G|
|Packet rate|6.2 M|
|Connection rate|0|
|Concurrent connections|3.4 K|
|Load average|54%|
|Acceleration load (avg/min/max)|58%/48%/68%|
|Instances load (avg/min/max)|3%/1%/5%|
|Memory usage|18%|
+-----+

+-----+
|Per SGM Distribution Summary|
+-----+
|SGM ID|Throughput|Packet rate|Conn.|Concurrent|Core usage|Core Instances|Memory|
| | | |Rate|Connections|avg/min/max %|avg/min/max %|Usage|
+-----+
|1_01|644.3 M|1.2 M|0|520|52/44/62|6/3/10|18%|
|1_02|526.7 M|997.1 K|0|512|61/51/68|2/0/5|18%|
|1_03|526.6 M|997.0 K|0|512|62/53/73|2/1/3|18%|
|1_04|526.7 M|997.0 K|0|804|54/48/60|2/1/3|18%|
|1_05|526.7 M|997.1 K|0|512|59/45/76|3/1/5|18%|
|1_06|526.7 M|997.1 K|0|512|61/52/70|4/4/5|18%|
+-----+
|Total|3.3 G|6.2 M|0|3.4 K|58/48/68|3/1/5|18%|
+-----+

+-----+
|Per Path Distribution Summary|
+-----+
| |Acceleration|Medium|Firewall|Dropped|
+-----+
|Throughput|3.2 G|0|2.1 M|117.6 M|
|Packet rate|6.0 M|0|1.4 K|222.8 K|
|Connection rate|0|0|0|0|
|Concurrent connections|3.2 K|0|156|0|
+-----+

+-----+
|VPN Performance|
+-----+
|VPN throughput|2.9 G|
|VPN connections|3.1 K|
+-----+
[Global] HostName-ch01-01>
```

**Example 5 - Virtual System Memory Summary with Performance Summary (asg perf -vs all -vv mem)**

The "-vv mem" parameter shows memory usage for each Virtual System across all active Security Group Members.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg perf -vs all -vv mem
Tue Jul 29 16:05:44 IDT 2014
Aggregated statistics (IPv4 Only) of SGMs: chassis_active VSs: all
+-----+
|Performance Summary                                     |
+-----+-----+
|Name                                                    |Value          |
+-----+-----+
|Throughput                                             |684.5 K       |
|Packet rate                                           |700           |
|Connection rate                                       |3             |
|Concurrent connections                               |144           |
|Load average                                          |2%            |
|Acceleration load (avg/min/max)                     |0%/0%/1%     |
|Instances load (avg/min/max)                         |2%/0%/12%    |
|Memory usage                                          |10%           |
+-----+-----+
* Instances / Acceleration Cores: 8 / 4
+-----+
|Per VS Memory Summary                                  |
+-----+-----+-----+-----+-----+-----+
| VS ID | User Space | Memory in | FWK memory | Total memory| CPU   |
|      | memory    | Kernel   |            |            | Usage % |
+-----+-----+-----+-----+-----+-----+
|  0 max|222.3M (1_01)|1.658G (1_04)|47.11M (1_04)|1.880G (1_04)| N/A   |
|      min|215.8M (1_03)|1.213G (1_01)|45.55M (1_03)|1.249G (1_01)| N/A   |
+-----+-----+-----+-----+-----+-----+
|  1 max|56.34M (1_02)| 0K (1_04) |31.16M (1_02)|56.34M (1_02)| N/A   |
|      min|54.24M (1_01)| 0K (1_04) |29.52M (1_03)|54.24M (1_01)| N/A   |
+-----+-----+-----+-----+-----+-----+
* Maximum and minimum values are calculated across all active SGMs
[Global] HostName-ch01-01>
```

**Notes:**

- The Security Group Member that uses the most user space memory on Virtual System 1 is Security Group Member 1\_01
- The Security Group Member that uses the least `fwk` daemon memory on Virtual System 3 is Security Group Member 1\_02
- This information shows only if `vsxmstat` is enabled for `perfanalyze use`
- Make sure that the `vsxmstat` feature is enabled (`vsxmstat status_raw`)



# Setting Port Priority

## Description

For each Security Group port, you can set a port priority - high or standard.

Use the "set chassis high-availability port ... priority ..." command in Gaia gClish on the Security Group.

## Syntax

```
set chassis high-availability port <Name of Interface> priority
<Priority>
```

## Parameters

Parameter	Description
<Name of Interface>	Specifies the interface name.
<Priority>	Specifies the port grade. Valid values: <ul style="list-style-type: none"> <li>▪ 1 - Standard priority</li> <li>▪ 2 - Other priority</li> </ul>

Use the "set chassis high-availability port ... priority ..." command together with the "set chassis high-availability factors port ..." command:

- Set the port grade as standard or high.

For example, to set the standard grade at 50, run:

```
set chassis high-availability factors port standard 50
```

- Set the port to high grade or standard grade.

For example, to assign the standard port grade to eth1-01, run:

```
set chassis high-availability port eth1-01 priority 1
```

## Searching for a Connection (asg search)

### *In This Section:*

Description .....	242
Searching in the Non-Interactive Mode .....	242
Searching in the Interactive Mode .....	246

This section describes how to search for a connection in the Connections Table.

### Description

Use the "asg search" command in Gaia gClish or the Expert mode to:

- Search for a connection or a filtered list of connections.
- See which Security Group Member handles the connection, actively or as backup, and on which Site.

You can run this command directly or in Interactive Mode. In the Interactive Mode, you can enter the parameters in the correct sequence.

The "asg search" command also runs a consistency test between Security Group Members.

This command supports both IPv4 and IPv6 connections.

### Searching in the Non-Interactive Mode

#### Syntax

```
asg search -help
```

```
asg search [-v] [-vs <VS IDs>] [<Source IP Address> <Source Port>
<Destination IP Address> <Destination Port> <Protocol>]
```

#### Parameters

Parameter	Description
No Parameters	Runs in the interactive mode.
-help	Shows the built-in help.

Parameter	Description
<code>-vs &lt;VS IDs&gt;</code>	<p>Applies to Virtual Systems as specified by the <code>&lt;VS IDs&gt;</code>.  <code>&lt;VS IDs&gt;</code> can be:</p> <ul style="list-style-type: none"> <li>▪ No <code>&lt;VS IDs&gt;</code> specified (default) - Applies to the context of the current Virtual System</li> <li>▪ One Virtual System</li> <li>▪ A comma-separated list of Virtual Systems (for example, 1, 2, 4, 5)</li> <li>▪ A range of Virtual Systems (for example, 3-5)</li> <li>▪ <code>all</code> - Shows all Virtual Systems</li> </ul> <p>This parameter is only applicable in a VSX environment.</p>
<code>&lt;Source IP Address&gt;</code>	Specifies the source IPv4 or IPv6 address.
<code>&lt;Source Port&gt;</code>	Specifies the source port number. See <a href="#">IANA Service Name and Port Number Registry</a> .
<code>&lt;Destination IP Address&gt;</code>	Specifies the destination IPv4 or IPv6 address.
<code>&lt;Destination Port&gt;</code>	Specifies the destination port number. See <a href="#">IANA Service Name and Port Number Registry</a> .
<code>&lt;Protocol&gt;</code>	Specifies the IP Protocol name or number. See <a href="#">IANA Protocol Numbers</a> .
<code>-v</code>	<p>Shows connection indicators for:</p> <ul style="list-style-type: none"> <li>▪ <b>A</b> - Active Security Group Member</li> <li>▪ <b>B</b> - Backup Security Group Member</li> <li>▪ <b>F</b> - Firewall Connections table</li> <li>▪ <b>S</b> - SecureXL Connections table</li> <li>▪ <b>C</b> - Correction Layer table</li> </ul> <p>This is in addition to the indicators for Active and Backup Security Group Members.</p>



### Notes:

- You must enter the all parameters in the sequence as appears in the above syntax.
- You can enter "`\*`" as a wildcard parameter (meaning, any value).
- The "`-vs`" parameter is only available for a Security Group in VSX mode.

## Examples

### Example 1 - Search for one IPv4 source address, one IPv4 destination address, all ports, and the TCP protocol

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg search -v 192.0.2.4 192.0.2.15 \* tcp
Lookup for conn: <192.0.2.4, 192.0.2.15, *, tcp>, may take few seconds...

<192.0.2.4, 1130, 192.0.2.15, 49829, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36323, 192.0.2.15, 1130, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130, 192.0.2.15, 49851, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36308, 192.0.2.15, 1130, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36299, 192.0.2.15, 1130, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130, 192.0.2.15, 49835, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130, 192.0.2.15, 49856, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36331, 192.0.2.15, 1130, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130, 192.0.2.15, 49857, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130, 192.0.2.15, 49841, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36315, 192.0.2.15, 1130, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 1130, 192.0.2.15, 49859, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36300, 192.0.2.15, 1130, tcp> -> [2_01 A, 1_04 A]
<192.0.2.4, 36301, 192.0.2.15, 1130, tcp> -> [2_01 A, 1_04 A]

Legend:
A - Active SGM
B - Backup SGM
C - Correction Layer table
F - Firewall connection table
S - SecureXL connection table
[Global] HostName-ch01-01>
```

### Example 2 - Search for one IPv6 source address, all destination IP addresses, destination port 8080, and TCP protocol

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg search 2620:0:2a03:16:2:33:0:1 \* 8080 tcp

<2620:0:2a03:16:2:33:0:1, 52117, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
<2620:0:2a03:16:2:33:0:1, 62775, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
<2620:0:2a03:16:2:33:0:1, 54378, 951::69cb:e42d:eac0:652f, 8080, tcp> -> [1_01 A, 2_01 B]
Legend:
A - Active SGM
B - Backup SGM
[Global] HostName-ch01-01>
```

**Example 3 - Search for all sources, destinations, ports, and protocols for VS0**

```

[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg search -vs 0 \* \* \* \* \*.
Lookup for conn: <*, *, *, *, *>, may take few seconds...

<172.23.9.130, 18192, 172.23.9.138, 43563, tcp> -> [1_01 A]
<172.23.9.130, 32888, 172.23.9.138, 257, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52120, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32963, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52104, tcp> -> [1_01 A]
<255.255.255.255, 67, 0.0.0.0, 68, udp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32864, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 32888, tcp> -> [1_01 A]
<172.23.9.138, 257, 172.23.9.130, 33465, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.40.23, 65515, tcp> -> [1_01 A]
<172.23.9.130, 22, 194.29.47.14, 52493, tcp> -> [1_01 A]
<172.23.9.130, 18192, 172.23.9.138, 49059, tcp> -> [1_01 A]
<172.23.9.130, 18192, 172.23.9.138, 33356, tcp> -> [1_01 A]
<172.23.9.138, 33356, 172.23.9.130, 18192, tcp> -> [1_01 A]
<172.23.9.138, 43563, 172.23.9.130, 18192, tcp> -> [1_01 A]
<172.23.9.130, 32864, 172.23.9.138, 257, tcp> -> [1_01 A]
<0.0.0.0, 68, 255.255.255.255, 67, udp> -> [1_01 A]
<172.23.9.130, 32963, 172.23.9.138, 257, tcp> -> [1_01 A]
<172.23.9.130, 33465, 172.23.9.138, 257, tcp> -> [1_01 A]
<194.29.47.14, 52120, 172.23.9.130, 22, tcp> -> [1_01 A]
<194.29.47.14, 52104, 172.23.9.130, 22, tcp> -> [1_01 A]
<fe80::d840:5de7:8dbe:2345, 546, ff02::1:2, 547, udp> -> [1_01 A]
<194.29.47.14, 52493, 172.23.9.130, 22, tcp> -> [1_01 A]
<172.23.9.138, 49059, 172.23.9.130, 18192, tcp> -> [1_01 A]
<194.29.40.23, 65515, 172.23.9.130, 22, tcp> -> [1_01 A]
Legend:
A - Active SGM
B - Backup SGM
[Global] HostName-ch01-01>

```

## Searching in the Interactive Mode

In the Interactive Mode, you enter the connection search parameters in the required sequence.

Step	Instructions
1	Connect to the command line on the Security Group.
2	Go to Gaia gClish: enter <code>gclish</code> and press Enter.
3	Run the command: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>&gt; asg search [-vs &lt;VS IDs&gt;] [-v]</pre> </div>
4	Enter these parameters in the order below: <ol style="list-style-type: none"> <li>1. Source IPv4 or IPv6 address.</li> <li>2. Destination IPv4 or IPv6 address.</li> <li>3. Destination port number. See <a href="#">IANA Service Name and Port Number Registry</a>.</li> <li>4. IP protocol. See <a href="#">IANA Protocol Numbers</a>.</li> <li>5. Source port number. See <a href="#">IANA Service Name and Port Number Registry</a>.</li> </ol> <p><b>Note</b> - Press the <b>Enter</b> key to enter a wildcard value (meaning, any value).</p>

**Example - Search for one IPv4 source and destination**

```

[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> asg search -v

Please enter conn's 5 tuple:
-----
Enter source IP (press enter for wildcard):
>192.0.2.4
Enter destination IP (press enter for wildcard):
>192.0.2.15
Enter destination port (press enter for wildcard):
>
Enter IP protocol ('tcp', 'udp', 'icmp' or enter for wildcard):
>tcp
Enter source port (press enter for wildcard):
>
Lookup for conn: <192.0.2.4, *, 192.0.2.15, *, tcp>, may take few seconds...
<192.0.2.4, 37408, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49670, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49653, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 37406, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49663, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 1130, 192.0.2.15, 49658, tcp> -> [2_01 AF, 1_04 AF]
<192.0.2.4, 37407, 192.0.2.15, 1130, tcp> -> [2_01 AF, 1_04 AF]

Legend:
A - Active SGM
B - Backup SGM
C - Correction Layer table
F - Firewall connection table
S - SecureXL connection table

[Global] HostName-ch01-01>

```

## Showing the Number of Firewall and SecureXL Connections (asg\_conns)

### Description

Use the "asg\_conns" command in Gaia gClish or the Expert mode to show the number of Firewall and SecureXL connections on each Security Group Member.

### Syntax

```
asg_conns -h
```

```
asg_conns [-b <SGM IDs>] [-6]
```

### Parameters

Parameter	Description
-h	Shows the built-in help.
-b <SGM IDs>	<p>Applies to Security Group Members as specified by the &lt;SGM IDs&gt;. &lt;SGM IDs&gt; can be:</p> <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul>
-6	Shows only IPv6 connections.



**Example**

```

[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > asg_conns
1_01:
  #VALS      #PEAK      #SLINKS
    246        1143        246
1_02:
  #VALS      #PEAK      #SLINKS
    45         172         45
1_03:
  #VALS      #PEAK      #SLINKS
    45         212         45
1_04:
  #VALS      #PEAK      #SLINKS
    223        624        223
1_05:
  #VALS      #PEAK      #SLINKS
    45         246         45

Total (fw1 connections table): 604 connections

1_01:
There are 60 conn entries in SecureXL connections table
Total conn entries @ DB 0: 4
Total conn entries @ DB 3: 2
.
.
Total conn entries @ DB 26: 4
Total conn entries @ DB 30: 2
1_02:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 0: 2
Total conn entries @ DB 1: 2
.
.
Total conn entries @ DB 26: 2
1_03:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 0: 2
Total conn entries @ DB 5: 2
.
.
Total conn entries @ DB 30: 2
1_04:
There are 260 conn entries in SecureXL connections table
Total conn entries @ DB 0: 10
Total conn entries @ DB 1: 6
.
.
Total conn entries @ DB 31: 94
1_05:
There are 16 conn entries in SecureXL connections table
Total conn entries @ DB 2: 2
.
.
Total conn entries @ DB 26: 2

Total (SecureXL connections table): 368 connections
[Global] HostName-ch01-01>

```

# Packet Drop Monitoring (drop\_monitor)

## In This Section:

---

### Description

Use the "drop\_monitor" command in the Expert mode to monitor dropped packets on interfaces in real time.

Drop statistics arrive from these modules:

- NICs
- CoreXL
- PSL
- SecureXL

### Notes:

- This command opens a monitor session and shows aggregated data from Security Group Members.  
To stop an open session, press **CTRL+C**.
- By default, this utility shows drop statistics for IPv4 traffic.


### Syntax

```
drop_monitor -h
```

```
drop_monitor [-d] [-v] [-m <SGM IDs>] [-i <List of Interfaces>]
[-f <Refresh Rate>] [-sf <Query Timeout>] [-le] [-e] [-dm] [-ds]
[-r] [-s] [-v6]
```

### Parameters

Parameter	Description
-h	Shows the built-in help.
-d --debug	Runs the command in the debug mode.
-v --verbose	Shows detailed drop statistics - for each Security Group Member and all SecureXL statistics.

Parameter	Description
-m <SGM IDs> --members <SGM IDs>	Applies to Security Group Members as specified by the <SGM IDs>. <SGM IDs> can be: <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul>
-i <List of Interfaces> --interfaces <List of Interfaces>	Shows drop statistics for the specified network interfaces. Enter the names of applicable interfaces separated a comma. By default, this utility shows drop statistics only for the backplane interfaces.
-f <Refresh Rate> --refresh-rate <Refresh Rate>	Specifies the output refresh rate in seconds. The default is 3 seconds.
-sf <Query Timeout> --ssms-refresh-rate <Query Timeout>	Specifies the query timeout in seconds. The default is 60 seconds.
-le --local-export	Exports drop statistics from the local Security Group Member in the JSON format.
-e --global-export	Exports drop statistics from all Security Group Members in the JSON format.
-dm --detailed-members	Shows drop statistics for each Security Group Member, in addition to the total drop statistics.
-ds --detailed-securexl	Shows detailed drop statistics for SecureXL.
-r --reset	Resets the statistics counters to 0 before it collects the data.  <b>Note</b> - Drop statistics are reset for CoreXL, PSL, SecureXL, and backplane interfaces.
-s --include-ssms-stats	Shows local drop statistics only. Only data links, management links, and downlinks are supported.

Parameter	Description
-v6 --ipv6	Shows drop statistics for IPv6 traffic.

### Example 1 - Default output

```
[Expert@HostName-ch0x-0x:0]# drop_monitor

Dropped packets statistics of network interfaces, CoreXL, SecureXL and PSL
+-----+-----+-----+
| Category | Statistics          | Total |
+-----+-----+-----+
+-----+-----+-----+
|          | RX Dropped         | 0     |
|  NIC     | TX Dropped         | 0     |
|          | Qdisc Dropped      | 0     |
+-----+-----+-----+
|          | Outbound Dropped  | 0     |
| CoreXL   | Inbound Dropped   | 0     |
|          | F2P Dropped       | 0     |
+-----+-----+-----+
| PSL      | Total Dropped     | 0     |
|          | Rejected          | 0     |
+-----+-----+-----+
| SecureXL | Total drops       | 0     |
+-----+-----+-----+

[Expert@HostName-ch0x-0x:0]#
```

## Example 2 - Verbose output

```
[Expert@HostName-ch0x-0x:0]# drop_monitor -v

Dropped packets statistics of network interfaces, CoreXL, SecureXL and PSL
+-----+-----+-----+-----+
| Category | Statistics          | 1_01 | 1_02 | Total |
+-----+-----+-----+-----+
|          | RX Dropped          | 0    | 0    | 0    |
|  NIC     | TX Dropped          | 0    | 0    | 0    |
|          | Qdisc Dropped       | 0    | 0    | 0    |
+-----+-----+-----+-----+
|          | Outbound Dropped    | 0    | 0    | 0    |
|  CoreXL  | Inbound Dropped     | 0    | 0    | 0    |
|          | F2P Dropped         | 0    | 0    | 0    |
+-----+-----+-----+-----+
|  PSL     | Total Dropped       | 0    | 0    | 0    |
|          | Rejected             | 0    | 0    | 0    |
+-----+-----+-----+-----+
|          | XMT error           | 0    | 0    | 0    |
|          | general reason      | 0    | 0    | 0    |
|          | Syn Defender        | 0    | 0    | 0    |
|          | Attack mitigation   | 0    | 0    | 0    |
|          | VPN forwarding      | 0    | 0    | 0    |
|          | corrupted packet    | 0    | 0    | 0    |
|          | hl - spoof viol     | 0    | 0    | 0    |
|          | encrypt failed      | 0    | 0    | 0    |
|          | cluster error       | 0    | 0    | 0    |
|          | anti spoofing       | 0    | 0    | 0    |
|          | monitored spoofed   | 0    | 0    | 0    |
|          | hl - new conn       | 0    | 0    | 0    |
|          | hl - TCP viol       | 0    | 0    | 0    |
|          | F2F not allowed     | 0    | 0    | 0    |
| SecureXL | fragment error      | 0    | 0    | 0    |
|          | Session rate exceed | 0    | 0    | 0    |
|          | PXL decision        | 0    | 0    | 0    |
|          | template quota      | 0    | 0    | 0    |
|          | drop template       | 0    | 0    | 0    |
|          | sanity error        | 0    | 0    | 0    |
|          | outb - no conn      | 0    | 0    | 0    |
|          | clr pkt on vpn      | 0    | 0    | 0    |
|          | partial conn        | 0    | 0    | 0    |
|          | decrypt failed      | 0    | 0    | 0    |
|          | Connections Limit by | 0    | 0    | 0    |
|          | Source IP exceed its | 0    | 0    | 0    |
|          | local spoofing      | 0    | 0    | 0    |
|          | interface down      | 0    | 0    | 0    |
+-----+-----+-----+-----+

[Expert@HostName-ch0x-0x:0]#
```



# Hardware Monitoring and Control

You can monitor the hardware components of your system.

## Showing Hardware State (asg stat)

### Description

Use the "asg stat" command in Gaia gClish or the Expert mode to show the state of the system and hardware components.

The command output shows:

- Security Gateway Mode (Gateway or VSX)
- Number of members in the Security Group
- Number of Virtual Systems
- Information related to VSX configuration
- Uptime
- Software Version

### Syntax

```
asg stat
  -h
  -i list_all
  -i sgm_info
  -i tasks
  -v [-amw]
  vs [all [-p]]
```

**Note** - If you run this command in the context of a Virtual System, the output applies only to that Virtual System.

### Parameters

Parameter	Description
No Parameters	Shows the Security Group status (short output).
-h	Shows the built-in help.

Parameter	Description
-i list_ all	<p>Shows:</p> <ul style="list-style-type: none"> <li>▪ The IDs of the Security Group Members, their state and IP addresses</li> <li>▪ Tasks and on which Security Group Member they run</li> </ul>
-i sgm_ info	Shows the IDs of the Security Group Members, their state and IP addresses
-i tasks	<p>Shows the list of Tasks and on which Security Group Member they run:</p> <ul style="list-style-type: none"> <li>▪ <b>SMO</b> - Single Management Object</li> <li>▪ <b>General</b> - General</li> <li>▪ <b>LACP</b> - Interface Bonding</li> <li>▪ <b>CH Monitor</b> - Site state monitor</li> <li>▪ <b>DR Manager</b> - Dynamic Routing manager</li> <li>▪ <b>UIPC</b> - Unique IP Address for each Site</li> <li>▪ <b>Alert</b> - Alerts</li> </ul>
-v [-amw]	Shows the detailed Security Group status (verbose output). The "-amw" parameter shows the update status for the applicable Software Blades.
vs [all [- p]]	<p>Shows the VSX information:</p> <ul style="list-style-type: none"> <li>▪ <code>vs</code> Shows general output for a Virtual System. Run this command in the context of the applicable Virtual System.</li> <li>▪ <code>vs all</code> Output also shows all Virtual Systems.</li> <li>▪ <code>vs all -p</code> Output shows a summary health status for all Virtual Systems.</li> </ul> <p>For more information on a specific Virtual System, run the "asg stat vs" command in the context of the Virtual System.</p>



## Examples

### Example 1 - Default Output (asg stat)

#### Syntax

```
asg stat
```

#### Example output from a Dual Site configuration

```
[Expert@HostName-ch0x-0x:0]# asg stat
-----
| System Status - Maestro |
-----
| Chassis Mode           | Active Up |
| Up time                | 21:29:56 hours |
| SGMs                   | 12/12 |
| Version                 | R81.20 (Build Number XXX) |
-----
| Chassis Parameters |
-----
| Unit | Chassis 1 | Chassis 2 |
-----
| SGMs | 6 / 6 | 6 / 6 |
| Ports | 5 / 5 | 5 / 5 |
| SSMs | 2 / 2 | 2 / 2 |
-----
[Expert@HostName-ch0x-0x:0]#
```

#### Example output from a Single Site configuration

```
[Expert@HostName-ch0x-0x:0]# asg stat
-----
| System Status - Maestro |
-----
| Up time                | 02:10:27 hours |
| SGMs                   | 30/30 |
| Version                 | R81.20 (Build Number XXX) |
-----
| Chassis Parameters |
-----
| Unit | Chassis 1 |
-----
| SGMs | 30 / 30 |
| Ports | 4 / 4 |
| SSMs | 2 / 2 |
-----
[Expert@HostName-ch0x-0x:0]#
```

### Example 2 - Detailed Output (asg stat -v)

#### Syntax

```
asg stat -v
```

### Example output from a Dual Site configuration - top section

This output shows a Security Group with 12 Security Group Members in the Active (UP) state (out of total 12).

The Site #1 is Active.

The Site #2 is Standby.


```
[Expert@HostName-ch0x-0x:0]# asg stat -v
-----
| System Status - Maestro |
-----
| Chassis Mode           | Active Up |
| Up time                | 21:30:50 hours |
| SGMs                  | 12/12 |
| Version               | R81.20 (Build Number XXX) |
-----
| SGM ID                | Chassis 1 | Chassis 2 |
|                       | ACTIVE    | STANDBY  |
-----
| 1                     | ACTIVE    | ACTIVE    |
| 2                     | ACTIVE    | ACTIVE    |
| 3                     | ACTIVE    | ACTIVE    |
| 4                     | ACTIVE    | ACTIVE    |
| 5                     | ACTIVE    | ACTIVE    |
| 6                     | ACTIVE    | ACTIVE    |
-----
... output was truncated for brevity - the example continues below ...
```

### Example output from a Single Site configuration - top section

This output shows a Security Group with 30 Security Group Members in the Active (UP) state (out of total 30).

```
[Expert@HostName-ch0x-0x:0]# asg stat -v
-----
| System Status - Maestro |
-----
| Up time                | 02:10:39 hours |
| SGMs                  | 30/30 |
| Version               | R81.20 (Build Number XXX) |
-----
| SGM ID                | Chassis 1 |
|                       | ACTIVE    |
-----
| 1                     | ACTIVE    |
| 2                     | ACTIVE    |
| 3                     | ACTIVE    |
... output was truncated for brevity ...
| 30                    | ACTIVE    |
-----
... output was truncated for brevity - the example continues below ...
```

Explanation about the output:

Field	Instructions
<b>SGM ID</b>	Identifier of the Security Group Member. The <code>(local)</code> is the Security Group Member, on which you ran the command.
<b>State</b>	<p>State of the Security Group Member:</p> <ul style="list-style-type: none"> <li>▪ <b>ACTIVE</b> - The Security Group Member is processing traffic.</li> <li>▪ <b>DOWN</b> - The Security Group Member is not processing traffic.</li> <li>▪ <b>DETACHED/LOST</b> - The Security Group Member is not communicating/reboot.</li> <li>▪ <b>INIT</b> - The Security Group Member is in the initialization phase after reboot.</li> <li>▪ <b>READY</b> - The Security Group Member is ready to become Active, and is waiting for all other remote Active members to acknowledge its state.</li> <li>▪ <b>Active (Sync)</b> - The Security Group Member is in a unicast connections sync.</li> </ul> <p> <b>Note</b> - To change manually the state of the Security Group Member, use the <code>"g_clusterXL_admin"</code> command (see <a href="#">"Configuring the Cluster State (g_clusterXL_admin)"</a> on page 180).</p>

### Example output from a Dual Site configuration - bottom section

```

... output was truncated for brevity - the example starts above ...
-----
| Chassis Parameters |
-----
| Unit | Chassis 1 | Chassis 2 | Weight |
-----
| SGMs | 6 / 6 | 6 / 6 | 6 |
| Ports | | | |
|   Standard | 5 / 5 | 5 / 5 | 11 |
|   Bond | 0 / 0 | 0 / 0 | 11 |
|   Other | 0 / 0 | 0 / 0 | 6 |
| Sensors | | | |
|   SSMs | 2 / 2 | 2 / 2 | 11 |
| Grade | 113 / 113 | 113 / 113 | - |
-----
| Minimum grade gap for chassis failover: | 11 |
| Synchronization | | |
|   Sync to Active chassis: Enabled |
|   Sync to Standby chassis: Enabled |
-----
| Chassis HA mode: Active Up |
-----

```

## Example output from a Single Site configuration - bottom section

```

... output was truncated for brevity - the example starts above ...
-----
| Chassis Parameters |
-----
| Unit | Chassis 1 | Weight |
-----
| SGMs | 30 / 30 | 6 |
| Ports | | |
|   Standard | 4 / 4 | 11 |
|   Bond | 0 / 0 | 11 |
|   Other | 0 / 0 | 6 |
| Sensors | | |
|   SSMS | 2 / 2 | 11 |
| Grade | 246 / 246 | - |
-----
| Synchronization |
|   Sync to Active chassis: Enabled |
-----

```

- Note** - In the notation "*<Number> / <Number>*", the left number shows the number of components that in the state "UP", and the right number shows the number the components that must be in the state "UP".
- For example, on the **SGMs** line, "30 / 30" means that there are currently 30 Security Group Members in the state "UP" out of the 30 that must be in the state "UP".

Field	Description
<b>Grade</b>	<p>The sum of the grades of all components.</p> <p>The grade of each component is the unit weight multiplied by the number of components that are in the state "UP".</p> <p>You can configure the unit weight of each component to show the importance of the component in the system.</p> <p>To configure the unit weight, run in Gaia gClish:</p> <pre>set chassis high-availability factors &lt;Hardware Component&gt;</pre> <p>For example, to change the weight of the Security Group Member to 12, run in Gaia Clish on that Security Group Member:</p> <pre>set chassis high-availability factors sgm 12</pre> <p>See "<a href="#">Configuring Security Group High Availability</a>" on page 374.</p> <p>If you run the "asg stat -v" command, the output shows a greater unit weight and system grade.</p>
<b>Minimum grade gap for chassis failover</b>	<p>Site failover occurs to the Site with the higher grade only if its grade is greater than the other Site by more than the minimum gap.</p> <p>Minimum threshold for traffic processing - the minimum grade required for the Site to become Active.</p>

Field	Description
<b>Synchronization</b>	Status of synchronization between Security Group Members: <ul style="list-style-type: none"><li>■ Within a Site - between Security Group Members located in the same Security Group</li><li>■ Between two Sites - between Security Group Members located in different Sites</li><li>■ Exception Rules - exception rules configured by an administrator with the "g_sync_exception" command.</li></ul>

**Example 3 - List of Tasks (asg stat -i tasks)****Syntax**

```
asg stat -i tasks
```

**Example output from a Security Group in a Dual Site configuration**

The SMO task runs on Site #2 - on the Security Group Member #3, on which you ran this command (see the string "(local)").

```
[Expert@HostName-ch0x-0x:0]# asg stat -i tasks
-----
| Task (Task ID)      |          Chassis 1          |          Chassis 2          |
-----
| SMO (0)            |                               | 3 (local)                 |
| General (1)         |                2            |                3 (local)    |
| LACP (2)            |                2            |                3 (local)    |
| CH Monitor (3)     |                2            |                3 (local)    |
| DR Manager (4)     |                               |                3 (local)    |
| UIPC (5)            |                2            |                3 (local)    |
| Alert (6)          |                               |                3 (local)    |
-----
[Expert@HostName-ch0x-0x:0]#
[Expert@HostName-ch0x-0x:0]# member 2_4
Moving to member 2_4
... ..
[Expert@HostName-ch0x-0x:0]# asg stat -i tasks
-----
| Task (Task ID)      |          Chassis 1          |          Chassis 2          |
-----
| SMO (0)            |                               |                3            |
| General (1)         |                2            |                3            |
| LACP (2)            |                2            |                3            |
| CH Monitor (3)     |                2            |                3            |
| DR Manager (4)     |                               |                3            |
| UIPC (5)            |                2            |                3            |
| Alert (6)          |                               |                3            |
-----
[Expert@HostName-ch0x-0x:0]#
```

Example output from all Security Group Members (in our example, there are two on each Site):

```
[Expert@HostName-ch0x-0x:0]# g_all asg stat -i tasks
1_01:
-----
| Task (Task ID) | Chassis 1 | Chassis 2 |
-----
| SMO (0) | 1(local) | |
| General (1) | 1(local) | 1 |
| LACP (2) | 1(local) | 1 |
| CH Monitor (3) | 1(local) | 1 |
| DR Manager (4) | 1(local) | |
| UIPC (5) | 1(local) | 1 |
| Alert (6) | 1(local) | |
-----

1_02:
-----
| Task (Task ID) | Chassis 1 | Chassis 2 |
-----
| SMO (0) | 1 | |
| General (1) | 1 | 1 |
| LACP (2) | 1 | 1 |
| CH Monitor (3) | 1 | 1 |
| DR Manager (4) | 1 | |
| UIPC (5) | 1 | 1 |
| Alert (6) | 1 | |
-----

2_01:
-----
| Task (Task ID) | Chassis 1 | Chassis 2 |
-----
| SMO (0) | 1 | |
| General (1) | 1 | 1(local) |
| LACP (2) | 1 | 1(local) |
| CH Monitor (3) | 1 | 1(local) |
| DR Manager (4) | 1 | |
| UIPC (5) | 1 | 1(local) |
| Alert (6) | 1 | |
-----

2_02:
-----
| Task (Task ID) | Chassis 1 | Chassis 2 |
-----
| SMO (0) | 1 | |
| General (1) | 1 | 1 |
| LACP (2) | 1 | 1 |
| CH Monitor (3) | 1 | 1 |
| DR Manager (4) | 1 | |
| UIPC (5) | 1 | 1 |
| Alert (6) | 1 | |
-----
[Expert@HostName-ch0x-0x:0]#
```

### Example output from a Security Group in a Single Site configuration

The SMO task runs on the Security Group Member #1, on which you ran this command (see the string "(local)").

```
[Expert@HostName-ch0x-0x:0]# asg stat -i tasks
```

```
-----  
| Task (Task ID)      | Chassis 1 |  
-----  
| SMO (0)            | 1 (local) |  
| General (1)         | 1 (local)  |  
| LACP (2)            | 1 (local)  |  
| CH Monitor (3)      | 1 (local)  |  
| DR Manager (4)      | 1 (local)  |  
| UIPC (5)            | 1 (local)  |  
| Alert (6)           | 1 (local)  |  
-----
```

```
[Expert@HostName-ch0x-0x:0]#
```




# Monitoring System and Component Status (asg monitor)

## Description

Use the "asg monitor" command in Gaia gClish or the Expert mode to monitor continuously the status of the system and its components.

This command shows the same information as the "[Showing Hardware State \(asg stat\)](#)" on [page 255](#), but the information stays on the screen and refreshes at intervals specified by the user. Default: 1 second). To stop the monitor session, press **CTRL+C**.

 **Note** - If you run this command in a Virtual System context, you only see the output for that Virtual System. You can also specify the Virtual System context as a command parameter.


## Syntax

asg monitor
asg monitor -h
asg monitor [-v   -all] [-amw] <Interval>
asg monitor -l

## Parameters

Parameter	Description
No Parameters	Shows the Security Group Member status.
-h	Shows the built-in help.
-amw	Shows the Anti-Malware policy date instead of the Firewall policy date.
-v	Shows only the System component status.
-all	Shows both Security Group Member and System component status.
<Interval>	Configures the data refresh interval (in seconds) for this session. Default is 10 seconds.
-l	Shows legend of column title abbreviations.

## Explanation about the Output

Field	Instructions
SGM ID	Identifier of the Security Group Member. The <code>(local)</code> is the Security Group Member, on which you ran the command.
State	<p>State of the Security Group Member:</p> <ul style="list-style-type: none"> <li>■ <code>ACTIVE</code> - The Security Group Member is processing traffic.</li> <li>■ <code>DOWN</code> - The Security Group Member is not processing traffic.</li> <li>■ <code>DETACHED/LOST</code> - The Security Group Member is not communicating/reboot.</li> <li>■ <code>INIT</code> - The Security Group Member is in the initialization phase after reboot.</li> <li>■ <code>READY</code> - The Security Group Member is ready to become Active, and is waiting for all other remote Active members to acknowledge its state.</li> <li>■ <code>Active(Sync)</code> - The Security Group Member is in a unicast connections sync.</li> </ul> <p> <b>Note</b> - To change manually the state of the Security Group Member, use the "<code>g_clusterXL_admin</code>" command (see "<a href="#">Configuring the Cluster State (g_clusterXL_admin)</a>" on page 180).</p>

## Examples

### Example 1 - Shows the Security Group Member status with the Anti-Malware policy date

```
[Expert@HostName-ch0x-0x:0]# asg monitor -amw
-----
| System Status - Maestro                                     |
-----
| Up time           | 12:03:48 hours |
| SGMs              | 2 / 2          |
| Version           | R81.20 (Build Number XX) |
| FW Policy Date    | 21Feb19 14:37  |
| AMW Policy Date   | 21Feb19 14:37  |
-----
| SGM ID           | Chassis 1     |
|                  | ACTIVE        |
-----
| 1                | ACTIVE        |
| 2                | ACTIVE        |
-----
```

**Example 2 - Shows the Security Group component status**

```
[Expert@HostName-ch0x-0x:0]# asg monitor -v
Thu Feb 21 21:07:11 IST 2019

-----
| Chassis Parameters |
-----
| Unit | Chassis 1 | Weight |
-----
| SGMs | 2 / 2 | 6 |
| Ports | | |
|   Standard | 8 / 8 | 11 |
|   Bond | 0 / 0 | 11 |
|   Mgmt | 1 / 1 | 11 |
|   Mgmt Bond | 0 / 0 | 11 |
|   Other | 0 / 0 | 6 |
| Sensors | | |
|   SSMs | 2 / 2 | 11 |
| | | |
| Grade | 133 / 133 | - |
-----
| Synchronization |
|   Sync to Active chassis: Enabled |
-----
```

# Configuring Alert Thresholds (set chassis alert\_threshold)

## Description

Use the "set chassis alert\_threshold" command in Gaia gClish to configure thresholds for performance and hardware alerts.

## Syntax to configure alert threshold

```
set chassis alert_threshold <Threshold Name> <Value>
```

## Syntax to view an alert threshold configuration

```
show chassis alert_threshold <Threshold Name>
```

## Parameters

Parameter	Description
<Threshold Name>	Threshold name as specified in the table below
<Value>	High or low value for the specified threshold

## Performance Alert Thresholds

Threshold Name	Scope	Description
concurr_conn_threshold_high	Security Group Member	Concurrent connections - High limit
concurr_conn_threshold_low_ratio	Security Group Member	Concurrent connections - Low limit (% of the High limit)
concurr_conn_total_threshold_high	Security Group	Concurrent connections - High limit
concurr_conn_total_threshold_low_ratio	Security Group	Concurrent connections - Low limit (% of the High limit)
conn_rate_threshold_high	Security Group Member	Connection rate per second - High limit

Threshold Name	Scope	Description
conn_rate_threshold_low_ratio	Security Group Member	Connection rate per second - Low limit (% of the High limit)
conn_rate_total_threshold_high	Security Group	Connection rate per second - High limit
conn_rate_total_threshold_low_ratio	Security Group	Connection rate per second - Low limit (% of the High limit)
cpu_load_threshold_perc_high	Security Group Member	CPU load (%) - High limit
cpu_load_threshold_perc_low_ratio	Security Group Member	CPU load (%) - Low limit (% of the High limit)
hd_util_threshold_perc_high	Security Group Member	Disk utilization (%) - High limit
hd_util_threshold_perc_low_ratio	Security Group Member	Disk utilization (%) - Low limit (% of the High limit)
mem_util_threshold_perc_high	Security Group Member	Memory utilization (%) - High limit
mem_util_threshold_perc_low_ratio	Security Group Member	Memory utilization (%) - Low limit (% of the High limit)
packet_rate_threshold_high	Security Group Member	Packet rate per second - High limit
packet_rate_threshold_low_ratio	Security Group Member	Packet rate per second - Low limit (% of the High limit)
packet_rate_total_threshold_high	Security Group	Packet rate per second - High limit
packet_rate_total_threshold_low_ratio	Security Group	Packet rate per second - Low limit (% of the High limit)
throughput_threshold_high	Security Group Member	Throughput (bps) - High limit

Threshold Name	Scope	Description
throughput_threshold_low_ratio	Security Group Member	Throughput (bps) - Low limit (% of the High limit)
throughput_total_threshold_high	Security Group	Throughput (bps) - High limit
throughput_total_threshold_low_ratio	Security Group	Throughput (bps) - Low limit (% of the High limit)

### Example - Set the high limit of the memory utilization to 70% of the installed memory

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01> set chassis alert_threshold mem_util_threshold_perc_high 70
[Global] HostName-ch01-01>
```

# Monitoring System Resources (asg resource)

## Description

Use the "asg resource" command in Gaia gClish or the Expert mode to show this information for Security Group Members:

- RAM and Storage usage and thresholds
- SSD Health

## Syntax

```
asg resource -h
```

```
asg resource [-b <SGM IDs>]
```

```
asg resource --ssd [-v]
```

## Parameters

Parameter	Description
No Parameters	Shows both the Resource (RAM and Storage) and SSD Health information.
-h	Shows the built-in help.
-b <SGM IDs>	Applies to Security Group Members as specified by the <SGM IDs>. <SGM IDs> can be: <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul>
--ssd [-v]	Shows only the SSD Health information for all Security Group Members: <ul style="list-style-type: none"> <li>▪ --ssd Shows summary information only (whether it passed the SMART test)</li> <li>▪ --ssd -v Shows the summary and verbose information (SSD SMART Attributes)</li> </ul>

## Examples

## Example 1 - Default output

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > asg resource
+-----+
|Resource Table|
+-----+
|Member ID   |Resource Name           |Usage   |Threshold |Total   |
+-----+
|1_01        |Memory                  |21%     |50%       |62.8G  |
|            |HD: /                   |16%     |80%       |33.9G  |
|            |HD: /var/log            |2%      |80%       |48.4G  |
|            |HD: /boot                |14%     |80%       |288.6M |
+-----+
|1_02        |Memory                  |21%     |50%       |62.8G  |
|            |HD: /                   |16%     |80%       |33.9G  |
|            |HD: /var/log            |2%      |80%       |48.4G  |
|            |HD: /boot                |14%     |80%       |288.6M |
+-----+
... output is cut for brevity ...
+-----+
|2_01        |Memory                  |21%     |50%       |62.8G  |
|            |HD: /                   |16%     |80%       |33.9G  |
|            |HD: /var/log            |2%      |80%       |48.4G  |
|            |HD: /boot                |14%     |80%       |288.6M |
+-----+
|2_02        |Memory                  |21%     |50%       |62.8G  |
|            |HD: /                   |16%     |80%       |33.9G  |
|            |HD: /var/log            |2%      |80%       |48.4G  |
|            |HD: /boot                |14%     |80%       |288.6M |
+-----+
... output is cut for brevity ...

+-----+
|SSD Health|
+-----+
|Member ID   |SMART overall-health|
+-----+
|1_01        |PASSED               |
+-----+
|1_02        |PASSED               |
+-----+
... output is cut for brevity ...
+-----+
|2_01        |PASSED               |
+-----+
|2_02        |PASSED               |
+-----+
... output is cut for brevity ...

SSD attributes verifier ended successfully.
[Global] HostName-ch01-01>
```



**Example 2 - Resource Table for a specific Security Group Member**

```
[Expert@HostName-ch0x-0x:0]# asg resource -b 1_01
+-----+
|Resource Table|
+-----+
|Member ID  |Resource Name      |Usage   |Threshold  |Total   |
+-----+
|1_01       |Memory             |21%     |50%        |62.8G  |
|           |HD: /              |16%     |80%        |33.9G  |
|           |HD: /var/log       |2%      |80%        |48.4G  |
|           |HD: /boot          |14%     |80%        |288.6M |
+-----+
+-----+
|SSD Health  |
+-----+
|Member ID  |SMART overall-health|
+-----+
|1_01       |PASSED              |
+-----+
|1_02       |PASSED              |
+-----+
|1_03       |PASSED              |
+-----+
|1_04       |PASSED              |
+-----+
|1_05       |PASSED              |
+-----+
|2_01       |PASSED              |
+-----+
|2_02       |PASSED              |
+-----+
|2_03       |PASSED              |
+-----+
|2_04       |PASSED              |
+-----+
|2_05       |PASSED              |
+-----+

SSD attributes verifier ended successfully.
[Expert@HostName-ch0x-0x:0]#
```

## Example 3 - Verbose SSD Health information

```
[Expert@HostName-ch0x-0x:0]# asg resource --ssd -v
+-----+
|SSD Health                                     |
+-----+
|Member ID      |SMART overall-health |
+-----+
|1_01           |PASSED                |
+-----+
|1_02           |PASSED                |
+-----+
... output is cut for brevity ...
+-----+
|2_01           |PASSED                |
+-----+
|2_02           |PASSED                |
+-----+
... output is cut for brevity ...

+-----+
|SSD Attributes                                     |
+-----+
Member 1_01
+-----+
|ID  |Attribute name          |Value |Trhesh |Last_failed |
+-----+
|5   |Reallocated_Sector_Ct  |100   |0      |-           |
+-----+
|9   |Power_On_Hours         |100   |0      |-           |
+-----+
|12  |Power_Cycle_Count      |100   |0      |-           |
+-----+
... output is cut for brevity ...
+-----+
|194 |Temperature_Celsius    |100   |0      |-           |
+-----+
... output is cut for brevity ...

+-----+
Member 1_02
+-----+
|ID  |Attribute name          |Value |Trhesh |Last_failed |
+-----+
|5   |Reallocated_Sector_Ct  |100   |0      |-           |
+-----+
... output is cut for brevity ...

[Expert@HostName-ch0x-0x:0]#
```

## Description for the Resource Table section

Column	Description
<b>Member ID</b>	Shows the Security Group Member ID.
<b>Resource Name</b>	Identifies the resource. There are four types of resources: <ul style="list-style-type: none"> <li>▪ <b>Memory</b></li> <li>▪ <b>HD</b> - Hard drive space (/)</li> <li>▪ <b>HD: /var/log</b> - Space on hard drive committed to log files</li> <li>▪ <b>HD: /boot</b> - Location of the kernel</li> </ul>
<b>Usage</b>	Shows the percentage of the resource in use.
<b>Threshold</b>	Indicates the health and functionality of the component. When the value of the resource is greater than the threshold, an alert is sent. You can modify the threshold in Gaia gClish.
<b>Total</b>	Total absolute value in units. For example, the first row shows that <code>Security Appliance1 on Chassis1</code> has 62.8 GB of RAM, and 21% of it are used. An alert is sent, if the usage is greater than 50%.

## Description for the SMART Attributes section

Column	Description
<b>SMART overall-health</b>	Shows the state of the SMART test - passed, or failed.
<b>ID</b>	Shows the attribute ID in the decimal format.
<b>Attribute name</b>	Shows the attribute name.
<b>Value</b>	Shows the current value as returned by the SSD. This is a most universal measurement, on the scale from 0 (bad) to some maximum (good) value. Maximum values are typically 100, 200 or 253. The higher the value, the better the SSD health is.
<b>Trhesh</b>	Shows the current threshold. This is the minimum value limit for the attribute. If the value falls below this threshold, the SSD should be checked for errors, and possibly replaced.
<b>Last_failed</b>	Shows when a failure was last reported for this attribute.

## Configuring Alerts for Security Group Member and Security Group Events (asg alert)

The "asg alert" command is an interactive wizard that configures alerts for Security Group Member and Security Group events.

These events include hardware failure, recovery, and performance-related events. You can create other general events.

An alert is sent when an event occurs. For example, when the value of a hardware resource is greater than the threshold.

The alert message includes the Site ID, Security Group Member ID, and/or unit ID.

The wizard has these options:

Option	Description
<b>Full Configuration Wizard</b>	Creates a new alert.
<b>Edit Configuration</b>	Changes an existing alert.
<b>Show Configuration</b>	Shows existing alert configuration.
<b>Run Test</b>	Runs a test simulation to make sure that the alert works correctly.

To create or change an alert:

Step	Instructions
1	Run in Gaia gClish of a Security Group: <div style="border: 1px solid black; padding: 5px; width: fit-content; margin: 5px 0;">asg alert</div>
2	Select <b>Full Configuration Wizard</b> or <b>Edit Configuration</b> .
3	Select and configure these parameters as prompted by the wizard: <ul style="list-style-type: none"> <li>▪ <b>SMS</b></li> <li>▪ <b>Email</b></li> <li>▪ <b>Log</b></li> </ul>

**SMS Alert Configuration**

Parameter	Description
<b>SMS provider URL</b>	Fully qualified URL to your SMS provider.
<b>HTTP proxy and port</b>	Optional. Configure only if the Security Gateway requires a proxy server to reach the SMS provider.
<b>SMS rate limit</b>	Maximum number of SMS messages sent per hour. If there are too many messages, they can be combined together.
<b>SMS user text</b>	Custom prefix for SMS messages.

**Email Alert Configuration**

Parameter	Description
<b>SMTP server IP</b>	One or more SMTP servers to which the email alerts are sent.
<b>Email recipient addresses</b>	One or more recipient email address for each SMTP server.
<b>Periodic connectivity checks</b>	Tests run periodically to confirm connectivity with the SMTP servers. If there is no connectivity, alert messages are saved and sent in one email when connectivity is restored.
<b>Interval</b>	Interval, in minutes, between connectivity tests.
<b>Sender email address</b>	Email address of the sender for alerts.
<b>Subject</b>	Subject header text for the email alert.
<b>Body text</b>	User defined text for the alert message.

## Log Alert Configuration

There are no parameters to configure.

You can configure the **Log Mode** to:

- **Enabled**
- **Disabled**
- **Monitor**

## System Event Types

System event types are:

```
-----
1      | SGM State
2      | Chassis State
3      | Port State
4      | Diagnostics
5      | Memory Leak Detection
6      | LSP Monitor Port State Change
7      | VS Monitor State Change
```

Hardware Monitor events:

```
8      | Fans
9      | SSM
10     | CMM
11     | Power Supplies
12     | CPU Temperature
```

Performance events:

```
13     | Concurrent Connections
14     | Connection Rate
15     | Packet Rate
16     | Throughput
17     | CPU Load
18     | Hard Drive Utilization
19     | Memory Utilization
```

Please choose event types for which to send alerts: [all]  
(format: all or 1,4 or 1,3-7,10)

You can select one or more event types:

- One event type.
- A comma-delimited list of more than one event type.
- All event types.

# Collecting System Diagnostics (smo verifiers)

## *In This Section:*

---

Diagnostic Tests .....	280
Showing the Tests .....	282
Showing the Last Run Diagnostic Tests .....	283
Running all Diagnostic Tests .....	284
Running Specific Diagnostic Tests .....	285
Collecting Diagnostic Information for a Report Specified Section .....	287
Error Types .....	288
Changing Compliance Thresholds .....	289
Changing the Default Test Behavior of the 'asg diag resource verifier' .....	289
Troubleshooting Failures .....	291

---

## Diagnostic Tests

### Description

Use the "smo verifiers" commands in Gaia gClish to run a specific set of diagnostic tests.

The full set of tests run by default, but you can manually select the tests to run.

The output shows the result of the test, `Passed` or `Failed`, and the location of the output log file.

### Syntax

```
show smo verifiers list
    [id <TestId1>,<TestId2>,...]
    [section <SectionName>]
```

```
show smo verifiers report [except]
    [id <TestId1>,<TestId2>,...]
    [name <TestName>]
    [section <SectionName>]
```

```
show smo verifiers print [except]
    [id <TestId1>,<TestId2>,...]
    [name <TestName>]
    [section <SectionName>]
```



```
show smo verifiers
    periodic
    last-run report
    print
```

```
delete smo verifiers purge [save <Num_Logs>]
```

## Parameters

Parameter	Description
list	Shows the list of tests to run.
report	Runs tests and shows a summary of the test results.
print	Runs tests and shows the full output and summary of the test results.
except	Runs all tests except the specified tests. Shows the requested results.
id < <i>TestId1</i> >,< <i>TestId2</i> >,...	Specifies the tests by their IDs (comma separated list). To see a list of test IDs, run: <pre>show smo verifiers list</pre>
name < <i>TestName</i> >	Specifies the tests by their names. Press the <b>Tab</b> key to see a full list of verifiers names.
section < <i>SectionName</i> >	Specifies the verifiers section by its name. Press the <b>Tab</b> key to see a full list of the existing sections.
purge	Deletes the old "smo verifiers" logs. Keeps the newest log.
save < <i>Num_Logs</i> >	Number of logs to save from the "smo verifiers" log files. Default: 5.
periodic	Shows the latest periodic run results.
last-run	Shows the latest run results.

## Showing the Tests

The "show smc verifiers list" command shows the full list of diagnostic tests.

The list shows the test "ID", test "Title" (name), and the "Command" the "smc verifiers" command runs.

### Example

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show smc verifiers list
-----
| ID | Title                | Command                |
-----
| System Components
-----
| 1 | System Health       | asg stat -v           |
| 2 | Firmware Verifier   | firmware_verifier -v  |
-----
| Policy and Configuration
-----
| 3 | Policy              | asg policy verify -a  |
| 4 | AMW Policy          | asg policy verify_amw -a |
| 5 | SWB Updates         | asg_swb_update_verifier -v |
| 6 | Security Group      | security_group_util diag |
| 7 | Cores Distribution  | cores_verifier        |
| 8 | Clock               | clock_verifier -v     |
| 9 | Licenses            | asg_license_verifier -v |
-----
| VSX Configuration
-----
| 10 | BMAC VMAC verify   | mac_verifier -x      |
-----
| Networking
-----
| 11 | MAC Setting        | mac_verifier -v      |
| 12 | ARP Consistency    | asg_arp -v           |
| 13 | Bond               | asg_bond -v          |
| 14 | IPv4 Route         | asg_route            |
| 15 | IPv6 Route         | asg_route -6        |
| 16 | Dynamic Routing    | asg_dr_verifier      |
| 17 | Local ARP          | asg_local_arp_verifier -v |
| 18 | IGMP Consistency   | asg_igmp             |
| 19 | PIM Neighbors      | asg_pim_neighbors    |
-----
| Run "show smc verifiers print id <TestNum>" to display test output
-----
[Global] HostName-ch01-01 >
```

## Showing the Last Run Diagnostic Tests

The "show smo verifiers last-run report" command shows the **default** output for the last run diagnostic tests.

The "show smo verifiers last-run print" command shows **verbose** output for the last run diagnostic tests.

### Example

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show smo verifiers last-run report
2023-04-20, 01:00:05
-----
| Tests Status |
-----
| ID | Title | Result | Reason |
-----
| System Components |
-----
| 1 | System Health | Failed (!) | (1)Chassis 1 error |
| 2 | Firmware Verifier | Passed | |
-----
| Policy and Configuration |
-----
| 3 | Policy | Passed | |
| 4 | AMW Policy | Passed | (1)Not configured |
| 5 | SWB Updates | Passed | (1)Not configured |
| 6 | Security Group | Passed | |
| 7 | Cores Distribution | Passed | |
| 8 | Clock | Passed | |
| 9 | Licenses | Failed (!) | (1)Trial license will expire within 2 |
| | | | weeks |
| | | | (2)Execution error |
-----
| Networking |
-----
| 10 | MAC Setting | Passed | |
| 11 | ARP Consistency | Passed | |
| 12 | Bond | Passed | (1)Not configured |
| 13 | IPv4 Route | Passed | |
| 14 | IPv6 Route | Passed | (1)Not configured |
| 15 | Dynamic Routing | Passed | (1)Not configured |
| 16 | Local ARP | Passed | (1)Not configured |
| 17 | IGMP Consistency | Passed | (1)Not configured |
| 18 | PIM Neighbors | Passed | (1)Not configured |
-----
| Tests Summary |
-----
| Passed: 16/18 tests |
| Run: "show smo verifiers list id 1,9" to view a complete list |
| of failed tests |
| Output file: /var/log/alert_verifier_sum.1-18.2023-04-20_01-00-05.txt |
-----
[Global] HostName-ch01-01 >
```

## Running all Diagnostic Tests

The "show smo verifiers report" command runs all diagnostic tests and shows their summary output.

When a test fails, the reasons for failure show in the **Reason** column.

### Example

```
[Global] HostName-ch01-01 > show smo verifiers report
Duration of tests vary and may take a few minutes to complete

-----
| Tests Status                                                                 |
-----
| ID | Title                | Result    | Reason                |
-----
| System Components                                                           |
-----
| 1 | System Health        | Failed (!) | (1)Chassis 1 error   |
| 2 | Firmware Verifier    | Passed    |                       |
-----
| Policy and Configuration                                                    |
-----
| 3 | Policy                | Passed    |                       |
| 4 | AMW Policy            | Passed    | (1)Not configured    |
| 5 | SWB Updates          | Passed    | (1)Not configured    |
| 6 | Security Group       | Passed    |                       |
| 7 | Cores Distribution   | Passed    |                       |
| 8 | Clock                | Passed    |                       |
| 9 | Licenses              | Failed (!) | (1)Trial license will expire within 2 |
|   |                       |           | weeks                 |
-----
| Networking                                                                  |
-----
| 10 | MAC Setting          | Passed    |                       |
| 11 | ARP Consistency      | Passed    |                       |
| 12 | Bond                 | Passed    | (1)Not configured    |
| 13 | IPv4 Route           | Passed    |                       |
| 14 | IPv6 Route           | Passed    | (1)Not configured    |
| 15 | Dynamic Routing      | Passed    | (1)Not configured    |
| 16 | Local ARP            | Passed    | (1)Not configured    |
| 17 | IGMP Consistency     | Passed    | (1)Not configured    |
| 18 | PIM Neighbors        | Passed    | (1)Not configured    |
-----
| Tests Summary                                                                |
-----
| Passed: 16/18 tests                                                         |
| Run: "show smo verifiers list id 1,9" to view a complete list of failed tes |
| ts                                                                           |
| Output file: /var/log/verifier_sum.1-18.2023-04-20_12-24-37.txt             |
| Run "show smo verifiers last-run print" to display verbose output           |
-----
[Global] HostName-ch01-01 >
```

## Running Specific Diagnostic Tests

These commands run the specified diagnostic tests only:

```
show smo verifiers report name
```

```
show smo verifiers report id
```

### Syntax to run a test by its name

```
show smo verifiers report name <Test Name>
```

**Note** - Press the **Tab** key after the "name" parameter to see a full list of verifier names.

### Example

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show smo verifiers report name System_Health
Duration of tests vary and may take a few minutes to complete

-----
| Tests Status                                                                 |
-----
| ID | Title                | Result    | Reason |
-----
| System Components                                                         |
-----
| 1 | System Health        | Passed |        |
-----
| Tests Summary                                                             |
-----
| Passed: 1/1 test                                                           |
| Output file: /var/log/verifier_sum.1-18.2023-04-20_12-24-37.txt           |
| Run "show smo verifiers last-run print" to display verbose output         |
-----
[Global] HostName-ch01-01 >
```

### Syntax to run a test by its ID

```
show smo verifiers report id <TestID1>,<TestID2>,...,<TestIDn>
```

**Note** - To see a list of test IDs, run the "show smo verifiers list" command.

### Example

This example collects diagnostic information for specified tests 1 and 2.

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show smo verifiers report id 1,2
Duration of tests vary and may take a few minutes to complete

-----
| Tests Status |
-----
| ID | Title | Result | Reason |
-----
| System Components |
-----
| 1 | System Health | Failed (!) | (1)Chassis 1 error |
| 2 | Firmware Verifier | Passed | |
-----
| Tests Summary |
-----
| Passed: 1/2 tests |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.1-18.2023-04-20_12-24-37.txt |
| Run "show smo verifiers last-run print" to display verbose output |
-----
[Global] HostName-ch01-01 >
```

## Collecting Diagnostic Information for a Report Specified Section

The "show smo verifiers report section" command runs all diagnostic tests in the specified section.

### Syntax

```
show smo verifiers report section <Test Name>
```

**Note** - Press the **Tab** key after the "section" parameter to see a full list of verifier sections.

### Example

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show smo verifiers report section System_Components
Duration of tests vary and may take a few minutes to complete

-----
| Tests Status |
-----
| ID | Title | Result | Reason |
-----
| System Components |
-----
| 1 | System Health | Failed (!) | (1)Chassis 1 error |
| 2 | Firmware Verifier | Passed | |
-----
| Tests Summary |
-----
| Passed: 1/2 tests |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.1-18.2023-04-20_12-24-37.txt |
| Run "show smo verifiers last-run print" to display verbose output |
-----
[Global] HostName-ch01-01 >
```

## Error Types

The "smo verifiers" command detects these errors:

Error Type	Error	Description
System health	Chassis <X> error	The Security Group quality grade is less than the defined threshold. We recommend that you correct this issue immediately.
Hardware	<Component> is missing	The component is not installed in the Chassis. <b>Note</b> - This applies only to 60000 / 40000 Appliances.
	<Component> is down	The component is installed in the Chassis, but is inactive. <b>Note</b> - This applies only to 60000 / 40000 Appliances.
Resources	<Resource> capacity	The specified resource capacity is not sufficient. You can change the defined resource capacity.
	<Resource> exceed threshold	The resource usage is greater than the defined threshold.
CPU type	Non compliant CPU type	CPU type is not configured in the list of compliant CPUs on at least one Security Group Member. You can define the compliant CPU types.
Security group	<Source> error	The information collected from this source is different between the Security Group Members.
	<Sources> differ	The information collected from many sources is different.



## Changing Compliance Thresholds

You can change some compliance thresholds that define a healthy, working system.

Change the threshold values in the `$SMODIR/conf/asg_diag_config` file.

These are the supported resources you can control:

Resource	Instructions
Memory	RAM memory capacity in GB.
HD: /	Disk capacity in GB for <code>&lt;disk&gt;</code> - the root (/) partition.
HD: /var/log	Disk capacity in GB for the <code>/var/log</code> partition.
HD: /boot	Disk capacity in GB for the <code>/boot</code> partition.
Skew	The maximum permissible clock difference, in seconds, between the SGMs and CMMs. <b>Note</b> - This resource applies only to 60000 / 40000 Appliances.
Certified cpu	Each line represents one compliant CPU type. <b>Note</b> - This resource applies only to 60000 / 40000 Appliances

## Changing the Default Test Behavior of the 'asg diag resource verifier'

By default, the "asg diag resource verifier" command only shows a warning about resource mismatches between Security Group Members.

The verification test results show as "Passed" in the output and no further action is taken.

You can change the default test behavior:

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the <code>\$FWDIR/conf/asg_diag_config</code> file: <pre>g_all vi \$FWDIR/conf/asg_diag_config</pre>
4	Search for this parameter: <pre>MismatchSeverity</pre>

Step	Instructions
5	<p>Set the value of this parameter to one of these values:</p> <ul style="list-style-type: none"><li data-bbox="357 286 1252 365">■ fail Verification test result is set to "Failed"</li><li data-bbox="357 371 1252 488">■ warn Verification test result is set to "Passed", and a warning is shown</li><li data-bbox="357 495 1252 611">■ ignore Verification test result is set to "Ignore", and no errors are shown</li></ul>
6	Save the changes in the file and exit the editor.

## Troubleshooting Failures

Use the "smo verifiers" command to troubleshoot a failed diagnostic test.

### Example

Below is the example procedure based on the **System Health** test that failed.

1. The **System Health** test failed:

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show smo verifiers report id 1
Duration of tests vary and may take a few minutes to complete
```

```
-----
| Tests Status |
-----
| ID | Title | Result | Reason |
-----
| System Components |
-----
| 1 | System Health | Failed (!) | (1)Chassis 1 error |
-----
| Tests Summary |
-----
| Passed: 0/1 test |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.1-18.2023-04-20_12-24-37.txt |
| Run "show smo verifiers last-run print" to display verbose output |
-----
[Global] HostName-ch01-01 >
```

## 2. Print the full report for this failed test:

```
[Global] HostName-ch01-01 > show smo verifiers print id 1
=====
System Health:
=====

-----
| VSX System Status - Maestro |
-----
| Up time | 06:44:48 hours |
| SGMs | 3 / 3 |
| Virtual Systems | 1 |
| Version | R81.20 (Build Number xxx) |
-----
| VS ID: 0 | VS Name: MyVSname |
-----
| SGM ID | Chassis 1 |
| | ACTIVE |
-----
| 2 | ACTIVE |
| 3 | ACTIVE |
| 4 | ACTIVE |
-----
| Chassis Parameters |
-----
| Unit | Chassis 1 |
-----
| SGMs | 3 / 3 |
| Ports | 0 / 0 |
| SSMs | 1 / 2 ! |
-----
| Synchronization |
| Sync to Active chassis: Enabled |
-----
-----
| Tests Status |
-----
| ID | Title | Result | Reason |
-----
| System Components |
-----
| 1 | System Health | Failed (!) | (1)Chassis 1 error |
-----
| Tests Summary |
-----
| Passed: 0/1 test |
| Run: "show smo verifiers list id 1" to view a complete list of failed tests |
| Output file: /var/log/verifier_sum.1-18.2023-04-20_12-24-57.txt |
-----
[Global] HostName-ch01-01 >
```

## 3. Examine which command produced the failed test:

```
[Global] HostName-ch01-01 > show smo verifiers list id 1
-----
| ID | Title                | Command                |
-----
| System Components                                     |
-----
| 1 | System Health       | asg stat -v         |
-----
| Run "show smo verifiers print id <TestNum>" to display test output |
-----
[Global] HostName-ch01-01 >
```

#### 4. Run the applicable command to understand what failed:

```
[Global] HostName-ch01-01 > asg stat -v
-----
| VSX System Status - Maestro                          |
-----
| Up time                | 06:45:06 hours        |
| SGMs                   | 3 / 3                 |
| Virtual Systems        | 1                     |
| Version                 | R81.20 (Build Number xxx) |
-----
| VS ID: 0              | VS Name: MyVSname     |
-----
| SGM ID                | Chassis 1             |
|                       | ACTIVE                |
-----
| 2                     | ACTIVE                |
| 3                     | ACTIVE                |
| 4                     | ACTIVE                |
-----
| Chassis Parameters                                     |
-----
| Unit          | Chassis 1              | Weight |
-----
| SGMs          | 3 / 3                  | 6      |
| Ports         |                        |        |
|   Standard    | 0 / 0                  | 11     |
|   Bond        | 0 / 0                  | 11     |
|   Other       | 0 / 0                  | 6      |
| Sensors       |                        |        |
| SSMs        | 1 / 2 !              | 11     |
|               |                        |        |
| Grade         | 29 / 40 !             | -      |
-----
| Synchronization                                     |
|   Sync to Active chassis: Enabled                 |
-----
[Global] HostName-ch01-01 >
```

# Alert Modes

## *In This Section:*

---

Diagnostic Events .....	295
Important Notes .....	296
Known Limitations of the SMO Verifiers Test .....	300

---

The Alert Modes are:

- **Enabled** - The system sends an alert for the selected events.
- **Disabled** - The system does not send alerts for the selected events.
- **Monitor** - The system generates a log entry instead of an alert.

## Diagnostic Events

- ★ **Best Practice** - Run the "smo verifiers" command (or the "show smo verifiers report" command) on a regular basis.

If the test fails, an alert appears. The alerts continue to appear in the **Message of the Day** (MOTD) until the issues are resolved.

When the issues are resolved, a **Clear Alert** message appears the next time the test runs.

You can manually run the "smo verifiers" command (the "show smo verifiers report" command) to confirm the issue is resolved.

## Important Notes

- By default, the tests run at 01h:00m each night.

### Changing the default time

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the <code>\$FWDIR/conf/asgsnmp.conf</code> file: <pre>vi \$FWDIR/conf/asgsnmp.conf</pre>
4	Change the value in this line: <pre>asg_diag_alert_wrapper</pre>
5	Save the changes in the file and exit the editor.
6	Copy this file to all other Security Group Members: <pre>asg_cp2blades \$FWDIR/conf/asgsnmp.conf</pre>



- By default, all tests run.

### Excluding the tests

**Note** - When you manually run the "show smo verifiers report" command, the complete set of tests runs, even those you excluded.

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: <pre>\$FWDIR/conf/asg_diag_config</pre>
4	Add this line to the file: <pre>excluded_tests=[&lt;Test1&gt;] [,&lt;Test2&gt;, ...]</pre>
5	Save the changes in the file and exit the editor.
6	Copy this file to all other Security Group Members: <pre>asg_cp2blades \$FWDIR/conf/asgsnmp.conf</pre>

- All failed tests show in the MOTD.

## Excluding failed test notifications from the MOTD

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Run: <pre>\$FWDIR/conf/asg_diag_config</pre>
4	Set the <code>failed_tests_motd</code> parameter to <code>off</code>
5	Copy this file to all other Security Group Members: <pre>asg_cp2blades \$FWDIR/conf/asg_diag_config</pre>
6	Go to Gaia gClish: enter <code>gclish</code> and press Enter.
7	Enforce the change: <pre>show smo verifiers report</pre> <p>You can also wait for the next time the "smo verifiers" run automatically.</p>

## Disabling the MOTD feature

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the <code>\$FWDIR/conf/asg_diag_config</code> file: <pre>vi \$FWDIR/conf/asg_diag_config</pre>
4	Set the value of the <code>motd</code> parameter to <code>off</code> .
5	Save the changes in the file and exit the editor.
6	Copy this file to all other Security Group Members: <pre>asg_cp2blades \$FWDIR/conf/asg_diag_config</pre>
7	Go to Gaia gClish: enter <code>gclish</code> and press Enter.
8	Enforce the change: <pre>show smo verifiers report</pre> <p>You can also wait for the next time the "smo verifiers" run automatically.</p>

## Known Limitations of the SMO Verifiers Test

By default, the "smo verifiers" command only shows a warning about resource mismatches between Security Group Members.

If the verification test results show **Passed** in the output, no more steps are necessary.

### Changing the default behavior

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	Edit the <code>\$FWDIR/conf/asg_diag_config</code> file: <pre>vi \$FWDIR/conf/asg_diag_config</pre>
4	Search for this parameter: <pre>MismatchSeverity</pre>
5	Set the value of this parameter to one of these values: <ul style="list-style-type: none"> <li>■ <code>fail</code> Verification test result is set to "Failed"</li> <li>■ <code>warn</code> Verification test result is set to "Passed", and a warning is shown</li> <li>■ <code>ignore</code> Verification test result is set to "Ignore", and no errors are shown</li> </ul>
6	Save the changes in the file and exit the editor.
7	Copy this file to all other Security Group Members: <pre>asg_cp2blades \$FWDIR/conf/asg_diag_config</pre>

# System Monitoring

This section describes features to monitor your system status.

## Showing System Serial Numbers (asg\_serial\_info)

### Description

Use the "asg\_serial\_info" command in Gaia gClish or the Expert mode to show the serial numbers of all the Security Group Members in the Security Group.

### Syntax

```
asg_serial_info
```

### Parameters

Parameter	Description
-h	Shows the built-in help.

### Example

```
[Expert@HostName-ch0x-0x:0]# asg_serial_info
Collecting SGMs information...
+-----+
|   Serial numbers   |
+-----+
| Chassis ID |      1 |
| SGM2       | 11xxxxxxx |
| SGM3       | 12xxxxxxx |
| SGM4       | 13xxxxxxx |
+-----+

[Expert@HostName-ch0x-0x:0]#
```

# Showing the Security Group Version (ver)

## Description

Use the "ver" command in Gaia gClish to show the Security Group software version.

## Syntax

```
ver
```

## Example

```
[Global] HostName-ch01-01 > ver
1_01:
Product version Check Point Gaia R81.20
OS build xxx
OS kernel version 3.10.0-693cpx86_64
OS edition 64-bit

1_02:
Product version Check Point Gaia R81.20
OS build xxx
OS kernel version 3.10.0-693cpx86_64
OS edition 64-bit

[Global] HostName-ch01-01 >
```

# Showing System Messages (show smo log)

## Description

Use the "show smo log" command in Gaia gClish to show the output of log files aggregated from all Security Group Members.

The output shows log files in a chronological sequence.

Each line shows the Security Group Member that created the log entry.

## Syntax

```
show smo log <Log File> [from <Date>] [to <Date>] [tail <N>]
[filter <String>]
```

## Parameters

Parameter	Description
tail <N>	Show only the last <i>n</i> lines of the log file for each Security Group Member. For example, tail 3 shows only the last three lines of the specified log file.
<Log File>	Enter the name of the common log file or the full path of the file.
from <Date>	Shows only the log from a given date and above.
to <Date>	Shows only the log until the given date.
filter <String>	Word or phrase to use as an output filter. For example, filter ospf shows only OSPF messages.

## Example

This example shows messages on Site 1 that contain the word "Restarted":

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > show smo log messages filter Restarted
Feb 5 12:40:07 1_03 HostName-ch01-03 pm[8465]: Restarted /bin/routed[8489], count=1
Feb 5 12:40:09 1_04 HostName-ch01-04 pm[8449]: Restarted /bin/routed[9995], count=1
Feb 5 12:40:09 1_04 HostName-ch01-04 pm[8449]: Restarted /opt/CPsuite-R81.20/fw1/bin/cmd[11291], count=1
Feb 5 12:40:09 1_04 HostName-ch01-04 pm[8449]: Restarted /usr/libexec/gexecd[11292], count=1
Feb 5 12:40:10 1_03 HostName-ch01-03 pm[8465]: Restarted /usr/libexec/gexecd[9701], count=1
Feb 5 12:40:10 1_03 HostName-ch01-03 pm[8465]: Restarted /bin/routed[11328], count=2
Feb 5 12:40:10 1_05 HostName-ch01-05 pm[8458]: Restarted /bin/routed[9734], count=1
Feb 5 12:40:10 1_05 HostName-ch01-05 pm[8458]: Restarted /usr/libexec/gexecd[11331], count=1
Feb 5 12:40:11 1_01 HostName-ch01-01 pm[8463]: Restarted /bin/routed[12253], count=3
Feb 5 12:40:11 1_04 HostName-ch01-04 pm[8449]: Restarted /bin/routed[11378], count=2
Feb 5 12:40:11 1_04 HostName-ch01-04 pm[8449]: Restarted /opt/CPsuite-R81.20/fw1/bin/cmd[11379], count=2
[Global] HostName-ch01-01 >
```

## Configuring a Dedicated Logging Port

The logging mechanism on each Security Group Member in Security Groups forwards the logs directly to a dedicated Log Server over the Quantum Maestro Orchestrator's management port assigned to this Security Group.

However, the Quantum Maestro Orchestrator's management ports can experience a high load when Security Group Members generate a large number of logs.

To reduce the load on the Quantum Maestro Orchestrator's management ports:

1. Assign a dedicated Quantum Maestro Orchestrator port of type `management` to a Security Group for logging
2. Configure the Security Group to send the logs to the dedicated Log Server

### Topology:

[Management Server] (some interface) <===> (management port 1 on Quantum Maestro Orchestrator) [Security Group]


[Management Server] (some interface) <===> (interface 1) [Log Server]  
(interface 2) <===> (management port 2 on Quantum Maestro Orchestrator) [Security Group]

### Procedure:

Step	Instructions
1	<p>Install a dedicated Log Server:</p> <ol style="list-style-type: none"> <li>a. Install a dedicated Log Server with two physical interfaces. See the applicable <i>Installation and Upgrade Guide</i> &gt; Chapter <i>Installing a Dedicated Log Server or SmartEvent Server</i>.</li> <li>b. Connect one physical interface on the dedicated Log Server to the Management Server.</li> <li>c. Connect another physical interface on the dedicated Log Server directly to an available management port on the Quantum Maestro Orchestrator. <b>Important</b> - Do not use the same port on the Quantum Maestro Orchestrator, which connects to the Management Server.</li> <li>d. In SmartConsole, create the required object that represents the dedicated Log Server. See the applicable <i>Installation and Upgrade Guide</i> &gt; Chapter <i>Installing a Dedicated Log Server or SmartEvent Server</i>.</li> </ol>
2	<p>On the Quantum Maestro Orchestrator, assign the dedicated port of type <code>management</code> to a Security Group and apply the changes.</p>



Step	Instructions
3	<p>In the Gaia OS of the Security Group, configure in Gaia gClish the dedicated management port.</p> <p>Syntax:</p> <pre data-bbox="325 353 1458 412">[Expert@HostName-ch0x-0x:0]# gclish [Global] HostName-ch01-01&gt; set interface ethX-MgmtY ipv4-address &lt;IPv4 Address&gt; mask-length &lt;Mask Length&gt;</pre> <p>Example:</p> <pre data-bbox="325 465 1458 501">[Global] HostName-ch01-01 &gt; set interface eth1-Mgmt2 ipv4-address 2.2.2.10 mask-length 24</pre> <p><b>Note</b> - You must assign an IPv4 address from the same subnet as assigned to the dedicated interface on the Log Server, which connects to the Quantum Maestro Orchestrator.</p>
4	<p>In SmartConsole, configure the Security Group object to send its logs to the dedicated Log Server.</p> <p>See the applicable <i>Logging and Monitoring Administration Guide</i> &gt; Chapter <i>Getting Started</i> &gt; Section <i>Deploying Logging Section</i> - Subsection <i>Configuring the Security Gateways for Logging</i>.</p>

 **Note** - The SMO makes sure that return traffic from the Log Server reaches the correct Security Group Member in the Security Group.

## Log Server Distribution (asg\_log\_servers)

### Description

In SmartConsole, you can configure multiple Log Servers for each Security Gateway object.

In this environment, the Security Gateway sends its logs to all of its configured Log Servers.

Each Security Group Member sends its logs to all Log Servers in the configuration.

To reduce the load on the Log Servers, enable the distribution of different Log Servers to different Security Groups.

When enabled, each Security Group Member sends its logs to one Log Server only.



**Note** - You cannot configure the Security Group Member to send its logs to a specific Log Server. Distribution is automatic.

The Security Group automatically decides which Log Server is assigned to which Security Group Member.

### Syntax

Run this command in Gaia gClish or the Expert mode.

```
asg_log_servers
```

**Example**

```
[Expert@HostName-ch0x-0x:0]# asg_log_servers

+-----+
|           Log Servers Distribution           |
+-----+
                        Log Servers Distribution Mode: Disabled

Available Log Servers:
* logServer
* Gaia
* LogServer2

Logs will be sent to all available servers.

Choose one of the following options:
-----
1) Configure Log Servers Distribution mode
2) Exit

>1
+-----+
|           Log Servers Distribution           |
+-----+
                        Log Servers Distribution Mode: Disabled

Choose the desired option:
-----
1) Enable Log Servers Distribution mode
2) Disable Log Servers Distribution mode
3) Back
```

If Log Servers Distribution is already enabled, the command shows which Log Servers are assigned to each Security Group Member:

```

+-----+
|           Log Servers Distribution           |
+-----+

                Log Servers Distribution Mode: Enabled

Available Log Servers:
* LogServer
* Gaia
* LogServer2

                Log Servers Distribution:

+-----+
| Blade id |           Chassis 1           |
+-----+
|    1    |           Gaia                |
|    2    |          LogServer2           |
|    3    |          LogServer            |
|    4    |           Gaia                |
|    5    |           -                   |
|    6    |          LogServer            |
|    7    |           -                   |
|    8    |           -                   |
|    9    |          LogServer            |
|   10    |           Gaia                |
|   11    |          LogServer2           |
|   12    |           -                   |
+-----+

("-" - Blade is not in Security Group)

Choose one of the following options:
-----
1) Configure Log Servers Distribution mode
2) Exit

```

## Viewing a Log File (asg log)

### Description

Use the "asg log" command in the Expert mode to see the contents of a specified log file.

### Syntax

```
asg log [-b <SGM IDs>] --file <Log File> [--from "<Timestamp>"] [-to "<Timestamp>"] [--tail <N>] [--filter <String>]
```

### Parameters

Parameter	Description
-b <SGM IDs>	<p>Applies to Security Group Members as specified by the &lt;SGM IDs&gt;.</p> <p>&lt;SGM IDs&gt; can be:</p> <ul style="list-style-type: none"> <li>■ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>■ One Security Group Member (for example, 1_1)</li> </ul>
<Log File>	<p>Specifies the log file by its type or full path:</p> <ul style="list-style-type: none"> <li>■ audit If you specify the log type, the output shows all audit logs in the /var/log/ directory. To specify a log file, enter its full path and name. For example: /var/log/asgaudit.log.1</li> <li>■ ports If you specify the log type, the output shows all ports logs in the /var/log/ directory. To specify a log file, enter its full path and name. For example: /var/log/ports</li> <li>■ dist_mode If you specify the log type, the output shows all logs for the Distribution Mode activity. To specify a log file, enter its full path and name. For example: /var/log/dist_mode See <a href="#">"Working with the Distribution Mode" on page 168</a>.</li> </ul>
--from "<Timestamp>"	<p>Shows only the log entries from the specified timestamp and above. You must use the timestamp as it appears in the log file.</p>

Parameter	Description
<code>--to</code> <code>"&lt;Timestamp&gt;"</code>	Shows only the log entries until the specified timestamp. You must use the timestamp as it appears in the log file.
<code>--tail &lt;N&gt;</code>	Show only the last <i>N</i> lines of the log file for each Security Group Member. For example, " <code>--tail 3</code> " shows only the last 3 lines of the specified log file. Default: 10 lines.
<code>--filter</code> <code>&lt;String&gt;</code>	Specifies a text string to use as a filter for the log entries. For example: <code>--filter debug</code>

## Examples

### Example 1 - Audit logs (specified by the log type)

```
[Expert@HostName-ch0x-0x:0]# asg log --file audit
Feb 02 17:36:12 1_01 WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:16:17 1_01 WARNING: Blade_admin down on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:17:40 1_01 WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:19:53 1_01 WARNING: Blade_admin down on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:22:33 1_01 WARNING: Blade_admin up on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:23:30 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 08:38:16 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 09:21:09 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 11:07:08 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
Feb 03 11:16:56 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 11:33:10 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 11:50:08 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 13:32:32 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 14:30:26 1_01 WARNING: Reset sic on blades: all, User: johndoe, Reason: test
Feb 03 14:48:03 1_01 WARNING: Reset sic on blades: all, User: johndoe, Reason: test
Feb 03 15:34:11 1_01 WARNING: Reset sic on blades: all, User: y, Reason: y
Feb 03 17:55:23 1_01 WARNING: Reboot on blades: 1_02,1_03,1_04,1_05,2_01,2_02,2_03,2_04,2_05, User: y, Reason: y
[Expert@HostName-ch0x-0x:0]#
```

### Example 2 - Port logs (specified by the log type), last 12 lines

```
[Expert@HostName-ch0x-0x:0]# asg log --file ports -tail 12
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-09 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-10 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-11 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-12 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-13 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-14 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-15 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-16 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-Mgmt1 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-Mgmt2 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-Mgmt3 link is down
Feb 3 18:01:40 2_05 HostName-ch02-05 cmd: Chassis 1 eth2-Mgmt4 link is down
[Expert@HostName-ch0x-0x:0]#
```

**Example 3 - Port logs (specified by the full path), filtered by timestamps**

```
[Expert@HostName-ch0x-0x:0]# asg log --file /var/log/ports --from "Feb 21 17:28:41 2019" --to "Feb 21 17:28:41 2019"
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-Mgmt1, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-57, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-59, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-61, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth1-63, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-57, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-59, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-61, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Setting link state: chassis: 1, interface: eth2-63, state: Up Full 10000M
Feb 21 17:28:41 2019 1_02 HostName-ch01-02 cphaprob: Link state command ended successfully
[Expert@HostName-ch0x-0x:0]#
```

**Example 4 - Distribution Mode logs (specified by the log type), filtered by the string "bridge"**

```
[Expert@HostName-ch0x-0x:0]# asg log -b 1_01,1_04 --file dist_mode -f bridge
Feb 2 18:10:30 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:10:30 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:12:31 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:12:31 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:14:14 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:14:14 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:14:30 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
Feb 2 18:14:30 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-vsbridges = 4
Feb 2 18:16:19 1_01 HostName-ch01-01 distutil:0: initialize_environment: vs-ids-bridges = 4
[Expert@HostName-ch0x-0x:0]#
```

# Monitoring Virtual Systems (cpha\_vsx\_util monitor)

## Description

Use the "cpha\_vsx\_util monitor" command in the Expert mode to stop or start monitoring of Virtual Systems.

The state of a Security Group Member is **not** affected by non-monitored Virtual Systems. For example, a non-monitored Virtual System in a problem state is ignored - the Security Group Member state does **not** change to DOWN.

## Use Case


A Virtual System that is not monitored is useful, if it is necessary for the Security Group Member to be in the state "UP", even if a specific Virtual System is DOWN or does not have a Security Policy (for example, after you unload the local policy).

## Syntax

```
cpha_vsx_util monitor show
```

```
cpha_vsx_util monitor {start | stop} <VS IDs>
```

## Parameters

Parameter	Description
show	Shows all non-monitored Virtual Systems.
stop	Stops the monitoring of the specified Virtual Systems.  <b>Important</b> - When you stop the monitoring of a Virtual System, you must run the "cpha_vsx_util monitor start <VS IDs>" command to start it again. Monitoring does not start automatically after a reboot.
start	Starts the monitoring of the specified Virtual Systems.



Parameter	Description
<VS IDs>	<p>Applies to Virtual Systems as specified by the &lt;VS IDs&gt;.</p> <p>&lt;VS IDs&gt; can be:</p> <ul style="list-style-type: none"> <li>▪ No &lt;VS IDs&gt; specified (default) - Applies to the context of the current Virtual System</li> <li>▪ One Virtual System</li> <li>▪ A comma-separated list of Virtual Systems (for example, 1, 2, 4, 5)</li> <li>▪ A range of Virtual Systems (for example, 3-5)</li> <li>▪ all - Shows all Virtual Systems</li> </ul> <p>This parameter is only applicable in a VSX environment.</p>

## Software Blades Update Verification (asg\_swb\_update\_verifier)

### Description

Use the "asg\_swb\_update\_verifier" command in Gaia gClish or Expert mode to make sure that the signatures are up-to-date for these Software Blades:

- Anti-Virus
- Anti-Bot
- Application Control
- URL Filtering

### Syntax

```
asg_swb_update_verifier [-v] [-b <SGM IDs> [-m <Product>] [-n [-p <IP Address>:<Port>]] ] [-u <Product>]
```

### Parameters

Parameter	Description
-v	Shows verbose output.
-b <SGM IDs>	<p>Applies to Security Group Members as specified by the &lt;SGM IDs&gt;.</p> <p>&lt;SGM IDs&gt; can be:</p> <ul style="list-style-type: none"> <li>▪ No &lt;SGM IDs&gt; specified, or all Applies to all Security Group Members and all Maestro Sites</li> <li>▪ One Security Group Member (for example, 1_1)</li> </ul>

Parameter	Description
<p>-m &lt;Product&gt;</p>	<p>Forces a manual update for the specified Software Blades on the Security Group Members specified with the "-b &lt;SGM IDs&gt;" parameter.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>■ all All applicable Software Blades</li> <li>■ Anti-Bot The Anti-Bot Software Blade</li> <li>■ Anti-Virus The Anti-Virus Software Blade</li> <li>■ APPI The Application Control Software Blade</li> <li>■ URLF The URL Filtering Software Blade</li> </ul>
<p>-n</p>	<p>Forces an update download from the Internet. Use with the "-m" parameter.</p>
<p>-p &lt;IP Address&gt; &gt;:&lt;Port&gt;</p>	<p>Forces an update download from the Internet and uses the specified HTTP proxy. Use with the "-m" parameter.</p> <ul style="list-style-type: none"> <li>■ &lt;IP Address&gt; - IP address of the HTTP proxy server</li> <li>■ &lt;Port&gt; - TCP port to use on the HTTP proxy server</li> </ul>
<p>-u &lt;Product&gt;</p>	<p>Forces a database update for the specified Software Blades.</p> <p>Valid values:</p> <ul style="list-style-type: none"> <li>■ all All applicable Software Blades</li> <li>■ Anti-Bot The Anti-Bot Software Blade</li> <li>■ Anti-Virus The Anti-Virus Software Blade</li> <li>■ APPI The Application Control Software Blade</li> <li>■ URLF The URL Filtering Software Blade</li> </ul>

## Example

```
[Expert@HostName-ch0x-0x:0]# gclish
[Global] HostName-ch01-01 > asg_swb_update_verifier
+-----+
| product      | sgm  | status          | DB version | next update check |
+-----+-----+-----+-----+-----+
| APPI         | 2_01 | failed          | 14061202  | Thu Jun 12 10:32:55 2014 |
| APPI         | 2_02 | failed          | 14061202  | Thu Jun 12 10:32:41 2014 |
| Anti-Bot     | 2_01 | up-to-date      | 1405220911 | Thu Jun 12 09:28:34 2014 |
| Anti-Bot     | 2_02 | up-to-date      | 1405220911 | Thu Jun 12 09:28:45 2014 |
| Anti-Virus   | 2_01 | up-to-date      | 1406121233 | Thu Jun 12 09:28:12 2014 |
| Anti-Virus   | 2_02 | new             | 1406121234 | Thu Jun 12 09:28:10 2014 |
| URLF        | 2_01 | not-installed   | N/A       | N/A                   |
| URLF        | 2_02 | not-installed   | N/A       | N/A                   |
+-----+-----+-----+-----+-----+

Report:
----- APPI -----
DB versions verification          [ OK ]
statuses verification             [ FAILED ]

----- URLF -----
DB versions verification          [ OK ]
statuses verification             [ OK ]

----- Anti-Bot -----
DB versions verification          [ OK ]
statuses verification             [ OK ]

----- Anti-Virus -----
DB versions verification          [ OK ]
statuses verification             [ OK ]
[Global] HostName-ch01-01 >
```

## Output description

Field	Description
<b>product</b>	Name of the Software Blade.
<b>sgm</b>	Security Group Member ID.
<b>status</b>	Update status.
<b>DB version</b>	Database version for a Software Blade.
<b>next update check</b>	Date and time for the next automatic update.
<b>DB versions verification</b>	<ul style="list-style-type: none"> <li>▪ <b>OK</b> - The database version is correct.</li> <li>▪ <b>FAILED</b> - The database version is incorrect.</li> </ul>
<b>statuses verification</b>	<ul style="list-style-type: none"> <li>▪ <b>OK</b> - The update installed correctly or no update is needed.</li> <li>▪ <b>FAILED</b> - The update did not install correctly.</li> </ul>

# Working with SNMP

You can use SNMP to monitor different aspects of Quantum Maestro Orchestrators and Security Groups.

## Monitoring Quantum Maestro Orchestrators over SNMP

### *In This Section:*

Enabling SNMP Monitoring on Quantum Maestro Orchestrators .....	316
Supported SNMP OIDs for Quantum Maestro Orchestrators .....	317
Supported SNMP Trap OIDs for Quantum Maestro Orchestrators .....	318

You can use SNMP to monitor different aspects of the Quantum Maestro Orchestrator:

- Software versions
- Key performance indicators

 **Note** - Hardware monitoring is not supported..

### Enabling SNMP Monitoring on Quantum Maestro Orchestrators

Step	Instructions
1	Upload these Check Point MIB files from the Quantum Maestro Orchestrator to your third-party SNMP monitoring software: <ul style="list-style-type: none"> <li>▪ The SNMP MIB file: \$CPDIR/lib/snmp/chkpnt.mib</li> <li>▪ The SNMP Trap MIB file: \$CPDIR/lib/snmp/chkpnt-trap.mib</li> </ul>
2	Connect to the command line on the Quantum Maestro Orchestrator.
3	Log in to Gaia Clish.
4	Enable the Gaia SNMP Agent: <pre style="border: 1px solid black; padding: 5px;">set snmp agent on save config</pre>

## Supported SNMP OIDs for Quantum Maestro Orchestrators

Only these branches are supported:

Branch	OID	
svn	Numerical	.1.3.6.1.4.1.2620.1.6
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.svn
mngmt	Numerical	.1.3.6.1.4.1.2620.1.7
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.mngmt

## Supported SNMP Trap OIDs for Quantum Maestro Orchestrators

Only these branches are supported:

Branch	OID	
chkpntTrapInfo	Numerical	.1.3.6.1.4.1.2620.1.2000.0
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapInfo
chkpntTrapNet	Numerical	.1.3.6.1.4.1.2620.1.2000.1
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapNet
chkpntTrapDisk	Numerical	.1.3.6.1.4.1.2620.1.2000.2
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapDisk
chkpntTrapCPU	Numerical	.1.3.6.1.4.1.2620.1.2000.3
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapCPU
chkpntTrapMemory	Numerical	.1.3.6.1.4.1.2620.1.2000.4
	Full Text	.iso.org.dod.internet.private.enterprises.checkpoint.products.chkpntTrap.chkpntTrapMemory



### Notes:

- The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.
- The `"set snmp traps"` command is not supported.



## Monitoring Security Groups over SNMP

### *In This Section:*

Enabling SNMP Monitoring of Security Groups .....	320
Supported SNMP OIDs for Security Groups .....	321
Supported SNMP Trap OIDs for Security Groups .....	321
SNMP Monitoring of Security Groups in VSX Mode .....	321
Common SNMP OIDs for Security Groups .....	322

You can use SNMP to monitor different aspects of the Security Group, including:

- Software versions
- Hardware status
- Key performance indicators
- High Availability status

### Enabling SNMP Monitoring of Security Groups

Step	Instructions
1	Upload these Check Point MIB files from a Security Group Member in the applicable Security Group to your third-party SNMP monitoring software: <ul style="list-style-type: none"> <li>▪ The SNMP MIB file: \$CPDIR/lib/snmp/chkpnt.mib</li> <li>▪ The SNMP Trap MIB file: \$CPDIR/lib/snmp/chkpnt-trap.mib</li> </ul>
2	Connect to the command line on the Security Group.
3	Log in to Gaia Clish.
4	Go to Gaia gClish: enter <code>gclish</code> and press Enter.
5	Enable the Gaia SNMP Agent: <pre style="border: 1px solid black; padding: 5px; margin-top: 10px;">set snmp agent on save config</pre>



## Supported SNMP OIDs for Security Groups

Only this branches is supported:

Branch	OID	
asg	Numerical	1.3.6.1.4.1.2620.1.48
	Full Text	.iso.org.dod.internet.private.enterprise.checkpoint.products.asg

## Supported SNMP Trap OIDs for Security Groups

Only this SNMP Trap is supported:

Branch	OID	
asgTrap	Numerical	1.3.6.1.4.1.2620.1.2001
	Full Text	.iso.org.dod.internet.private.enterprise.checkpoint.products.asgTrap

### Notes:

- The `/etc/snmp/GaiaTrapsMIB.mib` file is not supported.
- The `"set snmp traps"` command is not supported. You must use the `"asg alert"` configuration wizard for this purpose. See ["Configuring Alerts for Security Group Member and Security Group Events \(asg alert\)" on page 277](#).

## SNMP Monitoring of Security Groups in VSX Mode

For more information, see the:

- [R81.20 Gaia Administration Guide](#)
- [R81.20 VSX Administration Guide](#)
- [sk90860: How to configure SNMP on Gaia OS](#)

## Common SNMP OIDs for Security Groups

This table shows frequently used SNMP OIDs that are applicable to Security Groups:

Name	Type	Numerical OID	Comments
System Throughput	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.1 IPv6: .1.3.6.1.4.1.2620.1.48.21.1	
System Connection Rate (connections per second)	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.2 IPv6: .1.3.6.1.4.1.2620.1.48.21.2	
System Packet Rate (packet per second)	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.3 IPv6: .1.3.6.1.4.1.2620.1.48.21.3	
System Concurrent Connections	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.4 IPv6: .1.3.6.1.4.1.2620.1.48.21.4	
System Accelerated Connections Per Second	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.6 IPv6: .1.3.6.1.4.1.2620.1.48.21.6	
System non-accelerated Connections Per Second	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.7 IPv6: .1.3.6.1.4.1.2620.1.48.21.7	
System Accelerated Concurrent Connections	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.8 IPv6: .1.3.6.1.4.1.2620.1.48.21.8	
System Non-accelerated Concurrent Connections	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.9 IPv6: .1.3.6.1.4.1.2620.1.48.21.9	

Name	Type	Numerical OID	Comments
System CPU load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.10 IPv6: .1.3.6.1.4.1.2620.1.48.21.10	
System Acceleration CPU load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.11 IPv6: .1.3.6.1.4.1.2620.1.48.21.11	
System FW instances load - average	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.14 IPv6: .1.3.6.1.4.1.2620.1.48.21.14	
System VPN Throughput	String	IPv4: .1.3.6.1.4.1.2620.1.48.20.17 IPv6: .1.3.6.1.4.1.2620.1.48.21.17	
System Path distribution (fast, medium, slow, drops)	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.24 IPv6: .1.3.6.1.4.1.2620.1.48.21.24	Path distribution of: <ul style="list-style-type: none"> <li>■ throughput</li> <li>■ pps</li> <li>■ cps</li> <li>■ concurrent connections</li> </ul>
Per-Security Group Member counters	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.25 IPv6: .1.3.6.1.4.1.2620.1.48.21.25	Counters of: <ul style="list-style-type: none"> <li>■ throughput</li> <li>■ cps</li> <li>■ pps</li> <li>■ concurrent connections</li> <li>■ SecureXL CPU usage (avg / min / max)</li> <li>■ Firewall CPU usage (avg / min / max)</li> </ul>

Name	Type	Numerical OID	Comments
Performance peaks	Table	IPv4: .1.3.6.1.4.1.2620.1.48.20.26 IPv6: .1.3.6.1.4.1.2620.1.48.21.26	
Resources on every Security Group Member	Table	1.3.6.1.4.1.2620.1.48.23	Memory and Hard Disk utilization
CPU Utilization on every Security Group Member	Table	1.3.6.1.4.1.2620.1.48.29	

# System Optimization

This section describes some optimization steps you can take.

## Maestro Auto-Scaling

### Overview

The Maestro Auto-Scaling feature assigns available Security Appliances (Scale Units) to a Security Group when certain conditions are met.

You configure these conditions on the Quantum Maestro Orchestrator for each Security Group.


### Prerequisites

- A Maestro Security Group must contain Security Appliances of the same model.
- You must enable SMO Image Cloning in the Security Group.

Run in Gaia gClish on the Security Group:

```
set smo image auto-clone state on
```

```
show smo image auto-clone state
```

 **Important** - Various procedures for installing software packages require you to disable SMO Image Cloning. After you install the required software packages, you must enable SMO Image Cloning again.

- The Security Group must have internet connectivity for the Scale Unit to fetch the license from the User Center.

### Limitations

- In R81.20, it is not supported to configure Auto-Scaling Settings if a Maestro Security Group contains different appliance models.
- If the CPU utilization on the Security Group is high, the Orchestrator might consider the Security Group Members as "Expired".

## Terms

Term	Definition
KPI	Key Performance Indicator
Scale Unit	A Security Appliance that can automatically be assigned to a Security Group, if a minimum of one "Scale Up" policy rule is met, or automatically removed from a Security Group if all "Scale Down" policy rules are met.
Scale Up policy	A set of rules configured based on the Security Group's KPIs. If a minimum of one rule is matched (for a consecutive amount of seconds), a Scale Unit (of the same hardware) is assigned to that Security Group.
Scale Down Policy	A set of rules configured based on the Security Group's KPIs. If a minimum of one rule is matched (for a consecutive amount of seconds), a Scale Unit is marked as a release candidate.
Release Candidate	A Scale Unit that is currently assigned to a Security Group is ready to be moved to another Security Group if one of its "Scale Up" policy rules is met.

## Configuration

Configure Auto-Scaling on the Orchestrator in Gaia Portal or Gaia Clish.

### Configuration in Gaia Portal

1. Connect to the Gaia Portal on the Orchestrator.
2. From the left tree, click **Orchestrator**.
3. In the left pane **Unassigned Gateways / assigned Gateways** (if there is more than one appliance assigned to the Security Group), right-click a Security Appliance and click **Set Scale Unit**.
4. In the middle pane **Topology**, right-click the Security Group and click **Set Security Group configuration**.
5. Click the tab **Auto-Scaling settings**.
6. Configure the **Scale up policy** rules:

- a. Click **Add**.
- b. Select the applicable values in the fields:

Field	Available Values
<b>When</b>	<p><b>Each Member</b> Measures the value according to "Each Member" KPIs. "Asks" for new Security Appliances to be added to the Security Group when "Each Member" passes the threshold configured in the rule.</p> <p><b>Security Group (Average)</b> Measures the value according to "Security Group (Average)" KPIs. "Asks" for new Security Appliances to be added to the Security Group when the "Security Group (Average)" passes the threshold configured in the rule.</p>
<b>With</b>	<p><b>CPU Utilization (%)</b> <b>Throughput (Gbps)</b> <b>Packets (p/s)</b> <b>Connections</b> The KPI for the rule.</p>
<b>More than</b>	<p>Configure the threshold between:</p> <ul style="list-style-type: none"> <li>▪ 1 and 100 for the CPU utilization metric.</li> <li>▪ 1 and 1099511627776 (1TB) for other metrics.</li> </ul>
<b>For consecutive period of</b>	<p>Configure the duration between 1 and 86400 seconds (1 day).</p>

- c. Click **OK**.
- d. In the **Attach up to** field, configure the number of Security Appliances to attach to this Security Group.

## 7. Configure the **Scale down policy** rules:

- a. Click **Add**.
- b. Select the applicable values in the fields:

Field	Available Values
<b>When</b>	<p><b>Security Group (Average)</b>  Measures the value according to "Security Group (Average)" KPIs.  Marks the scale unit that is currently occupied by the Security Group (if there is such a one) as a release candidate when the "Security Group (Average)" is <b>less than</b> the threshold configured in the rule. This means the Security Group can release the current scale unit.</p>
<b>With</b>	<p><b>CPU Utilization (%)</b>  <b>Throughput (Gbps)</b>  <b>Packets (p/s)</b>  <b>Connections</b>  The KPI for the rule.</p>
<b>Less than</b>	<p>Configure the threshold between:</p> <ul style="list-style-type: none"> <li>▪ 1 and 100 for the CPU utilization metric.</li> <li>▪ 1 and 1099511627776 (1TB) for other metrics.</li> </ul>
<b>For consecutive period of</b>	<p>Configure the duration between 1 and 86400 seconds (1 day).</p>

- c. Click **OK**.
- d. In the **Detach single scale unit** field, configure the number of Security Appliances to detach from this Security Group.

8. Click **OK**.

### Configuration in Gaia Clish

1. Connect to the command line on the Orchestrator.
2. Log in to Gaia Clish.
3. Configure the **Scale up** policy rules:



```
add maestro auto-scale security-group-id <Security Group ID>
scale-up-policy when {Each-Member | Security-Group-Average}
with {CPU | bps | pps | connections} more-than <Threshold>
period <Duration>
```

4. Configure the number of Security Appliances to attach to this Security Group when conditions match a minimum of one of the configured scale up rules:

```
set maestro auto-scale security-group-id <Security Group ID>
scale-units-to-attach <1-4>
```


5. Configure the **Scale down policy** rules:

```
add maestro auto-scale security-group id <Security Group ID>
scale-down-policy when <Security-Group-Average> with {CPU |
bps | pps | connections} less-than <Threshold> period
<Duration>
```

6. Enable Auto-Scaling in this Security Group:

```
set maestro auto-scale security-group-id <Security Group ID>
state enable
```

7. Configure a scale Security Appliance on a specific site based on the Security Appliance serial number:

 **Important** - If this Security Appliance is the only one in the Security Group (and Site), then do **not** configure it as a scale Security Appliance.

```
set maestro auto-scale site-id <Site ID> scale-unit-serial
<Serial Number> state on
```

The applicable commands in Gaia Clish:

- add maestro auto-scale
- set maestro auto-scale
- show maestro auto-scale
- delete maestro auto-scale

## Monitoring on Orchestrator

### To view the state of the Auto-Scaling in a Security Group

1. Connect to the command line on the Orchestrator.
2. Log in to Gaia Clish.
3. Run:

```
show maestro auto-scale security-group-id <Security Group ID> state
```

### To view the Scale Units in a Security Group

1. Connect to the command line on the Orchestrator.
2. Log in to Gaia Clish.
3. Run:

```
show maestro auto-scale scale-units
```

### To view the Scale Up rules in a Security Group

1. Connect to the command line on the Orchestrator.
2. Log in to Gaia Clish.
3. Run:

```
show maestro auto-scale security-group-id <Security Group ID> scale-up-rules
```

### To view the Scale Down rules in a Security Group

1. Connect to the command line on the Orchestrator.
2. Log in to Gaia Clish.
3. Run:

```
show maestro auto-scale security-group-id <Security Group ID> scale-down-rules
```

## To view the current Security Groups and KPIs

1. Connect to the command line on the Orchestrator.
2. Log in.
3. Run this command:

- In Gaia Clish:

```
show maestro auto-scale interactive-status
```

- In the Expert mode:

```
mas_cli --interactive
```

### Example output:

```
-----
-----
Security Group: 1

  Site: 1
    Average:          | CPU Utilization: 9%          |
Pckt/s: 8            | Bytes/s: 5652              | Connections: 384
    Average (w/o 1 SU): | CPU Utilization: 13%        |
Pckt/s: 13          | Bytes/s: 8478              | Connections: 576

      Member: 1        | CPU Utilization: 7%          |
Pckt/s: 12           | Bytes/s: 8562              | Connections: 372
      Member: 2        | CPU Utilization: 9%          |
Pckt/s: 4            | Bytes/s: 2656              | Connections: 412
[Scale Unit]
      Member: 3        | CPU Utilization: 11%         |
Pckt/s: 10           | Bytes/s: 5739              | Connections: 369
[Scale Unit]

-----
-----
```

## To view the current Auto-Scaling rules

1. Connect to the command line on the Orchestrator.
2. Log in.
3. Run this command:

- In Gaia Clish:

```
show maestro auto-scale interactive-rules
```

- In the Expert mode:

```
mas_cli --interactive-rules
```

### Example output:

```
-----  
-----  
Security Group: 1  
  
Scale Up Rules:  
  ID 1: When Each member with CPU utilization exceeds 70% For  
60 seconds | No Match  
  
Scale Down Rules:  
  ID 1: When Security Group with CPU utilization less than 30%  
For 60 seconds | Match for 16 seconds  
-----  
-----
```

# Troubleshooting

## Auto-Scaling Service

To troubleshoot issues with Auto-Scaling, make sure that the `masd` service is running on the Orchestrator and Security Group Members:

1. On the Orchestrator:
  - a. Connect to the command line on the Orchestrator.
  - b. Log in to the Expert mode.
  - c. Get the status of the `masd` service:

```
service masd status
```

The output must be:

```
masd is running...
```

2. On the Security Group:
  - a. Connect to the command line on the Security Group.
  - b. Log in to the Expert mode.
  - c. Get the status of the `masd` service:

```
service masd status
```

The output must be:

```
masd is running...
```

## Auto-Scaling Log File

Examine the logs of the `masd` daemon on the Orchestrator and Security Group Members:

- On the Orchestrator:
  1. Connect to the command line on the Orchestrator.
  2. Log in to the Expert mode.
  3. Examine the `masd` log file in real time:

```
tail -F /var/log/masd.elg
```

- On the Security Group:

1. Connect to the command line on the Security Group.
2. Log in to the Expert mode.
3. Examine the `masd` log file in real time:

```
tail -F /var/log/masd.elg
```

### Auto-Scaling Rules

To make sure that the Orchestrator correctly applied the Auto-Scaling rules you configured in Gaia Portal or Gaia Clish:

1. Connect to the command line on the Orchestrator.
2. Log in to the Expert mode.
3. Get the list of rules:

```
mas_cli --interactive-rules
```

4. Compare the rules you see in the command line with the rules you configured on the Orchestrator.

### Security Group Members and their KPIs

To see if Security Group Members are reporting their KPIs to the Orchestrator:

1. Connect to the command line on the Orchestrator.
2. Log in to the Expert mode.
3. Get the KPI status:

```
mas_cli --interactive
```

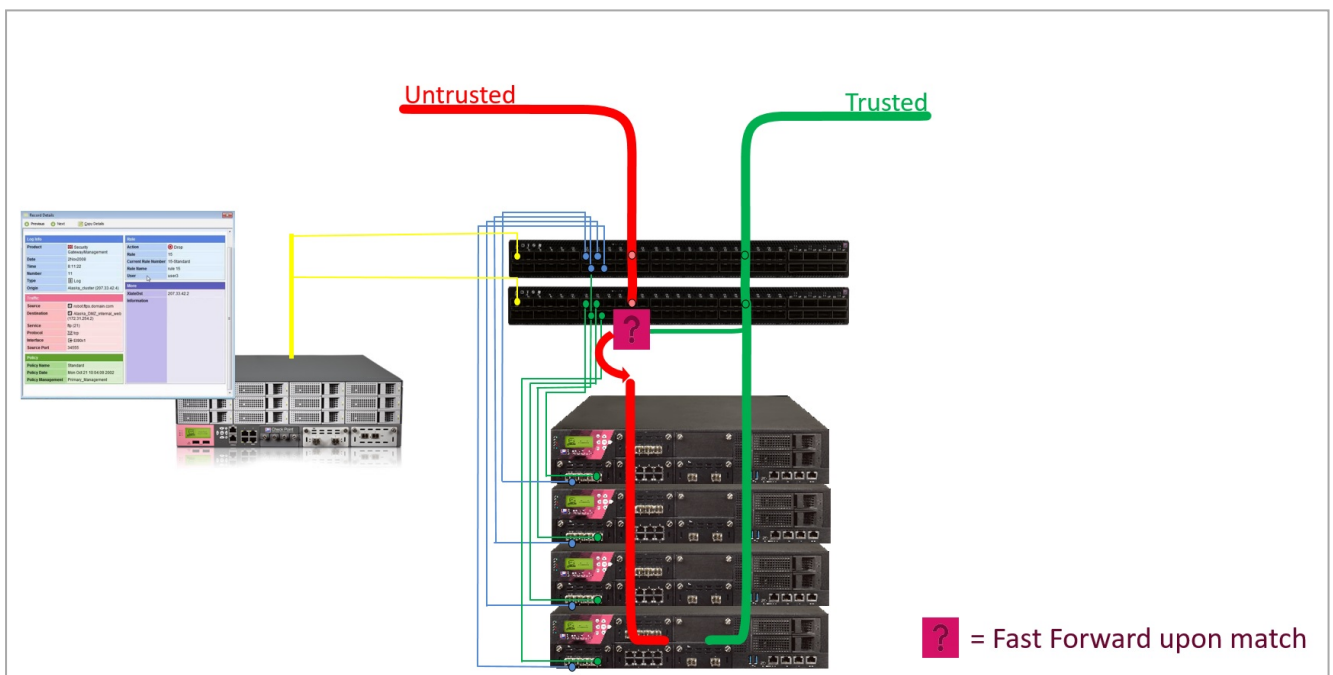
# Maestro Fastforward

## Introduction

The Maestro Fastforward feature offloads chosen policy rules for trusted connections to the Quantum Maestro Orchestrator for hardware acceleration of accept / drop rules.

### Benefits

- **Low latency:** Sub microsecond latency. The feature provides low latency for specific trusted sensitive flows (examples: voice, trading, internal trusted server-to-server communications and more).
- **Throughput:** Port line rate throughput (based on the connected interfaces bandwidth). Achieves as much as 200Gbps for one connection. You can enable the feature for high volume trusted connections such as server to server, backups and more.
- **Troubleshooting / Bypassing:** Forwards selected tuples as part of a troubleshooting process.



## How It Works

### Policy

The Administrator marks desired rules to be offloaded to the Orchestrator by giving the applicable rule names a specific prefix (the prefix is configurable). During policy installation, the applicable rules are translated into Access Control Lists (ACLs) and offloaded to the Orchestrator to be enforced on the hardware level.

### Routing

To accelerate a trusted connection on the Orchestrator at the Layer 3 level (routing), the Orchestrator has to know the networking information of the Security Gateway in order to send the packet through the correct outgoing interface to the correct next hop. The Orchestrator must have the same view of the topology as the Security Gateway. Therefore, the feature replicates the Security Gateway's / Virtual System's routing topology to accelerate traffic at the Orchestrator level. In addition, this logic occurs at the hardware level and is very robust.

#### Important:

- The offloaded rules are translated into stateless ACLs. Therefore, the offloaded rules are enforced without full stateful inspection capabilities.
- For TCP connections, for Accept Rules, the SYN packets are sent to the Security Group. Therefore, they enforce the opening of the connection (only source -> destination of the rule opens the TCP connection).
- The accelerated traffic is intended for trusted flows because it is a tradeoff between stateful-ness (in the Security Group) and stateless ACLs in the Orchestrator for performance gain.
- See "[Known Limitations](#)" on page 354.

## FAQ

### What are the supported deployment types?

- Single Site, or Dual Site.
- One Orchestrator, or two Orchestrators on a site.
- Gateway mode, or VSX mode (the configuration is for each Virtual System).

### Is there Firewall logging for the connections accelerated by Fastforward?

- For TCP connections:

For rules with the **Action "Accept"**, the Orchestrator sends the TCP SYN packets to the Security Group.

The Security Group generates a corresponding log.



- For UDP connections:

The Security Group does not generate logs.

### Do I need to add a rule for Client-to-Server, and Server-to-Client (return traffic)?

No. The rules should be created as in stateful inspection.

The ACL translation mechanism automatically adds Client-to-Server and Server-to-Client rules.

### Does the Firewall inspect traffic accelerated by Fastforward?

Only SYN / SYN-ACK packets (for Accept Rules).

The trade-off of the feature is to fully offload trusted connections to be handled on the Orchestrator hardware level, therefore allowing very low latency and very high throughput without having an effect on the Security Group Members.

## Topologies

Topology	Explanation
Single Site, One Orchestrator	With one Orchestrator on a Single Site, there are no restrictions on physical connectivity. Interfaces can be regular or bond interfaces.
Single Site, Two Orchestrators	With two Orchestrators on a Single Site, only "cross-Orchestrator" bond interfaces are allowed. Meaning, each bond interface has a subordinate interface on each Orchestrator. For more information, see <a href="#">"Special Considerations" on page 351</a> .
Dual Site	In Dual Site configuration, only "cross-Orchestrator" bond interfaces are allowed <b>on each site</b> . Meaning, each bond interface has a subordinate interface on each Orchestrator <b>on each site</b> . For more information, see <a href="#">"Special Considerations" on page 351</a> . In Dual Site configuration, only the active site enforces the ACLs. If there is a site failover, the new active site is activated.
VSX	In VSX mode, the feature works on each Virtual System, on which you enabled it.

## Configuration

The Fastforward feature is **disabled** by default.

You configure the Fastforward feature for each Security Group.

In VSX mode, you configure the feature on each Virtual System.

### To enable the Fastforward feature

#### Part 1 of 2 - Configuration on the Security Group:

1. Connect to the command line on the Security Group.
2. Log in to Gaia gClish.
3. In VSX mode, move to the context of the applicable Virtual System:

```
set virtual-system <VSID>
```

4. Configure a prefix for the Access Control rules:

```
set maestro fastforward rulebase-prefix enable prefix <Name  
Prefix>
```

For example, if your prefix is set to "ff\_rule", for the policy rule names use: "ff\_rule\_1", "ff\_rule\_2", and so on.

```
[Global] MyChassis-01> set maestro fastforward rulebase-  
prefix enable prefix ff_rule  
  
1_01:  
Fastforward prefix status: enabled. Prefix is "ff_rule"  
Please install policy from SmartConsole for the change to  
take effect.  
  
2_01:  
Fastforward prefix status: enabled. Prefix is "ff_rule"  
Please install policy from SmartConsole for the change to  
take effect.
```

5. Enable the Fastforward feature:

```
set maestro fastforward state on
```

Example output:

```

1_01:
Routing configuration validation finished successfully.
Fastforward status: enabled
Please install policy from SmartConsole for the change to
take effect.

2_01:
Routing configuration validation finished successfully.
Fastforward status: enabled
Please install policy from SmartConsole for the change to
take effect.


```


## Part 2 of 2 - Configuration in SmartConsole:

1. Connect with SmartConsole to the Management Server that manages this Security Group / Virtual System.
2. Configure the applicable Access Control rules with the prefix you configured earlier on the Security Group.

Example:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
ff_rule_1	Backup_Server_1	Backup_Server_2	Any	nfsd-tcp	Accept	Log	Policy Targets

 **Note** - You can configure these rules with API calls. See the [Check Point Management API Reference](#).

-  **Important:**
- You only have to configure the rules for the Client to Server (C2S) traffic.
  - For rules with the action "Accept", the Management Server automatically creates the corresponding rules for the Server to Client (S2C) traffic.
  - These rules support only the actions "Accept" and "Drop".

## Additional notes about the Access Control rules for Fastforward:

### Notes for rules with the action "Accept"

Rule Column	Notes
<b>Source</b>	<ul style="list-style-type: none"> <li>■ In the "Source" column, you can add one or more objects of these types only:               <ul style="list-style-type: none"> <li>• Host</li> <li>• Network</li> <li>• Group</li> <li>• Address Range</li> </ul> </li> <li>■ In the "Source" column, you cannot use the object "Any". You must add an explicit object.</li> <li>■ The Security Group must be able to connect to the IP address in the explicit object (you added in the "Source" column) through its Data interfaces (not the Management interface).</li> <li>■ In the "Source" column, you cannot use objects with IP addresses that belong to networks that are directly connected to the Security Group through its Data interfaces.</li> </ul>
<b>Destination</b>	<ul style="list-style-type: none"> <li>■ In the "Destination" column, you can add one or more objects of these types only:               <ul style="list-style-type: none"> <li>• Host</li> <li>• Network</li> <li>• Group</li> <li>• Address Range</li> </ul> </li> <li>■ In the "Destination" column, you cannot use the object "Any". You must add an explicit object.</li> <li>■ The Security Group must be able to connect to the IP address in the explicit object (you added in the "Destination" column) through its Data interfaces (not the Management interface).</li> <li>■ In the "Destination" column, you cannot use objects with IP addresses that belong to networks that are directly connected to the Security Group through its Data interfaces.</li> </ul>

Rule Column	Notes
<b>Services &amp; Applications</b>	<ul style="list-style-type: none"> <li>■ You can add one or more service objects of type "TCP" with these settings: <ul style="list-style-type: none"> <li>• single port</li> <li>• range of ports</li> <li>• source port</li> </ul> </li> <li>■ You can add one or more service objects of type "UDP" with these settings: <ul style="list-style-type: none"> <li>• single port</li> <li>• range of ports</li> <li>• source port</li> </ul> </li> <li>■ You can add one or more service objects of type "Other Service" with an IP-based Protocol.</li> </ul>

### Notes for rules with the action "Drop"

Note - Orchestrator drops the traffic at an early stage, at the hardware level.

Rule Column	Notes
<b>Source</b>	<ul style="list-style-type: none"> <li>■ In the "Source" column, you can add one or more objects of these types only: <ul style="list-style-type: none"> <li>• Host</li> <li>• Network</li> <li>• Group</li> <li>• Address Range</li> </ul> </li> <li>■ In the "Source" column, it is supported to use the object "Any". It is not necessary to add an explicit object.</li> <li>■ In the "Source" column, you cannot use objects with IP addresses that belong to networks that are directly connected to the Security Group through its Data interfaces.</li> </ul>

Rule Column	Notes
<b>Destination</b>	<ul style="list-style-type: none"> <li>■ In the "Destination" column, you can add one or more objects of these types only: <ul style="list-style-type: none"> <li>• Host</li> <li>• Network</li> <li>• Group</li> <li>• Address Range</li> </ul> </li> <li>■ In the "Destination" column, it is supported to use the object "Any". It is not necessary to add an explicit object.</li> <li>■ In the "Destination" column, you cannot use objects with IP addresses that belong to networks that are directly connected to the Security Group through its Data interfaces.</li> </ul>
<b>Services &amp; Applications</b>	<ul style="list-style-type: none"> <li>■ You can add one or more service objects of type "TCP" with these settings: <ul style="list-style-type: none"> <li>• single port</li> <li>• range of ports</li> <li>• source port</li> </ul> </li> <li>■ You can add one or more service objects of type "UDP" with these settings: <ul style="list-style-type: none"> <li>• single port</li> <li>• range of ports</li> <li>• source port</li> </ul> </li> <li>■ You can add one or more service objects of type "Other Service" with an IP-based Protocol.</li> </ul>

3. Install the Access Control Policy on the Security Gateway object / Virtual System object.

 **Notes:**

- During the policy installation process, the Security Group / Virtual System:
  - Translates these Access Control rules and sends them to the Orchestrator for enforcement.
  - Sends the current routing topology information to the Orchestrator.
- To remove a specific rule from Fastforward acceleration, remove the prefix from the **Name** column of that rule, and install the Access Control Policy.

## To disable the Fastforward feature

### Part 1 of 2 - Configuration on the Security Group:

1. Connect to the command line on the Security Group.
2. Log in to Gaia gClish.
3. In VSX mode, move to the context of the applicable Virtual System:

```
set virtual-system <VSID>
```

4. Disable the Fastforward feature:

```
set maestro fastforward state off
```

If this operation fails, it is possible to disable the feature forcefully. See ["Troubleshooting" on page 357](#).

Example output:

```
1_01:  
clearing ACLs from all relevant Orchestrators  
Fastforward status: disabled  
  
2_01:  
clearing ACLs from all relevant Orchestrators  
Fastforward status: disabled
```

### Part 2 of 2 - Configuration in SmartConsole:

1. Connect with SmartConsole to the Management Server that manages this Security Group / Virtual System.
2. Disable the applicable Access Control rules with the prefix you configured earlier on the Security Group.  
  
In the **No.** column, right-click the rule and click **Disable**.
3. Install the Access Control Policy on the Security Gateway object / Virtual System object.

## Monitoring

The Security Group logs TCP connections as usual. See the logs in SmartConsole or SmartView.

The "tor\_util fastforward" command on the Orchestrator shows additional information.

To see the hits for the Fastforward rules on the Orchestrator

1. Connect to the command line on the Orchestrator.
2. Log in to the Expert mode.
3. Get the hits for the Fastforward rules:

```
tor_util fastforward show rules <Security Group ID> {0 |
<Virtual System ID>}
```

### Notes:

- Rule IDs in the left-most column are based on the order of the Fastforward rules, and not on the real Access Control rule IDs. In Gateway mode, enter the digit 0 (zero) for the second argument.
- In VSX mode, enter the *Virtual System ID*.

Example output for the Security Group 1 (in the Gateway mode):

```
[Expert@MH01:0]# tor_util fastforward show rules 1 0
Fastforward Rule Hits:
=====
+-----+-----+-----+-----+-----+
|Counter ID |Hit Count          |Port          |Direction |Description
|          |                  |              |          |
+-----+-----+-----+-----+-----+
|66240512   |472065             |FF_SG1_VS0   |inbound   |Rule 1 C2S UDP, 1.1.1.0/24:ANY ->
2.2.2.0/24:3000, ACCEPT
|66256896   |23740853           |FF_SG1_VS0   |inbound   |Rule 1 S2C UDP, 2.2.2.0/24:3000 -
> 1.1.1.0/24:ANY, ACCEPT
|66273280   |102381             |FF_SG1_VS0   |inbound   |Rule 2 C2S UDP, 1.1.1.0/24:ANY ->
2.2.2.0/24:4000, DROP
|66289664   |589884             |FF_SG1_VS0   |inbound   |Rule 3 C2S TCP, 10.10.10.0/24:ANY
-> 20.20.20.0/24:22, ACCEPT
|66306048   |968405             |FF_SG1_VS0   |inbound   |Rule 3 S2C TCP, 20.20.20.0/24:22
-> 10.10.10.0/24:ANY, ACCEPT
|66322432   |0                  |FF_SG1_VS0   |inbound   |Rule 4 C2S UDP, 10.10.10.0/24:ANY
-> 20.20.20.0/24:445, ACCEPT
|66338816   |0                  |FF_SG1_VS0   |inbound   |Rule 4 S2C UDP, 20.20.20.0/24:445
-> 10.10.10.0/24:ANY, ACCEPT
|66371584   |0                  |FF_SG1_VS0   |inbound   |Rule 5 C2S ip proto ANY,
9.9.9.9/32:ANY -> 10.10.10.10/32:ANY, ACCEPT
|66027520   |0                  |FF_SG1_VS0   |inbound   |Rule 5 S2C ip proto ANY,
10.10.10.10/32:ANY -> 9.9.9.9/32:ANY, ACCEPT
+-----+-----+-----+-----+-----+
|          |                  |              |          |
+-----+-----+-----+-----+-----+
```



**To see the current configuration status on the Orchestrator:**

1. Connect to the command line on the Orchestrator.
2. Log in to the Expert mode.
3. Get the status:

```
tor_util fastforward show status <Security Group ID> {0 |  
<Virtual System ID>} [verbose]
```

** Notes:**

- In Gateway mode, enter the digit 0 (zero) for the second argument.
- In VSX mode, enter the *Virtual System ID* for the second argument.
- For more information, use the optional argument "verbose".

## Considerations for Administrators

Operation	Regular Flow	Additional Flow
Policy Installation	<p>The Management Server transfers the policy to the Security Group.</p>	<p>The Management Server translates into stateless ACLs the rules that contain the configured prefix in their <b>Name</b> column.</p> <p>The Security Group transfers these ACLs to all Orchestrators.</p> <p>If there are no changes in the policy, the Security Group skips this step.</p>
<p>Modifying topology (physical interfaces / routes / bond interfaces)</p>	<p>The administrator adds, modifies, or removes an interface or a route.</p> <ul style="list-style-type: none"> <li>▪ In Gateway mode, the administrator makes these changes in Gaia gClish / of the Security Group.</li> <li>▪ In VSX mode, the administrator makes these changes in Gaia PortalSmartConsole (except for bond interfaces).</li> </ul> <p>When done:</p> <ul style="list-style-type: none"> <li>▪ In Gateway mode, you must fetch the interface topology and install the policy.</li> <li>▪ In VSX mode, you must install the policy.</li> </ul> <p>This makes sure that enforcement is aware of the modifications (Firewall topology, Anti-Spoofing, and more).</p>	<p>During each policy installation, the Security Group transfers the networking topology to all Orchestrators (interfaces, neighbors, static routes).</p> <p>If there are no changes in the topology, the Security Group skips this step.</p>

# Routing Mechanism

## Explanation

During a policy installation, the Security Group updates the Orchestrators with the networking information:

- Interfaces (physical interfaces, VLAN, bond interfaces)
- Neighbors table (ARP table)
- Routing table

The Orchestrator builds the topology in its hardware.

If there are two Orchestrators, each Orchestrator builds its own topology based on its present interfaces.

For example, if bond1 with 2 subordinate interfaces eth1-01 and eth2-01 is in the topology, Orchestrator #1 has eth1-01 on its topology, while Orchestrator #2 has eth2-01 in its topology.

This is because each Orchestrator accelerates locally, with no forwarding between the Orchestrator.

When a packet is matched against the Access Control rules that are configured for acceleration, it is forwarded to the Routing mechanism in the Orchestrator to perform a routing decision. Based on the routing decision, it finds the outgoing interface through which to send the packet.

To see the routing topology, run this command on the Orchestrator in the Expert mode:

```
tor_util fastforward show status <Security Group ID> {0 |  
<Virtual System ID>} verbose
```

# Policy Mechanism

## Explanation

Policy rules for trusted flows that are to be enforced and accelerated on the Orchestrator level are defined by unique prefix to the rules' names.

During policy installation, the Management Server translates these rules into stateless ACLs, and transfers them to the Security Group. The Security Group transfers these ACLs to the Orchestrators for enforcement.

The accelerated connections must be trusted, as they bypass firewall security features to achieve high throughput and low latency for specific services.

UDP rules are fully accelerated on the Orchestrators.

TCP rules - for Accept Rules, the SYN and SYN-ACK packets are sent to the Security Group for the first match, and mainly for logging purposes. After that, the other packets are accelerated on the Orchestrator.

The acceleration is for each rule offloaded by the ACLs offloaded, and not for each connection / session as in SecureXL. The acceleration here is stateless.

To see the offloaded rules on the Orchestrator, run this command in the Expert mode (see ["Monitoring" on page 344](#)):

```
tor_util fastforward show status <Security Group ID> {0 |  
<Virtual System ID>}
```

Example output:

```

[Expert@MHO1:0]# tor_util fastforward show rules 1 0
Fastforward Rule Hits:
=====

+-----+-----+-----+-----+-----+
-----
---+
|Counter ID |Hit Count          |Port          |Direction
|Description
|
+-----+-----+-----+-----+-----+
-----
---+
|66240512   |472065             |FF_SG1_VS0   |inbound   |Rule
1 C2S UDP, 1.1.1.0/24:ANY -> 2.2.2.0/24:3000, ACCEPT
|
|66256896   |23740853           |FF_SG1_VS0   |inbound   |Rule
1 S2C UDP, 2.2.2.0/24:3000 -> 1.1.1.0/24:ANY, ACCEPT
|
|66273280   |102381             |FF_SG1_VS0   |inbound   |Rule
2 C2S UDP, 1.1.1.0/24:ANY -> 2.2.2.0/24:4000, DROP
|
|66289664   |589884             |FF_SG1_VS0   |inbound   |Rule
3 C2S TCP, 10.10.10.0/24:ANY -> 20.20.20.0/24:22, ACCEPT
|
|66306048   |968405             |FF_SG1_VS0   |inbound   |Rule
3 S2C TCP, 20.20.20.0/24:22 -> 10.10.10.0/24:ANY, ACCEPT
|
|66322432   |0                  |FF_SG1_VS0   |inbound   |Rule
4 C2S UDP, 10.10.10.0/24:ANY -> 20.20.20.0/24:445, ACCEPT
|
|66338816   |0                  |FF_SG1_VS0   |inbound   |Rule
4 S2C UDP, 20.20.20.0/24:445 -> 10.10.10.0/24:ANY, ACCEPT
|
|66371584   |0                  |FF_SG1_VS0   |inbound   |Rule
5 C2S ip proto ANY, 9.9.9.9/32:ANY -> 10.10.10.10/32:ANY, ACCEPT
|
|66027520   |0                  |FF_SG1_VS0   |inbound   |Rule
5 S2C ip proto ANY, 10.10.10.10/32:ANY -> 9.9.9.9/32:ANY, ACCEPT
|
+-----+-----+-----+-----+-----+
-----
---+

```

## Policy Installation Flow on SMO


1. The SMO receives the policy and converts the policy rules into stateless ACLs.
2. The SMO calculates a unique policy signature based on the content of the rules.

## Routing on SMO

1. "Check"- The SMO verifies if new routing topology changes were introduced
2. "Apply" - The SMO applies the routing changes on the Orchestrator.

## Policy

1. "Check"- The SMO checks if the Orchestrator has already installed the same policy signature.
2. "Upload and Prepare" - If the policy was not yet applied, the SMO uploads the ACLs to the Orchestrator for preparation.
3. "Apply" - The SMO applies the policy ACLs on the Orchestrator.
4. "Activate" - The SMO activates / deactivates the Fastforward operation state based on the site state (active site activates the feature, standby site deactivates the feature).

 **Note** - If there are two Orchestrators on the site, the procedure is applied to each Orchestrator.

## Packet Matching

1. A packet enters an uplink port on the Orchestrator (example, eth1-05, port 5).
2. If Fastforward is activated (on the active site), the packet is first matched against its ACL policy.
3. If the packet is accepted, it is forwarded to the Orchestrator routing topology to be routed outside through a routing decision.
4. If there is no match in the policy ACLs, the packet goes through the regular distribution process towards the Security Group members.

Some packets are sent to the Security Group regardless of a match:

- TCP SYN and TCP SYN-ACK packets (for rules with the action "Accept")
- Fragmented packets (for rules with a user-defined service)

## Special Considerations

### Multiple Orchestrators on the same site

#### Cross-bond requirement:

Each Orchestrator builds its own virtual routing topology.

There is no forwarding in between Orchestrators. Each side handles the "shortcut" path of Fastforward.

Therefore, you must configure interfaces as cross-Orchestrator bond interfaces, meaning that each bond has subordinate interfaces present on each Orchestrator.

Example	Bond Subordinate Interfaces
Good Example	Bond1 - eth1-05, eth2-05 Bond2 - eth1-06, eth2-06
Bad Example	Bond1 - eth1-05, eth1-06 Bond2 - eth2-05, eth2-06

#### Monitoring of bond subordinate interfaces:

If only one of the Orchestrators loses links on its subordinate interfaces, routing becomes inconsistent because one of the Orchestrators and the Security Group have full routing topology, while the other Orchestrator lost its subordinate interfaces and has no way to accelerate locally. Because one of the subordinate interfaces went down, it now routes the packets differently, probably through an alternate route / default gateway).

In such a scenario, the two Orchestrators enter the temporary bypass state and forward traffic to the Security Group.

When link state return to "up", the Orchestrators exit the temporary bypass state.

- ★ **Best Practice** - To avoid such a scenario, we recommend to configure two subordinate interfaces for each Orchestrator for a bond (total 4 subordinate interfaces - 2 for each Orchestrator).

#### Topology inconsistency:

Topology inconsistency may occur in deployments with multiple Orchestrators on the same site.

Because each Orchestrator accelerates the traffic locally, in a deployment with multiple Orchestrators, Fastforward requires the user to configure all interfaces as cross-Orchestrator bond interfaces.

As a result, each Orchestrator has a view of the entire topology and can complete the acceleration internally.

If the bond links fail on only one Orchestrator, it may cause traffic loss or wrong routing. In such a case, the Orchestrators on the current site enter into a special bypass mode - internal bypass.

When the topology is consistent again, the Orchestrators exit the internal bypass and go to the last desired state (active / inactive)

### Example:

A deployment with two Orchestrators and two bond interfaces.

Bond1 as external, and Bond2 as internal.

Each bond has a total of four subordinate interfaces, two for each Orchestrator:

- bond1: eth1-05, eth1-06, eth2-05, eth2-06
- bond2: eth1-07, eth1-07, eth2-08, eth2-08

If bond1 fully fails, the topology remains consistent.

If in bond1, only the subordinate interfaces eth2-05 and eth2-06 fail:

- Orchestrator2 has an inconsistent topology for bond1
- Orchestrator1 and the Security Group still have a consistent topology for bond1

In this scenario, the Orchestrators detect the topology inconsistency and enter into the `internal_bypass` mode. In this mode, all traffic flows to the Security Group until the inconsistency is resolved.

### Dual Site

Fastforward accelerates the traffic only on the active site .The standby site is in a deactivated state.

When a site failover occurs, the new SMO updates the Orchestrators with the new state and activates / deactivates them accordingly.

### Monitoring of Downlink Ports

Fastforward monitors link states on downlink ports connected to each Orchestrator.

When all downlink ports fail on an Orchestrator, by default, Fastforward enters the bypass mode on that Orchestrator. This makes sure no traffic is forwarded when there are no members in the Security Group.



## Support of Bond Interfaces

If there are multiple bond subordinate interfaces on an Orchestrator (for example, bond1 has eth1-01 and eth1-02), the Orchestrator chooses a primary subordinate interfaces to send traffic.

This is because bond interfaces are not configured on the Orchestrator, but only on the Security Group Members.

To overcome this:

- Ingress traffic - Incoming traffic on a bond subordinate interface is handled by Fastforward, as usual.
- Egress traffic - If traffic is routed out through a bond interface, the Orchestrator sends it through the **primary subordinate interface** of the bond interface. A primary subordinate interface is an interface with the lowest ID with the link in the "up" state.

# Known Limitations

## General

ID	Description
PMTR-76262	Fragments are forwarded to the Security Gateway for rules that contain a service.
PMTR-76274	<p>Complex connections (FTP, SIP, and more) do not open data connections dynamically.</p> <p>In general, there are two options for complex connections:</p> <ul style="list-style-type: none"><li>▪ Use the special service for the control connection (examples: FTP port 21, VoIP SIP 5060), and the Security Gateway automatically opens the data connections.</li><li>▪ Manually allow the control connection (examples: FTP port 21, VoIP SIP 5060) and manually allow the data connection range (example: a UDP port range).</li></ul>
-	You must <b>not</b> configure subnets for the VPN Encryption Domain as Fastforward rules. This makes sure the Security Gateway handles the encryption and decryption of traffic.

## Layer 3

ID	Description
PMTR-76277	Dynamic Routing is not supported.
PMTR-76258	IPv6 is not supported for Fastforward accelerated flows.
PMTR-76261	It is not supported to configure Fastforward rules for Multicast traffic.
PMTR-86316	Policy Based Routing (PBR) is not supported.
PMTR-86565	VPN encryption / decryption is not supported for Fastforward accelerated flows.
PMTR-76260	NAT is not supported for Fastforward accelerated flows.
PMTR-76271	Anti-Spoofing is not enforced for Fastforward accelerated flows.

## Security Group

ID	Description
PMTR-76273	The Security Group creates logs only for TCP connections (for Fastforward accelerated connections).
PMTR-86318	The rules Hit Count in SmartConsole does not reflect Fastforward acceleration.
PMTR-76267	Disabling / bypassing the feature can lead to traffic drops of Fastforward accelerated TCP connections.

## Topology

ID	Description
PMTR-76268	Fastforward acceleration towards the Management interface is not supported.
PMTR-76263	Fastforward acceleration is not supported for directly connected subnets.
PMTR-76270	In a configuration with two Orchestrators on each site, deployment interfaces must be configured as bond interfaces with subordinate interfaces on each Orchestrator.
PMTR-76272	When accelerating traffic through a bond interface, egress traffic goes out only through one subordinate interface (for each Orchestrator).

## Layer 2

ID	Description
PMTR-76275	Bridge Mode is not supported.
PMTR-76259	Source MAC address of the Fastforward accelerated traffic differs from source MAC address of the Security Group interfaces.
PMTR-76278	The "Same VMAC" feature is not supported.

# Troubleshooting

## How to track a traffic flow

On the Orchestrator check if the rules' hit counts show that counters are increasing.

For a TCP connection, capture the traffic (with the `tcpdump` command), or examine logs in SmartConsole.

## How to bypass and resume the feature on-the-fly

As part of troubleshooting, you can bypass the Fastforward feature.


Bypassing sends the traffic to the applicable Security Group and skips the matching to Fastforward offloaded rules.

This allows you to bypass, rather than disable, the feature.

Procedure:

1. Connect to the command line on the Security Group.
2. Log in to the Expert mode.
3. Connect to the command line on the applicable Orchestrator:


```
member {ssm1 | ssm2}
```

 **Note** - To bypass the feature, you must run the command on each Orchestrator.

4. Configure the applicable bypass state:

- To start the bypass:

```
tor_util fastforward policy operation_mode <Security
Group ID> {0 | <Virtual System ID>} bypass
```

 **Warning** - When you start the bypass, the Orchestrator might drop stateful TCP connections if already expired on the Security Group. See ["Known Limitations" on page 354](#).

- To resume the normal operation (to stop the bypass):

- a. Run this command:

```
tor_util fastforward policy operation_mode
<Security Group ID> {0 | <Virtual System ID>} skip_
bypass
```

- b. In SmartConsole, install the Access Control policy.

**Notes:**

- When you start the bypass, this configuration survives reboot of the Orchestrator and policy installations.
- In Gateway mode, enter the digit 0 (zero) for the second argument.
- In VSX mode, enter the *Virtual System ID* for the second argument.

Example output:

```
[Expert@MHO1:0]# tor_util fastforward policy operation_mode
1 0 bypass
operation mode was set successfully

[Expert@MHO1:0]# tor_util fastforward policy operation_mode
1 0 skip_bypass
operation mode was set successfully

It is required to install policy in order for the change to
take effect.
```

### How to troubleshoot policy failure

Examine these files on the SMO Security Group Member:

Type	File
Log	/var/log/acl_cli.log
Log	/var/log/policyparser.log

Examine these files on the Orchestrators:

Type	File	Contains	Comment
Log	/var/log/fastforward.log	Logging information	
Configuration	/etc/mlx_routing.json	Routing topology information	You must <b>not</b> edit this file
Configuration	/etc/mlx_conf.json	Fastforward policy information	You must <b>not</b> edit this file


## How to disable Fastforward forcefully

If the disable operation fails, it is possible to disable the feature forcefully.

### 1. On the Security Group:

- a. Connect to the command line on the Security Group.
- b. Log in to the Expert mode.
- c. Run:

```
g_all "/usr/scripts/acl_cli/acl_cli fastforward disable
--force"
```

 **Note** - This command removes the feature configuration on the Security Group (in VSX mode, from all Virtual Systems).

Example output:

```
1_01:
clearing ACLs from all relevant Orchestrators
Fastforward status: disabled
1_02:
clearing ACLs from all relevant Orchestrators
Fastforward status: disabled
1_03:
clearing ACLs from all relevant Orchestrators
Fastforward status: disabled
1_04:
clearing ACLs from all relevant Orchestrators
Fastforward status: disabled
```

### 2. On **each** Orchestrator in the environment:

- a. Connect to the command line on the Orchestrator.
- b. Log in to the Expert mode.
- c. Stop and start the `orchd` daemon:

```
orchd restart
```

 **Warnings:**

- No traffic flows through the Orchestrator until this daemon stops and starts.
- If there are several Orchestrators, then stop and start this daemon on the next Orchestrator only after this daemon starts on the current Orchestrator.

# Configuring Services to Synchronize After a Delay

Some TCP services (for example, HTTP) are characterized by connections with a very short duration. There is no point to synchronize these connections, because every synchronized connection consumes resources on the Security Group, and the connection is likely to have finished by the time an internal failover occurs.

For short-lived services, you can use the *Delayed Notifications* feature to delay telling the Security Group about a connection, so that the connection is only synchronized, if it still exists X seconds (by default, 3 seconds) after the connection was initiated. The Delayed Notifications feature requires SecureXL to be enabled on the Security Group (this is the default).

## Notes:

- By default, a connection is synchronized to backup Security Group Members only if it exists for more than 3 seconds.
- Asymmetric connections are synchronized to backup Security Group Members on the Active Site, if according to the DXL calculation, the Client-to-Server connection and the Server-to-Client connection are passing through different Security Group Members.



**To control the "Delayed Notifications" feature:**■ To **enable** this feature (this is the default):

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

- To enable temporarily in the current session, if you disabled it earlier (does not survive reboot):

```
g_fw ctl set int fw_cluster_use_delay_sync 1
```

- To enable permanently, if you disabled it earlier (survives reboot):

```
g_update_conf_file fwkern.conf fw_cluster_use_delay_sync=1
```

■ To **disable** this feature (this increases the CPU load):

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

- To disable temporarily in the current session (does not survive reboot):

```
g_fw ctl set int fw_cluster_use_delay_sync 0
```

- To disable permanently (survives reboot):

```
g_update_conf_file fw_cluster_use_delay_sync=0
```

**To configure an applicable delay:**

1. In SmartConsole, click **Objects > Object Explorer**.
2. In the left tree, click the small arrow on the left of the **Services** to expand this category.
3. In the left tree, select **TCP**.
4. Search for the applicable TCP service.
5. Double-click the applicable TCP service.
6. In the TCP service properties window, click **Advanced** page.
7. At the top, select **Override default settings**.

On Domain Management Server, select **Override global domain settings**.

8. At the bottom, in the **Cluster and synchronization** section:
  - a. Select **Synchronize connections on cluster if State Synchronization is enabled on the cluster**.
  - b. Select **Start synchronizing**.
  - c. Enter the applicable value.



**Important** - This change applies to all policies that use this service.

9. Click **OK**.
10. Close the **Object Explorer**.
11. Publish the SmartConsole session.
12. Install the Access Control Policy on the Scalable Platform Security Gateway object.



**Note** - The Delayed Notifications setting in the service object is ignored, if Connection Templates are not offloaded by the Firewall to SecureXL. For additional information about the Connection Templates, see the [R81.20 Performance Tuning Administration Guide](#).

# Firewall Connections Table Size for VSX Gateway

You can configure the limit for the Firewall Connections table on Virtual Systems:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Virtual System.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Open the Virtual System object.
4	From the left tree, click <b>Optimizations</b> .
5	In the <b>Calculate the maximum limit for concurrent connections</b> section, select <b>Manually</b> .
6	Enter or select a value.
7	Click <b>OK</b> .
8	Install the Access Control Policy on the Virtual System object.

# Forwarding specific inbound-connections to the SMO (asg\_excp\_conf)

You can configure the Security Group to forward specific inbound connections to the SMO Security Group Member.

## Important:

- This command supports only IPv4 connections.
- This command does not support local connections.
- In VSX mode, you must run this command in the context of the applicable Virtual System.
- This command supports a maximum of 15 exceptions (in VSX mode, this limit is global for all Virtual Systems).
- These exceptions are saved in the `$FWDIR/tmp/tmp_exception_entries.txt` file (IPv4 addresses are converted to a special format).

## Syntax

```
asg_excp_conf
  clear
  del <ID>
  get
  set <type> <src_ip> <sport> <dst_ip> <dport>
```

## Parameters

Parameter	Description
clear	Clears the table with all exception entries.
del <ID>	Deletes a specific exception entry by its ID. Use the "get" parameter to see the IDs. ID numbers start from 0 (zero).
get	Shows the table with all exception entries.

Parameter	Description														
<pre>set &lt;type&gt; &lt;src_ip&gt; &lt;sport&gt; &lt;dst_ip&gt; &lt;dport&gt;</pre>	<p>Configures a new exception entry.</p> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>This command does <b>not</b> support wildcard characters (* or ?) or the word "any". You must always configure the exact values of the connection 4-tuple.</li> <li>The order of these arguments is predefined (for example, "&lt;src_ip&gt;" is always the second argument).</li> </ul> <p>Arguments:</p> <ul style="list-style-type: none"> <li>&lt;type&gt; Configures the match condition - which connection parameters the Security Group must consider. Although you configure all connection parameters, the Security Group uses only specific parameters determined by the &lt;type&gt; value.</li> </ul> <table border="1" data-bbox="667 949 1461 1877"> <thead> <tr> <th>Value</th> <th>Description</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Match the inbound connection by the source IPv4 address only</td> </tr> <tr> <td>2</td> <td>Match the inbound connection by the destination IPv4 address only</td> </tr> <tr> <td>3</td> <td>Match the inbound connection by the source port only</td> </tr> <tr> <td>4</td> <td>Match the inbound connection by the destination port only</td> </tr> <tr> <td>5</td> <td>Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>source IPv4 address</li> <li>destination IPv4 address</li> </ul> </td> </tr> <tr> <td>6</td> <td>Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>source IPv4 address</li> <li>source port</li> </ul> </td> </tr> </tbody> </table>	Value	Description	1	Match the inbound connection by the source IPv4 address only	2	Match the inbound connection by the destination IPv4 address only	3	Match the inbound connection by the source port only	4	Match the inbound connection by the destination port only	5	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>source IPv4 address</li> <li>destination IPv4 address</li> </ul>	6	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>source IPv4 address</li> <li>source port</li> </ul>
Value	Description														
1	Match the inbound connection by the source IPv4 address only														
2	Match the inbound connection by the destination IPv4 address only														
3	Match the inbound connection by the source port only														
4	Match the inbound connection by the destination port only														
5	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>source IPv4 address</li> <li>destination IPv4 address</li> </ul>														
6	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>source IPv4 address</li> <li>source port</li> </ul>														

Parameter	Description			
	<table border="1"> <thead> <tr> <th data-bbox="667 219 826 300">Value</th> <th data-bbox="826 219 1461 300">Description</th> </tr> </thead> </table>	Value	Description	
Value	Description			
	7	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• source IPv4 address</li> <li>• destination port</li> </ul>		
	8	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• source port</li> <li>• destination IPv4 address</li> </ul>		
	9	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• destination IPv4 address</li> <li>• destination port</li> </ul>		
	10	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• source port</li> <li>• destination port</li> </ul>		
	11	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• source IPv4 address</li> <li>• source port</li> <li>• destination IPv4 address</li> </ul>		
	12	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• source IPv4 address</li> <li>• destination IPv4 address</li> <li>• destination port</li> </ul>		
	13	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• source IPv4 address</li> <li>• source port</li> <li>• destination port</li> </ul>		

Parameter	Description						
	<table border="1" data-bbox="667 226 1461 824"> <thead> <tr> <th data-bbox="675 226 826 300">Value</th> <th data-bbox="826 226 1461 300">Description</th> </tr> </thead> <tbody> <tr> <td data-bbox="675 300 826 539">14</td> <td data-bbox="826 300 1461 539">           Match the inbound connection by by all these parameters:           <ul style="list-style-type: none"> <li>• source port</li> <li>• destination IPv4 address</li> <li>• destination port</li> </ul> </td> </tr> <tr> <td data-bbox="675 539 826 824">15</td> <td data-bbox="826 539 1461 824">           Match the inbound connection by all these parameters:           <ul style="list-style-type: none"> <li>• source IPv4 address</li> <li>• source port</li> <li>• destination IPv4 address</li> <li>• destination port</li> </ul> </td> </tr> </tbody> </table> <ul style="list-style-type: none"> <li>■ <code>&lt;src_ip&gt;</code> Configures the Source IPv4 address</li> <li>■ <code>&lt;sport&gt;</code> Configures the Source port</li> <li>■ <code>&lt;dst_ip&gt;</code> Configures the Destination IPv4 address</li> <li>■ <code>&lt;dport&gt;</code> Configures the Destination port</li> </ul>	Value	Description	14	Match the inbound connection by by all these parameters: <ul style="list-style-type: none"> <li>• source port</li> <li>• destination IPv4 address</li> <li>• destination port</li> </ul>	15	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• source IPv4 address</li> <li>• source port</li> <li>• destination IPv4 address</li> <li>• destination port</li> </ul>
Value	Description						
14	Match the inbound connection by by all these parameters: <ul style="list-style-type: none"> <li>• source port</li> <li>• destination IPv4 address</li> <li>• destination port</li> </ul>						
15	Match the inbound connection by all these parameters: <ul style="list-style-type: none"> <li>• source IPv4 address</li> <li>• source port</li> <li>• destination IPv4 address</li> <li>• destination port</li> </ul>						



## Examples

### asg\_excp\_conf set

```
[Expert@HostName-ch0x-0x:0] asg_excp_conf set 2 192.168.20.30
40000 172.16.40.50 80
1_01:
Exception entry added successfully.
1_02:
Exception entry added successfully.
1_03:
Exception entry added successfully.
1_04:
Exception entry added successfully.
2_01:
Exception entry added successfully.
2_02:
Exception entry added successfully.
2_03:
Exception entry added successfully.
2_04:
Exception entry added successfully.
[Expert@HostName-ch0x-0x:0]
```

**asg\_excp\_conf get**

```
[Expert@HostName-ch0x-0x:0] asg_excp_conf get
```

```
1_01:
```

```
-----  
Exceptions table: -----  
-----
```

```
0 : Exception Type 2 , Source IP: 192.168.20.30 , Source Port:  
40000 , Destination IP: 172.16.40.50 Destination Port 80  
1 : Exception Type 4 , Source IP: 192.168.20.30 , Source Port:  
50000 , Destination IP: 172.16.40.50 Destination Port 8080  
-----  
-----
```

```
1_02:
```

```
-----  
Exceptions table: -----  
-----
```

```
0 : Exception Type 2 , Source IP: 192.168.20.30 , Source Port:  
40000 , Destination IP: 172.16.40.50 Destination Port 80  
1 : Exception Type 4 , Source IP: 192.168.20.30 , Source Port:  
50000 , Destination IP: 172.16.40.50 Destination Port 8080  
-----  
-----
```

```
1_03:
```

```
-----  
Exceptions table: -----  
-----
```

```
0 : Exception Type 2 , Source IP: 192.168.20.30 , Source Port:  
40000 , Destination IP: 172.16.40.50 Destination Port 80  
1 : Exception Type 4 , Source IP: 192.168.20.30 , Source Port:  
50000 , Destination IP: 172.16.40.50 Destination Port 8080  
-----  
-----
```

```
1_04:
```

```
-----  
Exceptions table: -----  
-----
```

```
0 : Exception Type 2 , Source IP: 192.168.20.30 , Source Port:  
40000 , Destination IP: 172.16.40.50 Destination Port 80  
1 : Exception Type 4 , Source IP: 192.168.20.30 , Source Port:  
50000 , Destination IP: 172.16.40.50 Destination Port 8080  
-----  
-----
```

```
2_01:
```

```
-----  
Exceptions table: -----  
-----
```

```

-----
0 : Exception Type 2 , Source IP: 192.168.20.30 , Source Port:
40000 , Destination IP: 172.16.40.50 Destination Port 80
1 : Exception Type 4 , Source IP: 192.168.20.30 , Source Port:
50000 , Destination IP: 172.16.40.50 Destination Port 8080
-----
-----
2_02:
-----
Exceptions table: -----
-----
0 : Exception Type 2 , Source IP: 192.168.20.30 , Source Port:
40000 , Destination IP: 172.16.40.50 Destination Port 80
1 : Exception Type 4 , Source IP: 192.168.20.30 , Source Port:
50000 , Destination IP: 172.16.40.50 Destination Port 8080
-----
-----
2_03:
-----
Exceptions table: -----
-----
0 : Exception Type 2 , Source IP: 192.168.20.30 , Source Port:
40000 , Destination IP: 172.16.40.50 Destination Port 80
1 : Exception Type 4 , Source IP: 192.168.20.30 , Source Port:
50000 , Destination IP: 172.16.40.50 Destination Port 8080
-----
-----
2_04:
-----
Exceptions table: -----
-----
0 : Exception Type 2 , Source IP: 192.168.20.30 , Source Port:
40000 , Destination IP: 172.16.40.50 Destination Port 80
1 : Exception Type 4 , Source IP: 192.168.20.30 , Source Port:
50000 , Destination IP: 172.16.40.50 Destination Port 8080
-----
-----
[Expert@HostName-ch0x-0x:0]

```

**asg\_excpc\_conf del**

```
[Expert@HostName-ch0x-0x:0]# asg_excpc_conf del 0
1_01:
Exception ID 0 deleted
1_02:
Exception ID 0 deleted
1_03:
Exception ID 0 deleted
1_04:
Exception ID 0 deleted
2_01:
Exception ID 0 deleted
2_02:
Exception ID 0 deleted
2_03:
Exception ID 0 deleted
2_04:
Exception ID 0 deleted
[Expert@HostName-ch0x-0x:0]
```

**asg\_excpc\_conf clear**

```
[Expert@HostName-ch0x-0x:0] asg_excpc_conf clear
1_01:
Exception table cleared
1_02:
Exception table cleared
1_03:
Exception table cleared
1_04:
Exception table cleared
2_01:
Exception table cleared
2_02:
Exception table cleared
2_03:
Exception table cleared
2_04:
Exception table cleared
[Expert@HostName-ch0x-0x:0]
```

# Configuring Security Group High Availability

*In This Section:*

---

Setting Security Group Weights (High Availability Factors) .....	374
Setting the Quality Grade Differential .....	376

---

**i** **Note** - Do not confuse this section with "[Configuring Weights for Security Group Members](#)" on page 108 that is related to traffic distribution inside a Security Group.

## Setting Security Group Weights (High Availability Factors)

Each hardware component in a Security Group Member has a quality weight factor, which sets its relative importance to overall Security Group health.

For example, ports are more important than other components and are typically assigned a higher weight value.

The Security Group Member grade is the sum of all component weight values.

In a dual Dual Site environment, the Security Group with the higher grade becomes Active and handles traffic.

The grade for each component is calculated based on this formula:

$$(\text{Unit Weight}) \times (\text{Number of components in the state "UP"})$$

To see the weight of each component, run in Gaia gClish on a Security Group:

```
asg stat -v
```

### Description

Use the "`set chassis high-availability factors`" command to configure a hardware component's weight.

## Syntax in Gaia gClish of the Security Group

```
set chassis high-availability factors sgm <SGM Factor>
```

```
set chassis high-availability factors port {other <Other Port Factor> | standard <Standard Port Factor> | mgmt <Management Port Factor> | bond <Bond Port Factor>}
```

## Parameters

Parameter	Description
<SGM Factor>	Weight factor for a Security Group Member. Valid range: integer between 0 and 1000.
<Other Port Factor>	High grade port factor. Valid range: integer between 0 and 1000.
<Standard Port Factor>	Standard grade port factor. Valid range: integer between 0 and 1000.
<Management Port Factor>	Management port factor. Valid range: integer between 0 and 1000.
<Bond Port Factor>	Bond interface factor. Valid range: integer between 0 and 1000.

## Examples

```
[Global] HostName-ch01-01 > set chassis high-availability factors sgm 100
```

```
[Global] HostName-ch01-01 > set chassis high-availability factors port other 70
```

```
[Global] HostName-ch01-01 > set chassis high-availability factors port standard 50
```

# Setting the Quality Grade Differential

## Description

Use the "set chassis high-availability failover" command in Gaia gClish to set the minimum quality grade differential that causes a failover.

## Syntax in Gaia gClish of the Security Group

```
set chassis high-availability failover <Trigger>
```

## Parameters

Parameter	Description
<Trigger>	Minimum difference in Chassis quality grade to trigger a failover. Valid values: 1 - 1000.



# Configuring Identity Based Access Control and Threat Prevention

For design guidelines, see [sk175587](#).

# Deploying a Security Group in Monitor Mode

## *In This Section:*

---

Introduction to Monitor Mode .....	378
Example Topology for Monitor Mode .....	379
Supported Software Blades in Monitor Mode .....	380
Limitations in Monitor Mode .....	382

---

## Introduction to Monitor Mode

You can configure Monitor Mode on one of the Security Group's interfaces.

The Security Group listens to traffic from a Mirror Port (or Span Port) on a connected switch.

Use the Monitor Mode to analyze network traffic without changing the production environment.

The mirror port on a switch duplicates the network traffic and sends it to the Security Group with an interface configured in Monitor Mode to record the activity logs.

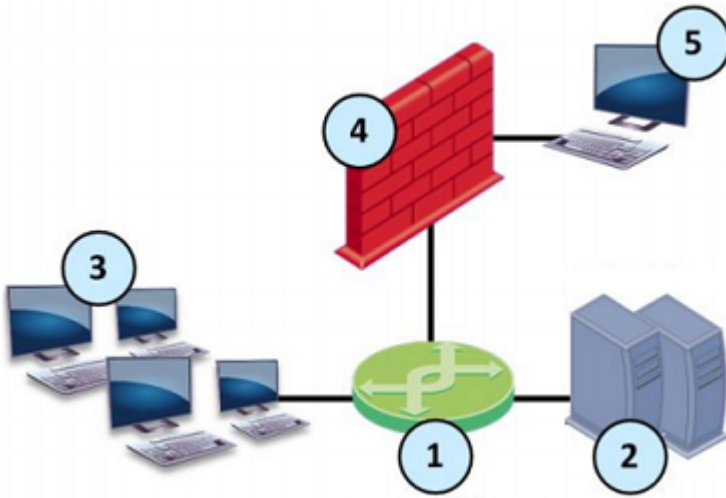
### You can use the Monitor Mode:

- To monitor the use of applications as a permanent part of your deployment
- To evaluate the capabilities of the Software Blades:
  - The Security Group neither enforces any security policy, nor performs any active operations (prevent / drop / reject) on the interface in the Monitor Mode.
  - The Security Group terminates and does not forward all packets that arrive at the interface in the Monitor Mode.
  - The Security Group does not send any traffic through the interface in the Monitor Mode.

### Benefits of the Monitor Mode include:

- There is no risk to your production environment.
- It requires minimal set-up configuration.
- It does not require TAP equipment, which is expensive.

## Example Topology for Monitor Mode



Item	Description
1	Switch with a mirror or SPAN port that duplicates all incoming and outgoing packets. The Security Group connects to a mirror or SPAN port on the switch.
2	Servers.
3	Clients.
4	Security Group with an interface in Monitor Mode.
5	Security Management Server that manages the Security Group.

# Supported Software Blades in Monitor Mode

This table lists Software Blades and their support for the Monitor Mode.

Software Blade	Support for the Monitor Mode
Firewall	Fully supports the Monitor Mode.
IPS	<p>These protections and features do <b>not</b> work:</p> <ul style="list-style-type: none"> <li>▪ The <b>SYN Attack</b> protection (SYNDefender).</li> <li>▪ The <b>Initial Sequence Number (ISN) Spoofing</b> protection.</li> <li>▪ The <b>Send error page</b> action in Web Intelligence protections.</li> <li>▪ Client and Server notifications about connection termination.</li> </ul>
Application Control	Does <b>not</b> support UserCheck.
URL Filtering	Does <b>not</b> support UserCheck.
Data Loss Prevention	<p>Does <b>not</b> support these:</p> <ul style="list-style-type: none"> <li>▪ UserCheck.</li> <li>▪ The "<b>Prevent</b>" and "<b>Ask User</b>" actions - these are automatically demoted to the "<b>Inform User</b>" action.</li> <li>▪ FTP inspection.</li> </ul>
Identity Awareness	<p>Does <b>not</b> support these:</p> <ul style="list-style-type: none"> <li>▪ Captive Portal.</li> <li>▪ Identity Agent.</li> </ul>
Threat Emulation	<p>Does <b>not</b> support these:</p> <ul style="list-style-type: none"> <li>▪ The Emulation Connection Prevent Handling Modes "<b>Background</b>" and "<b>Hold</b>". See <a href="#">sk106119</a>.</li> <li>▪ FTP inspection.</li> </ul>
Content Awareness	Does <b>not</b> support the FTP inspection.
Anti-Bot	Fully supports the Monitor Mode.
Anti-Virus	Does <b>not</b> support the FTP inspection.
IPsec VPN	Does <b>not</b> support the Monitor Mode.
Mobile Access	Does <b>not</b> support the Monitor Mode.

Software Blade	Support for the Monitor Mode
Anti-Spam & Email Security	Does <b>not</b> support the Monitor Mode.
QoS	Does <b>not</b> support the Monitor Mode.

# Limitations in Monitor Mode

These features and deployments are **not** supported in Monitor Mode:

- Passing production traffic through a Security Gateway, on which you configured Monitor Mode interface(s).
- If you configure more than one Monitor Mode interface on a Security Gateway, you must make sure the Security Gateway does not receive the same traffic on the different Monitor Mode interfaces.
- HTTPS Inspection
- NAT rules.
- HTTP / HTTPS proxy.
- Anti-Virus in Traditional Mode.
- User Authentication.
- Client Authentication.
- Check Point Active Streaming (CPAS).
- Cluster deployment.
- CloudGuard Gateways.
- CoreXL Dynamic Dispatcher ([sk105261](#)).
- Setting the value of the kernel parameters "psl\_tap\_enable" and "fw\_tap\_enable" to 1 (one) on-the-fly with the "fw ctl set int" command (Issue ID 02386641).

For more information, see [sk101670: Monitor Mode on Gaia OS and SecurePlatform OS](#).

# Configuring a Security Group in Gateway mode in Monitor Mode

## Important:

- For Cloud-based services (for example, Social Network widgets and URL Filtering), you must connect the Security Group in Monitor Mode to the Internet.
- You must install valid license and contracts file on the Security Group in Monitor Mode.

## Procedure:

### 1. Install the environment



For more information, see the [Quantum Maestro Getting Started Guide](#).

Step	Instructions
1	Install the Maestro environment.
2	Configure the applicable Security Group and assign the applicable interface(s).
3	If you did not configure the <b>First Time Wizard settings</b> when you created a Security Group, you must run the Gaia First Time Configuration Wizard for the Security Group.
4	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>▪ In the <b>Management Connection</b> window, select the interface, through which you connect to Gaia operating system.</li> <li>▪ In the <b>Internet Connection</b> window, do not configure IP addresses.</li> <li>▪ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>▪ In the <b>Products</b> window: <ul style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster, type</b>.</li> </ul> </li> <li>▪ In the <b>Dynamically Assigned IP</b> window, select <b>No</b>.</li> <li>▪ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

### 2. Configure the Monitor Mode on the applicable interface

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia gClish of the Security Group.

### Configuring the Monitor Mode in Gaia Portal

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <code>https://&lt;IP address of Gaia Management Interface&gt;</code> </div>
2	In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b> .
3	Select the applicable physical interface from the list and click <b>Edit</b> .
4	Select the <b>Enable</b> option to set the interface status to UP.
5	In the <b>Comment</b> field, enter the applicable comment text (up to 100 characters).
6	On the <b>IPv4</b> tab, select <b>Use the following IPv4 address</b> , but do not enter an IPv4 address.
7	On the <b>IPv6</b> tab, select <b>Use the following IPv6 address</b> , but do not enter an IPv6 address.  <b>Important</b> - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the <b>Ethernet</b> tab: <ul style="list-style-type: none"> <li>▪ Select <b>Auto Negotiation</b>, or select a link speed and duplex setting from the list.</li> <li>▪ In the <b>Hardware Address</b> field, enter the Hardware MAC address (if not automatically received from the NIC).                                <b>Caution</b> - Do not manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure.                         </li> <li>▪ In the <b>MTU</b> field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500).</li> <li>▪ Select <b>Monitor Mode</b>.</li> </ul>
9	Click <b>OK</b> .



## Configuring the Monitor Mode in Gaia gClish

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to Gaia Clish.
3	Go to Gaia gClish: enter <code>gclish</code> and press Enter.
4	Examine the configuration and state of the applicable physical interface: <pre>show interface &lt;Name of Physical Interface&gt;</pre>
5	If the applicable physical interface has an IP address assigned to it, remove that IP address. <ul style="list-style-type: none"> <li>■ To remove an IPv4 address:  <pre>delete interface &lt;Name of Physical Interface&gt; ipv4-address</pre> </li> <li>■ To remove an IPv6 address:  <pre>delete interface &lt;Name of Physical Interface&gt; ipv6-address</pre> </li> </ul>
6	Enable the Monitor Mode on the physical interface: <pre>set interface &lt;Name of Physical Interface&gt; monitor-mode on</pre>
7	Configure other applicable settings on the interface in the Monitor Mode: <pre>set interface &lt;Name of Physical Interface&gt; ...</pre>
8	Examine the configuration and state of the Monitor Mode interface: <pre>show interface &lt;Name of Physical Interface&gt;</pre>
9	Save the configuration: <pre>save config</pre>

## 3. Configure the Security Gateway object in SmartConsole

You can configure the applicable Security Gateway object in SmartConsole either in Wizard Mode, or in Classic Mode.

## Configuring the Security Gateway object in Wizard Mode


Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>▪ From the top toolbar, click the <b>New (*) &gt; Gateway</b>.</li> <li>▪ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; New Gateway</b>.</li> <li>▪ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Gateway</b></li> </ul>
4	In the <b>Check Point Security Gateway Creation</b> window, click <b>Wizard Mode</b> .
5	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>a. In the <b>Gateway name</b> field, enter the applicable name for this Security Gateway object.</li> <li>b. In the <b>Gateway platform</b> field, select <b>Maestro</b>.</li> <li>c. In the <b>Gateway IP address</b> section, select <b>Static IP address</b> and configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> <li>d. Click <b>Next</b>.</li> </ol>
6	<p>On the <b>Trusted Communication</b> page:</p> <ol style="list-style-type: none"> <li>a. Select the applicable option: <ul style="list-style-type: none"> <li>▪ If you selected <b>Initiate trusted communication now</b>, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard.</li> <li>▪ If you selected <b>Skip and initiate trusted communication later</b>, make sure to follow <b>Step 7</b>.</li> </ul> </li> <li>b. Click <b>Next</b>.</li> </ol>

Step	Instructions
7	<p>On the <b>End</b> page:</p> <ol style="list-style-type: none"> <li>Examine the <b>Configuration Summary</b>.</li> <li>Select <b>Edit Gateway properties for further configuration</b>.</li> <li>Click <b>Finish</b>.</li> </ol> <p><b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
8	<p>If during the Wizard Mode, you selected <b>Skip and initiate trusted communication later</b>:</p> <ol style="list-style-type: none"> <li>The <b>Secure Internal Communication</b> field shows <b>Uninitialized</b>.</li> <li>Click <b>Communication</b>.</li> <li>In the <b>Platform</b> field select <b>Maestro</b>.</li> <li>Enter the same <b>Activation Key</b> you entered during the Security Group's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>.</li> </ol> <p>Make sure the <b>Certificate state</b> field shows <b>Established</b>.</p> <ol style="list-style-type: none"> <li>Click <b>OK</b>.</li> </ol>
9	<p>On the <b>Network Security</b> tab, make sure to enable only the Firewall Software Blade.</p>
10	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Get Interfaces &gt; Get Interfaces with Topology</b>.</li> <li>Confirm the interfaces information.</li> </ol>
11	<p>Click <b>OK</b>.</p>
12	<p>Publish the SmartConsole session.</p>
13	<p>This Security Gateway object is now ready to receive the Security Policy.</p>

### Configuring the Security Gateway in Classic Mode

Step	Instructions
1	<p>Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.</p>
2	<p>From the left navigation panel, click <b>Gateways &amp; Servers</b>.</p>

Step	Instructions
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>▪ From the top toolbar, click the <b>New (*) &gt; Gateway</b>.</li> <li>▪ In the top left corner, click <b>Objects menu &gt; More object types &gt; Network Object &gt; Gateways and Servers &gt; New Gateway</b>.</li> <li>▪ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Gateway</b></li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b>.  <b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
5	<p>In the <b>Name</b> field, enter the applicable name for this Security Gateway object.</p>
6	<p>In the <b>IPv4 address</b> and <b>IPv6 address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Group's First Time Configuration Wizard.  Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</p>
7	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group:</p> <ol style="list-style-type: none"> <li>a. Near the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>b. In the <b>Platform</b> field select <b>Maestro</b>.</li> <li>c. Enter the same <b>Activation Key</b> you entered during the Security Group's First Time Configuration Wizard.</li> <li>d. Click <b>Initialize</b>.</li> <li>e. Click <b>OK</b>.</li> </ol>

Step	Instructions
	<p>If the <b>Certificate state</b> field does not show <i>Established</i>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).</li> <li>Run:           <div data-bbox="547 524 1460 589" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> </li> <li>Enter the number of this option:           <div data-bbox="547 636 1460 701" style="border: 1px solid #ccc; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
8	<p>In the <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>In the <b>Hardware</b> field, select <b>Maestro</b>.</li> <li>In the <b>Version</b> field, select <b>R81.20</b>.</li> <li>In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
9	<p>On the <b>Network Security</b> tab, make sure to enable only the Firewall Software Blade.</p> <p> <b>Important</b> - Do not select anything on the <b>Management</b> tab.</p>
10	<p>On the <b>Network Management</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Get Interfaces &gt; Get Interfaces with Topology</b>.</li> <li>Confirm the interfaces information.</li> </ol>
11	<p>Click <b>OK</b>.</p>
12	<p>Publish the SmartConsole session.</p>
13	<p>This Security Gateway object is now ready to receive the Security Policy.</p>

#### 4. Configure the Security Group to process packets that arrive in the wrong order

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	<p>Set the value of the kernel parameter <b>psl_tap_enable</b> to 1 in the <code>\$FWDIR/boot/modules/fwkernel.conf</code> file to enable the Passive Streaming Layer (PSL) Tap Mode::</p> <pre data-bbox="432 510 1458 568">g_update_conf_file fwkernel.conf psl_tap_enable=1</pre>
4	<p>Set the value of the kernel parameter <b>fw_tap_enable</b> to 1 in the <code>\$FWDIR/boot/modules/fwkernel.conf</code> file to enable the Firewall Tap Mode:</p> <pre data-bbox="432 734 1458 792">g_update_conf_file fwkernel.conf fw_tap_enable=1</pre>
5	<p>Set the value of the kernel parameter <b>fw_tap_enable</b> to 1 in the <code>\$PPKDIR/conf/simkernel.conf</code> file to enable the Firewall Tap Mode:</p> <pre data-bbox="432 920 1458 1016">g_update_conf_file \$PPKDIR/conf/simkernel.conf fw_tap_enable=1</pre>
6	Reboot the Security Group.
7	Connect to the command line on the Security Group.
8	Log in to the Expert mode.
9	<p>Make sure the Security Group loaded the new configuration:</p> <pre data-bbox="432 1323 1458 1382">g_fw ctl get int psl_tap_enable</pre> <pre data-bbox="432 1382 1458 1440">g_fw ctl get int fw_tap_enable</pre>

 **Notes:**

- This configuration helps the Security Group process packets that arrive in the wrong or abnormal order (for example, TCP [SYN-ACK] arrives before TCP [SYN]).
- This configuration helps the Security Group work better for the first 10-30 minutes when it processes connections, in which the TCP [SYN] packets did not arrive.
- This configuration is also required when you use a TAP device or Mirror / Span ports with separated TX/RX queues.
- This configuration will make the Mirror Port on Security Group work better for the first 10-30 minutes when processing connections, in which the TCP-SYN packet did not arrive.
- It is not possible to set the value of the kernel parameters "psl\_tap\_enable" and "fw\_tap\_enable" on-the-fly with the "g\_fw ctl set int <parameter>" command (Known Limitation 02386641).


## 5. Configure the required Global Properties for the Security Group in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Target Domain Management Server</i> that manages this Security Group.
2	In the top left corner, click <b>Menu &gt; Global properties</b> .
3	From the left tree, click the <b>Stateful Inspection</b> pane and configure: <ol style="list-style-type: none"> <li>a. In the <b>Default Session Timeouts</b> section:               <ol style="list-style-type: none"> <li>i. Change the value of the <b>TCP session timeout</b> from the default <b>3600</b> to <b>60</b> seconds.</li> <li>ii. Change the value of the <b>TCP end timeout</b> from the default <b>20</b> to <b>5</b> seconds.</li> </ol> </li> <li>b. In the <b>Out of state packets</b> section, you must clear all the boxes. Otherwise, the Security Group drops the traffic as out of state (because the traffic does not pass through the Security Group, it does not record the state information for the traffic).</li> </ol>
4	From the left tree, click the <b>Advanced</b> page > click the <b>Configure</b> button, and configure: <ol style="list-style-type: none"> <li>a. Click <b>FireWall-1 &gt; Stateful Inspection</b>.</li> <li>b. Clear <b>reject_x11_in_any</b>.</li> <li>c. Click <b>OK</b> to close the <b>Advanced Configuration</b> window.</li> </ol>
5	Click <b>OK</b> to close the <b>Global Properties</b> window.
6	Publish the SmartConsole session.

6. Configure the required Access Control Policy for the Security Group in SmartConsole

Step	Instructions																		
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.																		
2	From the left navigation panel, click <b>Security Policies</b> .																		
3	Create a new policy and configure the applicable layers: <ol style="list-style-type: none"> <li>At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>Click <b>Close</b>.</li> <li>On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>																		
4	Create the <b>Access Control</b> rule that accepts all traffic: <table border="1" data-bbox="379 887 1460 1352"> <thead> <tr> <th>No</th> <th>Name</th> <th>Source</th> <th>Destination</th> <th>VPN</th> <th>Services &amp; Applications</th> <th>Action</th> <th>Track</th> <th>Install On</th> </tr> </thead> <tbody> <tr> <td>1</td> <td>Accept All</td> <td>*Any</td> <td>*Any</td> <td>Any</td> <td>*Any</td> <td>Accept</td> <td>Log</td> <td>Object of Security Gateway in Monitor Mode</td> </tr> </tbody> </table>	No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On	1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Security Gateway in Monitor Mode
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On											
1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Security Gateway in Monitor Mode											



Step	Instructions
5	<p> <b>Best Practice</b></p> <p>We recommend these <b>Aggressive Aging</b> settings for the most common TCP connections:</p> <ol style="list-style-type: none"> <li>In the SmartConsole, click <b>Objects</b> menu &gt; <b>Object Explorer</b>.</li> <li>Open <b>Services</b> and select <b>TCP</b>.</li> <li>Search for the most common TCP connections in this network.</li> <li>Double-click the applicable TCP service.</li> <li>From the left tree, click <b>Advanced</b>.</li> <li>At the top, select <b>Override default settings</b>. On Domain Management Server, select <b>Override global domain settings</b>.</li> <li>Select <b>Match for 'Any'</b>.</li> <li>In the <b>Aggressive aging</b> section: Select <b>Enable aggressive aging</b>. Select <b>Specific</b> and enter <b>60</b>.</li> <li>Click <b>OK</b>.</li> <li>Close the <b>Object Explorer</b>.</li> </ol>
6	Publish the SmartConsole session.
7	Install the Access Control Policy on the Security Gateway object.

## 7. Connect the Security Group to the switch

Connect the interface in the Monitor Mode to the mirror or SPAN port on the switch.

For more information, see the:

- [Quantum Maestro Getting Started Guide](#).
- [R81.20 Gaia Administration Guide](#).
- [R81.20 Security Management Administration Guide](#).

# Configuring a Security Group in VSX mode in Monitor Mode

## Important:

- For Cloud-based services (for example, Social Network widgets and URL Filtering), you must connect the Security Group in Monitor Mode to the Internet (also, see [sk79700](#) and [sk106496](#)).
- You must install valid license and contracts file on the Security Group in Monitor Mode.

## Procedure:

### 1. Install the environment



For more information, see the [Quantum Maestro Getting Started Guide](#).

Step	Instructions
1	Install the Maestro environment.
2	Configure the applicable Security Group.
3	If you did not configure the <b>First Time Wizard settings</b> when you created a Security Group, you must run the Gaia First Time Configuration Wizard for the Security Group.
4	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>▪ In the <b>Management Connection</b> window, select the interface, through which you connect to Gaia operating system.</li> <li>▪ In the <b>Internet Connection</b> window, do not configure IP addresses.</li> <li>▪ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>▪ In the <b>Products</b> window: <ul style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster, type</b>.</li> </ul> </li> <li>▪ In the <b>Dynamically Assigned IP</b> window, select <b>No</b>.</li> <li>▪ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

### 2. Configure the Monitor Mode on the applicable interface

You can configure the Monitor Mode on an interface either in Gaia Portal, or Gaia gClish of the Security Group.

### Configuring the Monitor Mode in Gaia Portal

Step	Instructions
1	With a web browser, connect to Gaia Portal at: <div style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <code>https://&lt;IP address of Gaia Management Interface&gt;</code> </div>
2	In the left navigation tree, click <b>Network Management &gt; Network Interfaces</b> .
3	Select the applicable physical interface from the list and click <b>Edit</b> .
4	Select the <b>Enable</b> option to set the interface status to UP.
5	In the <b>Comment</b> field, enter the applicable comment text (up to 100 characters).
6	On the <b>IPv4</b> tab, select <b>Use the following IPv4 address</b> , but do not enter an IPv4 address.
7	On the <b>IPv6</b> tab, select <b>Use the following IPv6 address</b> , but do not enter an IPv6 address.  <b>Important</b> - This setting is available only after you enable the IPv6 Support in Gaia and reboot.
8	On the <b>Ethernet</b> tab: <ul style="list-style-type: none"> <li>▪ Select <b>Auto Negotiation</b>, or select a link speed and duplex setting from the list.</li> <li>▪ In the <b>Hardware Address</b> field, enter the Hardware MAC address (if not automatically received from the NIC).   <b>Caution</b> - Do not manually change the MAC address unless you are sure that it is incorrect or has changed. An incorrect MAC address can lead to a communication failure.</li> <li>▪ In the <b>MTU</b> field, enter the applicable Maximum Transmission Unit (MTU) value (minimal value is 68, maximal value is 16000, and default value is 1500).</li> <li>▪ Select <b>Monitor Mode</b>.</li> </ul>
9	Click <b>OK</b> .

## Configuring the Monitor Mode in Gaia gClish

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to Gaia Clish.
3	Go to Gaia gClish: enter <code>gclish</code> and press Enter.
4	Examine the configuration and state of the applicable physical interface: <pre>show interface &lt;Name of Physical Interface&gt;</pre>
5	If the applicable physical interface has an IP address assigned to it, remove that IP address. <ul style="list-style-type: none"> <li>■ To remove an IPv4 address:  <pre>delete interface &lt;Name of Physical Interface&gt; ipv4-address</pre> </li> <li>■ To remove an IPv6 address:  <pre>delete interface &lt;Name of Physical Interface&gt; ipv6-address</pre> </li> </ul>
6	Enable the Monitor Mode on the physical interface: <pre>set interface &lt;Name of Physical Interface&gt; monitor-mode on</pre>
7	Configure other applicable settings on the interface in the Monitor Mode: <pre>set interface &lt;Name of Physical Interface&gt; ...</pre>
8	Examine the configuration and state of the Monitor Mode interface: <pre>show interface &lt;Name of Physical Interface&gt;</pre>
9	Save the configuration: <pre>save config</pre>

## 3. Configure the Security Group to process packets that arrive in the wrong order

Step	Instructions
1	Connect to the command line on the Security Group.
2	Log in to the Expert mode.
3	<p>Set the value of the kernel parameter <b>psl_tap_enable</b> to 1 in the <code>\$FWDIR/boot/modules/fwkernel.conf</code> file to enable the Passive Streaming Layer (PSL) Tap Mode::</p> <pre data-bbox="432 506 1460 568">g_update_conf_file fwkernel.conf psl_tap_enable=1</pre>
4	<p>Set the value of the kernel parameter <b>fw_tap_enable</b> to 1 in the <code>\$FWDIR/boot/modules/fwkernel.conf</code> file to enable the Firewall Tap Mode:</p> <pre data-bbox="432 730 1460 792">g_update_conf_file fwkernel.conf fw_tap_enable=1</pre>
5	<p>Set the value of the kernel parameter <b>fw_tap_enable</b> to 1 in the <code>\$PPKDIR/conf/simkernel.conf</code> file to enable the Firewall Tap Mode:</p> <pre data-bbox="432 913 1460 1016">g_update_conf_file \$PPKDIR/conf/simkernel.conf fw_tap_enable=1</pre>
6	Reboot the Security Group.
7	Connect to the command line on the Security Group.
8	Log in to the Expert mode.
9	<p>Make sure the Security Group loaded the new configuration:</p> <pre data-bbox="432 1321 1460 1384">g_fw ctl get int psl_tap_enable</pre> <pre data-bbox="432 1384 1460 1447">g_fw ctl get int fw_tap_enable</pre>


 **Notes:**

- This configuration helps the Security Group process packets that arrive in the wrong or abnormal order (for example, TCP [SYN-ACK] arrives before TCP [SYN]).
- This configuration helps the Security Group work better for the first 10-30 minutes when it processes connections, in which the TCP [SYN] packets did not arrive.
- This configuration is also required when you use a TAP device or Mirror / Span ports with separated TX/RX queues.
- This configuration will make the Mirror Port on Security Group work better for the first 10-30 minutes when processing connections, in which the TCP-SYN packet did not arrive.
- It is not possible to set the value of the kernel parameters "psl\_tap\_enable" and "fw\_tap\_enable" on-the-fly with the "g\_fw ctl set int <parameter>" command (Known Limitation 02386641).

#### 4. Configure the VSX Gateway object in SmartConsole


Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Main Domain Management Server</i> that should manage this VSX Gateway.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
3	Create a new VSX Gateway object in one of these ways: <ul style="list-style-type: none"> <li>■ From the top toolbar, click the <b>New (*) &gt; VSX &gt; Gateway</b>.</li> <li>■ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; VSX &gt; New Gateway</b>.</li> <li>■ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; VSX &gt; Gateway</b></li> </ul> The <b>VSX Gateway Wizard</b> opens.
4	On the <b>VSX Gateway General Properties (Specify the object's basic settings)</b> page: <ol style="list-style-type: none"> <li>a. In the <b>Enter the VSX Gateway Name</b> field, enter the applicable name for this VSX Gateway object.</li> <li>b. In the <b>Enter the VSX Gateway IPv4</b> field, enter the same IPv4 address that you configured on the <b>Management Connection</b> page of the Security Group's First Time Configuration Wizard.</li> <li>c. In the <b>Enter the VSX Gateway IPv6</b> field, enter the same IPv6 address that you configured on the <b>Management Connection</b> page of the Security Group's First Time Configuration Wizard.</li> <li>d. In the <b>Select the VSX Gateway Version</b> field, select <b>R81.20</b>.</li> <li>e. Click <b>Next</b>.</li> </ol>

Step	Instructions
5	<p>On the <b>VSX Gateway General Properties (Secure Internal Communication)</b> page:</p> <ol style="list-style-type: none"> <li>In the <b>Activation Key</b> field, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard.</li> <li>In the <b>Confirm Activation Key</b> field, enter the same Activation Key again.</li> <li>Click <b>Initialize</b>.</li> <li>Click <b>Next</b>.</li> </ol> <p>If the <b>Trust State</b> field does not show <b>Trust established</b>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).</li> <li>Run:           <div data-bbox="512 887 1460 949" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>cpconfig</pre> </div> </li> <li>Enter the number of this option:           <div data-bbox="512 994 1460 1057" style="border: 1px solid black; padding: 2px; margin: 5px 0;"> <pre>Secure Internal Communication</pre> </div> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, on the <b>VSX Gateway General Properties</b> page, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
6	<p>On the <b>VSX Gateway Interfaces (Physical Interfaces Usage)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the list of the interfaces - it must show all the physical interfaces on the Security Group.</li> <li>If you plan to connect more than one Virtual System directly to the same physical interface, you must select <b>VLAN Trunk</b> for that physical interface.</li> <li>Click <b>Next</b>.</li> </ol>
7	<p>On the <b>Virtual Network Device Configuration (Specify the object's basic settings)</b> page:</p> <ol style="list-style-type: none"> <li>You can select <b>Create a Virtual Network Device</b> and configure the first applicable Virtual Device at this time (we recommend to do this later) - Virtual Switch or Virtual Router.</li> <li>Click <b>Next</b>.</li> </ol>

Step	Instructions
8	<p>On the <b>VSX Gateway Management (Specify the management access rules)</b> page:</p> <ol style="list-style-type: none"> <li>Examine the default access rules.</li> <li>Select the applicable default access rules.</li> <li>Configure the applicable source objects, if needed.</li> <li>Click <b>Next</b>.</li> </ol> <p> <b>Important</b> - These access rules apply only to the VSX Gateway (context of VS0), which is not intended to pass any "production" traffic.</p>
9	<p>On the <b>VSX Gateway Creation Finalization</b> page:</p> <ol style="list-style-type: none"> <li>Click <b>Finish</b> and wait for the operation to finish.</li> <li>Click <b>View Report</b> for more information.</li> <li>Click <b>Close</b>.</li> </ol>
10	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Log in to the Expert mode.</li> <li>Run:</li> </ol> <pre data-bbox="512 1010 1460 1072">vsx stat -v</pre>
11	<p>Install the default policy on the VSX Gateway object:</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the default policy for this VSX Gateway object. This policy is called:</li> </ol> <pre data-bbox="512 1319 1460 1382">&lt;Name of VSX Gateway object&gt;_VSX</pre> <ol style="list-style-type: none"> <li>Click <b>Install</b>.</li> </ol>
12	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Log in to the Expert mode.</li> <li>Run:</li> </ol> <pre data-bbox="512 1630 1460 1693">vsx stat -v</pre>

## 5. Configure the Virtual System object (and other Virtual Devices) in SmartConsole



Step	Instructions
1	Connect with SmartConsole to the Security Management Server, or each <i>Target Domain Management Server</i> that should manage each Virtual Device.
2	<p>Configure the applicable Virtual System (and other Virtual Devices) on this VSX Gateway.</p> <p>When you configure this Virtual System, for the Monitor Mode interface, add a regular interface. In the <b>IPv4 Configuration</b> section, enter a <i>random IPv4 address</i>.</p> <p> <b>Important</b> - This random IPv4 address must not conflict with existing IPv4 addresses on your network.</p>
3	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Log in to the Expert mode.</li> <li>Run: <div data-bbox="512 882 1458 947" style="border: 1px solid black; padding: 5px; margin-top: 5px;"> <pre>vsx stat -v</pre> </div> </li> </ol>
4	<p>Disable the Anti-Spoofing on the interface that is configured in the Monitor Mode:</p> <ol style="list-style-type: none"> <li>In SmartConsole, open the Virtual System object.</li> <li>Click the <b>Topology</b> page.</li> <li>Select the Monitor Mode interface and click <b>Edit</b>. The <b>Interface Properties</b> window opens.</li> <li>Click the <b>General</b> tab.</li> <li>In the <b>Security Zone</b> field, select <b>None</b>.</li> <li>Click the <b>Topology</b> tab.</li> <li>In the <b>Topology</b> section, make sure the settings are <b>Internal (leads to the local network)</b> and <b>Not Defined</b>.</li> <li>In the <b>Anti-Spoofing</b> section, clear <b>Perform Anti-Spoofing based on interface topology</b>.</li> <li>Click <b>OK</b> to close the <b>Interface Properties</b> window.</li> <li>Click <b>OK</b> to close the <b>Virtual System Properties</b> window.</li> <li>The Management Server pushes the VSX Configuration.</li> </ol>


6. Configure the required Global Properties for the Virtual System in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Target Domain Management Server</i> that manages this Virtual System.

Step	Instructions
2	In the top left corner, click <b>Menu &gt; Global properties</b> .
3	From the left tree, click the <b>Stateful Inspection</b> pane and configure: <ol style="list-style-type: none"> <li>a. In the <b>Default Session Timeouts</b> section:               <ol style="list-style-type: none"> <li>i. Change the value of the <b>TCP session timeout</b> from the default <b>3600</b> to <b>60</b> seconds.</li> <li>ii. Change the value of the <b>TCP end timeout</b> from the default <b>20</b> to <b>5</b> seconds.</li> </ol> </li> <li>b. In the <b>Out of state packets</b> section, you must clear all the boxes. Otherwise, the Security Group drops the traffic as out of state (because the traffic does not pass through the Security Group, it does not record the state information for the traffic).</li> </ol>
4	From the left tree, click the <b>Advanced</b> page > click the <b>Configure</b> button, and configure: <ol style="list-style-type: none"> <li>a. Click <b>FireWall-1 &gt; Stateful Inspection</b>.</li> <li>b. Clear <b>reject_x11_in_any</b>.</li> <li>c. Click <b>OK</b> to close the <b>Advanced Configuration</b> window.</li> </ol>
5	Click <b>OK</b> to close the <b>Global Properties</b> window.
6	Publish the SmartConsole session.

## 7. Configure the required Access Control Policy for the Virtual System in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or <i>Target Domain Management Server</i> that manages this Virtual System.
2	From the left navigation panel, click <b>Security Policies</b> .
3	Create a new policy and configure the applicable layers: <ol style="list-style-type: none"> <li>a. At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>b. On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>c. In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>d. Click <b>Close</b>.</li> <li>e. On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>

Step	Instructions																		
4	<p>Create the <b>Access Control</b> rule that accepts all traffic:</p> <table border="1" data-bbox="381 315 1460 781"> <thead> <tr> <th data-bbox="381 315 459 510">No</th> <th data-bbox="459 315 568 510">Name</th> <th data-bbox="568 315 692 510">Source</th> <th data-bbox="692 315 855 510">Destination</th> <th data-bbox="855 315 954 510">VPN</th> <th data-bbox="954 315 1128 510">Services &amp; Applications</th> <th data-bbox="1128 315 1241 510">Action</th> <th data-bbox="1241 315 1350 510">Track</th> <th data-bbox="1350 315 1460 510">Install On</th> </tr> </thead> <tbody> <tr> <td data-bbox="381 510 459 781">1</td> <td data-bbox="459 510 568 781">Accept All</td> <td data-bbox="568 510 692 781">*Any</td> <td data-bbox="692 510 855 781">*Any</td> <td data-bbox="855 510 954 781">Any</td> <td data-bbox="954 510 1128 781">*Any</td> <td data-bbox="1128 510 1241 781">Accept</td> <td data-bbox="1241 510 1350 781">Log</td> <td data-bbox="1350 510 1460 781">Object of Security Gateway in Monitor Mode</td> </tr> </tbody> </table>	No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On	1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Security Gateway in Monitor Mode
No	Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On											
1	Accept All	*Any	*Any	Any	*Any	Accept	Log	Object of Security Gateway in Monitor Mode											
5	<p> <b>Best Practice</b></p> <p>We recommend these <b>Aggressive Aging</b> settings for the most common TCP connections:</p> <ol style="list-style-type: none"> <li>In the SmartConsole, click <b>Objects</b> menu &gt; <b>Object Explorer</b>.</li> <li>Open <b>Services</b> and select <b>TCP</b>.</li> <li>Search for the most common TCP connections in this network.</li> <li>Double-click the applicable TCP service.</li> <li>From the left tree, click <b>Advanced</b>.</li> <li>At the top, select <b>Override default settings</b>. On Domain Management Server, select <b>Override global domain settings</b>.</li> <li>Select <b>Match for 'Any'</b>.</li> <li>In the <b>Aggressive aging</b> section: Select <b>Enable aggressive aging</b>. Select <b>Specific</b> and enter <b>60</b>.</li> <li>Click <b>OK</b>.</li> <li>Close the <b>Object Explorer</b>.</li> </ol>																		
6	Publish the SmartConsole session.																		
7	<p>Install the Access Control Policy on the Virtual System object.</p> <ol style="list-style-type: none"> <li>Click <b>Install Policy</b>.</li> <li>In the <b>Policy</b> field, select the applicable policy for this Virtual System object.</li> <li>Click <b>Install</b></li> </ol>																		

Step	Instructions
8	<p>Examine the VSX configuration:</p> <ol style="list-style-type: none"><li>Connect to the command line on the Security Group.</li><li>Log in to the Expert mode.</li><li>Run:</li></ol> <pre data-bbox="464 443 1460 510">vsx stat -v</pre>

## 8. Connect the Security Group to the switch

Connect the interface in the Monitor Mode to the mirror or SPAN port on the switch.

For more information, see the:

- [Quantum Maestro Getting Started Guide](#).
- [R81.20 Gaia Administration Guide](#)
- [R81.20 VSX Administration Guide](#)
- [R81.20 Security Management Administration Guide](#).

# Configuring Specific Software Blades for Monitor Mode


This section shows how to configure specific Software Blades for Monitor Mode.

 **Note** - For VSX, see:

- [sk79700: VSX supported features on R75.40VS and above](#)
- [sk106496: Software Blades updates on VSX R75.40VS and above - FAQ](#)

## Configuring the Threat Prevention Software Blades for Monitor Mode

Configure the settings below, if you enabled one of the Threat Prevention Software Blades (IPS, Anti-Bot, Anti-Virus, Threat Emulation or Threat Extraction) on the Security Group in Monitor Mode:

Step	Instructions								
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.								
2	From the left navigation panel, click <b>Security Policies &gt; Threat Prevention</b> .								
3	<p>Create the <b>Threat Prevention</b> rule that accepts all traffic:</p> <table border="1"> <thead> <tr> <th>Protected Scope</th> <th>Protection/Site/File/Blade</th> <th>Action</th> <th>Track</th> </tr> </thead> <tbody> <tr> <td>*Any</td> <td>-- N/A</td> <td>Applicable Threat Prevention Profile</td> <td>Log Packet Capture</td> </tr> </tbody> </table> <p> <b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ We recommend the <b>Optimized</b> profile.</li> <li>▪ The <b>Track</b> setting <b>Packet Capture</b> is optional.</li> </ul>	Protected Scope	Protection/Site/File/Blade	Action	Track	*Any	-- N/A	Applicable Threat Prevention Profile	Log Packet Capture
Protected Scope	Protection/Site/File/Blade	Action	Track						
*Any	-- N/A	Applicable Threat Prevention Profile	Log Packet Capture						
4	Right-click the selected Threat Prevention profile and click <b>Edit</b> .								
5	<p>From the left tree, click the <b>General Policy</b> page and configure:</p> <ol style="list-style-type: none"> <li>a. In the <b>Blades Activation</b> section, select the applicable Software Blades.</li> <li>b. In the <b>Activation Mode</b> section: <ul style="list-style-type: none"> <li>▪ In the <b>High Confidence</b> field, select <b>Detect</b>.</li> <li>▪ In the <b>Medium Confidence</b> field, select <b>Detect</b>.</li> <li>▪ In the <b>Low Confidence</b> field, select <b>Detect</b>.</li> </ul> </li> </ol>								

Step	Instructions
6	<p>From the left tree, click the <b>Anti-Virus</b> page and configure:</p> <ol style="list-style-type: none"><li data-bbox="347 286 1394 360">a. In the <b>Protected Scope</b> section, select <b>Inspect incoming and outgoing files</b>.</li><li data-bbox="347 371 1337 533">b. In the <b>File Types</b> section:<ul style="list-style-type: none"><li data-bbox="437 412 884 450">▪ Select <b>Process all file types</b>.</li><li data-bbox="437 454 1337 533">▪ <b>Optional:</b> Select <b>Enable deep inspection scanning (impacts performance)</b>.</li></ul></li><li data-bbox="347 539 1337 613">c. <b>Optional:</b> In the <b>Archives</b> section, select <b>Enable Archive scanning (impacts performance)</b>.</li></ol>
7	<p>From the left tree, click the <b>Threat Emulation</b> page &gt; click <b>General</b> and configure:</p> <ul style="list-style-type: none"><li data-bbox="357 712 1394 786">▪ In the <b>Protected Scope</b> section, select <b>Inspect incoming files from the following interfaces</b> and from the menu, select <b>All</b>.</li></ul>
8	<p>Configure other applicable settings for the Software Blades.</p>
9	<p>Click <b>OK</b>.</p>
10	<p>Install the Threat Prevention Policy on the Security Gateway object.</p>

**For more information:**

See the [R81.20 Threat Prevention Administration Guide](#).

## Configuring the Application Control and URL Filtering Software Blades for Monitor Mode

Configure the settings below, if you enabled Application Control or URL Filtering Software Blade on the Security Group in Monitor Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click <b>Manage &amp; Settings &gt; Blades</b> .
3	In the <b>Application Control &amp; URL Filtering</b> section, click <b>Advanced Settings</b> . The <b>Application Control &amp; URL Filtering Settings</b> window opens.
4	On the <b>General</b> page: <ul style="list-style-type: none"><li>▪ In the <b>Fail mode</b> section, select <b>Allow all requests (fail-open)</b>.</li><li>▪ In the <b>URL Filtering</b> section, select <b>Categorize HTTPS websites</b>.</li></ul>
5	On the <b>Check Point online web service</b> page: <ul style="list-style-type: none"><li>▪ In the <b>Website categorization mode</b> section, select <b>Background</b>.</li><li>▪ Select <b>Categorize social networking widgets</b>.</li></ul>
6	Click <b>OK</b> to close the <b>Application Control &amp; URL Filtering Settings</b> window.
7	Install the Access Control Policy on the Security Gateway object.


For more information:

See the [R81.20 Security Management Administration Guide](#).



## Configuring the Data Loss Prevention Software Blade for Monitor Mode

Configure the settings below, if you enabled the Data Loss Prevention Software Blade on the Security Group in Monitor Mode:

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click <b>Manage &amp; Settings &gt; Blades</b> .
3	In the <b>Data Loss Prevention</b> section, click <b>Configure in SmartDashboard</b> . The SmartDashboard window opens.
4	<p>In SmartDashboard:</p> <ol style="list-style-type: none"> <li>Click the <b>My Organization</b> page.</li> <li>In the <b>Email Addresses or Domains</b> section, configure with full list of company's domains. There is no need to include subdomains (for example, <code>mydomain.com</code>, <code>mydomain.uk</code>).</li> <li>In the <b>Networks</b> section, select <b>Anything behind the internal interfaces of my DLP gateways</b>.</li> <li>In the <b>Users</b> section, select <b>All users</b>.</li> </ol>
5	<p>Click the <b>Policy</b> page. Configure the applicable rules:</p> <ul style="list-style-type: none"> <li>▪ In the <b>Data</b> column, right-click the pre-defined data types and select <b>Edit</b>. <ul style="list-style-type: none"> <li>• On the <b>General Properties</b> page, in the <b>Flag</b> field, select <b>Improve Accuracy</b>.</li> <li>• In the <b>Customer Names</b> data type, we recommend to add the company's real customer names.</li> </ul> </li> <li>▪ In the <b>Action</b> column, you must select <b>Detect</b>.</li> <li>▪ In the <b>Severity</b> column, select <b>Critical</b> or <b>High</b> in all applicable rules.</li> <li>▪ You may choose to disable or delete rules that are not applicable to the company or reduce the Severity of these rules.</li> </ul> <p> <b>Note</b> - Before you can configure the DLP rules, you must configure the applicable objects in SmartConsole.</p>

Step	Instructions
6	<p>Click the <b>Additional Settings &gt; Protocols</b> page.</p> <p>Configure these settings:</p> <ul style="list-style-type: none"> <li>▪ In the <b>Email</b> section, select <b>SMTP (Outgoing Emails)</b>.</li> <li>▪ In the <b>Web</b> section, select <b>HTTP</b>. Do not configure the <b>HTTPS</b>.</li> <li>▪ In the <b>File Transfer</b> section, do not select <b>FTP</b>.</li> </ul>
7	Click <b>Launch Menu &gt; File &gt; Update</b> (or press the <b>CTRL S</b> keys).
8	Close the SmartDashboard.
9	Install the Access Control Policy on the Security Gateway object.
10	<p>Make sure the Security Group enabled the SMTP Mirror Port Mode:</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the Security Group.</li> <li>b. Log in to the Expert mode.</li> <li>c. Run this command: <div data-bbox="395 898 1460 965" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>dlp_smtp_mirror_port status</pre> </div> </li> <li>d. Make sure the value of the kernel parameter <code>dlp_force_smtp_kernel_inspection</code> is set to 1 (one). Run these two commands: <div data-bbox="395 1093 1460 1261" style="border: 1px solid #ccc; padding: 5px; margin: 5px 0;"> <pre>g_fw ctl get int dlp_force_smtp_kernel_inspection g_all grep dlp_force_smtp_kernel_inspection \$FWDIR/boot/modules/fwkernel.conf</pre> </div> </li> </ol>

**For more information:**

See the [R81.20 Data Loss Prevention Administration Guide](#).

# Configuring the Security Group in Monitor Mode Behind a Proxy Server

If you connect a Proxy Server between the Security Group in Monitor Mode and the switch, then configure these settings to see Source IP addresses and Source Users in the Security Gateway logs:

Step	Instructions
1	On the Proxy Server, configure the "X Forward-For header". See the applicable documentation for your Proxy Server.
2	On the Security Group in Monitor Mode, enable the stripping of the X-Forward-For (XFF) field. Follow the <a href="#">sk100223: How to enable stripping of X-Forward-For (XFF) field</a> .

# Deploying a Security Group in Bridge Mode

## *In This Section:*

---

Introduction to Bridge Mode .....	412
Example Topology for Bridge Mode .....	413
Supported Software Blades in Bridge Mode .....	414
Limitations in Bridge Mode .....	416

---

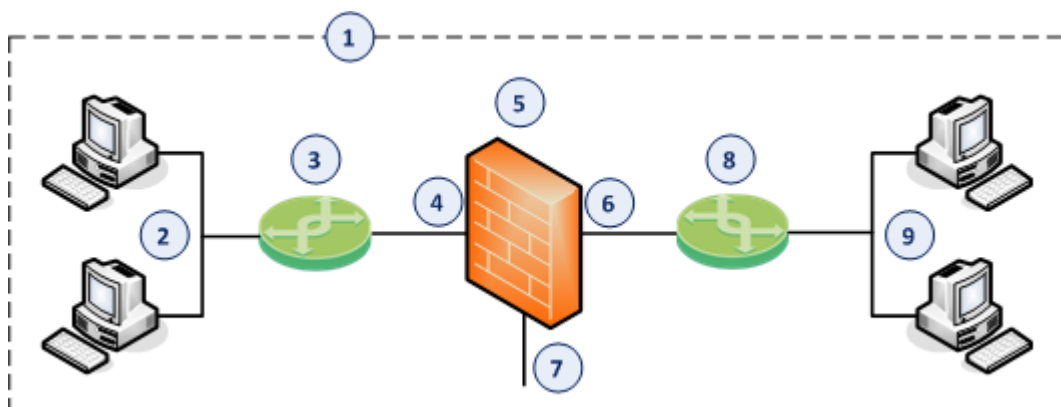
## Introduction to Bridge Mode

If it is not possible divide the existing network into several networks with different IP addresses, you can configure a Security Group in the Bridge Mode.

A Security Group in Bridge Mode is invisible to Layer 3 traffic.

When traffic arrives at one of the bridge slave interfaces, the Security Group inspects it and passes it to the second bridge slave interface.

## Example Topology for Bridge Mode



Item	Description
1	Network, which an administrator needs to divide into two Layer 2 segments. The Security Group in Bridge Mode connects between these segments.
2	First network segment.
3	Switch that connects the first network segment to one bridged slave interface (4) on the Security Group in Bridge Mode.
4	One bridged slave interface (for example, <code>eth1-05</code> ) on the Security Group in Bridge Mode.
5	Security Group in Bridge Mode.
6	Another bridged slave interface (for example, <code>eth1-07</code> ) on the Security Group in Bridge Mode.
7	Dedicated Gaia Management Interface (for example, <code>eth1-Mgmt1</code> ) on the Security Group.
8	Switch that connects the second network segment to the other bridged slave interface (6) on the Security Group in Bridge Mode.
9	Second network segment.

## Supported Software Blades in Bridge Mode

This table lists Software Blades, features, and their support for the Bridge Mode.

Software Blade or Feature	Support of a Security Gateway in Bridge Mode	Support of VSX Virtual Systems in Bridge Mode
Firewall	Yes	Yes
IPsec VPN	No	No
IPS	Yes	Yes
URL Filtering	Yes	Yes
DLP	Yes	No
Anti-Bot	Yes	Yes
Anti-Virus	Yes <sup>(1)</sup>	Yes <sup>(1)</sup>
Application Control	Yes	Yes
HTTPS Inspection	Yes <sup>(2)</sup>	No
Identity Awareness	Yes <sup>(3)</sup>	No
Threat Emulation - ThreatCloud emulation	Yes	Yes in Active/Active Bridge Mode No in Active/Standby Bridge Mode
Threat Emulation - Local emulation	Yes	No in all Bridge Modes

Software Blade or Feature	Support of a Security Gateway in Bridge Mode	Support of VSX Virtual Systems in Bridge Mode
Threat Emulation - Remote emulation	Yes	Yes in Active/Active Bridge Mode No in Active/Standby Bridge Mode
Mobile Access	No	No
UserCheck	Yes	No
Multi-Portal (Mobile Access Portal, Identity Awareness Captive Portal, Data Loss Prevention Portal, and so on)	Yes	No
QoS	Yes (see <a href="#">sk89581</a> )	No (see <a href="#">sk79700</a> )
HTTP / HTTPS proxy	Yes	No
Security Servers - SMTP, HTTP, FTP, POP3	Yes	No
Client Authentication	Yes	No
User Authentication	Yes	No

 **Notes:**

- Does not support the Anti-Virus in Traditional Mode.
- HTTPS Inspection in Layer 2 works as Man-in-the-Middle, based on MAC addresses:
  - Client sends a TCP [SYN] packet to the MAC address X.
  - Security Gateway creates a TCP [SYN-ACK] packet and sends it to the MAC address X.
  - Security Gateway in Bridge Mode does not need IP addresses, because CPAS takes the routing and the MAC address from the original packet.

**Note** - To be able to perform certificate validation (CRL/OCSP download), Security Gateway needs at least one interface to be assigned with an IP address. Probe bypass can have issues with Bridge Mode. Therefore, we do not recommend Probe bypass in Bridge Mode configuration.
- Identity Awareness in Bridge Mode supports only the AD Query authentication.

## Limitations in Bridge Mode

You can configure only **two** slave interfaces in one Bridge interface. You can think of this Bridge interface as a two-port Layer 2 switch. Each port can be a Physical interface, a VLAN interface, or a Bond interface.

These features and deployments are **not** supported in Bridge Mode:

- NAT rules (specifically, Firewall kernel in logs shows the traffic as accepted, but Security Gateway does not actually forward it). For more information, see [sk106146](#).
- Access to Multi-Portal (Mobile Access Portal, Identity Awareness Captive Portal, Data Loss Prevention Portal, and so on) from bridged networks, if the bridge does not have an assigned IP address.

For more information, see [sk101371: Bridge Mode on Gaia OS and SecurePlatform OS](#).



# Configuring a Security Group in Bridge Mode

## Procedure:

### 1. Install the environment

For more information, see the [Quantum Maestro Getting Started Guide](#).

Step	Instructions
1	Install the Maestro environment.
2	Configure the applicable Security Group and assign the applicable interfaces.
3	Run the Gaia First Time Configuration Wizard for the Security Group.
4	<p>During the First Time Configuration Wizard, you must configure these settings:</p> <ul style="list-style-type: none"> <li>▪ In the <b>Management Connection</b> window, select the interface, through which you connect to Gaia operating system.</li> <li>▪ In the <b>Internet Connection</b> window, do not configure IP addresses.</li> <li>▪ In the <b>Installation Type</b> window, select <b>Security Gateway and/or Security Management</b>.</li> <li>▪ In the <b>Products</b> window: <ul style="list-style-type: none"> <li>a. In the <b>Products</b> section, select <b>Security Gateway</b> only.</li> <li>b. In the <b>Clustering</b> section, clear <b>Unit is a part of a cluster, type</b>.</li> </ul> </li> <li>▪ In the <b>Dynamically Assigned IP</b> window, select <b>No</b>.</li> <li>▪ In the <b>Secure Internal Communication</b> window, enter the applicable <b>Activation Key</b> (between 4 and 127 characters long).</li> </ul>

### 2. Configure the Bridge interface on the Security Group

You configure the Bridge interface in either in Gaia Portal, or Gaia gClish of the Security Group.

#### Configuring the Bridge interface in Gaia Portal





**Note** - You must connect to the Gaia Portal of the applicable Security Group.

Step	Instructions
1	In the navigation tree, click <b>Network Management &gt; Network Interfaces</b> .
2	Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses.
3	Click <b>Add &gt; Bridge</b> . To configure an existing Bridge interface, select the Bridge interface and click <b>Edit</b> .
4	On the <b>Bridge</b> tab, enter or select a <b>Bridge Group ID</b> (unique integer between 1 and 1024).
5	Select the interfaces from the <b>Available Interfaces</b> list and then click <b>Add</b> . <b>i</b> <b>Notes:</b> <ul style="list-style-type: none"> <li>▪ Make sure that the slave interfaces do not have any IP addresses or aliases configured.</li> <li>▪ Do <b>not</b> select the interface that you configured as Gaia Management Interface.</li> <li>▪ A Bridge interface in Gaia can contain only two slave interfaces.</li> </ul>
6	On the <b>IPv4</b> tab, enter the IPv4 address and subnet mask. <b>i</b> <b>Important -</b>
7	<b>Optional:</b> On the <b>IPv6</b> tab, enter the IPv6 address and mask length. <b>i</b> <b>Important:</b> <ul style="list-style-type: none"> <li>▪ First, you must enable the IPv6 Support and reboot (see the <a href="#">R81.20 Gaia Administration Guide</a>).</li> </ul>
8	Click <b>OK</b> .

### Configuring the Bridge interface in Gaia gClish

Step	Instructions
1	Connect to the command line on the applicable Security Group.
2	Log in to Gaia Clish. Go to Gaia gClish: enter <code>gclish</code> and press Enter.

Step	Instructions
3	<p>Make sure that the slave interfaces, which you wish to add to the Bridge interface, do not have IP addresses assigned:</p> <pre data-bbox="467 320 1460 504">show interface &lt;Name of Slave Interface&gt; ipv4-address show interface &lt;Name of Slave Interface&gt; ipv6-address</pre>
4	<p>Add a new bridging group:</p> <pre data-bbox="467 584 1460 647">add bridging group &lt;Bridge Group ID 0 - 1024&gt;</pre> <p> <b>Note</b> - Do not change the state of bond interface manually using the "set interface &lt;Bridge Group ID&gt; state" command. This is done automatically by the bridging driver.</p>
5	<p>Add slave interfaces to the new bridging group:</p> <pre data-bbox="467 855 1460 1039">add bridging group &lt;Bridge Group ID&gt; interface &lt;Name of First Slave Interface&gt; add bridging group &lt;Bridge Group ID&gt; interface &lt;Name of Second Slave Interface&gt;</pre> <p> <b>Notes:</b></p> <ul data-bbox="571 1088 1442 1323" style="list-style-type: none"> <li>▪ Do not select the interface that you configured as Gaia Management Interface.</li> <li>▪ Only Ethernet, VLAN, and Bond interfaces can be added to a bridge group.</li> <li>▪ A Bridge interface in Gaia can contain only two slave interfaces.</li> </ul>

Step	Instructions
6	<p>Assign an IP address to the bridging group.</p> <p><b>Note</b> - You configure an IP address on a Bridging Group in the same way as you do on a physical interface (see the <a href="#">R81.20 Gaia Administration Guide</a>).</p> <ul style="list-style-type: none"> <li>To assign an IPv4 address, run: <pre>set interface &lt;Name of Bridging Group&gt; ipv4-address &lt;IPv4 Address&gt; {subnet-mask &lt;Mask&gt;   mask-length &lt;Mask Length&gt;}</pre> <p>You can optionally configure the bridging group to obtain an IPv4 Address automatically.</p> </li> <li>To assign an IPv6 address, run: <pre>set interface &lt;Name of Bridging Group&gt; ipv6-address &lt;IPv6 Address&gt; mask-length &lt;Mask Length&gt;</pre> <p>You can optionally configure the bridging group to obtain an IPv6 Address automatically.</p> </li> </ul> <p><b>Important</b> - First, you must enable the IPv6 Support and reboot (see the <a href="#">R81.20 Gaia Administration Guide</a>).</p>
7	<p>Save the configuration:</p> <pre>save config</pre>



### 3. Configure the Security Gateway object in SmartConsole

You can configure the Security Gateway object in either Wizard Mode, or Classic Mode.

#### Configuring the Security Gateway object in Wizard Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .



Step	Instructions
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>▪ From the top toolbar, click the <b>New (*) &gt; Gateway</b>.</li> <li>▪ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; New Gateway</b>.</li> <li>▪ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Gateway</b></li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Wizard Mode</b>.</p>
5	<p>On the <b>General Properties</b> page:</p> <ol style="list-style-type: none"> <li>a. In the <b>Gateway name</b> field, enter the applicable name for this Security Gateway object.</li> <li>b. In the <b>Gateway platform</b> field, select <b>Maestro</b>.</li> <li>c. In the <b>Gateway IP address</b> section, select <b>Static IP address</b> and configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Group's First Time Configuration Wizard. Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</li> <li>d. Click <b>Next</b>.</li> </ol>
6	<p>On the <b>Trusted Communication</b> page:</p> <ol style="list-style-type: none"> <li>a. Select the applicable option: <ul style="list-style-type: none"> <li>▪ If you selected <b>Initiate trusted communication now</b>, enter the same Activation Key you entered during the Security Group's First Time Configuration Wizard.</li> <li>▪ If you selected <b>Skip and initiate trusted communication later</b>, make sure to follow <b>Step 7</b>.</li> </ul> </li> <li>b. Click <b>Next</b>.</li> </ol>
7	<p>On the <b>End</b> page:</p> <ol style="list-style-type: none"> <li>a. Examine the <b>Configuration Summary</b>.</li> <li>b. Select <b>Edit Gateway properties for further configuration</b>.</li> <li>c. Click <b>Finish</b>.</li> </ol> <p><b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>

Step	Instructions
8	<p>If during the Wizard Mode, you selected <b>Skip and initiate trusted communication later</b>:</p> <ol style="list-style-type: none"> <li>The <b>Secure Internal Communication</b> field shows <b>Uninitialized</b>.</li> <li>Click <b>Communication</b>.</li> <li>In the <b>Platform</b> field select <b>Maestro</b>.</li> <li>Enter the same <b>Activation Key</b> you entered during the Security Group's First Time Configuration Wizard.</li> <li>Click <b>Initialize</b>. Make sure the <b>Certificate state</b> field shows <b>Established</b>.</li> <li>Click <b>OK</b>.</li> </ol>
9	<p>On the <b>General Properties</b> page, on the <b>Network Security</b> tab, enable the applicable Software Blades.</p> <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">Deploying a Security Group in Bridge Mode</a>" on page 412.</p>
10	<p>On the <b>Network Management</b> page, configure the <b>Topology</b> of the Bridge interface.</p> <p> <b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If a Bridge interface connects to the Internet, then set the <b>Topology</b> to <b>External</b>.</li> <li>▪ If you use this Bridge Security Gateway object in Access Control Policy rules with <b>Internet</b> objects, then set the <b>Topology</b> to <b>External</b>.</li> </ul>
11	Click <b>OK</b> .
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

### Configuring the Security Gateway object in Classic Mode

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that should manage this Security Group.
2	From the left navigation panel, click <b>Gateways &amp; Servers</b> .


Step	Instructions
3	<p>Create a new Security Gateway object in one of these ways:</p> <ul style="list-style-type: none"> <li>▪ From the top toolbar, click the <b>New (*) &gt; Gateway</b>.</li> <li>▪ In the top left corner, click <b>Objects</b> menu &gt; <b>More object types &gt; Network Object &gt; Gateways and Servers &gt; New Gateway</b>.</li> <li>▪ In the top right corner, click <b>Objects Pane &gt; New &gt; More &gt; Network Object &gt; Gateways and Servers &gt; Gateway</b></li> </ul>
4	<p>In the <b>Check Point Security Gateway Creation</b> window, click <b>Classic Mode</b>.</p> <p><b>Check Point Gateway</b> properties window opens on the <b>General Properties</b> page.</p>
5	<p>In the <b>Name</b> field, enter the applicable name for this Security Gateway object.</p>
6	<p>In the <b>IPv4 address</b> and <b>IPv6 address</b> fields, configure the same IPv4 and IPv6 addresses that you configured on the <b>Management Connection</b> page of the Security Group's First Time Configuration Wizard.</p> <p>Make sure the Security Management Server or Multi-Domain Server can connect to these IP addresses.</p>
7	<p>Establish the Secure Internal Communication (SIC) between the Management Server and this Security Group:</p> <ol style="list-style-type: none"> <li>a. Near the <b>Secure Internal Communication</b> field, click <b>Communication</b>.</li> <li>b. In the <b>Platform</b> field select <b>Maestro</b>.</li> <li>c. Enter the same <b>Activation Key</b> you entered during the Security Group's First Time Configuration Wizard.</li> <li>d. Click <b>Initialize</b>.</li> <li>e. Click <b>OK</b>.</li> </ol>

Step	Instructions
	<p>If the <b>Certificate state</b> field does not show <code>Established</code>, perform these steps:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Make sure there is a physical connectivity between the Security Group and the Management Server (for example, pings can pass).</li> <li>Run:           <pre>cpconfig</pre> </li> <li>Enter the number of this option:           <pre>Secure Internal Communication</pre> </li> <li>Follow the instructions on the screen to change the Activation Key.</li> <li>In SmartConsole, click <b>Reset</b>.</li> <li>Enter the same Activation Key you entered in the <code>cpconfig</code> menu.</li> <li>In SmartConsole, click <b>Initialize</b>.</li> </ol>
8	<p>In the <b>Platform</b> section, select the correct options:</p> <ol style="list-style-type: none"> <li>In the <b>Hardware</b> field, select <b>Maestro</b>.</li> <li>In the <b>Version</b> field, select <b>R81.20</b>.</li> <li>In the <b>OS</b> field, select <b>Gaia</b>.</li> </ol>
9	<p>On the <b>General Properties</b> page, on the <b>Network Security</b> tab, enable the applicable Software Blades.</p> <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">Deploying a Security Group in Bridge Mode</a>" on page 412.</p>
10	<p>On the <b>Network Management</b> page, configure the <b>Topology</b> of the Bridge interface.</p> <p> <b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ If a Bridge interface connects to the Internet, then set the <b>Topology</b> to <b>External</b>.</li> <li>▪ If you use this Bridge Security Gateway object in Access Control Policy rules with <b>Internet</b> objects, then set the <b>Topology</b> to <b>External</b>.</li> </ul>
11	Click <b>OK</b> .



Step	Instructions
12	Publish the SmartConsole session.
13	This Security Gateway object is now ready to receive the Security Policy.

#### 4. Configure the applicable Security Policies for the Security Gateway in SmartConsole

Step	Instructions
1	Connect with SmartConsole to the Security Management Server or Domain Management Server that manages this Security Group.
2	From the left navigation panel, click <b>Security Policies</b> .
3	Create a new policy and configure the applicable layers: <ol style="list-style-type: none"> <li>At the top, click the <b>+</b> tab (or press <b>CTRL T</b>).</li> <li>On the <b>Manage Policies</b> tab, click <b>Manage policies and layers</b>.</li> <li>In the <b>Manage policies and layers</b> window, create a new policy and configure the applicable layers.</li> <li>Click <b>Close</b>.</li> <li>On the <b>Manage Policies</b> tab, click the new policy you created.</li> </ol>
4	Create the applicable rules in the Access Control and Threat Prevention policies. <p> <b>Important</b> - See the <i>Supported Software Blades in Bridge Mode</i> and <i>Limitations in Bridge Mode</i> sections in "<a href="#">Deploying a Security Group in Bridge Mode</a>" on page 412.</p>
5	Install the Access Control Policy on the Security Gateway object.
5	Install the Threat Prevention Policy on the Security Gateway object.

For more information, see the:

- [Quantum Maestro Getting Started Guide](#).
- [R81.20 Gaia Administration Guide](#).
- [R81.20 Security Management Administration Guide](#).
- Applicable *Administration Guides* on the [R81.20 Home Page for Scalable Platforms](#).
- Applicable *Administration Guides* on the [R81.20 Home Page](#).

# Accept, or Drop Ethernet Frames with Specific Protocols

By default, Security Gateway in the Bridge mode *allows* Ethernet frames that carry protocols other than IPv4 (0x0800), IPv6 (0x86DD), or ARP (0x0806) protocols.

You can configure a Security Group in the Bridge Mode to either accept, or drop Ethernet frames that carry specific protocols.

When Access Mode VLAN (VLAN translation) is configured, BPDU frames can arrive with the wrong VLAN number to the switch ports through the Bridge interface. This mismatch can cause the switch ports to enter blocking mode.

In Active/Standby Bridge Mode only, you can disable BPDU forwarding to avoid such blocking mode:

Step	Instructions
1	Connect to the command line on the applicable Security Group.
2	Log in to the Expert mode.
3	Back up the current <code>/etc/rc.d/init.d/network</code> file: <pre>cp -v /etc/rc.d/init.d/network{, _BKP}</pre>
4	Edit the current <code>/etc/rc.d/init.d/network</code> file: <pre>vi /etc/rc.d/init.d/network</pre>
5	After the line: <pre>./etc/init.d/functions</pre> Add this line: <pre>/sbin/sysctl -w net.bridge.bpdu_ forwarding=0</pre>
6	Save the changes in the file and exit the editor.
7	Reboot the Security Group: <pre>reboot -b all</pre>
8	Connect to the command line on the applicable Security Group.
9	Log in to the Expert mode.

Step	Instructions
10	<p data-bbox="312 226 916 264"><b>Make sure the new configuration is loaded:</b></p> <pre data-bbox="320 271 1203 331">sysctl net.bridge.bpdu_forwarding</pre> <p data-bbox="312 338 612 376"><b>The expected output:</b></p> <pre data-bbox="320 383 1203 443">net.bridge.bpdu_forwarding = 0</pre>

# Routing and Bridge Interfaces

Security Gateways with a Bridge interface can support Layer 3 routing over non-bridged interfaces.

If you configure a Bridge interface with an IP address on a Security Group, the Bridge interface functions as a regular Layer 3 interface.

The Bridge interface participates in IP routing decisions on the Security Group and supports Layer 3 routing.

- Cluster deployments do not support this configuration.
- You cannot configure the Bridge interface to be the nexthop gateway for a route.
- A Security Group can support multiple Bridge interfaces, but only one Bridge interface can have an IP address.
- A Security Group cannot filter or transmit packets that it inspected before on a Bridge interface (to avoid double-inspection).

# IPv6 Neighbor Discovery

Neighbor discovery works over the ICMPv6 Neighbor Discovery protocol, which is the functional equivalent of the IPv4 ARP protocol.

ICMPv6 Neighbor Discovery Protocol must be explicitly permitted in the Access Control Rule Base for all bridged networks.

This is different from ARP. ARP traffic is Layer 2 only, therefore it permitted regardless of the Rule Base.

This is an example of an explicit Rule Base that permits ICMPv6 Neighbor Discovery protocol:

Name	Source	Destination	VPN	Services & Applications	Action	Track	Install On
IPv6 Neighbor Discovery	Network object that represents the Bridged Network	Network object that represents the Bridged Network	Any	neighbor-advertisement neighbor-solicitation router-advertisement router-solicitation redirect6	Accept	Log	Policy Targets

# Managing Ethernet Protocols

It is possible to configure a Security Gateway with bridge interface to allow or drop protocols that are not based on IP that pass through the bridge interface. For example, protocols that are not IPv4, IPv6, or ARP.


By default, these protocols are allowed by the Security Gateway.

Frames for protocols that are not IPv4, IPv6, or ARP are allowed if:

- On the Security Gateway, the value of the kernel parameter `fwaccept_unknown_protocol` is 1 (all frames are accepted)
- OR in the applicable `user.def` file on the Management Server, the protocol IS defined in the `allowed_ethernet_protocols` table.
- AND in the applicable `user.def` file on the Management Server, the protocol is NOT defined in the `dropped_ethernet_protocols` table.

To configure the Security Group to accept only specific protocols that are not IPv4, IPv6, or ARP:

Step	Instructions
1	<p>On the Security Group, configure the value of the kernel parameter <code>fwaccept_unknown_protocol</code> to 0.</p> <ol style="list-style-type: none"> <li>a. Connect to the command line on the Security Group.</li> <li>b. Log in to the Expert mode.</li> <li>c. Configure the value of the kernel parameter <code>fwaccept_unknown_protocol</code> to 0:           <pre style="border: 1px solid black; padding: 5px; margin: 5px 0;">g_update_conf_file fwkern.conf fwaccept_unknown_protocol=0</pre> </li> <li>d. Reboot the Security Group.           <p>If the reboot is not possible at this time, then:</p> <ul style="list-style-type: none"> <li>▪ Run this command to make the required change:               <pre style="border: 1px solid black; padding: 5px; margin: 5px 0;">g_fw ctl set int fwaccept_unknown_protocol 0</pre> </li> <li>▪ Run this command to make sure the required change was accepted:               <pre style="border: 1px solid black; padding: 5px; margin: 5px 0;">g_fw ctl get int fwaccept_unknown_protocol</pre> </li> </ul> </li> </ol>

Step	Instructions
2	<p>On the Management Server, edit the applicable <code>user.def</code> file.</p> <p> <b>Note</b> - For the list of <code>user.def</code> files, see <a href="#">sk98239</a>.</p> <ol style="list-style-type: none"> <li>Back up the current applicable <code>user.def</code> file.</li> <li>Edit the current applicable <code>user.def</code> file.</li> <li>Add these directives: <ul style="list-style-type: none"> <li><code>allowed_ethernet_protocols</code> - contains the EtherType numbers (in Hex) of protocols to accept</li> <li><code>dropped_ethernet_protocols</code> - contains the EtherType numbers (in Hex) of protocols to drop</li> </ul> </li> </ol> <p><b>Example</b></p> <pre data-bbox="416 734 1458 1272"> \$ifndef __user_def__ \$define __user_def__  \\ \\ User defined INSPECT code \\  <b>allowed_ethernet_protocols={</b> <b>&lt;0x0800,0x86DD,0x0806&gt;);</b> <b>dropped_ethernet_protocols={ &lt;0x8137,0x8847,0x9100&gt;</b> <b>);</b>  endif /* __user_def__ */ </pre> <p>For the list of EtherType numbers, see <a href="http://standards-oui.ieee.org/ethertype/eth.csv">http://standards-oui.ieee.org/ethertype/eth.csv</a>.</p> <ol style="list-style-type: none"> <li>Save the changes in the file and exit the editor.</li> </ol>
3	<p>In SmartConsole, install the Access Control Policy on the Security Gateway object.</p>

# Installing and Uninstalling a Hotfix

This section provides instructions for installing and uninstalling a Hotfix:

- On Quantum Maestro Orchestrators  
See "[Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators](#)" below
- On Security Group Members  
See "[Installing and Uninstalling a Hotfix on Security Group Members](#)" on page 435

## Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators

*In This Section:*

---


Installing a Hotfix Package on Orchestrators .....	433
Uninstalling a Hotfix Package on Orchestrators .....	434
Deleting a Hotfix Package on Orchestrators .....	434

---

You use the CPUSE on each Quantum Maestro Orchestrator to install the applicable hotfixes.

### Important:

- It is not supported to upgrade the CPUSE Agent on Quantum Maestro Orchestrators.
- For the CPUSE instructions, see [sk92449](#).
- Jumbo Hotfix Accumulator reboots the Quantum Maestro Orchestrator after you install or uninstall it.
- Quantum Maestro Orchestrator stops processing traffic from the start of the Jumbo Hotfix Accumulator installation or uninstall and until Quantum Maestro Orchestrator comes up from the reboot.
- You must install the same Take of Jumbo Hotfix Accumulator on all Quantum Maestro Orchestrators on all Maestro Sites.
- For the CPUSE instructions, see [sk92449](#).

 **Best Practice** - Before you install or uninstall a hotfix, take a Gaia Snapshot on each Quantum Maestro Orchestrator either in Gaia Portal, or Gaia Clish. For instructions, see the [R81.20 Gaia Administration Guide](#) > Chapter *Maintenance* > Section *Snapshot Management*.



## Installing a Hotfix Package on Orchestrators

Internet Connection	Installation Methods	Action Plan
Quantum Maestro Orchestrator <b>is</b> connected to the Internet	You can perform only an offline installation.	See the instructions for a Quantum Maestro Orchestrator that is <b>not</b> connected to the Internet.
Quantum Maestro Orchestrator is <b>not</b> connected to the Internet	You can perform only an offline installation.	<p><b>To install a CPUSE package in Gaia Portal</b></p> <ol style="list-style-type: none"> <li>1. Use the computer, from which you connect to Gaia Portal on Quantum Maestro Orchestrator.</li> <li>2. Download the applicable CPUSE Software Package from the <a href="#">Check Point Support Center</a>.</li> <li>3. Connect to Gaia Portal on each Quantum Maestro Orchestrator.</li> <li>4. Import the applicable CPUSE Software Package.</li> <li>5. Verify the applicable CPUSE Software Package.</li> <li>6. Install the applicable CPUSE Software Package.</li> </ol> <p><b>To install a CPUSE package in Gaia Clish</b></p> <ol style="list-style-type: none"> <li>1. Use the computer, from which you connect to Gaia Clish on Quantum Maestro Orchestrator.</li> <li>2. Download the applicable CPUSE Software Package from the <a href="#">Check Point Support Center</a>.</li> <li>3. Transfer the applicable CPUSE Offline Software Package to each Quantum Maestro Orchestrator to some directory (for example, <code>/var/log/path_to_CPUSE_packages/</code>). Make sure to transfer the CPUSE packages in the binary mode.</li> <li>4. Connect to the command line on each Quantum Maestro Orchestrator and log in to Gaia Clish.</li> <li>5. Import the applicable CPUSE Software Package.</li> <li>6. Verify the applicable CPUSE Software Package.</li> <li>7. Install the applicable CPUSE Software Package.</li> </ol>

## Uninstalling a Hotfix Package on Orchestrators

### To uninstall a CPUSE package in Gaia Portal

1. Connect to Gaia Portal on each Quantum Maestro Orchestrator.
2. From the left navigation tree, click **Upgrades (CPUSE) > Status and Actions**.
3. Right-click the applicable CPUSE Software Package and click **Uninstall**.

### To uninstall a CPUSE package in Gaia Clish

1. Connect to the command line on each Quantum Maestro Orchestrator.
2. Log in to Gaia Clish.
3. Uninstall the applicable CPUSE Software Package:

```
installer uninstall [Press the Tab key]  
installer uninstall <Number of CPUSE Package>
```

## Deleting a Hotfix Package on Orchestrators

This section applies to a Hotfix package that exists on the Quantum Maestro Orchestrator, but is not installed.

- ★ **Best Practice** - To free the disk space, we recommend to delete CPUSE Software Packages you did not install.

### To delete a CPUSE package in Gaia Portal

1. Connect to Gaia Portal on each Quantum Maestro Orchestrator.
2. From the left navigation tree, click **Upgrades (CPUSE) > Status and Actions**.
3. Right-click the applicable CPUSE Software Package and click **Delete From Disk**.

### To delete a CPUSE package in Gaia Clish

1. Connect to the command line on each Quantum Maestro Orchestrator.
2. Log in to Gaia Clish..
3. Delete the applicable CPUSE Software Package:

```
installer delete [Press the Tab key]  
installer delete <Number of CPUSE Package>
```

# Installing and Uninstalling a Hotfix on Security Group Members

*In This Section:*

---

Installing a Hotfix Package on Security Group Members .....	436
Uninstalling a Hotfix Package on Security Group Members .....	446

---

This section describes the Full Connectivity installation and uninstall of an Offline CPUSE package.

## Installing a Hotfix Package on Security Group Members

### Important:

- **It is not supported to upgrade the CPUSE Agent on Security Group Members.**
- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in both Security Gateway and VSX mode.

In VSX mode, you must run all the commands in the context of VS0.

- **Do not install the hotfix on all the Security Group Members in a specific Security Group at the same time.**
- In this procedure, you divide all Security Group Members in a specific Security Group into two or more logical groups.  
In the procedure below, we use **two** logical groups denoted below as "A" and "B".

You install the hotfix on one logical group of the Security Group Members at one time.

The other logical group(s) of the Security Group Members continues to handle traffic.

Each logical group should contain the same number of Security Group Members - as close as possible.

### Examples

Environment	Description
Single Site	<ul style="list-style-type: none"> <li>• There are 8 Security Group Members in the Security Group.</li> <li>• The Logical Group "A" contains Security Group Members from 1_1 to 1_4.</li> <li>• The Logical Group "B" contains Security Group Members from 1_5 to 1_8.</li> </ul>
Single Site	<ul style="list-style-type: none"> <li>• There are 5 Security Group Members in the Security Group.</li> <li>• The Logical Group "A" contains Security Group Members from 1_1 to 1_3.</li> <li>• The Logical Group "B" contains Security Group Members from 1_4 to 1_5.</li> </ul>
Dual Site	<ul style="list-style-type: none"> <li>• There are 4 Security Group Members in the Security Group (on each Site).</li> <li>• The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4.</li> <li>• The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.</li> </ul>



## Installation Procedure

**Step 1 - Perform the preliminary steps****For Offline CPUSE packages**

Step	Instructions
A	Make sure you have the applicable CPUSE Offline package.
B	Transfer the CPUSE Offline package to the Security Group (into some directory, for example <code>/var/log/</code> ).
C	Connect to the command line on the Security Group.
D	<p>If your default shell is <code>/bin/bash</code> (the Expert mode), then go to Gaia gClish:</p> <pre data-bbox="391 712 1460 779">gclish</pre>
E	<p>Import the CPUSE Offline package from the hard disk:</p> <pre data-bbox="391 855 1460 958">installer import local /&lt;Full Path&gt;/&lt;Name of the CPUSE Offline Package&gt;</pre> <p>Example:</p> <pre data-bbox="391 1008 1460 1111">[Global] HostName-ch01-01 &gt; installer import local /var/log/Check_Point_R81.20_Hotfix_Bundle_FULL.tgz</pre>
F	<p>Show the imported CPUSE packages:</p> <pre data-bbox="391 1191 1460 1258">show installer packages imported</pre>

Step	Instructions
G	<p>Make sure the imported CPUSE package can be installed on this Security Group:</p> <pre data-bbox="391 315 1461 483"> installer verify [<b>Press the Tab key</b>] installer verify &lt;Number of CPUSE Package&gt; member_ids all </pre> <p><b>Example:</b></p> <pre data-bbox="391 533 1461 1003"> [Global] HostName-ch01-01 &gt; installer verify 2 member_ids all ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+-----+  1_01 (local) Installation is allowed.                     1_02         Installation is allowed.                     1_03         Installation is allowed.                     1_04         Installation is allowed.                     1_05         Installation is allowed.                     1_06         Installation is allowed.                     1_07         Installation is allowed.                     1_08         Installation is allowed.                    +-----+-----+ [Global] HostName-ch01-01 &gt; </pre>



**Step 2 - On the Security Group, make sure to disable the SMO Image Cloning feature**

**Note** - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is <code>/bin/bash</code> (Expert mode), then go to Gaia gClish: <pre>gclish</pre>
C	Examine the state of the SMO Image Cloning feature: <pre>show smo image auto-clone state</pre>
D	Disable the SMO Image Cloning feature, if it is enabled: <pre>set smo image auto-clone state off</pre>
E	Examine the state of the SMO Image Cloning feature: <pre>show smo image auto-clone state</pre>

**Step 3 - Install the Hotfix on the Security Group Members in the Logical Group "A"**

Step	Instructions
A	Connect in one of these ways: <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" <b>through the console.</b></li> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" <b>over SSH.</b></li> </ul>
B	If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then go to the Expert mode: <pre data-bbox="352 600 1458 663">expert</pre>
C	Set the Security Group Members in the Logical Group "A" to the state "DOWN": <pre data-bbox="352 741 1458 804">g_clusterXL_admin -b &lt;SGM IDs in Group "A"&gt; down</pre> Example: <pre data-bbox="352 853 1458 954">[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_1-1_4 down</pre>
D	Connect to one of the Security Group Members in the Logical Group "A": <pre data-bbox="352 1037 1458 1099">member &lt;Member ID&gt;</pre> Example: <pre data-bbox="352 1149 1458 1211">member 1_1</pre>
E	Go from the Expert mode to Gaia gClish: <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run:               <pre data-bbox="432 1357 1458 1420">gclish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run:               <pre data-bbox="432 1469 1458 1532">exit</pre> </li> </ul>

Step	Instructions
F	<p>Install the CPUSE hotfix package on the Security Group Members in the Logical Group "A":</p> <pre>installer install [<b>Press the Tab key</b>]</pre> <pre>installer install &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre> <p><b>Example:</b></p> <pre>[Global] HostName-ch01-01 &gt; installer install 2 member_ids 1_1-1_4 ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+-----+  1_01 (local) Package is ready for installation            1_02         Package is ready for installation            1_03         Package is ready for installation            1_04         Package is ready for installation           +-----+-----+ The machines (1_02,1_02,1_03,1_04) will automatically reboot after install. Do you want to continue? ([y]es / [n]o) <b>y</b> [Global] HostName-ch01-01 &gt;</pre>
G	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>exit</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>expert</pre> </li> </ul>
H	<p>Monitor the system until the Security Group Members in the Logical Group "A" are in the state "UP" and enforce the Security Policy again:</p> <pre>asg monitor</pre>

**Step 4 - Install the Hotfix on the Security Group Members in the Logical Group "B"**

Step	Instructions
A	Connect in one of these ways: <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" <b>through the console.</b></li> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" <b>over SSH.</b></li> </ul>
B	If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then go to the Expert mode: <pre data-bbox="352 600 1458 663">expert</pre>
C	Set the Security Group Members in the Logical Group "B" to the state "DOWN": <pre data-bbox="352 741 1458 804">g_clusterXL_admin -b &lt;SGM IDs in Group "B"&gt; down</pre> Example: <pre data-bbox="352 853 1458 954">[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_5-1_8 down</pre>
D	Connect to one of the Security Group Members in the Logical Group "B": <pre data-bbox="352 1037 1458 1099">member &lt;Member ID&gt;</pre> Example: <pre data-bbox="352 1149 1458 1211">member 1_5</pre>
E	Go from the Expert mode to Gaia gClish: <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run:               <pre data-bbox="432 1357 1458 1420">gclish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run:               <pre data-bbox="432 1469 1458 1532">exit</pre> </li> </ul>

Step	Instructions
F	<p>Install the CPUSE hotfix package on the Security Group Members in the Logical Group "B":</p> <pre>installer install [Press the Tab key]</pre> <pre>installer install &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "B"&gt;</pre> <p><b>Example:</b></p> <pre>[Global] HostName-ch01-01 &gt; installer install 2 member_ids 1_5-1_8 ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+-----+  1_05 (local) Package is ready for installation            1_06         Package is ready for installation            1_07         Package is ready for installation            1_08         Package is ready for installation           +-----+-----+ The machines (1_05,1_06,1_07,1_08) will automatically reboot after install. Do you want to continue? ([y]es / [n]o) <b>y</b> [Global] HostName-ch01-01 &gt;</pre>
G	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>exit</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>expert</pre> </li> </ul>
H	<p>Monitor the system until the Security Group Members in the Logical Group "B" are in the state "UP" and enforce the security policy again:</p> <pre>asg monitor</pre>

### Step 5 - Make sure the Hotfix is installed on all Security Group Members

Step	Instructions
A	Connect to the command line on the Security Group.
B	<p>If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then go to the Expert mode:</p> <pre>expert</pre>
C	<p>Run:</p> <pre>asg diag verify</pre>

## Uninstalling a Hotfix Package on Security Group Members

 **Important:**

- **It is not supported to upgrade the CPUSE Agent on Security Group Members.**
- This procedure keeps the current connections in a Security Group.
- This procedure applies to Security Groups in both Security Gateway and VSX mode.  
In VSX mode, you must run all the commands in the context of VS0.
- **Do not uninstall the hotfix from all the Security Group Members in a specific Security Group at the same time.**
- You uninstall the hotfix from one logical group of the Security Group Members at one time.

The other logical group of the Security Group Members continues to handle traffic.

You divide all Security Group Members in a specific Security Group into two logical groups - denoted below as "A" and "B".

1. You uninstall the hotfix from the Security Group Members in the Logical Group "A"
2. You uninstall the hotfix from the Security Group Members in the Logical Group "B"

Each logical group should contain the same number of Security Group Members - as close as possible.

### Examples

Environment	Description
Single Site	<ul style="list-style-type: none"> <li>• There are 8 Security Group Members in the Security Group.</li> <li>• The Logical Group "A" contains Security Group Members from 1_1 to 1_4.</li> <li>• The Logical Group "B" contains Security Group Members from 1_5 to 1_8.</li> </ul>
Single Site	<ul style="list-style-type: none"> <li>• There are 5 Security Group Members in the Security Group.</li> <li>• The Logical Group "A" contains Security Group Members from 1_1 to 1_3.</li> <li>• The Logical Group "B" contains Security Group Members from 1_4 to 1_5.</li> </ul>
Dual Site	<ul style="list-style-type: none"> <li>• There are 4 Security Group Members in the Security Group (on each Site).</li> <li>• The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4.</li> <li>• The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.</li> </ul>

## Uninstall Procedure

### Step 1 - On the Security Group, make sure to disable the SMO Image Cloning feature

- Note** - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is <code>/bin/bash</code> (Expert mode), then go to Gaia gClish: <pre>gclish</pre>
C	Examine the state of the SMO Image Cloning feature: <pre>show smo image auto-clone state</pre>
D	Disable the SMO Image Cloning feature, if it is enabled: <pre>set smo image auto-clone state off</pre>
E	Examine the state of the SMO Image Cloning feature: <pre>show smo image auto-clone state</pre>



**Step 2 - Uninstall the Hotfix from the Security Group Members in the Logical Group "A"**

Step	Instructions
A	Connect in one of these ways: <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" <b>through the console.</b></li> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" <b>over SSH.</b></li> </ul>
B	Go to the Expert mode.
C	Set Security Group Members in the Logical Group "A" to the state "DOWN": <pre data-bbox="352 674 1458 734">g_clusterXL_admin -b &lt;SGM IDs in Group "A"&gt; down</pre> Example: <pre data-bbox="352 786 1458 887">[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_1-1_4 down</pre>
D	Connect to one of the Security Group Members in the Logical Group "A": <pre data-bbox="352 969 1458 1028">member &lt;Member ID&gt;</pre>
E	Go from the Expert mode to Gaia gClish: <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run:               <pre data-bbox="432 1173 1458 1234">gclish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run:               <pre data-bbox="432 1285 1458 1346">exit</pre> </li> </ul>

Step	Instructions
F	<p>Uninstall the CPUSE hotfix package on the Security Group Members in the Logical Group "A":</p> <pre data-bbox="352 320 1458 376">installer uninstall [Press the Tab key]</pre> <pre data-bbox="352 389 1458 483">installer uninstall &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre> <p>Example:</p> <pre data-bbox="352 539 1458 943">[Global] HostName-ch01-01 &gt; installer uninstall 2 member_ids 1_1-1_4 ... .. Update Service Engine +-----+  Member ID    Status   +-----+-----+  1_01 (local) Package is ready for uninstallation                 1_02         Package is ready for uninstallation                 1_03         Package is ready for uninstallation                 1_04         Package is ready for uninstallation                +-----+-----+ The machines (1_02,1_02,1_03,1_04) will automatically reboot after uninstall. Do you want to continue? ([y]es / [n]o) y [Global] HostName-ch01-01 &gt;</pre>
G	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre data-bbox="432 1093 1458 1155">exit</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre data-bbox="432 1205 1458 1267">expert</pre> </li> </ul>
H	<p>Monitor the system until the Security Group Members in the Logical Group "A" are in the state "UP" and enforce the Security Policy again:</p> <pre data-bbox="352 1391 1458 1453">asg monitor</pre>

**Step 3 - Uninstall the Hotfix from the Security Group Members in the Logical Group "B"**

Step	Instructions
A	Connect in one of these ways: <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" <b>through the console.</b></li> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" <b>over SSH.</b></li> </ul>
B	Go to the Expert mode: <pre data-bbox="352 600 1458 663">expert</pre>
C	Set Security Group Members in the Logical Group "B" to the state "DOWN": <pre data-bbox="352 741 1458 804">g_clusterXL_admin -b &lt;SGM IDs in Group "B"&gt; down</pre> Example: <pre data-bbox="352 853 1458 954">[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_5-1_8 down</pre>
D	Connect to one of the Security Group Members in the Logical Group "A": <pre data-bbox="352 1039 1458 1102">member &lt;Member ID&gt;</pre>
E	Go from the Expert mode to Gaia gClish: <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run:               <pre data-bbox="432 1245 1458 1308">gclish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run:               <pre data-bbox="432 1357 1458 1420">exit</pre> </li> </ul>

Step	Instructions
F	<p>Uninstall the CPUSE hotfix package on the Security Group Members in the Logical Group "B":</p> <pre>installer uninstall [Press the Tab key]</pre> <pre>installer uninstall &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "B"&gt;</pre> <p><b>Example:</b></p> <pre>[Global] HostName-ch01-01 &gt; installer uninstall 2 member_ids 1_5-1_8 ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+-----+  1_05 (local) Package is ready for uninstallation          1_06         Package is ready for uninstallation          1_07         Package is ready for uninstallation          1_08         Package is ready for uninstallation         +-----+-----+ The machines (1_05,1_06,1_07,1_08) will automatically reboot after uninstall. Do you want to continue? ([y]es / [n]o) y [Global] HostName-ch01-01 &gt;</pre>
G	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>exit</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>expert</pre> </li> </ul>
H	<p>Monitor the system until the Security Group Members in the Logical Group "A" are in the state "UP" and enforce the Security Policy again:</p> <pre>asg monitor</pre>

#### Step 4 - Make sure the Hotfix is uninstalled from all Security Group Members

Step	Instructions
A	Connect to the command line on the Security Group.
B	<p>If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then go to the Expert mode:</p> <pre>expert</pre>
C	<p>Run:</p> <pre>asg diag verify</pre>

# Upgrading Maestro to R81.20


This section describes the steps for upgrading and rolling back a Maestro environment - the Quantum Maestro Orchestrators and the Security Groups.

## Upgrading Maestro Environment - Zero Downtime

This section describes the steps for upgrading a Maestro environment (the Quantum Maestro Orchestrators and the Security Groups) with Zero Downtime - as a Multi-Version Cluster (MVC).

This procedure supports only these upgrade paths for Security Groups:

- from R81.10 to R81.20
- from R81 to R81.20

 **Warning** - Multi-Version Cluster (Zero Downtime) upgrade from R81 to R81.20 is **not** supported if a Security Group has Bond interfaces in the 802.3ad (LACP) mode on Uplink ports (Known Limitation PMTR-88191).

 **Important** - See these rollback procedures:

- ["Rolling Back a Failed Upgrade of a Maestro Orchestrator" on page 507](#)
- ["Rolling Back a Failed Upgrade of a Security Group - After Partial Upgrade" on page 510](#)
- ["Rolling Back a Failed Upgrade of a Security Group - Zero Downtime" on page 513](#)
- ["Rolling Back a Failed Upgrade of a Security Group - Minimum Downtime" on page 521.](#)

## Important Notes for Quantum Maestro Orchestrators:

- We recommend to schedule a maintenance window for all Orchestrators on all sites.
- The major software version on the Orchestrators must be equal to or higher than the major software version on the managed Security Group (PMTR-86785).
- This procedure **keeps** the current configuration on the Orchestrators.
- Upgrade all Orchestrators and only then upgrade the Security Groups.
- Upgrade one Orchestrator at a time.
- In a Dual Site environment:

### Procedure

1. Upgrade the Orchestrators on the Standby Site (Site 2)
2. Initiate a fail-over in each Security Group from the non-upgraded Active Site (Site 1) to the upgraded Standby Site (Site 2):
  - a. Connect to the command line on each Security Group.
  - b. If your default shell is Gaia gClish, then go to the Expert mode:

```
expert
```

- c. Initiate a fail-over:

```
chassis_admin -c <ID of Active Site> down
```

```
chassis_admin -c <ID of Former Active Site> up
```

3. Upgrade the Orchestrators on the new Standby Site (Site 1).

## Important Notes for Security Groups:

- Before you upgrade the Security Groups, you must upgrade the Management Server that manages the Security Groups.  
See the [R81.20 Installation and Upgrade Guide](#).
- This procedure applies to Security Groups in the Gateway mode and the VSX mode.  
In VSX mode, you must run all the commands in the context of VS0.
- **During the upgrade process, it is:**
  - **Forbidden to install policy on the Security Group, unless the upgrade procedure explicitly shows how to do it.**
  - **Forbidden to reboot Security Group Members, unless the upgrade procedure explicitly shows how to do it.**
  - **Forbidden to change the configuration of the Security Group and its Security Group Members.**
  - **Forbidden to install Hotfixes on the Security Group Members, unless Check Point Support or R&D explicitly instructs you to do so.**
  - **Forbidden to install the Jumbo Hotfix Accumulator on the Security Group Members, unless Check Point Support or R&D explicitly instructs you to do so.**
- To prevent down time, do **not** upgrade all the Security Group Members in a specific Security Group at the same time.
- In this upgrade procedure, you divide all Security Group Members in a specific Security Group into two or more logical groups.  
In the procedure below, we use **two** logical groups denoted below as "A" and "B".  
You upgrade one logical group of the Security Group Members at one time.  
The other logical group(s) of the Security Group Members continues to handle traffic.  
Each logical group should contain the same number of Security Group Members - as close as possible.

### Examples

Environment	Description
Single Site	<ul style="list-style-type: none"> <li>• There are 8 Security Group Members in the Security Group.</li> <li>• The Logical Group "A" contains Security Group Members from 1_1 to 1_4.</li> <li>• The Logical Group "B" contains Security Group Members from 1_5 to 1_8.</li> </ul>

Environment	Description
Single Site	<ul style="list-style-type: none"><li>• There are 5 Security Group Members in the Security Group.</li><li>• The Logical Group "A" contains Security Group Members from 1_1 to 1_3.</li><li>• The Logical Group "B" contains Security Group Members from 1_4 to 1_5.</li></ul>
Dual Site	<ul style="list-style-type: none"><li>• There are 4 Security Group Members in the Security Group (on each Site).</li><li>• The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4.</li><li>• The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.</li></ul>



- In a Dual Site environment:
  - We recommend to upgrade all Security Group Members in each Security Group on one Site, and then upgrade all Security Group Members in the same Security Group on the next Site.  
Do this on one Security Group at a time.
  - To prevent a fail-over between Sites during the upgrade, we recommend these steps for each Security Group:

#### Procedure

1. Connect to the command line on a Security Group.
2. If your default shell is the Expert mode, then go to Gaia gClish:

```
gclish
```

3. Get the current Dual Site Active/Standby mode:

```
show chassis high-availability mode
```

#### Available Modes:

Mode ID	Mode Title	Mode Description
0	<b>Active/Standby - Active Up</b>	No primary Site. The currently Active Site stays Active unless it goes DOWN, or the Standby Site has a higher Site quality grade.
1	<b>Active/Standby - Primary Up</b>	Active Site, always stays Active unless it goes DOWN, or the Standby Site has a higher Site quality grade.
2	Not available	Not supported.
3	<b>Standby Chassis VSL Mode</b>	In VSX, provides Virtual System Load Sharing.

4. Decide which of the Sites is Active.
5. Change the Dual Site Active/Standby mode to "Active/Standby - Primary Up":

```
set chassis high-availability mode 1
```

6. Change the Site Priority (enter the number of the currently Active Site):

```
set chassis high-availability vs chassis_
priority {1 | 2}
```

7. Upgrade all Security Group Members on the "Standby" Site.
8. On the upgraded Site, change the Dual Site Active/Standby mode to "Primary Up":

```
set chassis high-availability mode 1
```

9. On the upgraded Site, change the Site Priority (enter the number of the currently Active Site):

```
set chassis high-availability vs chassis_
```

**Required software packages:**

Download the required software packages from [sk177624](#):

1. The required Take of the Jumbo Hotfix Accumulator
2. The required CPUSE Deployment Agent for Scalable Platforms
3. The R81.20 Upgrade Package for Scalable Platforms

**Workflow:**


1. On the Management Server - Upgrade to the required version that can manage an R81.20 Security Group (see [sk113113](#)).
2. On the Orchestrator - Upgrade to R81.20 and install the R81.20 Jumbo Hotfix Accumulator.
3. On the Security Group - Run the Pre-Upgrade Verifier to make sure it is possible to upgrade the Security Group.
4. On the Security Group - Install the required Jumbo Hotfix Accumulator (using two logical groups of Security Group Members).
5. On the Security Group - Install the required CPUSE Deployment Agent package for the Security Group.
6. On the Security Group - Upgrade to R81.20 (using two logical groups of Security Group Members).
7. In SmartConsole, install the policy.

**Procedure:**

**Step 1 - Upgrade the Management Server**

Upgrade the Management Server to the required version that can manage an R81.20 Security Group (see the [R81.20 Release Notes](#)).


## Step 2 - On the Quantum Maestro Orchestrator, upgrade to R81.20 and install the R81.20 Jumbo Hotfix Accumulator


Step	Instructions
A	If the Orchestrator runs R80.20SP, then install the <a href="#">R80.20SP Jumbo Hotfix Accumulator</a> Take 326 or higher on the Orchestrator.
B	In the Orchestrator's Gaia Portal, from the left tree, go to <b>Upgrades (CPUSE) &gt; Status and Actions</b> .
C	In the top right section, click <b>Import Package</b> .
D	Click <b>Browse</b> .
E	Go to the folder where you put the <i>R81.20 Upgrade Package for Scalable Platforms</i> from <a href="#">sk177624</a> .
F	Select the <i>R81.20 Upgrade Package for Scalable Platforms</i> .
G	Click <b>Open</b> .
H	Click <b>Import</b> .
I	Above the list of packages, near the help icon, click the filter button that currently says " <b>Showing Recommended packages</b> " and click " <b>All</b> ". The filter must change to " <b>Showing All packages</b> ".
J	Right-click the imported R81.20 CPUSE Offline Package and click <b>Verify Update</b> .
K	Right-click the imported R81.20 CPUSE Offline Package and click <b>Upgrade</b> .  <b>Important:</b> <ul style="list-style-type: none"> <li>▪ Make sure to click <b>Upgrade</b> (do <b>not</b> click <b>Install</b> because it performs a clean install, which deletes all configuration and reboots all Security Group Members).</li> <li>▪ At the end of the upgrade, the Orchestrator reboots automatically.</li> </ul>
L	Install the Recommended Take of the <a href="#">R81.20 Jumbo Hotfix Accumulator</a> . See " <i>Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators</i> " on page 432.

**Step 3 - On the Security Group, run the Pre-Upgrade Verifier to make sure it is possible to upgrade the Security Group**

Step	Instructions
A	Download this script to your computer: <a href="https://supportcenter.checkpoint.com/file_download?id=124062">https://supportcenter.checkpoint.com/file_download?id=124062</a>
B	Copy this script from your computer to the Security Group. Copy the script to some directory (for example, /var/log/).
C	Connect to the command line on the Security Group.
D	Log in to the Expert mode.
E	Run these commands in the order listed below: <pre>cd /var/log/ chmod +x pre_upgrade_verifier.sh ./pre_upgrade_verifier.sh</pre>

**Step 4 - On the Management Server, change the version of the VSX Gateway object**

 **Important** - This step applies only when the Security Group works in the VSX mode.

Step	Instructions
A	Connect to the command line on the Management Server.
B	Log in to the Expert mode.
C	On a Multi-Domain Server, go to the context of the applicable Domain Management Server that manages this Security Group in VSX mode: <pre data-bbox="352 618 1458 678">mdsens &lt;IP Address or Name of Domain Management Server&gt;</pre>
D	Upgrade the version of a VSX Gateway object in the management database:  <b>Warning</b> - Make sure to close all SmartConsole clients connected to this Management Server. <pre data-bbox="352 853 1458 913">vsx_util upgrade [-s &lt;Mgmt Server&gt;] [-u &lt;UserName&gt;]</pre> For more information, see the <a href="#">R81.20 VSX Administration Guide</a> > Chapter "Command Line Reference" > Section "vsx_util".
E	Log in with the Management Server administrator credentials.
F	Select the VSX Gateway object for this Security Group.
G	Change the version to <b>R81.20</b> .

**Step 5 - On the Security Group, disable the SMO Image Cloning feature**

**Note** - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is <code>/bin/bash</code> (Expert mode), then go to Gaia gClish: <pre>gclish</pre>
C	Examine the state of the SMO Image Cloning feature: <pre>show smo image auto-clone state</pre>
D	Disable the SMO Image Cloning feature, if it is enabled: <pre>set smo image auto-clone state off</pre>
E	Examine the state of the SMO Image Cloning feature: <pre>show smo image auto-clone state</pre>

**Step 6 - On the Security Group, install the required Take of the Jumbo Hotfix Accumulator for the current version****Important:**

- You must install the required Jumbo Hotfix Accumulator on **all** Security Group Members in the Security Group.
- Before you install Jumbo Hotfix Accumulator, this procedure requires you to disable the SMO Image Cloning feature on the Security Group. Do **not** enable the SMO Image Cloning feature on the Security Group until the upgrade procedure instructs you to do so.

Follow these instructions to install the required Jumbo Hotfix Accumulator from [sk177624](#):

*"Installing a Hotfix Package on Security Group Members" on page 436*

**Step 7 - On the Security Group, upgrade the CPUSE Deployment Agent**

**Important** - You must do this step even if you upgrade again after a rollback procedure on the Security Group.

Step	Instructions
A	Transfer the CPUSE Deployment Agent package for Scalable Platforms (from <a href="#">sk177624</a> ) to the Security Group (into some directory, for example /var/log/).
B	Connect to the command line on the Security Group.
C	<p>If your default shell is /etc/gclish (Gaia gClish), then go to the Expert mode:</p> <pre data-bbox="352 696 1458 757">expert</pre>
D	<p>Make sure the CPUSE Deployment Agent package exists:</p> <pre data-bbox="352 842 1458 943">ls -l /&lt;Full Path&gt;/&lt;Name of CPUSE Deployment Agent Package&gt;</pre>
E	<p>Upgrade the CPUSE Deployment Agent:</p> <pre data-bbox="352 1021 1458 1122">update_sp_da /&lt;Full Path&gt;/&lt;Name of CPUSE Deployment Agent Package&gt;</pre> <p>Example:</p> <pre data-bbox="352 1173 1458 1234">update_sp_da /var/log/DeploymentAgent_XXXXXXXXX.tgz</pre>
F	<p>Go from the Expert mode to Gaia gClish:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is /bin/bash (the Expert mode), then run: <pre data-bbox="432 1379 1458 1440">gclish</pre> </li> <li>▪ If your default shell is /etc/gclish (Gaia gClish), then run: <pre data-bbox="432 1491 1458 1552">exit</pre> </li> </ul>
G	<p>Make sure all Security Group Members have the same build of the CPUSE Deployment Agent:</p> <pre data-bbox="352 1675 1458 1736">show installer status build</pre>




## Step 8 - On the Security Group, import the R81.20 upgrade package

Step	Instructions
A	Make sure you have the applicable CPUSE Offline package: R81.20 Upgrade Package for Scalable Platforms
B	Transfer the CPUSE Offline package to the Security Group (into some directory, for example <code>/var/log/</code> ).
C	Connect to the command line on the Security Group.
D	If your default shell is <code>/bin/bash</code> (the Expert mode), then go to Gaia gClish: <pre>gclish</pre>
E	Import the CPUSE Offline package from the hard disk: <pre>installer import local /&lt;Full Path&gt;/&lt;Name of the CPUSE Offline Package&gt;</pre> Example: <pre>[Global] HostName-ch01-01 &gt; installer import local /var/log/Check_Point_R81.20_SP_Install_and_Upgrade.tar</pre>
F	Show the imported CPUSE packages: <pre>show installer packages imported</pre>
G	Make sure the imported CPUSE package can be installed on this Security Group: <pre>installer verify [Press Tab]</pre> <pre>installer verify &lt;Number of CPUSE Package&gt; member_ids all</pre> Example: <pre>[Global] HostName-ch01-01 &gt; installer verify 2 member_ids all ... .. Update Service Engine +-----+  Member ID   Status        +-----+  1_01 (local) Upgrade is     1_02        Upgrade is     1_03        Upgrade is     1_04        Upgrade is     1_05        Upgrade is     1_06        Upgrade is     1_07        Upgrade is     1_08        Upgrade is    +-----+ [Global] HostName-ch01-01 &gt;</pre>

**Step 9 - On the Security Group, upgrade the Security Group Members in the Logical Group "A"**

Step	Instructions
A	Connect in one of these ways: <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" <b>through the console.</b></li> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" <b>over SSH.</b></li> </ul>
B	Go to the context of one of the Security Group Members in the Logical Group "A": <pre data-bbox="352 636 1458 701">member &lt;Member ID&gt;</pre> Example: <pre data-bbox="352 748 1458 813">member 1_1</pre>
C	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre data-bbox="352 931 1458 996">expert</pre>
D	Set the Security Group Members in the Logical Group "A" to the state "DOWN": <pre data-bbox="352 1077 1458 1142">g_clusterXL_admin -b &lt;SGM IDs in Group "A"&gt; down</pre> Example: <pre data-bbox="352 1189 1458 1290">[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_1-1_4 down</pre>
E	Go from the Expert mode to Gaia gClish: <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run:               <pre data-bbox="432 1435 1458 1500">gclish</pre> </li> <li>▪ If your default shell is <code>/etc/gclish</code> (Gaia gClish), then run:               <pre data-bbox="432 1547 1458 1612">exit</pre> </li> </ul>

Step	Instructions
F	<p>Upgrade the Security Group Members in the Logical Group "A":</p> <pre>installer upgrade [<b>Press the Tab key</b>]</pre> <pre>installer upgrade &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre> <p><b>Example:</b></p> <pre>[Global] HostName-ch01-01 &gt; installer upgrade 2 member_ids 1_1-1_4 ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+-----+  1_01 (local) Package is ready for installation            1_02         Package is ready for installation            1_03         Package is ready for installation            1_04         Package is ready for installation           +-----+-----+ The machines (1_02,1_02,1_03,1_04) will automatically reboot after upgrade. Do you want to continue? ([y]es / [n]o) <b>y</b> [Global] HostName-ch01-01 &gt;</pre>
G	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>■ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>exit</pre> </li> <li>■ If your default shell is <code>/etc/gclish</code> (Gaia gClish), then run: <pre>expert</pre> </li> </ul>
H	<p>Monitor the Security Group Members in the Logical Group "A" until they boot:</p> <pre>asg monitor</pre> <p> <b>Important</b> - By design, these Security Group Members boot into the "Down" state because these Critical Devices report their state as "problem" (run the "cphaprob state" command):</p> <ul style="list-style-type: none"> <li>■ Fullsync</li> <li>■ during_upgrade</li> <li>■ DSD</li> </ul>

**Step 10 - On the Security Group, run the 'sp\_upgrade' script on the Security Group Members in the Logical Group "A"**

Step	Instructions
A	Connect to one of the Security Group Members in the Logical Group "A" <b>through the console.</b>
B	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre data-bbox="352 528 1458 595">expert</pre>
C	Run the upgrade script and follow the steps below: <pre data-bbox="352 674 1458 741">sp_upgrade</pre>

## Step 11 - On the Security Group, install the required critical Hotfix on the Security Group Members in the Logical Group "A"

**Warning** - This step applies only if Check Point Support or R&D explicitly instructed you to install a **specific** Hotfix on your **specific** Security Group in the middle of the upgrade.

For example, your Security Group might require a specific hotfix or a Jumbo Hotfix Accumulator Take to resolve a specific issue.

You are still connected to one of the Security Group Members in the Logical Group "A" and you are still working in the Expert mode.

Step	Instructions
A	<p>Back up the current <code>\$SMODIR/bin/sp_upgrade</code> script to your home directory:</p> <pre>cp -v \$SMODIR/bin/sp_upgrade ~</pre> <pre>ls -l ~/sp_upgrade</pre>
B	Transfer the CPUSE package for this Hotfix to the Security Group (into some directory, for example <code>/var/log/</code> ).
C	<p>Go from the Expert mode to Gaia gClish:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>gclish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>exit</pre> </li> </ul>
D	<p>Import the CPUSE package from the hard disk:</p> <pre>installer import local /&lt;Full Path&gt;/&lt;Name of the CPUSE Offline Package&gt;</pre>
E	<p>Show the imported CPUSE packages:</p> <pre>show installer packages imported</pre>
F	<p>Make sure the imported CPUSE package can be installed on this Security Group:</p> <pre>installer verify [<b>Press Tab</b>]</pre> <pre>installer verify &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre>

Step	Instructions
G	Install the CPUSE package on the Security Group Members in the Logical Group "A": <pre data-bbox="352 320 1458 488">installer install [<b>Press the Tab key</b>]</pre> <pre data-bbox="352 389 1458 488">installer install &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre>
H	Go from Gaia gClish to the Expert mode: <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run:               <pre data-bbox="432 629 1458 696">exit</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run:               <pre data-bbox="432 741 1458 808">expert</pre> </li> </ul>
I	Go to your home directory: <pre data-bbox="352 887 1458 954">cd ~</pre> <pre data-bbox="352 954 1458 1021">pwd</pre>
J	Continue the upgrade procedure: <pre data-bbox="352 1095 1458 1162">./sp_upgrade</pre>

**Step 12 - In SmartConsole, change the version of the Security Gateway object**

- Note** - This step applies only to a Security Group in the Gateway mode. In the VSX mode, you changed the object version earlier with the "vsx\_util upgrade" command.

Step	Instructions
A	Connect with SmartConsole to the Management Server that manages this Security Group.
B	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
C	Double-click the Security Gateway object for this Security Group.
D	In the left tree, click <b>General</b> .
E	In the <b>Version</b> field, select <b>R81.20</b> .
F	Click <b>OK</b> .
G	Publish the session (do <b>not</b> install the policy).
H	In the 'sp_upgrade' shell script session, enter <b>y</b> or <b>yes</b> to confirm.

**Step 13 - On the Management Server, install the policy with the API command**

- i Important** - This step applies only to a Security Group in the Gateway mode. In the VSX mode, the "vsx\_util upgrade" command installed the required policy earlier.

Step	Instructions
A	Connect to the command line on the Management Server.
B	Go to the Expert mode: <pre>expert</pre>
C	<p>Run the "install-policy" API (see the <a href="#">Check Point Management API Reference</a> - search for <i>install-policy</i>).</p> <p>On a <b>Security Management Server</b>, run:</p> <pre>mgmt_cli -d "SMC User" --format json install-policy policy-package &lt;Name of Policy Package&gt; --sync false targets &lt;Name of Security Gateway Object&gt; prepare-only true [--port &lt;Apache Gaia Port&gt;]</pre> <p><b>i Notes:</b></p> <ul style="list-style-type: none"> <li>▪ "SMC User" is a mandatory name of the Domain.</li> <li>▪ The default Apache Gaia port on the Management Server is 443. If you configured a different port, you must specify it explicitly in the syntax. To see the configured port, run this command in the Expert mode:  <pre>api status   grep "APACHE Gaia Port"</pre> </li> <li>▪ This API prompts you to log in. Use the Management Server's administrator credentials.</li> </ul> <p><b>Example:</b></p> <pre>mgmt_cli -d "SMC User" --format json install-policy policy-package MyPolicyPackage --sync false targets MySecurityGroup prepare-only true --port 443</pre>



Step	Instructions
	<p>On a <b>Multi-Domain Server</b>, run:</p> <pre data-bbox="352 277 1458 539">mgmt_cli -d "&lt;IP Address or Name of Domain Management Server that manages this Security Gateway Object&gt;" --format json install-policy policy-package &lt;Name of Policy Package&gt; --sync false targets &lt;Name of Security Gateway Object&gt; prepare-only true [--port &lt;Apache Gaia Port&gt;]</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>▪ The default Apache Gaia port on the Management Server is 443. If you configured a different port, you must specify it explicitly in the syntax. To see the configured port, run this command in the Expert mode: <pre data-bbox="496 779 1458 842">api status   grep "APACHE Gaia Port"</pre> </li> <li>▪ This API prompts you to log in. Use the Domain Management Server's administrator credentials.</li> </ul> <p><b>Example:</b></p> <pre data-bbox="352 999 1458 1137">mgmt_cli -d "MyDomainServer" --format json install-policy policy-package MyPolicyPackage --sync false targets MySecurityGroup prepare-only true --port 443</pre>
D	In the 'sp_upgrade' shell script session, enter <b>y</b> or <b>yes</b> to confirm.

#### Step 14 - On the Security Group, confirm the activation of Security Group Members (Multi-Version Cluster mode) in the Logical Group "A"

In the 'sp\_upgrade' shell script session, enter **y** or **yes** to activate the Security Group Members that were upgraded in the Multi-Version Cluster mode.

**Note** - If the SSH session closed, connect again and run:

```
sp_upgrade --continue
```

**Step 15 - On the Security Group, change the state of Security Group Members in the Logical Group "B" to Down**

- i Important** - In the Multi-Version Cluster mode, it is not necessary to choose all of the remaining Security Group Members that you did not upgrade yet. You can repeat the previous steps for different logical groups of Security Group Members until you upgrade all Security Group Members in the Security Group.

Step	Instructions
A	Connect in one of these ways: <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" through the console.</li> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" over SSH.</li> </ul>
B	Set the Security Group Members in the Logical Group "B" to the state "DOWN": <pre data-bbox="352 801 1458 864">g_clusterXL_admin -b &lt;SGM IDs in Group "B"&gt; down</pre> Example: <pre data-bbox="352 913 1458 1016">[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 2_1-2_4 down</pre>

**Step 16 - On the Security Group, upgrade the Security Group Members in the Logical Group "B"**

**Note** - It is not necessary to set the Security Group Members in the Logical Group "B" to the state "DOWN", because the 'sp\_upgrade' shell script already made this change.

Step	Instructions
A	Connect in one of these ways: <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" <b>through the console.</b></li> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" <b>over SSH.</b></li> </ul>
B	Go to the context of one Security Group Members in the Logical Group "B": <pre data-bbox="352 712 1458 775">member &lt;Member ID&gt;</pre> Example: <pre data-bbox="352 824 1458 887">member 1_5</pre>
C	If your default shell is /bin/bash (the Expert mode), then go to Gaia gClish: <pre data-bbox="352 965 1458 1028">gclish</pre>
D	Upgrade the Security Group Members in the Logical Group "B": <pre data-bbox="352 1115 1458 1178">installer upgrade [<b>Press the Tab key</b>]</pre> <pre data-bbox="352 1189 1458 1274">installer upgrade &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "B"&gt;</pre> Example: <pre data-bbox="352 1335 1458 1711">[Global] HostName-ch01-01 &gt; installer upgrade 2 member_ids 1_5-1_8 ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+  1_05 (local) Package is ready for installation            1_06         Package is ready for installation            1_07         Package is ready for installation            1_08         Package is ready for installation           +-----+ The machines (1_05,1_06,1_07,1_08) will automatically reboot after upgrade. Do you want to continue? ([y]es / [n]o) <b>y</b> [Global] HostName-ch01-01 &gt;</pre>

Step	Instructions
E	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run:           <pre>exit</pre> </li> <li>▪ If your default shell is <code>/etc/gclish</code> (Gaia gClish), then run:           <pre>expert</pre> </li> </ul>
F	<p>Monitor the Security Group Members in the Logical Group "B" until they boot:</p> <pre>asg monitor</pre>

**Step 17 - On the Security Group, confirm the upgrade of the Security Group Members in the Logical Group "B"**

Step	Instructions
A	<p>Connect to Security Group Members in the Logical Group "B", and run in the Expert mode):</p> <pre>sp_upgrade</pre>
B	<p>In the 'sp_upgrade' shell script session, enter <b>y</b> or <b>yes</b> to confirm.</p>

## Step 18 - On the Security Group, install the required critical Hotfix on the Security Group Members in the Logical Group "B"

**Warning** - This step applies only if Check Point Support or R&D explicitly instructed you to install a **specific** Hotfix on your **specific** Security Group in the middle of the upgrade.

For example, your Security Group might require a specific hotfix or a Jumbo Hotfix Accumulator Take to resolve a specific issue.

You are still connected to one of the Security Group Members in the Logical Group "A" and you are still working in the Expert mode.

Step	Instructions
A	<p>Back up the current <code>\$SMODIR/bin/sp_upgrade</code> script to your home directory:</p> <pre>cp -v \$SMODIR/bin/sp_upgrade ~</pre> <pre>ls -l ~/sp_upgrade</pre>
B	Transfer the CPUSE package for this Hotfix to the Security Group (into some directory, for example <code>/var/log/</code> ).
C	<p>Go from the Expert mode to Gaia gClish:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>gclish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>exit</pre> </li> </ul>
D	<p>Import the CPUSE package from the hard disk:</p> <pre>installer import local /&lt;Full Path&gt;/&lt;Name of the CPUSE Offline Package&gt;</pre>
E	<p>Show the imported CPUSE packages:</p> <pre>show installer packages imported</pre>
F	<p>Make sure the imported CPUSE package can be installed on this Security Group:</p> <pre>installer verify [<b>Press Tab</b>]</pre> <pre>installer verify &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre>

Step	Instructions
G	<p>Install the CPUSE package on the Security Group Members in the Logical Group "A":</p> <pre>installer install [<b>Press the Tab key</b>]</pre> <pre>installer install &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre>
H	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>exit</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>expert</pre> </li> </ul>
I	<p>Go to your home directory:</p> <pre>cd ~</pre> <pre>pwd</pre>
J	<p>Continue the upgrade procedure:</p> <pre>./sp_upgrade</pre>

### Step 19 - In SmartConsole, install the policy

Step	Instructions
A	Connect with SmartConsole to the Management Server that manages this Security Group.
B	<p>Install the applicable Access Control policy on the Security Gateway object for this Security Group.</p> <p>If this Security Group is configured in the VSX mode, you must install the applicable Access Control policy on each Virtual System.</p>
C	On the Security Group, in the 'sp_upgrade' shell script session, enter <b>y</b> or <b>yes</b> to confirm.

**Step 20 - On the Security Group, make sure the upgrade was successful**


Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>
C	Run these commands: <pre>asg diag verify</pre> <pre>hcp -m all -r all</pre>

# Upgrading Maestro Environment - Minimum Downtime

This section describes the steps for upgrading a Maestro environment (the Quantum Maestro Orchestrators and the Security Groups) with Minimum Downtime.

This procedure supports only these upgrade paths for Security Groups:

- from R81.10 to R81.20
- from R81 to R81.20
- from R80.30SP to R81.20
- from R80.20SP to R81.20

 **Best Practice** - To upgrade from versions R81 or higher, we recommend ["Upgrading Maestro Environment - Zero Downtime" on page 453](#).

 **Important** - See these rollback procedures:

- ["Rolling Back a Failed Upgrade of a Maestro Orchestrator" on page 507](#)
- ["Rolling Back a Failed Upgrade of a Security Group - After Partial Upgrade" on page 510](#)
- ["Rolling Back a Failed Upgrade of a Security Group - Zero Downtime" on page 513](#)
- ["Rolling Back a Failed Upgrade of a Security Group - Minimum Downtime" on page 521](#).



**Important Notes for Quantum Maestro Orchestrators:**

- We recommend to schedule a maintenance window for all Orchestrators on all sites.
- The major software version on the Orchestrators must be equal to or higher than the major software version on the managed Security Group (PMTR-86785).
- This procedure **keeps** the current configuration on the Orchestrators.
- Upgrade all Orchestrators and only then upgrade the Security Groups.
- Upgrade one Orchestrator at a time.
- In a Dual Site environment:

**Procedure**

1. Upgrade the Orchestrators on the Standby Site (Site 2)
2. Initiate a fail-over in each Security Group from the non-upgraded Active Site (Site 1) to the upgraded Standby Site (Site 2):

- a. Connect to the command line on each Security Group.
- b. If your default shell is Gaia gClish, then go to the Expert mode:

```
expert
```

- c. Initiate a fail-over:

```
chassis_admin -c <ID of Active Site> down
```

```
chassis_admin -c <ID of Former Active Site> up
```

3. Upgrade the Orchestrators on the new Standby Site (Site 1).

## Important Notes for Security Groups:

- Before you upgrade the Security Groups, you must upgrade the Management Server that manages the Security Groups.  
See the [R81.20 Installation and Upgrade Guide](#).
- This procedure applies to Security Groups in the Gateway mode and the VSX mode.  
In VSX mode, you must run all the commands in the context of VS0.
- **During the upgrade process, it is:**
  - **Forbidden to install policy on the Security Group, unless the upgrade procedure explicitly shows how to do it.**
  - **Forbidden to reboot Security Group Members, unless the upgrade procedure explicitly shows how to do it.**
  - **Forbidden to change the configuration of the Security Group and its Security Group Members.**
  - **Forbidden to install Hotfixes on the Security Group Members, unless Check Point Support or R&D explicitly instructs you to do so.**
  - **Forbidden to install the Jumbo Hotfix Accumulator on the Security Group Members, unless Check Point Support or R&D explicitly instructs you to do so.**
- To prevent down time, do **not** upgrade all the Security Group Members in a specific Security Group at the same time.
- In this upgrade procedure, you divide all Security Group Members in a specific Security Group into two or more logical groups.  
In the procedure below, we use **two** logical groups denoted below as "A" and "B".  
You upgrade one logical group of the Security Group Members at one time.  
The other logical group(s) of the Security Group Members continues to handle traffic.  
Each logical group should contain the same number of Security Group Members - as close as possible.

### Examples

Environment	Description
Single Site	<ul style="list-style-type: none"> <li>• There are 8 Security Group Members in the Security Group.</li> <li>• The Logical Group "A" contains Security Group Members from 1_1 to 1_4.</li> <li>• The Logical Group "B" contains Security Group Members from 1_5 to 1_8.</li> </ul>

Environment	Description
Single Site	<ul style="list-style-type: none"><li>• There are 5 Security Group Members in the Security Group.</li><li>• The Logical Group "A" contains Security Group Members from 1_1 to 1_3.</li><li>• The Logical Group "B" contains Security Group Members from 1_4 to 1_5.</li></ul>
Dual Site	<ul style="list-style-type: none"><li>• There are 4 Security Group Members in the Security Group (on each Site).</li><li>• The Logical Group "A" contains Security Group Members on Site 1 from 1_1 to 1_4.</li><li>• The Logical Group "B" contains Security Group Members on Site 2 from 2_1 to 2_4.</li></ul>



**Required software packages:**

Download the required software packages from [sk177624](#):

1. The required Take of the Jumbo Hotfix Accumulator
2. The required CPUSE Deployment Agent for Scalable Platforms
3. The R81.20 Upgrade Package for Scalable Platforms

**Workflow:**


1. On the Management Server - Upgrade to the required version that can manage an R81.20 Security Group (see [sk113113](#)).
2. On the Orchestrator - Upgrade to R81.20 and install the R81.20 Jumbo Hotfix Accumulator.
3. On the Security Group - Run the Pre-Upgrade Verifier to make sure it is possible to upgrade the Security Group.
4. On the Security Group R80.30SP in the Gateway mode with the Mobile Access Software Blade - Back up the Mobile Access configuration files.
5. On the Security Group - Install the required Jumbo Hotfix Accumulator (using two logical groups of Security Group Members).
6. On the Security Group - Install the required CPUSE Deployment Agent package for the Security Group.
7. On the Security Group - Upgrade to R81.20 (using two logical groups of Security Group Members).
8. In SmartConsole, install the policy.
9. On the Security Group in the Gateway mode with the Mobile Access Software Blade - Restore the Mobile Access configuration.

**Procedure:**

**Step 1 - Upgrade the Management Server**

Upgrade the Management Server to the required version that can manage an R81.20 Security Group (see the [R81.20 Release Notes](#)).

## Step 2 - On the Quantum Maestro Orchestrator, upgrade to R81.20 and install the R81.20 Jumbo Hotfix Accumulator


Step	Instructions
A	If the Orchestrator runs R80.20SP, then install the <a href="#">R80.20SP Jumbo Hotfix Accumulator</a> Take 326 or higher on the Orchestrator.
B	In the Orchestrator's Gaia Portal, from the left tree, go to <b>Upgrades (CPUSE) &gt; Status and Actions</b> .
C	In the top right section, click <b>Import Package</b> .
D	Click <b>Browse</b> .
E	Go to the folder where you put the <i>R81.20 Upgrade Package for Scalable Platforms</i> from <a href="#">sk177624</a> .
F	Select the <i>R81.20 Upgrade Package for Scalable Platforms</i> .
G	Click <b>Open</b> .
H	Click <b>Import</b> .
I	Above the list of packages, near the help icon, click the filter button that currently says " <b>Showing Recommended packages</b> " and click " <b>All</b> ". The filter must change to " <b>Showing All packages</b> ".
J	Right-click the imported R81.20 CPUSE Offline Package and click <b>Verify Update</b> .
K	Right-click the imported R81.20 CPUSE Offline Package and click <b>Upgrade</b> .  <b>Important:</b> <ul style="list-style-type: none"> <li>▪ Make sure to click <b>Upgrade</b> (do <b>not</b> click <b>Install</b> because it performs a clean install, which deletes all configuration and reboots all Security Group Members).</li> <li>▪ At the end of the upgrade, the Orchestrator reboots automatically.</li> </ul>
L	Install the Recommended Take of the <a href="#">R81.20 Jumbo Hotfix Accumulator</a> . See " <i>Installing and Uninstalling a Hotfix on Quantum Maestro Orchestrators</i> " on page 432.


**Step 3 - On the Security Group, run the Pre-Upgrade Verifier to make sure it is possible to upgrade the Security Group**

Step	Instructions
A	Download this script to your computer: <a href="https://supportcenter.checkpoint.com/file_download?id=124062">https://supportcenter.checkpoint.com/file_download?id=124062</a>
B	Copy this script from your computer to the Security Group. Copy the script to some directory (for example, /var/log/).
C	Connect to the command line on the Security Group.
D	Log in to the Expert mode.
E	Run these commands in the order listed below: <pre>cd /var/log/ chmod +x pre_upgrade_verifier.sh ./pre_upgrade_verifier.sh</pre>



**Step 4 - On the Management Server, change the version of the VSX Gateway object**

 **Important** - This step applies only when the Security Group works in the VSX mode.

Step	Instructions
A	Download the script " <code>vsx_util_upgrade_verifier.sh</code> " to your computer: <a href="https://supportcenter.checkpoint.com/file_download?id=123847">https://supportcenter.checkpoint.com/file_download?id=123847</a>
B	Copy this script from your computer to the Management Server that manages this Security Group in VSX mode. Copy the script to some directory (for example, <code>/var/log/</code> ).
C	Connect to the command line on the Management Server.
D	Log in to the Expert mode.
E	On a Multi-Domain Server, go to the context of the applicable Domain Management Server that manages this Security Group in VSX mode: <pre data-bbox="352 887 1460 949" style="border: 1px solid black; padding: 5px;">mdsend &lt;IP Address or Name of Domain Management Server&gt;</pre>
F	Upgrade the version of a VSX Gateway object in the management database: <p> <b>Warning</b> - Make sure to close all SmartConsole clients connected to this Management Server.</p> <pre data-bbox="352 1122 1460 1184" style="border: 1px solid black; padding: 5px;">vsx_util upgrade [-s &lt;Mgmt Server&gt;] [-u &lt;UserName&gt;]</pre> For more information, see the <a href="#">R81.20 VSX Administration Guide</a> > Chapter "Command Line Reference" > Section " <code>vsx_util</code> ".
G	Log in with the Management Server administrator credentials.
H	Select the VSX Gateway object for this Security Group.
I	Change the version to <b>R81.20</b> .
J	Run the script you copied earlier to make sure the " <code>vsx_util upgrade</code> " command made the required changes. Run the commands in the order listed below: <pre data-bbox="352 1648 1460 1877" style="border: 1px solid black; padding: 5px;">cd /var/log/ chmod +x vsx_util_upgrade_verifier.sh ./vsx_util_upgrade_verifier.sh &lt;Name of the VSX Gateway object&gt; R81.20</pre>

**Step 5 - On the Security Group R80.30SP, back up the Mobile Access configuration**

If you upgrade a Security Group **R80.30SP** in the Gateway mode with the Mobile Access Software Blade enabled, then back up the Mobile Access configuration files on the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>
C	Create a directory for the Mobile Access configuration files: <pre>mkdir /var/log/MAB</pre>
D	Copy the Mobile Access configuration files to the new directory. For the list of the files you must collect, see <a href="#">sk175087</a> . <pre>cp -v /&lt;Path&gt;/&lt;File&gt; /var/log/MAB/&lt;Path&gt;-&lt;File&gt;</pre> Example: <pre>cp -v \$CVPNDIR/conf/ReverseProxy_conf/ReverseProxyConf.xml /var/log/MAB/CVPNDIR-conf-ReverseProxy_conf-ReverseProxyConf.xml</pre>
E	Compress the directory with the Mobile Access configuration files: <pre>tar cvf /var/log/MAB.tar /var/log/MAB</pre>
F	Transfer the TAR file from the Security Group to your computer.

**Step 6 - On the Security Group, disable the SMO Image Cloning feature**

**Note** - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is <code>/bin/bash</code> (Expert mode), then go to Gaia gClish: <pre>gclish</pre>
C	Examine the state of the SMO Image Cloning feature: <pre>show smo image auto-clone state</pre>
D	Disable the SMO Image Cloning feature, if it is enabled: <pre>set smo image auto-clone state off</pre>
E	Examine the state of the SMO Image Cloning feature: <pre>show smo image auto-clone state</pre>

**Step 7 - On the Security Group, install the required Take of the Jumbo Hotfix Accumulator for the current version****Important:**

- You must install the required Jumbo Hotfix Accumulator on **all** Security Group Members in the Security Group.
- Before you install Jumbo Hotfix Accumulator, this procedure requires you to disable the SMO Image Cloning feature on the Security Group. Do **not** enable the SMO Image Cloning feature on the Security Group until the upgrade procedure instructs you to do so.

Follow these instructions to install the required Jumbo Hotfix Accumulator from [sk177624](#):

*"Installing a Hotfix Package on Security Group Members" on page 436*

**Step 8 - On the Security Group, upgrade the CPUSE Deployment Agent**

**Important** - You must do this step even if you upgrade again after a rollback procedure on the Security Group.


Step	Instructions
A	Transfer the CPUSE Deployment Agent package for Scalable Platforms (from <a href="#">sk177624</a> ) to the Security Group (into some directory, for example /var/log/).
B	Connect to the command line on the Security Group.
C	If your default shell is /etc/gclish (Gaia gClish), then go to the Expert mode: <pre>expert</pre>
D	Make sure the CPUSE Deployment Agent package exists: <pre>ls -l /&lt;Full Path&gt;/&lt;Name of CPUSE Deployment Agent Package&gt;</pre>
E	Upgrade the CPUSE Deployment Agent: <pre>update_sp_da /&lt;Full Path&gt;/&lt;Name of CPUSE Deployment Agent Package&gt;</pre> <p>Example:</p> <pre>update_sp_da /var/log/DeploymentAgent_XXXXXXXXXX.tgz</pre>
F	Go from the Expert mode to Gaia gClish: <ul style="list-style-type: none"> <li>▪ If your default shell is /bin/bash (the Expert mode), then run:               <pre>gclish</pre> </li> <li>▪ If your default shell is /etc/gclish (Gaia gClish), then run:               <pre>exit</pre> </li> </ul>
G	Make sure all Security Group Members have the same build of the CPUSE Deployment Agent: <pre>show installer status build</pre>

Step 9 - On the Security Group, import the R81.20 upgrade package

Step	Instructions
A	<p>Make sure you have the applicable CPUSE Offline package: R81.20 Upgrade Package for Scalable Platforms</p>
B	<p>Transfer the CPUSE Offline package to the Security Group (into some directory, for example <code>/var/log/</code>).</p>
C	<p>Connect to the command line on the Security Group.</p>
D	<p>If your default shell is <code>/bin/bash</code> (the Expert mode), then go to Gaia gClish:</p> <pre data-bbox="352 640 1460 705">gclish</pre>
E	<p>Import the CPUSE Offline package from the hard disk:</p> <pre data-bbox="352 786 1460 887">installer import local /&lt;Full Path&gt;/&lt;Name of the CPUSE Offline Package&gt;</pre> <p>Example:</p> <pre data-bbox="352 943 1460 1043">[Global] HostName-ch01-01 &gt; installer import local /var/log/Check_Point_R81.20_SP_Install_and_Upgrade.tar</pre>
F	<p>Show the imported CPUSE packages:</p> <pre data-bbox="352 1122 1460 1187">show installer packages imported</pre>
G	<p>Make sure the imported CPUSE package can be installed on this Security Group:</p> <pre data-bbox="352 1312 1460 1469">installer verify [<b>Press Tab</b>]</pre> <pre data-bbox="352 1379 1460 1469">installer verify &lt;Number of CPUSE Package&gt; member_ids all</pre> <p>Example:</p> <pre data-bbox="352 1525 1460 1984">[Global] HostName-ch01-01 &gt; installer verify 2 member_ids all ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+-----+  1_01 (local) Upgrade is allowed.                          1_02         Upgrade is allowed.                          1_03         Upgrade is allowed.                          1_04         Upgrade is allowed.                          1_05         Upgrade is allowed.                          1_06         Upgrade is allowed.                          1_07         Upgrade is allowed.                          1_08         Upgrade is allowed.                         +-----+-----+ [Global] HostName-ch01-01 &gt;</pre>

## Step 10 - On the Security Group, upgrade the Security Group Members in the Logical Group "A"

Step	Instructions
A	Connect in one of these ways: <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" <b>through the console.</b></li> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" <b>over SSH.</b></li> </ul>
B	Go to the context of one of the Security Group Members in the Logical Group "A": <pre data-bbox="352 636 1458 701">member &lt;Member ID&gt;</pre> Example: <pre data-bbox="352 748 1458 813">member 1_1</pre>
C	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre data-bbox="352 931 1458 996">expert</pre>
D	Set the Security Group Members in the Logical Group "A" to the state "DOWN": <pre data-bbox="352 1077 1458 1142">g_clusterXL_admin -b &lt;SGM IDs in Group "A"&gt; down</pre> Example: <pre data-bbox="352 1189 1458 1288">[Expert@HostName-ch0x-0x:0]# g_clusterXL_admin -b 1_1-1_4 down</pre>
E	Go from the Expert mode to Gaia gClish: <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run:               <pre data-bbox="432 1435 1458 1500">gclish</pre> </li> <li>▪ If your default shell is <code>/etc/gclish</code> (Gaia gClish), then run:               <pre data-bbox="432 1547 1458 1612">exit</pre> </li> </ul>

Step	Instructions
F	<p>Upgrade the Security Group Members in the Logical Group "A":</p> <pre>installer upgrade [<b>Press the Tab key</b>]</pre> <pre>installer upgrade &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre> <p><b>Example:</b></p> <pre>[Global] HostName-ch01-01 &gt; installer upgrade 2 member_ids 1_1-1_4 ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+-----+  1_01 (local) Package is ready for installation            1_02         Package is ready for installation            1_03         Package is ready for installation            1_04         Package is ready for installation           +-----+-----+ The machines (1_02,1_02,1_03,1_04) will automatically reboot after upgrade. Do you want to continue? ([y]es / [n]o) <b>y</b> [Global] HostName-ch01-01 &gt;</pre>
G	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>■ If your default shell is /bin/bash (the Expert mode), then run: <pre>exit</pre> </li> <li>■ If your default shell is /etc/gclish (Gaia gClish), then run: <pre>expert</pre> </li> </ul>
H	<p>Monitor the Security Group Members in the Logical Group "A" until they boot:</p> <pre>asg monitor</pre> <p> <b>Important</b> - By design, these Security Group Members boot into the "Down" state because these Critical Devices report their state as "problem" (run the "cphaprob state" command):</p> <ul style="list-style-type: none"> <li>■ Fullsync</li> <li>■ during_upgrade</li> <li>■ DSD</li> </ul>

**Step 11 - Optional. On the Security Group, install the required Hotfix on the Security Group Members in the Logical Group "A"**

**Warning** - This step applies only if Check Point Support or R&D explicitly instructed you to install a **specific** Hotfix on your **specific** Security Group in the middle of the upgrade.

For example, your Security Group might require a specific hotfix or a Jumbo Hotfix Accumulator Take to resolve a specific issue.

You are still connected to one of the Security Group Members in the Logical Group "A" and you are still working in the Expert mode.

Step	Instructions
A	<p>Back up the current <code>\$SMODIR/bin/sp_upgrade</code> script to your home directory:</p> <pre data-bbox="352 734 1461 864">cp -v \$SMODIR/bin/sp_upgrade ~ ls -l ~/sp_upgrade</pre>
B	<p>Transfer the CPUSE package for this Hotfix to the Security Group (into some directory, for example <code>/var/log/</code>).</p>
C	<p>Go from the Expert mode to Gaia gClish:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre data-bbox="432 1122 1461 1182">gclish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre data-bbox="432 1234 1461 1294">exit</pre> </li> </ul>
D	<p>Import the CPUSE package from the hard disk:</p> <pre data-bbox="352 1379 1461 1480">installer import local /&lt;Full Path&gt;/&lt;Name of the CPUSE Offline Package&gt;</pre>
E	<p>Show the imported CPUSE packages:</p> <pre data-bbox="352 1559 1461 1619">show installer packages imported</pre>
F	<p>Make sure the imported CPUSE package can be installed on this Security Group:</p> <pre data-bbox="352 1749 1461 1906">installer verify [<b>Press Tab</b>] installer verify &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre>




Step	Instructions
G	<p>Install the CPUSE package on the Security Group Members in the Logical Group "A":</p> <pre>installer install [Press the Tab key]</pre> <pre>installer install &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "A"&gt;</pre>
H	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>exit</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>expert</pre> </li> </ul>
I	<p>Go to your home directory:</p> <pre>cd ~</pre> <pre>pwd</pre>
J	<p>Continue the upgrade procedure:</p> <pre>./sp_upgrade</pre>

**Step 12 - On the Security Group, run the 'sp\_upgrade' script on the Security Group Members in the Logical Group "A"**

Step	Instructions
A	<p>Connect to one of the Security Group Members in the Logical Group "A" <b>through the console.</b></p>
B	<p>If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode:</p> <pre>expert</pre>
C	<p>Run the upgrade script and follow the steps below:</p> <pre>sp_upgrade</pre>

**Step 13 - In SmartConsole, edit the version of the Security Gateway object**

-  **Note** - This step applies only to a Security Group in the Gateway mode. In the VSX mode, you changed the object version earlier with the "vsx\_util upgrade" command.

Step	Instructions
A	Connect with SmartConsole to the Management Server that manages this Security Group.
B	From the left navigation panel, click <b>Gateways &amp; Servers</b> .
C	Double-click the Security Gateway object for this Security Group.
D	In the left tree, click <b>General</b> .
E	In the <b>Version</b> field, select <b>R81.20</b> .
F	Click <b>OK</b> .
G	Publish the session (do <b>not</b> install the policy).
H	In the 'sp_upgrade' shell script session, enter <b>y</b> or <b>yes</b> to confirm.

**Step 14 - On the Management Server, install the policy using the API command**

- i Important** - This step applies only to a Security Group in the Gateway mode. In the VSX mode, the "vsx\_util upgrade" command installed the required policy earlier.

Step	Instructions
A	Connect to the command line on the Management Server.
B	Go to the Expert mode: <pre data-bbox="352 539 1460 607">expert</pre>
C	<p>Run the "install-policy" API (see the <a href="#">Check Point Management API Reference</a> - search for <i>install-policy</i>).</p> <p>On a <b>Security Management Server</b>, run:</p> <pre data-bbox="352 797 1460 981">mgmt_cli -d "SMC User" --format json install-policy policy-package &lt;Name of Policy Package&gt; --sync false targets &lt;Name of Security Gateway Object&gt; prepare-only true [--port &lt;Apache Gaia Port&gt;]</pre> <p><b>i Notes:</b></p> <ul style="list-style-type: none"> <li>▪ "SMC User" is a mandatory name of the Domain.</li> <li>▪ The default Apache Gaia port on the Management Server is 443. If you configured a different port, you must specify it explicitly in the syntax. To see the configured port, run this command in the Expert mode:           <pre data-bbox="496 1261 1460 1328">api status   grep "APACHE Gaia Port"</pre> </li> <li>▪ This API prompts you to log in. Use the Management Server's administrator credentials.</li> </ul> <p><b>Example:</b></p> <pre data-bbox="352 1480 1460 1621">mgmt_cli -d "SMC User" --format json install-policy policy-package MyPolicyPackage --sync false targets MySecurityGroup prepare-only true --port 443</pre>

Step	Instructions
	<p>On a <b>Multi-Domain Server</b>, run:</p> <pre>mgmt_cli -d "&lt;IP Address or Name of Domain Management Server that manages this Security Gateway Object&gt;" --format json install-policy policy-package &lt;Name of Policy Package&gt; --sync false targets &lt;Name of Security Gateway Object&gt; prepare-only true [--port &lt;Apache Gaia Port&gt;]</pre> <p><b>Notes:</b></p> <ul style="list-style-type: none"> <li>The default Apache Gaia port on the Management Server is 443. If you configured a different port, you must specify it explicitly in the syntax. To see the configured port, run this command in the Expert mode: <pre>api status   grep "APACHE Gaia Port"</pre> </li> <li>This API prompts you to log in. Use the Domain Management Server's administrator credentials.</li> </ul> <p><b>Example:</b></p> <pre>mgmt_cli -d "MyDomainServer" --format json install-policy policy-package MyPolicyPackage --sync false targets MySecurityGroup prepare-only true --port 443</pre>
D	In the 'sp_upgrade' shell script session, enter <b>y</b> or <b>yes</b> to confirm.

### Step 15 - On the Security Group, confirm the cluster failover

In the 'sp\_upgrade' shell script session, enter **y** or **yes** to confirm the cluster failover from the Security Group Members in the Logical Group "B" to the Security Group Members in the Logical Group "A".

**Note** - If the SSH session closed, connect again and run:

```
sp_upgrade --continue
```

**Step 16 - On the Security Group, upgrade the Security Group Members in the Logical Group "B"**

**Note** - It is not necessary to set the Security Group Members in the Logical Group "B" to the state "DOWN", because the 'sp\_upgrade' shell script already made this change.

Step	Instructions
A	<p>Connect in one of these ways:</p> <ul style="list-style-type: none"> <li>▪ Connect to one of the Security Group Members in the Logical Group "B" <b>through the console.</b></li> <li>▪ Connect to one of the Security Group Members in the Logical Group "A" <b>over SSH.</b></li> </ul>
B	<p>Go to the context of one Security Group Members in the Logical Group "B":</p> <pre>member &lt;Member ID&gt;</pre> <p>Example:</p> <pre>member 1_5</pre>
C	<p>If your default shell is /bin/bash (the Expert mode), then go to Gaia gClish:</p> <pre>gclish</pre>
D	<p>Upgrade the Security Group Members in the Logical Group "B":</p> <pre>installer upgrade [<b>Press the Tab key</b>]</pre> <pre>installer upgrade &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "B"&gt;</pre> <p>Example:</p> <pre>[Global] HostName-ch01-01 &gt; installer upgrade 2 member_ids 1_5-1_8 ... .. Update Service Engine +-----+  Member ID    Status                                       +-----+-----+  1_05 (local) Package is ready for installation            1_06         Package is ready for installation            1_07         Package is ready for installation            1_08         Package is ready for installation           +-----+-----+ The machines (1_05,1_06,1_07,1_08) will automatically reboot after upgrade. Do you want to continue? ([y]es / [n]o) <b>y</b> [Global] HostName-ch01-01 &gt;</pre>

Step	Instructions
E	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"><li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>exit</pre></li><li>▪ If your default shell is <code>/etc/gclish</code> (Gaia gClish), then run: <pre>expert</pre></li></ul>
F	<p>Monitor the Security Group Members in the Logical Group "B" until they boot:</p> <pre>asg monitor</pre>

**Step 17 - Optional. On the Security Group, install the required Hotfix on the Security Group Members in the Logical Group "B"**

**Warning** - This step applies only if Check Point Support or R&D explicitly instructed you to install a **specific** Hotfix on your **specific** Security Group in the middle of the upgrade.

For example, your Security Group might require a specific hotfix or a Jumbo Hotfix Accumulator Take to resolve a specific issue.

If earlier you installed the specific Hotfix on the Security Group Members in the Logical Group "A", then you must install the same Hotfix on the Security Group Members in the Logical Group "B".

You are still connected to one of the Security Group Members in the Logical Group "B" and you are still working in the Expert mode.

Step	Instructions
A	<p>Back up the current <code>\$SMODIR/bin/sp_upgrade</code> script to your home directory:</p> <pre>cp -v \$SMODIR/bin/sp_upgrade ~</pre> <pre>ls -l ~/sp_upgrade</pre>
B	Transfer the CPUSE package for this Hotfix to the Security Group (into some directory, for example <code>/var/log/</code> ).
C	<p>Go from the Expert mode to Gaia gClish:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>gclish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>exit</pre> </li> </ul>
D	<p>Import the CPUSE package from the hard disk:</p> <pre>installer import local /&lt;Full Path&gt;/&lt;Name of the CPUSE Offline Package&gt;</pre>
E	<p>Show the imported CPUSE packages:</p> <pre>show installer packages imported</pre>

Step	Instructions
F	<p>Make sure the imported CPUSE package can be installed on this Security Group:</p> <pre>installer verify [Press Tab]</pre> <pre>installer verify &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "B"&gt;</pre>
G	<p>Install the CPUSE package on the Security Group Members in the Logical Group "B":</p> <pre>installer install [Press the Tab key]</pre> <pre>installer install &lt;Number of CPUSE Package&gt; member_ids &lt;SGM IDs in Group "B"&gt;</pre>
H	<p>Go from Gaia gClish to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>exit</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>expert</pre> </li> </ul>
I	<p>Go to your home directory:</p> <pre>cd ~</pre> <pre>pwd</pre>
J	<p>Continue the upgrade procedure:</p> <pre>./sp_upgrade</pre>

### Step 18 - On the Security Group, confirm the upgrade of the Security Group Members in the Logical Group "B"

In the 'sp\_upgrade' shell script session, enter **y** or **yes** to confirm the upgrade.



**Note** - If the SSH session closed, connect again and run:

```
sp_upgrade --continue
```



**Step 19 - In SmartConsole, install the policy**


Step	Instructions
A	Connect with SmartConsole to the Management Server that manages this Security Group.
B	Install the applicable Access Control policy on the Security Gateway object for this Security Group. If this Security Group is configured in the VSX mode, you must install the applicable Access Control policy on each Virtual System.
C	On the Security Group, in the 'sp_upgrade' shell script session, enter <b>y</b> or <b>yes</b> to confirm.

**Step 20 - On the Security Group, make sure the upgrade was successful**

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>
C	Run these commands: <pre>asg diag verify</pre> <pre>hcp -m all -r all</pre>

**Step 21 - On the Security Group, restore the Mobile Access configuration**

If you upgraded a Security Group **R80.30SP** in the Gateway mode with the Mobile Access Software Blade enabled, then to restore the Mobile Access configuration, you must manually merge the content of the backed up files into the existing files on the Security Group.

Step	Instructions
A	Connect to the command line on the Security Group.
B	If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then go to the Expert mode: <pre>expert</pre>
C	Edit the applicable files: <pre>vi /&lt;Path&gt;/&lt;File&gt;</pre> <p> <b>Important</b> - Do <b>not</b> copy the backed up files to the upgraded Security Group. The file syntax and content change between versions.</p>
D	Save the changes in the file and exit the editor.
E	Copy the modified file to all Security Group Members: <pre>asg_cp2blades /&lt;Path&gt;/&lt;File&gt;</pre> <p>Example:</p> <pre>asg_cp2blades \$CVPNDIR/conf/ReverseProxy_ conf/ReverseProxyConf.xml</pre>
F	Restart the Mobile Access services: <pre>cvpnrestart</pre>

# Rolling Back a Failed Upgrade of a Maestro Orchestrator

This section describes the steps for rolling back a failed upgrade of a Maestro Orchestrator to R81.20.

**Warning** - If after an upgrade of the Orchestrator to R81.20 you made changes in topology of Security Groups (added or removed Security Appliances, added or removed interfaces, changed settings of physical ports), then do **NOT** use this rollback procedure on the Orchestrator.

You must contact [Check Point Support](#) for assistance.

## Important:

- If you also upgraded Security Groups to R81.20, then **before** you revert the Orchestrator, you must revert all Security Groups.

See these rollback procedures:

- ["Rolling Back a Failed Upgrade of a Security Group - After Partial Upgrade" on page 510](#)
- ["Rolling Back a Failed Upgrade of a Security Group - Zero Downtime" on page 513](#)
- ["Rolling Back a Failed Upgrade of a Security Group - Minimum Downtime" on page 521.](#)
- This rollback procedure reverts the Orchestrator to the configuration prior to the upgrade (Gaia configuration, topology of Security Groups, configuration of physical ports, and so on).
- Perform this rollback procedure on one Orchestrator at a time.
- In a Dual Site environment:
  - Perform this rollback procedure on each Orchestrator on the Standby site.
  - Initiate the fail-over from the Active site to the Standby site.

Run this command in the Expert mode:

```
asg chassis_admin -c <ID of Active Site> down
```

- Perform this rollback procedure on each Orchestrator on the former Active site.

## Procedure for each Orchestrator:

Step	Instructions
1	Connect to the command line on the Orchestrator (in our example, "Orchestrator 1_1").

Step	Instructions
2	<p>If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then go to the Expert mode:</p> <pre>expert</pre>
3	<p>Stop the Orchestrator service:</p> <pre>orchd stop</pre>
4	<p>Go from the Expert mode to Gaia Clish:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (the Expert mode), then run: <pre>clish</pre> </li> <li>▪ If your default shell is <code>/etc/cli.sh</code> (Gaia Clish), then run: <pre>exit</pre> </li> </ul>
5	<p>Restore the Gaia snapshot, which was created automatically during the upgrade:</p> <pre>set snapshot revert</pre> <p>The Orchestrator automatically reboots and starts the revert. For more information, see the <a href="#">R81.20 Gaia Administration Guide</a> &gt; Chapter <i>Maintenance</i> &gt; Section <i>Snapshot Management</i>.</p>
6	<p>Wait for the reverted Orchestrator to boot.</p>
7	<p>Configure the same date and time settings on all other Orchestrators in your environment. For more information, see the <a href="#">R81.20 Gaia Administration Guide</a> &gt; Chapter <i>System Management</i> &gt; Section <i>Time</i>.</p>
8	<p>Make sure all Orchestrators in your environment can communicate with each other. Connect to the command line on the reverted Orchestrator (in our example, "1_1"). Send pings to other Orchestrator(s):</p> <ul style="list-style-type: none"> <li>▪ In a Single Site environment: <pre>ping 1_2</pre> </li> <li>▪ In a Dual Site environment: <pre>ping 1_2</pre> <pre>ping 2_1</pre> <pre>ping 2_2</pre> </li> </ul>

Step	Instructions
9	<p>Make sure the Security Group Members can pass traffic to each other:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode:           <pre>expert</pre> </li> <li>Examine the cluster state of the Security Group Members. On the SMO Security Group Member, run:           <pre>cphaprob state</pre> <p>The output must show that all Security Group Members are active.</p> </li> <li>Send pings between Security Group Members:           <ol style="list-style-type: none"> <li>Connect to one of the Security Group Members (in our example, we connect to the first one - "1_1"):               <pre>member 1_1</pre> </li> <li>On this Security Group Member, send ping to any other Security Group Member (in our example, we send pings to the second one - "1_2" / "2_2"):               <ul style="list-style-type: none"> <li>■ In a Single Site environment:                   <pre>ping 1_2</pre> </li> <li>■ In a Dual Site environment:                   <pre>ping 1_2</pre> <pre>ping 2_2</pre> </li> </ul> </li> </ol> </li> </ol>
10	<p>On each Security Group Member, make sure all links are up in the Security Group:</p> <ol style="list-style-type: none"> <li>Connect to the command line on the Security Group.</li> <li>Examine the state of links:           <pre>asg_if</pre> </li> </ol>

# Rolling Back a Failed Upgrade of a Security Group - After Partial Upgrade

This section describes the steps for rolling back a failed upgrade of a Security Group to R81.20.

This procedure supports only these downgrade paths for Security Groups:

- from R81.20 to R81
- from R81.20 to R81.10
- from R81.20 to R80.30SP
- from R81.20 to R80.20SP

**i Important** - Use this rollback procedure if you upgraded only **some (not all)** Security Group Members in the Security Group.

Step	Instructions
1	Connect to the command line on the Security Group.
2	If your default shell is <code>/bin/bash</code> (Expert mode), then go to the Gaia gClish: <pre>gclish</pre>
3	Disable the SMO Image Cloning feature: <p><b>i Note</b> - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.</p> <ol style="list-style-type: none"> <li>a. Examine the state of the SMO Image Cloning feature:               <pre>show smo image auto-clone state</pre> </li> <li>b. Disable the SMO Image Cloning feature, if it is enabled:               <pre>set smo image auto-clone state off</pre> </li> <li>c. Examine the state of the SMO Image Cloning feature:               <pre>show smo image auto-clone state</pre> </li> </ol>

Step	Instructions
4	<p>Go to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (Expert mode):           <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">exit</pre> </li> <li>▪ If your default shell is <code>/etc/gclish</code> (Gaia gClish):           <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">expert</pre> </li> </ul>
5	<p>Go to the context of one of the Security Group Members that were upgraded to R81.20:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">member 1_1</pre>
6	<p>Run the upgrade script with the "revert" parameter and follow the instructions on the screen:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">sp_upgrade --revert</pre>
7	<p>On each Security Group Member that was upgraded to R81.20, restore the Gaia automatic snapshot:</p> <ol style="list-style-type: none"> <li>a. Go to the context of each Security Group Member:       <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">member 1_2</pre> </li> <li>b. Go to Gaia Clish (do not use the Gaia gClish):       <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">clish</pre> </li> <li>c. Restore the Gaia automatic snapshot that was saved automatically before the upgrade.       <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">set snapshot revert AutoSnapShot_&lt;Original-Version&gt;_&lt;Take&gt;</pre> <p>Example:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">set snapshot revert AutoSnapShot_AutoSnapShot_R81_47</pre> </li> <li>d. Wait for the Security Group Member to complete the reboot.</li> <li>e. Repeat Steps a-d for the next Security Group Member that was upgraded.</li> </ol>
8	<p>Connect to the command line on the Security Group.</p>

Step	Instructions
9	<p>If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode:</p> <pre data-bbox="316 264 1460 331">expert</pre>
10	<p>Run the upgrade script with the <code>"revert"</code> parameter <b>again</b> and follow the instructions on the screen:</p> <pre data-bbox="316 450 1460 517">sp_upgrade --revert</pre>
11	<p>Make sure the downgrade was successful:</p> <pre data-bbox="316 595 1460 663">asg diag verify</pre>



# Rolling Back a Failed Upgrade of a Security Group - Zero Downtime

This section describes the steps to roll back a failed upgrade of a Security Group from R81.20 with Zero Downtime.


This section describes the steps for rolling back a failed upgrade of a Security Group to R81.20.

This procedure supports only these downgrade paths for Security Groups:


- from R81.20 to R81.10
- from R81.20 to R81

## Warnings:


- Multi-Version Cluster (Zero Downtime) downgrade from R81.20 to R81 is **not** supported if a Security Group has Bond interfaces in the 802.3ad (LACP) mode on Uplink ports (Known Limitation PMTR-88191).
- Before you follow the downgrade procedure, **revert** all changes in the topology you made after the upgrade procedure. For example, after the upgrade you added / removed interfaces, you changed the configuration of interfaces, you added / removed Security Group Members in the Security Group.

 **Important** - While the Security Group still contains Security Group Members that run the R81.20 version, you can only run the script "`sp_upgrade --revert`" on the R81.20 Security Group Members.

## Rolling Back If Only Some of the Security Group Members Were Upgraded

 **Important** - Use this rollback procedure if you upgraded only **some (not all)** Security Group Members in the Security Group.

Step	Instructions
1	Connect to the command line on the Security Group.
2	If your default shell is <code>/bin/bash</code> (Expert mode), then go to the Gaia gClish: <div style="border: 1px solid #ccc; padding: 5px; margin-top: 5px;"> <pre>gclish</pre> </div>

Step	Instructions
3	<p>Disable the SMO Image Cloning feature:</p> <p> <b>Note</b> - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.</p> <p>a. Examine the state of the SMO Image Cloning feature:</p> <pre data-bbox="395 577 1461 640">show smo image auto-clone state</pre> <p>b. Disable the SMO Image Cloning feature, if it is enabled:</p> <pre data-bbox="395 689 1461 752">set smo image auto-clone state off</pre> <p>c. Examine the state of the SMO Image Cloning feature:</p> <pre data-bbox="395 801 1461 864">show smo image auto-clone state</pre>
4	<p>Go to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (Expert mode):</li> </ul> <pre data-bbox="395 1010 1461 1072">exit</pre> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/etc/gclish</code> (Gaia gClish):</li> </ul> <pre data-bbox="395 1122 1461 1184">expert</pre>
5	<p>Go to the context of one of the Security Group Members that were upgraded to R81.20:</p> <pre data-bbox="316 1305 1461 1368">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre data-bbox="316 1417 1461 1480">member 1_1</pre>
6	<p>Run the upgrade script with the "revert" parameter and follow the instructions on the screen:</p> <pre data-bbox="316 1597 1461 1659">sp_upgrade --revert</pre>

Step	Instructions
7	<p>On each Security Group Member that was upgraded to R81.20, restore the Gaia automatic snapshot:</p> <ol style="list-style-type: none"><li data-bbox="347 331 1461 434">a. Go to the context of each Security Group Member: <pre>member &lt;Member ID&gt;</pre><p>Example:</p><pre>member 1_2</pre></li><li data-bbox="347 555 1461 658">b. Go to Gaia Clish (do <b>not</b> use the Gaia gClish): <pre>clish</pre></li><li data-bbox="347 667 1461 855">c. Restore the Gaia automatic snapshot that was saved automatically before the upgrade. <pre>set snapshot revert AutoSnapShot_&lt;Original-Version&gt;_&lt;Take&gt;</pre><p>Example:</p><pre>set snapshot revert AutoSnapShot_AutoSnapShot_R81_47</pre></li><li data-bbox="347 967 1235 1003">d. Wait for the Security Group Member to complete the reboot.</li><li data-bbox="347 1012 1430 1048">e. Repeat Steps a-d for the next Security Group Member that was upgraded.</li></ol>
8	Connect to the command line on the Security Group.
9	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>
10	Run the upgrade script with the "revert" parameter <b>again</b> and follow the instructions on the screen: <pre>sp_upgrade --revert</pre>
11	Make sure the downgrade was successful: <pre>asg diag verify</pre>

## Rolling Back the Whole Security Group

Use this rollback procedure if you upgraded **all** Security Group Members in the Security Group and it **is** necessary to keep the current connections.

### Important:

- This procedure does **not** interrupt the traffic and does **not** require down time. However, this procedure takes more time comparing with the procedure ["Rolling Back a Failed Upgrade of a Security Group - Minimum Downtime" on page 521](#).
- In this rollback procedure, you divide all upgraded Security Group Members in a specific Security Group into two logical groups - denoted below as "A" and "B". You revert one logical group of the Security Group Members at one time. The other logical group of the Security Group Members continues to handle traffic. Each logical group should contain the same number of Security Group Members - as close as possible.

Example 1:

- There are 8 Security Group Members in the Security Group.
- The Logical Group "A" contains Security Group Members from 1\_1 to 1\_4.
- The Logical Group "B" contains Security Group Members from 1\_5 to 1\_8.

Example 2:

- There are 5 Security Group Members in the Security Group.
- The Logical Group "A" contains Security Group Members from 1\_1 to 1\_3.
- The Logical Group "B" contains Security Group Members 1\_4 and 1\_5.

### Procedure

Step	Instructions
1	Connect to the command line on the Security Group.
2	Go to the context of one of the Security Group Members in the Logical Group "A": <pre>member &lt;Member ID&gt;</pre> Example: <pre>member 1_1</pre>
3	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>

Step	Instructions
4	<p>Run the upgrade script with the "revert" parameter and follow the instructions on the screen:</p> <pre data-bbox="352 315 1461 383">sp_upgrade --revert</pre>
5	<p>Restore the Gaia automatic snapshot on each Security Group Member in the <b>Logical Group "A"</b> that was upgraded to R81.20:</p> <ol style="list-style-type: none"> <li data-bbox="384 524 1461 741"> <p>Go to the context of the Security Group Member:</p> <pre data-bbox="432 562 1461 629">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre data-bbox="432 674 1461 741">member 1_2</pre> </li> <li data-bbox="384 748 1461 853"> <p>Go to Gaia Clish (do <b>not</b> use the Gaia gClish):</p> <pre data-bbox="432 786 1461 853">clish</pre> </li> <li data-bbox="384 860 1461 1043"> <p>Restore the Gaia automatic snapshot that was saved automatically before the upgrade.</p> <pre data-bbox="432 943 1461 1043">set snapshot revert AutoSnapShot_&lt;Original-Version&gt;_&lt;Take&gt;</pre> <p>Example:</p> <pre data-bbox="432 1088 1461 1189">set snapshot revert AutoSnapShot_AutoSnapShot_R81_47</pre> </li> <li data-bbox="384 1196 1461 1240"> <p>Wait for the Security Group Member to complete the reboot.</p> </li> <li data-bbox="384 1240 1461 1330"> <p>Repeat Steps a-d for the next Security Group Member in the Logical Group "A" that was upgraded.</p> </li> </ol>
6	<p>Connect to the command line on the Security Group.</p>
7	<p>Go to the context of one of the Security Group Members in the Logical Group "A" that was downgraded from R81.20:</p> <pre data-bbox="352 1514 1461 1581">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre data-bbox="352 1626 1461 1693">member 1_1</pre>
8	<p>Run the upgrade script with the "revert" parameter <b>again</b> and follow the instructions on the screen:</p> <pre data-bbox="352 1805 1461 1872">sp_upgrade --revert</pre>

Step	Instructions
9	<p>Restore the Gaia automatic snapshot on each Security Group Member in the <b>Logical Group "B"</b> that was upgraded to R81.20:</p> <ol style="list-style-type: none"> <li>Go to the context of the Security Group Member:           <pre data-bbox="432 383 1460 445">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre data-bbox="432 495 1460 557">member 1_5</pre> </li> <li>Go to Gaia Clish (do not use the Gaia gClish):           <pre data-bbox="432 607 1460 669">clish</pre> </li> <li>Restore the Gaia automatic snapshot that was saved automatically before the upgrade.           <pre data-bbox="432 757 1460 860">set snapshot revert AutoSnapShot_&lt;Original- Version&gt;_&lt;Take&gt;</pre> <p>Example:</p> <pre data-bbox="432 909 1460 1012">set snapshot revert AutoSnapShot_AutoSnapShot_R81_ 47</pre> </li> <li>Wait for the Security Group Member to complete the reboot.</li> <li>Repeat Steps a-d for the next Security Group Member in the Logical Group "B" that was upgraded.</li> </ol>
10	Connect to the command line on the Security Group.
11	<p>If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode:</p> <pre data-bbox="352 1330 1460 1393">expert</pre>
12	<p>Run the upgrade script with the "revert" parameter <b>again</b> and follow the instructions on the screen:</p> <pre data-bbox="352 1514 1460 1576">sp_upgrade --revert</pre>
13	<p>Make sure the downgrade was successful:</p> <pre data-bbox="352 1659 1460 1722">asg diag verify</pre>

## Rolling Back the Whole Security Group - With Downtime

Use this rollback procedure if you upgraded **all** Security Group Members in the Security Group and it is **not** necessary to keep the current connections.

**Important** - Schedule a maintenance window because this procedure interrupts all traffic that passes through the Security Group.

This rollback procedure save time because you revert all upgraded Security Group Members in a specific Security Group at the same time.

If traffic must **not** be interrupted, then follow the procedure ["Rolling Back a Failed Upgrade of a Security Group - Zero Downtime" on page 513](#).

### Procedure

Step	Instructions
1	Connect to the command line on the Security Group.
2	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>
3	Go from the Expert mode to Gaia gClish. <ul style="list-style-type: none"> <li>If your default shell is <code>/etc/gclish</code> (Gaia gClish), then run:  <pre>exit</pre> </li> <li>If your default shell is <code>/etc/bash</code> (Expert mode), then run:  <pre>gclish</pre> </li> </ul>
4	Restore the Gaia automatic snapshot that was saved automatically before the upgrade. <pre>set snapshot revert AutoSnapShot_&lt;Original-Version&gt;_&lt;Take&gt;</pre> <p>Example:</p> <pre>set snapshot revert AutoSnapShot_AutoSnapShot_R81_47</pre>
5	Wait for the Security Group Members to complete the reboot.
6	Connect to the command line on the Security Group.
7	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>

Step	Instructions
8	<p>Run the upgrade script with the "revert" parameter and follow the instructions on the screen:</p> <pre data-bbox="352 320 1460 383">sp_upgrade --revert</pre>
9	<p>Make sure the downgrade was successful:</p> <pre data-bbox="352 465 1460 528">asg diag verify</pre>




# Rolling Back a Failed Upgrade of a Security Group - Minimum Downtime


This section describes the steps to roll back a failed upgrade of a Security Group from R81.20 with Minimum Downtime.

This procedure supports only these downgrade paths for Security Groups:

- from R81.20 to R81.10
- from R81.20 to R81
- from R81.20 to R80.30SP
- from R81.20 to R80.20SP

## Rolling Back If Only Some of the Security Group Members Were Upgraded

 **Important** - Use this rollback procedure if you upgraded only **some (not all)** Security Group Members in the Security Group.

Step	Instructions
1	Connect to the command line on the Security Group.
2	If your default shell is <code>/bin/bash</code> (Expert mode), then go to the Gaia gClish: <pre>gclish</pre>
3	<p>Disable the SMO Image Cloning feature:</p> <p> <b>Note</b> - The SMO Image Cloning feature automatically clones all the required software packages to the Security Group Members during their boot. When you install or remove software packages gradually on Security Group Members, it is necessary to disable this feature, so that after a reboot the updated Security Group Members do not clone the software packages from the existing non-updated Security Group Members.</p> <p>a. Examine the state of the SMO Image Cloning feature:</p> <pre>show smo image auto-clone state</pre> <p>b. Disable the SMO Image Cloning feature, if it is enabled:</p> <pre>set smo image auto-clone state off</pre> <p>c. Examine the state of the SMO Image Cloning feature:</p> <pre>show smo image auto-clone state</pre>

Step	Instructions
4	<p>Go to the Expert mode:</p> <ul style="list-style-type: none"> <li>▪ If your default shell is <code>/bin/bash</code> (Expert mode):           <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">exit</pre> </li> <li>▪ If your default shell is <code>/etc/gclish</code> (Gaia gClish):           <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">expert</pre> </li> </ul>
5	<p>Go to the context of one of the Security Group Members that were upgraded to R81.20:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">member 1_1</pre>
6	<p>Run the upgrade script with the "revert" parameter and follow the instructions on the screen:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">sp_upgrade --revert</pre>
7	<p>On each Security Group Member that was upgraded to R81.20, restore the Gaia automatic snapshot:</p> <ol style="list-style-type: none"> <li>a. Go to the context of each Security Group Member:       <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">member 1_2</pre> </li> <li>b. Go to Gaia Clish (do not use the Gaia gClish):       <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">clish</pre> </li> <li>c. Restore the Gaia automatic snapshot that was saved automatically before the upgrade.       <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">set snapshot revert AutoSnapShot_&lt;Original-Version&gt;_&lt;Take&gt;</pre> <p>Example:</p> <pre style="border: 1px solid black; padding: 2px; margin: 5px 0;">set snapshot revert AutoSnapShot_AutoSnapShot_R81_47</pre> </li> <li>d. Wait for the Security Group Member to complete the reboot.</li> <li>e. Repeat Steps a-d for the next Security Group Member that was upgraded.</li> </ol>
8	<p>Connect to the command line on the Security Group.</p>

Step	Instructions
9	<p>If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode:</p> <pre data-bbox="316 264 1461 331">expert</pre>
10	<p>Run the upgrade script with the <code>"revert"</code> parameter <b>again</b> and follow the instructions on the screen:</p> <pre data-bbox="316 450 1461 517">sp_upgrade --revert</pre>
11	<p>Make sure the downgrade was successful:</p> <pre data-bbox="316 595 1461 663">asg diag verify</pre>

## Rolling Back the Whole Security Group - Zero Downtime

Use this rollback procedure if you upgraded **all** Security Group Members in the Security Group and it **is** necessary to keep the current connections.

### Important:

- This procedure does **not** interrupt the traffic and does **not** require down time. However, this procedure takes more time comparing with the procedure ["Rolling Back a Failed Upgrade of a Security Group - Minimum Downtime" on page 521](#).
- In this rollback procedure, you divide all upgraded Security Group Members in a specific Security Group into two logical groups - denoted below as "A" and "B". You revert one logical group of the Security Group Members at one time. The other logical group of the Security Group Members continues to handle traffic. Each logical group should contain the same number of Security Group Members - as close as possible.

Example 1:

- There are 8 Security Group Members in the Security Group.
- The Logical Group "A" contains Security Group Members from 1\_1 to 1\_4.
- The Logical Group "B" contains Security Group Members from 1\_5 to 1\_8.

Example 2:

- There are 5 Security Group Members in the Security Group.
- The Logical Group "A" contains Security Group Members from 1\_1 to 1\_3.
- The Logical Group "B" contains Security Group Members 1\_4 and 1\_5.

### Procedure

Step	Instructions
1	Connect to the command line on the Security Group.
2	Go to the context of one of the Security Group Members in the Logical Group "A": <pre>member &lt;Member ID&gt;</pre> <p>Example:</p> <pre>member 1_1</pre>
3	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>

Step	Instructions
4	<p>Run the upgrade script with the "revert" parameter and follow the instructions on the screen:</p> <pre data-bbox="352 315 1461 383">sp_upgrade --revert</pre>
5	<p>Restore the Gaia automatic snapshot on each Security Group Member in the <b>Logical Group "A"</b> that was upgraded to R81.20:</p> <ol style="list-style-type: none"> <li data-bbox="384 524 1461 629">Go to the context of the Security Group Member: <pre data-bbox="432 562 1461 629">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre data-bbox="432 674 1461 741">member 1_2</pre> </li> <li data-bbox="384 748 1461 853">Go to Gaia Clish (do <b>not</b> use the Gaia gClish): <pre data-bbox="432 786 1461 853">clish</pre> </li> <li data-bbox="384 860 1461 1043">Restore the Gaia automatic snapshot that was saved automatically before the upgrade. <pre data-bbox="432 943 1461 1043">set snapshot revert AutoSnapShot_&lt;Original-Version&gt;_&lt;Take&gt;</pre> <p>Example:</p> <pre data-bbox="432 1088 1461 1189">set snapshot revert AutoSnapShot_AutoSnapShot_R81_47</pre> </li> <li data-bbox="384 1196 1461 1240">Wait for the Security Group Member to complete the reboot.</li> <li data-bbox="384 1240 1461 1323">Repeat Steps a-d for the next Security Group Member in the Logical Group "A" that was upgraded.</li> </ol>
6	Connect to the command line on the Security Group.
7	<p>Go to the context of one of the Security Group Members in the Logical Group "A" that was downgraded from R81.20:</p> <pre data-bbox="352 1514 1461 1581">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre data-bbox="352 1626 1461 1693">member 1_1</pre>
8	<p>Run the upgrade script with the "revert" parameter <b>again</b> and follow the instructions on the screen:</p> <pre data-bbox="352 1805 1461 1872">sp_upgrade --revert</pre>

Step	Instructions
9	<p>Restore the Gaia automatic snapshot on each Security Group Member in the <b>Logical Group "B"</b> that was upgraded to R81.20:</p> <ol style="list-style-type: none"> <li>Go to the context of the Security Group Member:           <pre data-bbox="432 383 1458 445">member &lt;Member ID&gt;</pre> <p>Example:</p> <pre data-bbox="432 495 1458 557">member 1_5</pre> </li> <li>Go to Gaia Clish (do not use the Gaia gClish):           <pre data-bbox="432 607 1458 669">clish</pre> </li> <li>Restore the Gaia automatic snapshot that was saved automatically before the upgrade.           <pre data-bbox="432 757 1458 860">set snapshot revert AutoSnapShot_&lt;Original- Version&gt;_&lt;Take&gt;</pre> <p>Example:</p> <pre data-bbox="432 909 1458 1012">set snapshot revert AutoSnapShot_AutoSnapShot_R81_ 47</pre> </li> <li>Wait for the Security Group Member to complete the reboot.</li> <li>Repeat Steps a-d for the next Security Group Member in the Logical Group "B" that was upgraded.</li> </ol>
10	Connect to the command line on the Security Group.
11	<p>If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode:</p> <pre data-bbox="352 1330 1458 1393">expert</pre>
12	<p>Run the upgrade script with the "revert" parameter <b>again</b> and follow the instructions on the screen:</p> <pre data-bbox="352 1514 1458 1576">sp_upgrade --revert</pre>
13	<p>Make sure the downgrade was successful:</p> <pre data-bbox="352 1655 1458 1718">asg diag verify</pre>

## Rolling Back the Whole Security Group - With Downtime

Use this rollback procedure if you upgraded **all** Security Group Members in the Security Group and it is **not** necessary to keep the current connections.

**Important** - Schedule a maintenance window because this procedure interrupts all traffic that passes through the Security Group.

This rollback procedure save time because you revert all upgraded Security Group Members in a specific Security Group at the same time.

If traffic must **not** be interrupted, then follow the procedure ["Rolling Back a Failed Upgrade of a Security Group - Zero Downtime" on page 513](#).

### Procedure


Step	Instructions
1	Connect to the command line on the Security Group.
2	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>
3	Go from the Expert mode to Gaia gClish. <ul style="list-style-type: none"> <li>If your default shell is <code>/etc/gclish</code> (Gaia gClish), then run:  <pre>exit</pre> </li> <li>If your default shell is <code>/etc/bash</code> (Expert mode), then run:  <pre>gclish</pre> </li> </ul>
4	Restore the Gaia automatic snapshot that was saved automatically before the upgrade. <pre>set snapshot revert AutoSnapShot_&lt;Original-Version&gt;_&lt;Take&gt;</pre> <p>Example:</p> <pre>set snapshot revert AutoSnapShot_AutoSnapShot_R81_47</pre>
5	Wait for the Security Group Members to complete the reboot.
6	Connect to the command line on the Security Group.
7	If your default shell is <code>/etc/gclish</code> (Gaia gClish), then go to the Expert mode: <pre>expert</pre>

Step	Instructions
8	<p>Run the upgrade script with the "revert" parameter and follow the instructions on the screen:</p> <pre data-bbox="352 320 1460 383">sp_upgrade --revert</pre>
9	<p>Make sure the downgrade was successful:</p> <pre data-bbox="352 465 1460 528">asg diag verify</pre>



# Troubleshooting

This section provides troubleshooting commands.

-  **Note** - Maestro Orchestrators do not support the Hardware Diagnostic tool that you run from the Gaia OS Boot Menu (Known Limitation MBS-17809).

## Collecting System Information

These tools are available to collect the applicable information for [Check Point Support](#):

- CPInfo utility - use the "`cpinfo -Q`" command as described in [sk92739](#).
- HealthCheck Point (HCP) as described in [sk171436](#).

In addition, see:

- ["Collecting System Diagnostics \(smo verifiers\)" on page 280](#)
- ["CPView" on page 196](#)

# General Diagnostic in Security Groups

Based on the OSI model, you can run these commands:

Layer Number	Layer Name	Recommended Diagnostic Commands
7	Application	N / A
6	Presentation	<ul style="list-style-type: none"> <li> <span style="display: inline-block; width: 1em; margin-left: -1em;">■</span> For information about the Firewall drops, run this command in the Expert mode:           <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0; width: fit-content;">drop_monitor</div>           See <a href="#">"Packet Drop Monitoring (drop_monitor)" on page 250.</a> </li> <li> <span style="display: inline-block; width: 1em; margin-left: -1em;">■</span> For information about the Firewall drops, run this command in the Expert mode:           <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0; width: fit-content;">g_fw ctl zdebug + drop</div> </li> <li> <span style="display: inline-block; width: 1em; margin-left: -1em;">■</span> For information about the Software Blade Updates, run this command in the Expert mode:           <div style="border: 1px solid #ccc; padding: 2px; margin: 5px 0; width: fit-content;">asg_swb_update_verifier</div>           See <a href="#">"Collecting System Diagnostics (smo verifiers)" on page 280.</a> </li> <li> <span style="display: inline-block; width: 1em; margin-left: -1em;">■</span> Examine the Security Gateway logs on the Management Server or Log Server           </li> </ul>

Layer Number	Layer Name	Recommended Diagnostic Commands
5	Session	<ul style="list-style-type: none"> <li>■ For information about the Connections table, run this command in the Expert mode:  <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>g_fw tab -t connections -s</code></div> </li> <li>■ For information about the Firewall drops, run this command in the Expert mode:  <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>g_fw ctl zdebug + drop</code></div> </li> <li>■ For information about the performance, run this command in Gaia gClish or the Expert mode:  <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>asg perf -v -p</code></div> <p>See <a href="#">"Monitoring Performance (asg perf)" on page 225.</a></p> </li> <li>■ For information about the VSX mode, run this command:  <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>asg perf -vs all -v --vvxxx</code></div> <p>See <a href="#">"Monitoring Performance (asg perf)" on page 225.</a></p> </li> </ul>
4	Transport	<ul style="list-style-type: none"> <li>■ For information about the Correction Layer and traffic flow, use the <code>g_tcpdump</code> command in the Expert mode  <p>See <a href="#">"Multi-blade Traffic Capture (tcpdump)" on page 220.</a></p> </li> <li>■ For information about the VPN, examine the Security Gateway logs on the Management Server or Log Server</li> </ul>

Layer Number	Layer Name	Recommended Diagnostic Commands
3	Network	<ul style="list-style-type: none"> <li>■ In the Expert mode, run these commands: <ul style="list-style-type: none"> <li>• For information about the traffic: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>asg_ifconfig</code></div> See <a href="#">"Monitoring Traffic (asg_ifconfig)" on page 202.</a> </li> <li>• For information about the routes: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>asg_route</code></div> See <a href="#">"Collecting System Diagnostics (smo verifiers)" on page 280.</a> </li> <li>• For information about the routes: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>asg_dr_verifier</code></div> See <a href="#">"Collecting System Diagnostics (smo verifiers)" on page 280.</a> </li> <li>• For information about the routes: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>netstat -rn</code></div> </li> <li>• For information about the routes: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>route</code></div> </li> </ul> </li> <li>■ In Gaia gClish, run these commands: <ul style="list-style-type: none"> <li>• For information about the traffic: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>asg_ifconfig</code></div> See <a href="#">"Monitoring Traffic (asg_ifconfig)" on page 202.</a> </li> <li>• For information about the routes: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>asg_route</code></div> See <a href="#">"Collecting System Diagnostics (smo verifiers)" on page 280.</a> </li> <li>• For information about the routes: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>show route ...</code></div> </li> </ul> </li> </ul>
2	Data Link	<ul style="list-style-type: none"> <li>■ For information about the Bridge interfaces, run this command in Gaia gClish or the Expert mode: <div style="border: 1px solid black; padding: 2px; margin: 5px 0;"><code>asg_br_verifier</code></div> See <a href="#">"Layer 2 Bridge Verifier (asg_br_verifier, asg_brs_verifier)" on page 536.</a> </li> </ul>

Layer Number	Layer Name	Recommended Diagnostic Commands
1	Physical	<ul style="list-style-type: none"> <li data-bbox="663 264 1181 297">■ Run this command in Gaia gClish:</li> <div data-bbox="699 304 1461 371" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre data-bbox="722 322 1185 349">show maestro port &lt;Port&gt;</pre> </div> <li data-bbox="663 376 1404 450">■ For information about the Bond interfaces, run this command in the Expert mode:</li> <div data-bbox="699 456 1461 562" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre data-bbox="722 474 1401 539">cat /proc/net/bonding/&lt;Name of Bond Interface&gt;</pre> </div> <li data-bbox="663 566 1457 640">■ For information about the Port Link, run this command in the Expert mode:</li> <div data-bbox="699 647 1461 714" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre data-bbox="722 665 1145 692">ethtool ethsBP&lt;X&gt;-&lt;XX&gt;</pre> </div> <li data-bbox="663 719 1437 792">■ For information about the interface statistics, run this command in the Expert mode:</li> <div data-bbox="699 799 1461 866" style="border: 1px solid black; padding: 5px; margin: 5px 0;"> <pre data-bbox="722 817 1203 844">ethtool -S ethsBP&lt;X&gt;-&lt;XX&gt;</pre> </div> </ul>

# Configuration Verifiers

## *In This Section:*

---

MAC Verification (mac_verifier) .....	534
Layer 2 Bridge Verifier (asg_br_verifier, asg_brs_verifier) .....	536
Verifying VSX Gateway Configuration (asg_vsx_verify) .....	538

---

## MAC Verification (mac\_verifier)

You can run verifiers to make sure the configuration is correct and consistent.

### Description

Each MAC address contains information about the Site ID, Security Group Member ID, and interfaces.

Use this command to make sure that the virtual MAC addresses on physical and bond interfaces are the same for all Security Group Members.

You must run this command in the Expert mode.

### Syntax

```
mac_verifier -h
```

```
mac_verifier [-l] [-v]
```

### Parameters

Parameter	Description
-h	Shows the built-in help.
-l	Shows MAC address consistency on the Active Site.
-v	Shows information for each interface MAC Address.

## Examples

### Example 1

```
[Expert@HostName-ch0x-0x:0]# mac_verifier
-----
Collecting information from SGMs...
-----
Verifying FW1 mac magic value on all SGMs...
Success
-----
Verifying IPV4 and IPV6 kernel values...
Success
-----
Verifying FW1 mac magic value in /etc/smodb.json...
Success
-----
Verifying MAC address on local chassis (Chassis 1)...
Success
-----
[Expert@HostName-ch0x-0x:0]#
```

### Example 2

```
[Expert@HostName-ch0x-0x:0]# mac_verifier -v
-----
Collecting information from SGMs...
-----
Verifying FW1 mac magic value on all SGMs...
FW1 mac magic value on all SGMs:
Command completed successfully

Success
-----
Verifying IPV4 and IPV6 kernel values...
IPV6 is not enabled
Success
-----
Verifying FW1 mac magic value in /etc/smodb.json...
FW1 mac magic value and /etc/smodb.json value are the same (160)
Success
-----
Verifying MAC address on local chassis (Chassis 1)...
-*- 2 blades: 1_01 1_02 -*-
BPETH0      MAC address of BPETH0 is correct

-*- 2 blades: 1_01 1_02 -*-
BPETH1      MAC address of BPETH1 is correct

-*- 2 blades: 1_01 1_02 -*-
eth1-05 00:1c:7f:81:05:a0

-*- 2 blades: 1_01 1_02 -*-
eth1-06 00:1c:7f:81:06:a0

-*- 2 blades: 1_01 1_02 -*-
eth1-07 00:1c:7f:81:07:a0

... output was truncated for brevity ...

-*- 2 blades: 1_01 1_02 -*-
eth2-64 00:1c:7f:82:40:a0

Success
-----
[Expert@HostName-ch0x-0x:0]#
```

## Layer 2 Bridge Verifier (asg\_br\_verifier, asg\_brs\_verifier)

### Description

Use the "asg\_br\_verifier" command in Gaia gClish or the Expert mode to confirm that there are no bridge configuration problems in Virtual Systems in the Bridge Mode.

### Notes:

- You must run the "asg\_br\_verifier" command in the context of the specific Virtual System in the Bridge Mode.
- This command also confirms that the "fdb\_shadow" tables are the same for the Virtual System on different Security Group Members.
- You can run the "asg\_brs\_verifier" command in the Expert mode from the context of any Virtual System to get the output for all Virtual Systems in the Bridge Mode.

### Syntax for the asg\_br\_verifier command

```
asg_br_verifier -h
```

```
asg_br_verifier [-c] [-d] [-s] [-t] [-v]
```

### Syntax for the asg\_brs\_verifier command

```
asg_brs_verifier -h
```

```
asg_brs_verifier [-d] [-s] [-t] [-v]
```

### Parameters

Parameter	Description
-h	Shows the built-in help.
No Parameters	Runs bridge verification on all Virtual Systems.
-c	Also shows the table entries (unformatted output).
-d	Shows verbose unformatted output. The "-d" and "-v" options are mutually exclusive.
-s	Also shows the table summary.
-t	Also shows the table entries (formatted output).



Parameter	Description
-v	Shows verbose formatted output. The "-v" and "-d" options are mutually exclusive.

## Examples

### Example 1 - Output in a normal state

```
[Expert@HostName-ch0x-0x:0]# asg_br_verifier
=====
vs #3
=====

Number of entries in fdb_shadow table:

-- 10 blades: 1_01 1_02 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 --
11

Status: OK

=====
[Expert@HostName-ch0x-0x:0]#
```

### Example 2 - Output in a state of wrong configuration

```
[Expert@HostName-ch0x-0x:0]# asg_br_verifier -v
=====
vs #3
=====

Number of entries in fdb_shadow table:

-- 9 blades: 1_01 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 --
11
-- 1 blade: 1_02 --
0

Status: number of entries is different

=====

Collecting table info from all SGMs. This may take a while.

Table entries in fdb_shadow table:

-- 9 blades: 1_01 1_03 1_04 1_05 2_01 2_02 2_03 2_04 2_05 --
address="00:00:00:00:00:00" Interface="eth1-07"
address="00:10:AA:7D:08:81" Interface="eth2-07"
address="00:1E:9B:56:08:81" Interface="eth1-07"
address="00:23:FA:4E:08:81" Interface="eth1-07"
address="00:49:DC:58:08:81" Interface="eth2-07"
address="00:7E:60:77:08:81" Interface="eth1-07"
address="00:80:EA:55:08:81" Interface="eth1-07"
address="00:8D:86:52:08:81" Interface="eth2-07"
address="00:9E:8C:7F:08:81" Interface="eth1-07"
address="00:E5:DB:78:08:81" Interface="eth2-07"
address="00:E5:F7:78:08:81" Interface="eth2-07"
-- 1 blade: 1_02 --
fdb_shadow table is empty
Status: Table entries in fdb_shadow table is different between SGMs

=====
[Expert@HostName-ch0x-0x:0]#
```

# Verifying VSX Gateway Configuration (asg vsx\_verify)

## Description

The "asg vsx\_verify" command replaces the old verifier in the "smo verifiers" command and runs on a VSX system only.

Use this command to confirm that all Security Group Members have the same VSX configuration - Interfaces, Routes, and Virtual Systems.

- The same MD5 of configuration files that must be identical between Security Group Members.
- Similarity in configuration files that must be identical, but not necessarily written that way (like the /config/active file).

The command uses the "db\_cleanup" report to do this.

- The same VSX configuration on Security Group Members.
- Similarity of VMAC and BMAC addresses.

Use output when there is an inconsistency in the configuration.

The differences are compared in two ways:

- The return value of the command run on the Security Group Members with the "gexec\_inner\_command"
- The output of the commands

Example of a difference in the command output:

```
Difference between blade: 1_01 and blade: 2_01 found.
=====
--- 1_01
+++ 2_01
-73b4c20e598d6b495de7515ad4ea2fdc /opt/CPsuite-R81.20/fw1/conf/fwha_vsx_conf_id.conf
+b21dfa3feab817c3640bbb984346cdf1 /opt/CPsuite-R81.20/fw1/conf/fwha_vsx_conf_id.conf
```

When a command fails, the output contains:

```
Command "asg xxx" failed to run on blade "2_01"
```

## Syntax

```
asg vsx_verify [{-a | -c | -v}]
```

## Parameters

Parameter	Description
-a	Includes Security Group Members in the Administrative DOWN state
-c	Compares: <ul style="list-style-type: none"> <li>■ Database configuration between Security Group Members</li> <li>■ Operating system and database configuration on each Security Group Member</li> </ul>
-v	Includes Virtual Systems configuration verification table

## Examples

### Example 1 - 'asg vsx\_verify -v'

```

> asg vsx_verify -v
+-----+
|Chassis 1 SGMs:                                     |
|1_01 1_02 1_03                                     |
+-----+

+-----+
|VSX Global Configuration Verification               |
+-----+
|SGM  |VSX Configuration Signature      |Virtual Systems |State |
|      |VSX Configuration ID             |Installed\Allowed|      |
+-----+
|all   |8ef02b3e73386afd6e044c78e466ea82 |5\25           |UP   |
|      |9                                     |               |     |
+-----+

+-----+
|Virtual Systems Configuration Verification         |
+-----+
|VS  |SGM  |VS Name      |VS Type          |Policy Name      |SIC State|Status |
+-----+
|0   |all  |VSX_OBJ     |VSX Gateway     |Standard         |Trust   |Success|
+-----+
|1   |all  |VSW-INT    |Virtual Switch  |<Default Policy>|Trust   |Success|
+-----+
|2   |all  |VSW-INT    |Virtual Switch  |<Not Applicable>|Trust   |Success|
+-----+
|3   |all  |VS-1       |Virtual System  |Standard         |Trust   |Success|
+-----+
|4   |all  |VS-2       |Virtual System  |Standard         |Trust   |Success|
+-----+
Comparing Routes DB & OS. This procedure may take some time...
Press 'y' to skip this procedure...
Comparing..

+-----+
|Summary                                           |
+-----+
|VSX Configuration Verification completed successfully|
+-----+

All logs collected to /var/log/vsx_verify.1360846320.log
>

```

## Example 2 - 'asg vsx\_verify -a -v'

```

> asg vsx_verify -v -a
Output
-----+
|Chassis 1 SGMs:
|1_01* 1_02 1_03 1_04
-----+

-----+
|VSX Global Configuration Verification
-----+
|SGM   |VSX Configuration Signature      |Virtual Systems |State |
|      |VSX Configuration ID            |Installed\Allowed|      |
-----+
|1_01  |8ef02b3e73386afd6e044c78e466ea82|5\25            |UP   |
|      |9                                |                |     |
-----+
|1_02  |8ef02b3e73386afd6e044c78e466ea82|5\25            |UP   |
|      |9                                |                |     |
-----+
|1_03  |8ef02b3e73386afd6e044c78e466ea82|5\25            |UP   |
|      |9                                |                |     |
-----+
|1_04  |8ef02b3e73386afd6e044c78e466ea82|5\25            |DOWN |
|      |9                                |                |     |
-----+
|2_01  |8ef02b3e73386afd6e044c78e466ea82|5\25            |UP   |
|      |9                                |                |     |
-----+
|2_02  |8ef02b3e73386afd6e044c78e466ea82|5\25            |UP   |
|      |9                                |                |     |
-----+
|2_03  |8ef02b3e73386afd6e044c78e466ea82|5\25            |UP   |
|      |9                                |                |     |
-----+
|2_04  |8ef02b3e73386afd6e044c78e466ea82|5\25            |UP   |
|      |9                                |                |     |
-----+

-----+
|Virtual Systems Configuration Verification
-----+
|VS  |SGM |VS Name   |VS Type       |Policy Name   |SIC State|Status |
-----+
|0   |all |VSX_OBJ   |VSX Gateway   |Standard      |Trust    |Success|
-----+
|1   |all |VSW-INT   |Virtual Switch|<Default Policy>|Trust    |Success|
-----+
|2   |all |VSW-INT   |Virtual Switch|<Not Applicable>|Trust    |Success|
-----+
|3   |all |VS-1      |Virtual System|Standard      |Trust    |Success|
-----+
|4   |all |VS-2      |Virtual System|Standard      |Trust    |Success|
-----+
Comparing Routes DB & OS. This procedure may take some time...
Press 'y' to skip this procedure...
Comparing..

-----+
|Summary
-----+
|VSX Configuration Verification completed with the following errors:
|1. [1_02:1] eth1-06 operating system address doesn't match
|2. [1_02:1] eth1-06 DB address doesn't match
|3. [1_01:1] Found inconsistency between addresses in operating system ,DB and NCS ofeth1-06
|
|
-----+
All logs collected to /var/log/vsx_verify.1360886320.log
>

```

# Log and Configuration Files

This section describes some log and configuration files you can examine during the troubleshooting.

## Files on Security Group Members in Security Groups

Feature	File
Additional cluster information	\$FWDIR/log/cpha_ policy.log.*
All logs that do not have a dedicated log file	/var/log/junk.log.dbg
Command auditing	/var/log/asgaudit.log*
CPD daemon	\$CPDIR/log/cpd.elg
Discovering the hardware components	/var/log/start_ linker.log.dbg
Distribution	/var/log/dist_mode.log*
Dividing physical interfaces to slave BackPlane interfaces and assembling the bond (BPEth) interfaces	/var/log/start_tor_ sgm.log.dbg /var/log/start_ bfm.log.dbg
Dynamic Routing	/var/log/routed.log
Early boot configuration cloning	/var/log/image_ clone.log.dbg
Expert mode shell auditing	/var/log/command_ logger.log*
FWD daemon	\$FWDIR/log/fwd.elg
FWK daemon (VSX information)	\$FWDIR/log/fwk.elg.* <b>(in the context of each Virtual System)</b>
Gaia Alerts	/var/log/send_alert.*
Gaia Clish auditing	/var/log/auditlog*
Gaia First Time Configuration Wizard	/var/log/ftw_install.log

Feature	File
Gaia OS installation	/var/log/anaconda.log
General log file	/var/log/messages*
Information about the dedicated Sync interfaces	/var/log/start_smo.log.dbg
LLDP updates	/var/log/smardd.log.dbg <b>Also, run the <code>lldpneighbors</code> command</b>
Log Servers	/var/log/log_servers*
Pulling the Security Group configuration, rebooting, cluster configuration	\$FWDIR/log/blade_config.*
Reboot logs	/var/log/reboot.log
Security Group installation	/var/log/start_mbs.log
Silent install when adding a new Security Group Member to an existing Security Group	/var/log/silent_install.log.dbg
Synchronization of the new configuration to the Gaia database	/var/log/start_smo_1.log.dbg
VPND daemon	\$FWDIR/log/vpnd.elg*

## Files on Quantum Maestro Orchestrators

Feature	File
All logs that do not have a dedicated log file	<code>/var/log/junk.log.dbg</code>
Applying Security Group configuration	<code>/var/log/ssm_sg.log.dbg</code>
Configuring the SDK	<code>/var/log/messages</code>
Information about Security Groups	<code>/etc/sgdb.json</code>
Information about detected Security Group Members	<code>/etc/rsrddb.json</code>
LLDP updates	<code>/var/log/smardd.log.dbg</code> <b>Also, run the <code>lldpctl</code> command</b>
Starting of the SDK	<code>/var/log/start_tor_ssm.log.dbg</code>

# Installing the Gaia Operating System on a Quantum Maestro Orchestrator

To perform a clean installation of the Gaia Operating System on a Quantum Maestro Orchestrator, you can:

- Restore your Quantum Maestro Orchestrator to Factory Defaults.
  - Note** - This removes all existing configurations.
- Perform a clean install of the supported Gaia image with a bootable USB device.


## Reset an Orchestrator to Factory Defaults

**Important** - This operation reverts the Quantum Maestro Orchestrator to the last Gaia that was installed using the Clean Install method.

Step	Instructions
1	Connect to the Quantum Maestro Orchestrator using the serial console.
2	Log in to the Gaia Clish.
3	Restart the Quantum Maestro Orchestrator. Run: <pre>reboot</pre>
4	During boot, press any key within 4 seconds to enter the Boot menu when you see this prompt at the top of the screen: <pre>Loading the system Press any key to see the boot menu [Booting in 5 seconds]</pre>
5	In the menu, select <b>Reset to factory defaults</b> and press Enter.
6	Type <b>yes</b> and press Enter.
7	Wait for the Quantum Maestro Orchestrator to boot.
8	With a web browser, connect to the Gaia Portal on the Quantum Maestro Orchestrator: <pre>https://&lt;IP Address of MGMT Port&gt;</pre>
9	Run the Gaia First Time Configuration Wizard.



## Clean Install of the Gaia Image on an Orchestrator with a Bootable USB Device

Step	Instructions
1	Contact <a href="#">Check Point Support</a> to configure the Quantum Maestro Orchestrator to boot from the USB device by default.
2	Download the required Clean Install package (ISO) for Maestro Orchestrators from <a href="#">sk177624</a> .
3	Follow <a href="#">sk65205</a> to create a bootable USB device.  <b>Important:</b> <ul style="list-style-type: none"> <li>▪ Always use the latest available build of the ISomorphic Tool. If you use an outdated build, the installation can fail.</li> <li>▪ Select the option <b>Open Server with console</b>.</li> </ul>
4	Insert the bootable USB device into the Quantum Maestro Orchestrator.
5	Connect to the Quantum Maestro Orchestrator through the console port.
6	Restart the Quantum Maestro Orchestrator. Run: <pre>reboot</pre>
7	Wait for the Quantum Maestro Orchestrator to boot from the USB device.
8	Select the boot option <b>Open Server with console</b> .
9	Install the Gaia Operating System.
10	<b>Before the reboot, remove the USB device.</b>
11	Confirm the reboot.
12	With a web browser, connect to the Gaia Portal on the Quantum Maestro Orchestrator: <pre>https://&lt;IP Address of MGMT Port&gt;</pre>
13	Run the Gaia First Time Configuration Wizard.

# Replacing a Quantum Maestro Orchestrator

Follow the steps in [sk174202](#).

# Glossary